博士論文

サイバー外交政策に関する研究

-キャパシティビルディングを中心に-

A Study on Foreign Policy on Cybersecurity

Issues with an Emphasis on Capacity Building

Hiromu MURAKAMI
村上　啓

情報セキュリティ大学院大学

情報セキュリティ研究科情報セキュリティ専攻

２０１８年３月

目次

略称一覧

	英文	和文（定訳がない場合は筆者訳）
AIIB	Asian Infrastructure Investment Bank	アジアインフラ投資銀行
APEC	Asia-Pacific Enonomic Cooperation	アジア太平洋経済協力
APWG	Anti Phishing Working Group	フィッシング対策ワーキンググループ
ARF	ASEAN Regional Forum	ASEAN 地域フォーラム
ARPA	Advanced Research Projects Agency	（米国防総省）高等研究計画局
ARPANET	Advanced Research Projects Agency Network	（米国防総省）高等研究計画局ネットワーク
ASEAN	Association of Southeast Asian Nations	東南アジア諸国連合
AU	African Union	アフリカ連合
BRICS	Brazil, Russia, India, China, South Africa	ブラジル、ロシア、インド、中国、南アフリカ
CAMP	Cybersecurity Alliance for Mutual Progress	相互発展のためのサイバーセキュリティ連合
CBM	Confidence Building Measures	信頼醸成措置
CCDCoE	Cooperative Cyber Defence Centre of Excellence	協調的サイバー防衛センター
CCW	Convention on Certain Conventional Weapons	特定通常兵器使用禁止制限条約
CERT	Computer Emergency Response Team	コンピュータ緊急対応チーム

CFR	Council on Foreign Relations	外交問題評議会
CFSP	Common Foreign and Security Policy	共通外交・安全保障政策
CIIP	Critical Infomration Infrastructure Protection	重要情報インフラ防護
CIS	Commonwealth of Independent States	独立国家共同体
CLMV	Cambodia, Laos, Myanmar, Vietnam	カンボジア，ラオス，ミャンマー，ベトナム（CLMV 諸国／東南アジア後発４カ国）
CoE	Council of Europe	欧州評議会
COMECON	Council for Mutual Economic Assitance	経済相互援助会議
CPA UK	Commonwealth Parliamentary Association UK	英連邦議会協会
CPS	Crown Prosecution Service	英検察庁
CSIRT	Computer Security Incident Response Team	コンピュータセキュリティインシデント対応チーム
CSCE	Conference on Security and Co-operation in Europe	欧州安全保障協力会議
CSDP	Common Security and Defence Policy	共通安全保障・防衛政策
CSTO	Collective Security Treaty Organization	集団安全保障条約機構
CTO	Commonwealth Telecommunications Organisation	英連邦電気通信機構
DARPA	Defense Advanced Research Projects Agency	米国防高等研究計画局

DHS	Department of Homeland Security	米国土安全保障省
DoD	Department of Defense	米国防省
EC	European Community	欧州共同体
ECOWAS	Economic Community of West African States	西アフリカ諸国経済共同体
ECSC	European Coal and Steel Community	欧州石炭鉄鋼共同体
EC3	European Cybercrime Centre	欧州サイバー犯罪センター
EEA	European Economic Area	欧州経済領域
EEAS	European Union External Action Service	欧州対外行動庁
EEC	European Economic Community	欧州経済共同体
eGA	e-Governance Academy	エストニア e ガバナンス・アカデミー
EMS	European Monetary System	欧州通貨制度
ENISA	European Union Agency for Network and Information Security	欧州連合ネットワーク・情報セキュリティ庁
EU	European Union	欧州連合
FBI	Federal Bureau of Investigation	米連邦捜査局
FCO	Foreign & Commonwealth Office	英国外務省
FIRST	Forum of Incident Response and Security Teams	インシデント対応・セキュリティチーム・フォーラム
GCC	Gulf Cooperation Council	湾岸協力理事会
GCCS	Global Conference on Cyber Space	サイバー空間に関する国際会議

GCSCC	Global Cyber Security Capacity Centre	グローバル・サイバーセキュリティ・キャパシティセンター
GFCE	Global Forum on Cyber Expertise	サイバーの専門的知見に関するグローバル・フォーラム
GGE	Group of Governmental Experts	政府専門家グループ
HTML	Hyper Text Markup Language	ハイパーテキストマークアップランゲージ
ICT	Information and Communications Technology	情報通信技術
IGF	Internet Governance Forum	インターネットガバナンスフォーラム
INF	Intermediate-range Nuclear Forces	中距離核戦力
INTERPOL	International Criminal Police Organization	国際刑事警察機構
ITU	International Telecommunication Union	国際電気通信連合
JAIF	Japan-ASEAN Integration Fund	日・ASEAN 統合基金
JICA	Japan International Cooperation Agency	独立行政法人国際協力機構
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center	JPCERT コーディネーションセンター
KISA	Korea Internet & Security Agency	韓国インターネット振興院
MILNET	Military Network	軍事用ネットワーク
NATO	North Atlantic Treaty Organization	北大西洋条約機構

NCA	National Crime Agency	英国家犯罪対策庁
NCSA	National Cyber Security Alliance	全米サイバーセキュリティ連盟
NGO	Non-Governmental Organization	非政府組織
NICT	National Institute of Information and Communications	情報通信研究機構
OAS	Organization of American States	米州機構
ODA	Official Development Assistance	政府開発援助
OECD	Organisation for Economic Co-operation and Development	経済協力開発機構
OSCE	Organization for Security and Co-operation in Europe	欧州安全保障協力機構
QDR	Quadrennial Defense Review	米国 4 年毎国防計画見直し
SCO	Shanghai Cooperation Organization	上海協力機構
TICAD	Tokyo International Conference on African Development	アフリカ開発会議
TCP/IP	Transmission Control Protocol / Internet Protocol	
UNAFRI	United Nations African Institute for the Prevention of Crime and Treatment of Offenders	国連アフリカ犯罪防止・加害者治療研修所
UNCTAD	United Nations Conference on Trade and Development	国連貿易開発会議
UNDP	United Nations Development Programme	国連開発計画
UNECA	United Nations Economic Commission for Africa	国連アフリカ経済委員会

UNIDIR	United Nations Institute for Disarmament Research	国連軍縮研究所
UNODC	United Nations Office on Drugs and Crime	国連薬物・犯罪事務所
WMD	Weapons of Mass Destruction	大量破壊兵器
WWW	World Wide Web	ワールド・ワイド・ウェブ

１．序論

1.1. 問題意識

1.1.1. サイバー空間の重要性の高まり

本論文の研究対象である「サイバー外交」という営みやそれに関する国家の政策である「サイバー外交政策」が対象とする問題は，「サイバー空間（cyberspace）」の脅威である。では，そもそも「サイバー空間」とは何であろうか。サイバー空間については，領海の範囲の定義等を明確に定めた国連海洋法条約（United Nations Convention on the Law of the Sea）のようなものがないため，その普遍的な定義は存在しない。しかし，我々が一般的にいうサイバー空間は，大雑把に言えば，「インターネット等を含むコンピュータネットワークに繋がっているあらゆるネットワークの集合体が構成する人工的な仮想空間」と捉えることが可能であり，本書はサイバー空間自体に関する研究ではないため，ほぼインターネットと同義としてサイバー空間という用語を用いることにする。

1997 年の日本のインターネット利用者数は 1155 万人であったが，2016 年には 1 億 84 万人となり，20 年間で約 9000 万人増加した。人口普及率で言えば，1997 年は日本の人口のわずか 9.2%がインターネットを利用していたのに対し，2016 年は人口の 83.5%が利用している[1]。世界に目を向けると，2005 年のインターネット利用者数は世界全体で 10.2 億

[1] インターネット普及率の推移―総務省　www.soumu.go.jp/johotsusintokei/field/data/gt010102.xls（最終アクセス日：2017 年 12 月 18 日）

人であったが，2016 年には 34 億 9 千万人まで増え[2]，世界の 74 億 3300 万人[3]の約 47%がインターネットを利用している。

人口のおよそ半分の約 35 億人が利用しているインターネット，すなわちサイバー空間[4]は，その利用者数と普及率とともに日々重要性が増しており，電子メールの送受信などの通信手段としての機能や報道機関のニュースのテキストや動画の配信はもとより，個人，民間企業，国，地方公共団体等の情報共有，サービス提供，表現，経済，教育，宗教活動，交流などを目的とする幅広い社会・経済・政治・文化・娯楽等を行う場として人類にとって不可欠の存在となりつつある。しかし，このようなサイバー空間の重要性の高まりとともに，その脅威もまた，日々拡大，巧妙化している。

これを受け，外務省は，各国との連携をより一層強化するとともに，サイバー空間の安全を確保するための国際的な議論をリードしていく必要性が増大しているため，サイバー安全保障政策室を設置し，関係省庁及び幅広い民間関係者とも連携しながら，サイバー空間における法の支配の推進，信頼醸成及び開発途上国に対する能力構築支援といった取組を中心にサイバー分野における外交を積極的に推進していくとの方針を打ち出した[5]。

1.1.2. サイバー空間の脅威の増大と強化

サイバー空間の脅威は，時代とともに，量が増加し，また，その質も強化していった。まず，量の増加として，日本の政府機関や民間企業に対する国内及び海外からのサイバー攻撃関連の通信量は，年々増えている[6]。

サイバー攻撃[7]の質の変化として，2000 年代後半に入ると，それまで個人や民間企業に対する個人や犯罪者集団によるハッキング能力の自己顕示，知的財産や企業情報，財産の窃取・奪取等を目的とするサイバー攻撃が主流だったのに対し，国家や背後に国家が関与していると思われる組織による他国の政府機関や重要インフラ，軍事施設の機能麻痺を目

---

[2] インターネットの統計―総務省　http://www.soumu.go.jp/joho_tsusin/kids/internet/statistics/internet_01.html（最終アクセス日：2017 年 12 月 18 日）

[3] 世界の統計―総務省統計局　www.stat.go.jp/data/sekai/pdf/2017al.pdf（最終アクセス日：2017 年 12 月 18 日）

[4] Cyber-space という語を初めて用いたのは，米国の SF 小説家ウィリアム・ギブソン（William Gibson）の 1982 年の短編『クローム襲撃（Burning Chrome)』と言われている。（荒井良雄『情報化社会とサイバースペースの地理学，2005 年，人文地理第 57 巻第 1 号）

[5] 外務省：日本のサイバー外交 www.mofa.go.jp/mofaj/files/000172488.pdf（最終アクセス日：2017 年 12 月 18 日）

[6] ダークネット・トラフィック上の 1 IP アドレス当たりの年間総観測パケット数は，2005 年の 19,000 から 2015 年の 213,000 件に増加（情報通信研究機構（NICT 観測レポート 2016: www.nict.go.jp/cyber/report/NICTER_report_2016.pdf）（最終アクセス日：2018 年 2 月 13 日）

[7] ここでいう「サイバー攻撃」とは，一般的な用語として用いる「攻撃」すなわち，サイバー空間を利用した不正な行為であり，国際法上の「武力攻撃」に該当するという意味で「攻撃」という言葉を用いているのではない。

的とするサイバー攻撃の増加が顕著になった[8]。

特に，2007 年 4 月にエストニアの政府機関や金融機関等が大規模なサイバー攻撃を受け，一時機能不全に陥った事件は，エストニアのみならず米国を中心とする西側諸国に，サイバー攻撃はもはや個人による愉快犯やハッカー集団による犯罪のレベルを超え，国家の安全保障・外交上の脅威であるというサイバー攻撃の脅威認識を改める契機となった[9]。このサイバー攻撃は，エストニア政府が事件前に，同国のソビエト統治下時代に首都タリンに設置されたソビエト兵の銅像を郊外に移すことを決定した日から始まり，その主な加害者は，ロシア政府とされる[10]。翌年 5 月には，タリンに北大西洋条約機構（North Atlantci Treaty Organization。以下「NATO」という。）協調的サイバー防衛センター（Cooperative Cyber Defence Centre of Excellence。以下「CCDCoE」という。）が設置され，エストニアは，初の大規模サイバー攻撃の被害国という経験を活かし，NATO 加盟国におけるサイバー防衛の要として重要な役割を担っている[11]。

その後 2008 年 8 月にジョージアが南オセチアとの軍事衝突の際に，ロシアが介入し，物理的な攻撃とともに DDoS 攻撃やウェブサイトの改竄を受けたとされる事例[12]や，2009 年 7 月，米国及び韓国の国防部を含む政府機関のウェブサイトが（北朝鮮からと思われる）DDoS 攻撃により一時閲覧不能状態になった事例[13]がある。

サイバー空間の脅威の質の変化を象徴的に表しているのが米国政府の「第 5 の戦場」である。米国は，2010 年の米国国防省（Department of Defense。以下「DoD」という。）の「4 年毎の国防計画見直し」（Quadrennial Defense Review。以下「QDR」という。）において，「人為的な領域であるが，サイバー空間は現在，元来存在する陸・海・空・宇宙とともに DoD の活動にとって関係のある領域である」[14] とし，2011 年 7 月の同省のサイバー空間作戦戦略では，「サイバー空間を構成するネットワーク及びシステムは人為的なもの

---

[8] 総務省：最近のサイバーセキュリティにおける脅威動向について www.soumu.go.jp/main_content/000463653.pdf
[9] 朝日新聞グローバル：「銀行とめたエストニアへの攻撃（最終アクセス日：2017 年 12 月 18 日）
「犯人」は分からぬまま」http://globe.asahi.com/feature/101004/02_1.html
[10] Russia accused of unleashing cyberwar to disable Estonia:
https://www.theguardian.com/world/2007/may/17/topstories3.russia（最終アクセス日：2018 年 2 月 13 日）
[11] CCDCOE: History (https://ccdcoe.org/history.html)（最終アクセス日：2017 年 12 月 18 日）
[12] The Telegraph: Georgia: Russia 'conducting cyber
war'http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html（最終アクセス日：2017 年 12 月 18 日）
[13] New York Times: Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea
http://www.nytimes.com/2009/07/09/technology/09cyber.html（最終アクセス日：2017 年 12 月 18 日）
[14] DoD Quadrennial Defense Review Report February2010
（https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf）37 頁（最終アクセス日：2017 年 12 月 18 日）

であり，多くの場合は私有であり，主に民間人が利用しているものであるが，サイバー空間を（作戦）領域として扱うことは，DoD の国家安全保障の任務のための組織概念にとって重要」[15]であり，「国家安全保障戦略の指示に従い，DoD は，空，陸，海，宇宙及びサイバー空間の全ての領域において効果的に作戦を実行できる必要な能力を整備しなければならない。すべてのレベルにおいて，DoD は，サイバー空間の複雑な課題及び幅広い機会のために，組織し，訓練を行い，態勢を整える。」[16]との方針を公表し，サイバー空間は，陸，海，空，宇宙に次ぐ「第 5 の戦場」との認識を世に示した。

2009 年から 2010 年にかけて，イランの核開発施設のウラン濃縮制御システムがウイルス感染を受け稼働不能に陥った「スタックスネット（Stuxnet）事件」[17]では，米国及びイスラエル政府の関与が疑われているほか，2011 年 9 月には日本の三菱重工業のサーバーがウイルス感染を受け，機密情報の漏洩の危険にさらされた事件[18]では，中国政府の関与が疑われるなど，サイバー空間は，西側諸国の安全保障関係当局のみならず，敵対する，あるいは歴史的に遺恨がある国家間の争いの場として名実ともに「第 5 の戦場」となりつつある。

表 1　2007 年以降の主なサイバー攻撃年表[19]

年	攻撃の名称・概要	加害者[20]
2007	エストニア政府・金融機関等のウェブサイトへの攻撃	ロシア
	シリア軍の防空システムに対する攻撃	イスラエル
2008	ジョージアの政府機関等のウェブサイトへの攻撃	ロシア
2009	米国・韓国の国防部を含む政府機関等のウェブサイトへの攻撃	北朝鮮
2010	スタックスネット（Stuxnet）：イランのウラン濃縮制御システムのウイルス感染	米国及びイスラエル

[15] Department of Defense Strategy for Operating in Cyberspace（https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf）5 頁（最終アクセス日：2017 年 12 月 18 日）
[16] ibid.
[17] The Washington Post: Stuxnet was work of U.S. and Israeli experts, officials say（https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.873c0a01b9a1）（最終アクセス日：2017 年 12 月 18 日）
[18] Reuters: Japan's defense industry hit by its first cyber attack（https://www.reuters.com/article/us-mitsubishiheavy-computer/japans-defense-industry-hit-by-its-first-cyber-attack-idUSTRE78I0EL20110919）（最終アクセス日：2017 年 12 月 18 日）
[19] 全体として，外務省：日本のサイバー外交（www.mofa.go.jp/mofaj/files/000172488.pdf）を参照（最終アクセス日：2017 年 12 月 18 日）
[20] 報道ベースで「加害者」の疑いがある者。

2011	三菱重工業に対するサイバー攻撃	中国
2012	最高裁判所，文化庁等のウェブサイトに対する攻撃[21]	中国
2013	韓国の複数の放送局，金融機関等の情報システムへの攻撃[22]	北朝鮮
2014	ソニー・ピクチャーズ・エンタテインメントに対するサイバー攻撃[23]	北朝鮮
2015	フランスの TV モンド 5 へのサイバー攻撃[24]	ISIL
	米国連邦人事管理局（OPM）からの約 2100 万人分の個人情報流出[25]	中国
	日本年金機構からの約 125 万件の個人情報流出[26]	不明
	安倍総理のウェブサイトへの攻撃[27]	アノニマス
	ウクライナ電力システムに対するサイバー攻撃[28]	ロシア
2016	バングラデシュ中央銀行に対するサイバー攻撃[29]	北朝鮮
	米国民主党議会選挙委員会の情報システムに対するサイバー攻撃[30]	ロシア
	ベトナムの国際空港に対するサイバー攻撃[31]	中国

[21] 総務省：「電気通信事業におけるサイバー攻撃への適正な 対処に関する研究会」について (www.soumu.go.jp/main_content/000264105.pdf)（最終アクセス日：2017 年 12 月 18 日）
[22] The New York Times: Computer Networks in South Korea Are Paralyzed in Cyberattacks (http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html)（最終アクセス日：2017 年 12 月 18 日）
[23] The Washington Post: The Sony Pictures hack, explained (https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.84e91881eb3e)（最終アクセス日：2017 年 12 月 18 日）
[24] The Telegraph: ISIL hackers seize control of France's TV5Monde network in 'unprecedented' attack (https://www.telegraph.co.uk/news/worldnews/europe/france/11525016/Isil-hackers-seize-control-of-Frances-TV5Monde-network-in-unprecedented-attack.html)（最終アクセス日：2017 年 12 月 18 日）
[25] The Washington Post: Chinese national arrested for allegedly using malware linked to OPM hack (https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html?utm_term=.1af8b5cb169c)（最終アクセス日：2017 年 12 月 18 日）
[26] 日本年金機構：日本年金機構における不正アクセスによる情報流出事案について (http://www.nenkin.go.jp/oshirase/topics/2015/0104.html)（最終アクセス日：2017 年 12 月 18 日）
[27] 日本経済新聞：首相サイトに攻撃か 「アノニマス」が声明 (https://www.nikkei.com/article/DGKKASFS10H1W_Q5A211C1EAF000/)（最終アクセス日：2017 年 12 月 18 日）
[28] Reuters: Ukraine's power outage was a cyber attack: Ukrenergo (https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA)（最終アクセス日：2017 年 12 月 18 日）
[29] Reuters: Cyber security firm: more evidence North Korea linked to Bangladesh heist (https://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea/cyber-security-firm-more-evidence-north-korea-linked-to-bangladesh-heist-idUSKBN1752I4)（最終アクセス日：2017 年 12 月 18 日）
[30] Reuters: U.S. formally accuses Russian hackers of political cyber attacks (https://www.reuters.com/article/us-usa-cyber-russia/u-s-formally-accuses-russian-hackers-of-political-cyber-attacks-idUSKCN12729B)（最終アクセス日：2017 年 12 月 18 日）
[31] Viet Nam News: Chinese hackers attack VN's airports and Vietnam Airlines' websites

2017	フランス，マクロン大統領候補陣営（当時）へのサイバー攻撃[32]	ロシア
	WannaCry：世界各国に対するランサムウェア[33]	北朝鮮

1.1.3. サイバー空間の脅威に対処するためのサイバー外交の出現

このような状況の中，国境を越えるサイバー空間の脅威に各国が協力して対処し，外交的解決を目指す新たな分野としてサイバー外交（cyber diplomacy）という語が用いられるようになった。海上の安全保障や資源等海洋の諸問題について国際的に取り組む「海洋外交」や宇宙空間の平和的利用や信頼醸成措置（Confidence-Building Measures。以下「CBM」という。）に関する国際連携等を行う「宇宙外交」と同様に，2010 年代に入り「サイバー外交」という新しい外交分野が確立したといっていい[34]。このサイバー外交の喫緊の課題として最も活発に議論されているのが，①サイバー空間を利用した行為に関する国際的なルール作り，②サイバー空間における CBM 及び③サイバーセキュリティ分野におけるキャパシティビルディングである。日本はこれを「サイバー外交の三本柱」と位置付けている[35]。この三点を主に議論しているサイバー外交の中心的な枠組みが国連サイバー政府専門家会合（Group of Governmental Experts。以下「GGE」という。）であった。GGE は，1998 年にロシアが国連総会において提案し，2004 年に第 1 回会合が設置され，2017 年まで 5 回開催された。しかし，2017 年の第 5 回 GGE では，サイバー空間の国際的なルール作りに関し，参加 25 カ国のコンセンサスを得られず，成果文書をまとめられないまま会議は終わり，サイバー外交の進展に陰りが見えた。

---

http://vietnamnews.vn/society/300416/chinese-hackers-attack-vns-airports-and-vietnam-airlines-website.html#3eWzfblWssuEBQ5W.97)（最終アクセス日：2017 年 12 月 18 日）

[32] Independent: Emmanuel Macron email leaks 'linked to Russian-backed hackers who attacked Democratic National Committee' (http://www.independent.co.uk/news/world/europe/emmanuel-macron-leaks-hack-en-marche-cyber-attack-russia-dnc-marine-le-pen-election-france-latest-a7721796.html)（最終アクセス日：2017 年 12 月 18 日）

[33] Reuters: 米政権，サイバー攻撃「ワナクライ」に北朝鮮が関与と非難(https://jp.reuters.com/article/us-wannacry-northkorea-idJPKBN1ED05N)（最終アクセス日：2017 年 12 月 19 日）

[34] 例として米シンクタンク CSIS（https://www.csis.org/programs/technology-policy-program/cyber-diplomacy-and-deterrence）（最終アクセス日：2017 年 12 月 18 日），the Diplomat 誌（https://thediplomat.com/tag/cyber-diplomacy/）（最終アクセス日：2017 年 12 月 18 日），ライデン大学（https://www.universiteitleiden.nl/en/events/2017/09/cyber-diplomacy-after-the-un-GGE）（最終アクセス日：2017 年 12 月 18 日）等が cyber diplomacy の用語を使っているほか，外務省（http://www.mofa.go.jp/mofaj/annai/page5_000250.html）（最終アクセス日：2017 年 12 月 18 日）も「サイバー外交」という語を用いている。また，外務省のサイバー政策担当大使の設置，サイバー安全保障政策室の設置等外交実務上，サイバー問題に対処するための要職や組織体制の確立を行っていることもサイバー外交が既に存在し，取り組まれていることを裏付けている。

[35] 外務省―日本のサイバー外交（www.mofa.go.jp/mofaj/files/000172488.pdf）（最終アクセス日：2017 年 12 月 18 日）

1.2. 本研究の目的と意義

本論文は，日本のサイバー外交政策として，キャパシティビルディング（capacity building)，すなわち途上国の能力構築支援を積極的に推進すべきという提言を試みることを目的とするものである。

その前提として，まず第 2 章で「サイバー外交」,「サイバーセキュリティ」，そして「サイバー空間」という概念の特徴を，それぞれ伝統的な外交，伝統的な安全保障，伝統的な空間と比較したうえで明らかにする。

次に，第 3 章では，国連サイバーGGE の第 1 回会合から第 5 回会合までの取り組みを概観し，GGE の意義と失敗の理由を分析し，ポスト GGE 後のサイバー外交の展開を考察する。

第 4 章では，伝統的なキャパシティビルディング（capacity building）という概念の発展の経緯と概要を示し，サイバーセキュリティ分野におけるキャパシティビルディングを概観した上で，主な援助の主体毎のキャパシティビルディングに関する取り組みを外交・安全保障的アプローチ，経済・開発援助的アプローチという視点から分析して概説する。

第 5 章では，現在の日本のサイバーセキュリティ分野におけるキャパシティビルディングの方針と取り組みを，第 4 章と同様，外交・安全保障的アプローチ，経済・開発援助的アプローチという視点から分析して概観する。

第 6 章では，第 4 章及び第 5 章における取り組みを踏まえ，サイバーセキュリティ分野のキャパシティビルディングの在り方を考察する。

第 7 章の結論では，第 6 章の考察を踏まえ，日本のサイバー外交政策としてキャパシティビルディングのあるべき方向性を提示する。

2. サイバー外交の特異性

本章では,「サイバー外交」とは何かを明らかにするために，伝統的な外交概念と比較した「サイバー外交」概念を第 1 節で概説する。第 2 節では，サイバー外交の主たる目的である「サイバーセキュリティ」を伝統的な外交における中核的な意義である安全保障概念と比較して明らかにする。第 3 節では，サイバーセキュリティが確保されるべき「第 5 の戦場」とも言われる「サイバー空間」の特徴を、これまで人類がその利権を得るために幾多もの争いを繰り広げ、その度に様々な対策を講じてきた第 1 から第 4 の「戦場」である陸、海、空及び宇宙空間と比較して明らかにする。

2.1 伝統的外交とサイバー外交

2.1.1 伝統的外交

外交（diplomacy）とは,「外国との交際。国際間の事柄を交渉で処理すること」[36]、「交渉による国際関係の処理であり，大公使によってこれらの関係が調整され処理される方法であり，外交官の職務あるいは技術」[37]、「独立国家の政府間の公式関係における，知性と機転の応用である。より簡潔に言えば，平和的手段による諸国間の実務の行動」[38]、あるいは、「主権国家が自国の国益や安全そして繁栄を促進するため，また国際社会において国家間の関係をより安定的に維持しその友好関係を強化するため，政府間で行われる交渉あるいは政策を示す言葉」[39]というように定義されている。外交を構成する要素として、第一に、外交を行う主体として国家や大使、公使、外交官があり、第二に、外交の目的として国際関係の処理や国益・安全・繁栄の促進などがあり、第三に、外交の手段として、「交渉や政策などがあることが分かる。そして、ディプロマシーという用語をこのような意味で使うようになったのは、1796 年に英国のエドマンド・バークが最初と言われている[40]。それ以前は「交渉（negotiation）」や「持続的な交渉（*négotiation continuelle*）」といった言葉を用いていた。他国との交渉という意味での外交の起源は紀元前 2500 年頃の古代シリアの都市国家エブラ王国からイラン北部のハマジ王国へとおくられた書簡や紀元前 14 世

[36] 新村出編『広辞苑第五版』（岩波書店，1998 年）
[37] H・ニコルソン、斎藤眞・深谷満雄訳『外交』（東京大学出版会，1968 年）7 頁（オックスフォード英語辞典による定義）
[38] 細谷雄一『外交』（有斐閣，2007 年）23 頁（アーネスト・サトウによる定義）
[39] ibid.15 頁
[40] Independent: （https://www.independent.co.uk/life-style/words-diplomacy-1295894.html）（最終アクセス日：2017 年 12 月 18 日）

紀エジプトのアマルナ時代の「アマルナ文書」を外交文書として用いられてきた時代まで遡ることができ、そこでは、現代の職業外交官としての外交使節は、国王の個人的な使節にすぎなかった[41]。

外交の歴史は表 2 のとおり、戦争（三十年戦争、ナポレオン戦争、第一次世界大戦）とそれを終結し、安定した秩序、勢力均衡を保つための条約や国際システム（ウェストファリア体制、ウィーン体制、ヴェルサイユ体制等）の歴史である。また、第二次世界大戦後の国際秩序は、国連を中心とする集団安全保障体制や北大西洋条約機構（「NATO」）等の地域的安全保障体制と自由主義や資本主義を掲げる米国と共産主義・社会主義体制のソ連の二国の超大国の均衡が冷戦終結まで続いた。

2.1.1.1「旧外交」

外交の本質や文化、方式、制度等の違いから、ハロルド・ニコルソンは、外交を「旧外交」と「新外交」に分類した。ニコルソン等の古典的な外交理論を参照して「旧外交」と「新外交」を描き、外交の歴史を述べた慶應義塾大学法学部の細谷雄一教授によれば、「旧外交」とは、「『主として、常駐大使[42]に代表される職業外交官による秘密交渉』に依拠したもの」[43]であり、その特徴は、高坂正堯が著書『古典外交の成熟と崩壊』において「古典外交」の特質として指摘した「同質性」、「貴族性」、「自立性」を基礎とする 1814 年から 1815 年にかけて開かれたウィーン会議によって形作られた「欧州協調（Concert of Europe）」における「首脳外交（summit diplomacy）」、「会議体制（Congress System）」及び「会議外交（Conference Diplomacy）」とされる[44]。「同質性」とは、使用する共通言語としてのラテン語やフランス語、キリスト教等の同質の文化を持つ欧州諸国を指し、「貴族性」とは、外交の主体が各王朝の貴族であり、貴族階級が独占して行う「秘密外交（secret diplomacy）」を示し、「自立性」は、これらの国の外交官が相当の自立性、排他性を持っていたことを表している。

「旧外交」の方法として、「首脳外交」は、平時に大国の首脳や外交指導者が結集して多数国間の外交会議を行うことを指し、「会議体制」とは、平時における大国間会議により国家間の紛争の解決を目指す外交協議の制度のことである。また、「会議外交」とは、大国す

---

[41] 細谷雄一『外交　多文明時代の対話と交渉』（有斐閣，2007 年）29 頁
[42] 1446 年、ミラノ公国がフィレンツェのコジモ・ディ・メディチ（Cosimo de' Medici）に派遣したニコデマス・ディ・ポントラモーリ（Nicodemo da Pontremoli）が最初と言われる。（ibid. 46 頁）.。また、常駐大使の相互的な受け入れの最初の例は 1425 年頃のミラノ公国とハンガリー王国間のものと言われる（ibid. 47 頁）。
[43] ibid. 69 頁
[44] ibid. 69～70 頁

べての参加は必須ではなく、特定の紛争に関して協議をする場であり、出席者は、議長役に開催国の外相がつき、開催国に駐在する各国の大使・公使クラスに限定されていたとされる[45]。また、伝統的に常駐外交使節を通じた交渉形式である二国間外交（bilateral diplomacy）や、一国が一方的な外交的宣言を行う単独行動主義「unilateralism」などもその特徴とされる[46]。さらに、「旧外交」の目的として、一国の覇権の阻止や平和の維持があげられ、勢力均衡や同盟関係が重視された。

「旧外交」を一言で表せば、「ルネサンス期のイタリアで発明されて、リシュリュー[47]によって精緻化され、カリエール[48]によって理論化され、サトウ[49]によってマニュアルが提供されたもの」である[50]。

2.1.1.2「新外交」

このような欧州の伝統的な「旧外交」の外交体系を嫌悪し、主張されたのが「新外交」である。

まず、「新外交」の目的は、「『旧外交』の外交文化や外交慣習を批判してそれを改宗し、世界を新しく塗り替えること」であった[51]。具体的には、「新外交」における宮廷文化や貴族階級の世界によって外交を独占し、秘密裡に行う「秘密外交（secret diplomacy）」の文化を批判し、一般市民が外交を見守り、その同意を得る民主的な外交、「公開外交（open diplomacy）」を主張した。さらに、「旧外交」における勢力均衡や同盟関係を締結する外交慣習ではなく、会議外交や国際機関によって、公開の討議により紛争を解決することを主張した[52]。それは、一般市民、世論といった民主主義的イデオロギーを外交に導入する、「民主的外交」といえる外交であった。

「新外交」を提唱した代表的な人物には、米国第 28 代大統領ウッドロー・ウィルソンが挙げられる。ウィルソンは、英国自由党の指導者として 4 度首相を務めたウィリアム・グ

---

[45] ibid. 73 頁
[46] ibid. 121 頁
[47] Armand Jean du Plessis de Richelieu。フランスのルイ 13 世（位 1610～43）時代の宰相を務めた枢機卿。外交における「持続的な交渉」を説き、そのための国内的な意思統一と組織的な統合を重視。これにより対外政策をフランス外務省の管轄とし、権限を強化。国家があたかも 1 つの意思を持つかのように「国家理性」を前提とした外交を展開。
[48] François de Callières。17 世紀後半から 18 世紀前半のフランス外交官。『君主たちと交渉の方法について（*De la manière de négocier avec les souverains*）』（板野正高による邦訳は『外交談判法』）の著者。
[49] Sir Ernest Mason Satow。18 世紀後半から 19 世紀前半の英国外交官。駐日公使や駐清公使を務めた。『外交実務案内（*A Guide to Diplomatic Practice*）』を 1917 年に刊行。外交実務経験を活かし、外交交渉を体系化、マニュアル化した。
[50] ibid. 69 頁
[51] ibid 104 頁
[52] ibid.

ラッドストンや「国際連盟（League of Nations）」という言葉を生み出したゴールドワージー・ローズ・ディキンソンらの思想から影響を受け、「新外交」の理念を米国議会教書演説において「14 か条の原則」として主張した[53]。そこでは、「民主的外交」や「公開外交」のほか、公海自由の原則、自由貿易の原則、軍縮の原則、民族自決の原則等を平和のための重要な要素として列挙した。また、民主主義的なイデオロギーではないが、外交のイデオロギー化、外交の宮廷文化を批判して「新外交」を唱えた者には、1917 年にボリシェヴィキ革命を起こしたソ連のトロツキーがいる[54]。

また、「新外交」の方法として、多国間外交（multilateral diplomacy）が主張され、これは国際連盟そして現代の国際連合へと発展していった。さらに、「新外交」において、外交言語として英語が用いられるようになった。しかし、こうした「新外交」の特質について、「世論」はプロパガンダとして利用され、「民族自決」は排外的なナショナリズムや人種主義を生み、「外交におけるイデオロギー化」は日本における「アジア主義」やナチス・ドイツの台頭の契機となった[55]。結局、「新外交」の理念に基づく 1919 年のパリ講和会議後のヴェルサイユ体制は、20 年後に第 2 次世界大戦勃発により崩壊した。「新外交」を痛烈に批判し、「旧外交」を擁護したニコルソンは、外交において「素人が世論の前で交渉を行う危険性を強調し、あくまでも『外交交渉』を職業外交官の手に委ねさせて、民主主義が関与する領域を『外交政策』の立案過程のみに閉じ込めようとした」[56]。このようなニコルソンの指摘もあり、現在に至るまで、外交政策の立案過程において有識者等の意見を参考にしつつ、各国は外交の専門試験を合格し、外交文化、外交の教養、プロトコル等を十分に習得したエリートから構成される組織化された外交当局を置き、外交関係がある国に常駐外交使節を置き、外交のプロによる外交交渉を行っている。

2.1.1.3 戦後外交

第二次世界大戦後の外交の特徴の一つは、グローバル化であり、国際レジームの中心は、「国連外交」である。国連は「旧外交」の「会議外交」の伝統を、拒否権を有する大国が常任理事国を務める安全保障理事会が「欧州協調」時代の「会議体制」の伝統を受け継いだものといえる[57]。また、「新外交」が掲げた「公開外交」の原則について、一部の国連総会の一般討論演説がテレビカメラで中継されているという点や外交青書・白書等が刊行さ

[53] ibid. 112 頁
[54] ibid. 102 頁
[55] ibid. 136～137 頁
[56] ibid. 119 頁
[57] ibid. 154 頁

れ、各国の外交政策や毎年の外交活動の結果等をインターネット上でアクセス可能であることなどからすれば、その理念を導入していると言えなくもないが、重要な事項の外交交渉自体については、現代においても外交使節や政府関係者が「秘密外交」の形式で行っている。しかし、「新外交」の世論の重視という点に関して言えば、国連のみならず、各国政府は、ヒト、モノ、カネ、情報等のグローバル化が進展する現代において、国際世論を無視して外交を展開すれば国際社会において孤立するのは必然であり、20 世紀初頭以上に、情報を積極的に発信し、国内外の世論に働きかけて、自国に対する共感を得る広報外交（public diplomacy）が重要になっている。

また、戦後から 20 世紀末にかけての外交の最大の関心事の一つは、米国を中心とする自由主義・資本主義体制の西側諸国とソ連を中心とする共産主義・社会主義体制の東側諸国とのパワーやイデオロギーに関する対立である冷戦であった。キューバ危機など核兵器による戦争の危機もあったが、米ソ大国間同士の直接の戦争はホットラインの設置に代表される信頼醸成措置などの様々な外交努力により回避できた。しかし、東西ドイツの分裂、朝鮮戦争、ベトナム戦争等両大国の代理戦争が相次いだ。

戦後外交には、経済や政治・防衛分野に関する地域統合（regionalism）が多いのも特徴的である。その最たる例が、欧州連合（European Union、以下「EU」という。）である。6 カ国であった原加盟国は 28 カ国まで拡大した。EU 以外にも、欧州における欧州評議会（CoE）、米国や欧州を中心とする北大西洋条約機構（NATO）、欧州安全保障協力機構（OSCE）、旧ソ連構成国を中心とする独立国家共同体（CIS）、ロシア主導の集団安全保障条約機構（CSTO）、アジアにおける東南アジア諸国連合（ASEAN）、南北アメリカの米州機構（OAS）、アフリカのアフリカ連合（AU）や西アフリカ諸国経済共同体（ECOWAS）、アラブ諸国による湾岸協力理事会（GCC）やアラブ連盟、太平洋諸国から成る太平洋・島サミットなどがある。

外交の主体について、1964 年には、外交使節団の組織や任務、外交上の特権や免除等について規定した外交関係に関するウィーン条約が発効し、世界各地で働く各国の国際公務員の外交使節としての身分保障が明文化された。このような外交使節団の制度化のほか、実際に外交交渉を行っているのではないが、アルカイダやイスラム国（Islamic State of Iraq and Syria、「ISIS」）等の国際的なテロリストのネットワークを始めとする非国家主体が国際社会の脅威として台頭してきており、テロ対策の国際協調としての外交は存在しており、「対テロ戦争」という言葉があるように、これまでの国家対国家ではない形の「新

しい戦争」が 21 世紀以降重大な課題となっている。

外交の目的として、伝統的な平和の問題のみならず、経済、文化、人権、海洋問題、テロ対策など幅広い問題を経済外交や広報文化外交、人権外交、海洋外交などの多国間外交によって協議するようになったのも戦後外交の特徴である。共通の安全保障上の脅威に対する条約に基づく軍事同盟のみならず、条約等国際法に基づかない非公式な事実上の同盟関係、経済・通貨同盟、関税同盟などが形成されている。

現代においても古代から存在する伝統的な二国間外交は行われているが、鉄道、飛行機等の交通手段の発達や情報通信技術の発展によるテレビ、固定電話、ファックス、インターネット、電子メール等の普及により、外交に携わる者があらゆる問題を瞬時に、同時に共有し、世界中の都市に赴くことが可能になったこともあり、「国際的な組織化（international organization）、あるいは国家間の結合（association of states）の動きが、20 世紀の国際関係の最も大きな特徴」[58]と言える。「旧外交」時代から重視されてきた「首脳外交」もこうした交通手段の発展と情報通信技術の進展により容易に行うことが可能になり、1975 年以降主要国首脳会議（Summit。現在は G7）が毎年行われている。G7 と新興国の首脳を合わせた G20 の枠組みもある。

海洋、空、宇宙空間、南極等のあらゆる空間に関する利権をめぐる国家間の争いに対しても、多国間外交の枠組みによって国際的なルール作りや信頼醸成に努めるのも戦後外交の特色である。

2.1.2 サイバー外交

以上のような伝統的な外交に対し、「サイバー外交」とは何か。

サイバー外交とは、細谷教授の「外交」の定義に当てはめて考えれば、「国家等のサイバー空間のステークホルダーが、国益や安全、社会経済文化的発展を可能にする情報通信技術に基づき構成される人工的な空間であるサイバー空間の安全を強化するため、また国際社会においてサイバー空間のステークホルダー間の関係をより安定的に維持しその友好関係を強化するため、政府間等で行われる交渉又は政策」というように定義することできる。

サイバー外交政策やサイバー外交交渉を行う主体は、伝統的な外交に比べ、より非国家主体の関与が重要になっているのが特徴的である。それが顕著に現れているのが、サイバ

[58] ibid. 156 頁

一空間に関する国際会議（Global Conference on Cyberspace、以下「GCCS」）、いわゆるロンドン・プロセスである。ロンドン・プロセスは 2011 年、当時の英国の外相ウィリアム・ヘイグが提唱して始まったサイバー空間に関する諸問題に関する包括的な議論を政府機関、国際機関、民間企業、NGO 等のマルチステークホルダーが一堂に会し行うハイレベルかつ最大規模の国際会議である。GCCS は、2011 年にロンドン、2012 年にブダペスト、2013 年にソウル、2015 年にオランダ、ハーグそして 2017 年にニューデリーで開催された[59]。ただし、この国際会議は、サイバー問題の重要事項に関する外交交渉をするような場ではなく、各ステークホルダーのサイバーセキュリティに関する立場を表明するようなさながらスピーチ合戦という性質が強く、重要事項を決定する本質的な議論を交わすばとは言えない。しかし、これまでサイバー空間に関する問題は、外交上想定していなかった新しい脅威であり、かつ、職業外交官は国際関係や安全保障、政治、経済、国際法、国際儀礼、語学等についての専門性は高いが、これまで外交交渉や外交政策の対象として想定していなかったサイバーセキュリティのとりわけ技術的な知見について専門性を有する者が多いとは考えにくく、サイバー問題に関して外交固有の政府関係者のみでの対応は難しいという面がある。そこでサイバー外交においては、国防や情報通信技術当局等の外交専門機関以外の政府関係者やサイバーセキュリティの知見があるサイバーセキュリティ業者等の民間企業や CERT/CSIRT 等のセキュリティ関連団体等が政策立案過程において関与している例が高いと考えられる。ただし、外交交渉自体はサイバー外交においても、外交交渉の専門家である外務省の職員が行っている場合が多いのは付属資料 2 の国連 GGE の政府専門家一覧を見ても明らかである。

マルチステークホルダー型外交とは別に、トラック 1.5（官民）外交として、ニューヨークのシンクタンク東西研究所（East West Institute）が主催するグローバルサイバーサミットがある。

首脳外交として、2016 年の伊勢志摩サミットにおいて、「サイバーに関する G7 の原則と行動」が発表された[60]。この文書において、インターネットの開放性、相互運用性、信頼性及び安全、インターネットによる自由、民主主義、人権の価値の促進、情報の自由な流通によるグローバルな経済及び開発の促進、プライバシー、データ保護及びサイバーセキ

[59] 外務省：日本のサイバー外交多国間会議等（http://www.mofa.go.jp/mofaj/fp/nsp/page24_000686.html）（最終アクセス日：2017 年 12 月 18 日）
[60] 外務省：G7 伊勢志摩サミット（http://www.mofa.go.jp/mofaj/ms/is_s/page3_001697.html）（最終アクセス日：2017 年 12 月 18 日）

ュリティの尊重、インターネットガバナンスに関するマルチステークホルダー・アプローチへのコミットメント、オンラインにおける人権及び法の支配の原則の促進と保護、テロリストによるサイバー空間の利用に対する懸念、サイバー空間への国連憲章を含む国際法の適用の容認、サイバー活動の国連憲章及び国際慣習法上の「武力行使」又は「武力攻撃」の該当性の確認とそれに対する国連憲章第 51 条に基づく個別的又は集団的自衛権行使の可能性の認識、CERT 間の協力、キャパシティビルディング及び意識啓発の促進等の国家間の協力強化によるサイバー空間の安全及び安定の促進等を行うことについて、G7 諸国が同意した。

多国間外交として、サイバーセキュリティのキャパシティビルディングに関するベストプラクティスの共有と援助国と被援助国を繋ぐためのプラットフォームとしての「サイバーの専門的知見に関するグローバルフォーラム（Global Forum on Cyber Expertise、以下「GFCE」という。）」、安全保障分野でのサイバー空間における国際法の適用、国家の責任ある行動規範、信頼醸成措置、キャパシティビルディング等に関する政府専門家会合である国連サイバーGGE、サイバーセキュリティの信頼醸成措置やキャパシティビルディングに関する議論が活発化している ASEAN 地域フォーラム（ARF）や欧州安全保障協力機構（OSCE）、重要情報インフラ防護に関する国際連携を議論するメリディアン会合、サイバー犯罪に関する国際規範の在り方や国際協力について議論する国連サイバー犯罪に関する政府専門家会合、国連犯罪防止刑事司法委員会、サイバー犯罪条約関連会合、オンラインにおいても表現の自由やその他の基本的人権は保障されるべきとの主張を促進するためのフリーダム・オンライン会合などの枠組みがある。

二国間外交として、日本の例を挙げると、これまで 2011 年以降、米国と 5 回、英国、豪州、イスラエル、エストニアと 3 回、インド、EU、ASEAN、ロシアと 2 回、ドイツ、ウクライナ、韓国と 1 回、サイバー会議（名称はサイバー対話、サイバー政策協議、サイバー協議、サイバー犯罪対策対話等）を行っている。なお、日中韓の三国間外交も 2 回実施している。また、日英共催で ASEAN 諸国向けサイバーワークショップを本年 2 月に実施した[61]。

サイバー二国間外交において特徴的なのは、他の分野において特別関係が緊密とはいえ

---

61 外務省日本のサイバー外交　二国間協議・対話等
（http://www.mofa.go.jp/mofaj/fp/nsp/page24_000687.html）（最終アクセス日：2018 年 2 月 24 日）

ないようなエストニアと 3 回も協議を行っていることにみられるように、地政学的に重要ではなく、国際政治上のプレゼンスや経済力、人口、国土面積等の国力からみれば小国であっても、サイバーという特定の分野を強みにしているような国との外交を重視している点である。なお、尖閣諸島問題等により関係が良好とは必ずしも言えない中国との二国間サイバー協議は現在のところ実現されていない。

サイバーに関する多国間外交や二国間外交が数多く実施されるようになったのは，CS の問題が外交上の重要な喫緊の課題として認識され，国際連携の必要性の高まりという国際社会の傾向とともに，2012 年 2 月のサイバー政策担当大使（総合外交政策局審議官）の創設や 2016 年 7 月のサイバー安全保障政策室の設置等サイバー外交体制の強化による諸外国等との調整の円滑化が背景にある。

こうした様々なサイバーの問題に関する多国間，3 国間，2 国間及び地域枠組みが構築され，国際連携に向けた動きが活発に行われているが，国際社会においては，サイバー空間の在り方を巡る激しい対立の構図が存在する。すなわち，サイバー空間における情報の自由な流通及び政府のみならず民間企業や市民社会を含むマルチステークホルダー・アプローチを基本原則として，国際連合憲章（第 51 条の武力攻撃に対する個別的・集団的自衛権規定を含む）や武力紛争法・国際人道法，国際人権法（オンラインにおける表現の自由等の人権の保障），国際慣習法等の既存の国際法がサイバー空間を利用した行為にも適用されるという立場をとる日本や米国，欧州等と，サイバー空間において国家主権に基づく国内管理を優先し，反政府的な言論等の情報統制，コンテンツの規制等国内法に基づく規制の強化やソースコードの開示要求等を重視し，従来の国際法の適用について慎重な立場をとる中露等の対立が前述の様々な多国間及び地域枠組み等において顕在化している。それはさながら新冷戦構造とも呼べる構図であり，G7 諸国や EU 加盟国，豪州，ニュージーランド等を含む「西側諸国」と上海協力機構（Shanghai Cooperation Organization，以下「SCO」という。）加盟国を中心とする「中露等」の両陣営が激しく鍔迫り合いを展開し，サイバー空間の諸問題について議論が平行線を辿り，国際的な同意形成が困難な場面が多々見受けられる。

このような状況において，同意形成の鍵を握るのが国際社会において多数派を占める「開発途上国」や「新興国」である。これらの国々の多くでは，経済成長に不可欠なツールとしてインターネットの利用者数が急激に増えているが，政府のコンピュータ緊急対応チーム（Computer Emergency Response Team。以下「CERT」という。）等のサイバー

セキュリティの能力が不十分な国や，国民全体のサイバーセキュリティへの意識が低い国も多い。また，西側諸国と中露等のいわばサイバー空間の秩序の在り方を巡る国際政治的イデオロギーの争いがあること自体を認識していない，あるいはその争いの場に参加していない国も多く，どちら側に付くのかそれとも両陣営とは異なる別の立場をとるのか，社会経済的発展等の国益の追求と同盟関係や政治的スタンス等を考慮した国際連携の双方の視点に加え，固有の文化的要素等を含めた総合的かつ慎重な判断が求められており，両陣営は多数派形成の活動として途上国等に働きかけ，取り込みを狙っている。

大規模なサイバー攻撃に対する対処能力が不十分な国の脆弱なネットワークの基盤が踏み台にされサイバー攻撃が実施されることは当該国のみならず国際社会全体のリスク要因であるという認識の下，途上国のサイバーセキュリティ能力構築支援の国際連携を目指す動きが西側諸国を中心に見られる。

途上国のサイバーセキュリティのを底上げをすることにより，自国のセキュリティの強化にも繋がるという理由などから西側諸国，中露等も重要性を認識している。サイバー攻撃に対する対処能力や知見が不十分な途上国としては，サイバーセキュリティの技術協力や資金援助，意識啓発等が最大の関心事である。キャパシティビルディングはサイバー問題に関する最重要課題の一つとして国際社会で共通認識が形成されている。しかし，西側と中露等は双方の陣営が能力構築支援を政策的に利用して，現行国際法の適用に関する立場などが不明確な国に働きかけて自陣に取り込もうという意図も伺える。「政府開発援助（ODA）によって援助を行う際には，援助国は国益への配慮に重点をおき，援助の源泉である税金を納めている国民に対する説明責任を果たすことが求められる」 というように，国家による開発協力・開発援助には，人道上の動機以上に外交戦略上の動機，すなわち国益が重視される傾向がある。

西側諸国の取組としては，英オックスフォード大学にグローバルサイバーセキュリティキャパシティセンター（Global Cyber Security Capacity Centre。以下「GCSCC」という。）を設置し，サイバー政策・戦略の策定及びサイバー法制度の構築などを含む 5 分野を研究し，その効果的な手法を英国内外の政府や企業等に共有して能力構築を支援しようと努めている。また，2015 年に行われたサイバー空間に関するハーグ会議において，サイバーの専門的知見に関するグローバル（GFCE (Global Forum on Cyber Expertise：以下「GFCE」という。）と)という各国政府，政府間組織及び民間企業のための枠組が立ち上げられ，能力構築支援の経験を共有し，支援国と被支援国が支援を行う場を提供していく予

定ですある。立ち上げメンバーとして，露伊を除く G8 諸国すべてを含む西側先進国や民間企業及び途上国等 45 の政府，政府間組織及び民間企業が参加した。

国連の GGE においては，コンピュータ緊急対応チーム（Computer Emergency Response Team。以下「CERT」という。）の協力強化支援，重要インフラのセキュリティの改善等のための支援及び研修，サイバーセキュリティ技術へのアクセスの提供支援，迅速なインシデント対応等の手続の構築，重要インフラの脆弱性に対処するための国境を越えた協力の円滑化，国民や企業のサイバーセキュリティ教育のための意識啓発プログラムの策定などの提言がなされている 。

中露等は，GCSCC オックスフォード大学のセンターや GFCE などは，西側主導のイニシアティブで，かつ，国家のみならず，民間企業，市民社会等サイバー空間の多様な利害関係人（multi-stakeholders）が議論や意思決定プロセスに参加し，合意形成を行う手法であるマルチステークホルダー・アプローチに基づくものであるためであり，サイバー空間の在り方に関する異なる立場をとる西側陣営に主導権を握られるのを嫌い，評価していないと考えられる。中露には西側と協力して積極的に能力構築を行うという姿勢は見受けられない。なお，中国は 2015 年 7 月に ASEAN 地域フォーラム（ASEAN Regional Forum。以下「ARF」という。）の枠組でマレーシアとともにサイバーセキュリティの能力構築に関するワークショップを実施している。

キャパシティビルディングは，サイバー攻撃への対処能力が不十分な途上国のネットワークの脆弱性が国際社会全体のリスクとなることに鑑み，先進国が中心となりサイバー活動の対処能力構築支援や意識啓発などを行い，国際的な協力支援体制を強化することによるサイバー活動のリスクの低減という効果が期待できる。他方，一方で、支援をすることによる見返り，すなわち現行国際法の適用などに関する立場が不明確な被支援国の支持を期待する西側と中露の主導権争いを有利にするための手段という側面があると考えられる。サイバー空間に関する国際秩序の多数派形成の鍵を握る途上国を何としても自陣に取り込みたい西側及び中露両陣営の懐柔策と被支援国としては強かに援助してもらえるものは援助してもらい，最も自国のニーズに合致した援助を行う側に与するという互恵的関係を構築するためにキャパシティビルディングは双方にとって戦略的に重要になり，今後両陣営の熾烈な能力構築競争が展開されると考えられる。

日本は，2015 年に策定されたサイバーセキュリティ戦略において，キャパシティビルディングに関する戦略を明示し，国際社会の平和と安定のためにサイバーセキュリティの

キャパシティビルディングに関する国際協調を行うことが重要であるとしており，とりわけアジア大洋州太平洋地域の途上国の能力構築を目指す方針を固めた 。2016 年現在，既に数か国のサイバーセキュリティに関するニーズの調査を行うためにへの数か国の調査団を派遣したり，UNODC(国連薬物犯罪事務所)を通じて米国及び豪州と東南アジア諸国におけるサイバー犯罪の防止を目的とする資金援助を行ったり，アジア初のサイバー犯罪に関するブダペスト条約の締結国として，その締結までの法制度整備等の経験を ASEAN 諸国に伝授するための日・ASEAN サイバー犯罪対話をの主催したり，途上国へのサイバー犯罪対策の教育・研修を実施したり，各国の法執行機関との人材交流や人材育成，人材派遣等を行ったりしている。

表 2　主な外交の主体と外交関連史

	日本	米国	中国	露	英	仏	独	伊その他欧州	その他
15C	室町～戦国時代	欧州列強による「新大陸」の発見	明朝（1368～1644） 冊封体制	モスクワ大公国イヴァン 3 世,「全ロシアのツァーリ（皇帝)」と称（位 1462～1505)、キプチャク＝ハン国の「タタールの軛」からロシアを解放	百年戦争（1339～1453） 薔薇戦争（1455～85)、ヘンリー 7 世（位 1485～1509）のテューダー朝（～1603）	百年戦争（1339～1453） シャルル 7 世（位 1422～61） ルイ 11 世（位 61～83）	神聖ローマ帝国 ルネサンスの三大発明 グーテンベルクの活版印刷術、羅針盤、火薬（火器）	北イタリアで「旧外交」（近代外交）誕生（常駐大使制度）北イタリア諸国間のローディの和約（1454） カスティーリャ王国イサベル 1 世とアラゴン王国のフェルナンド 2 世結婚によりスペイン王国成立（1469） 大航海時代（葡バルトロメウ・ディアス、アフ	オスマン帝国メフメト 2 世（位 1444～46、51～81)、コンスタンティノープル征服（ビザンティン帝国滅亡、1453）

								リカ南端喜望峰到達（1488）、ヴァスコ・ダ・ガマ、インド西岸カリカット到達（98）、カブラル、ブラジル漂着（1500）、マヌエル１世、フィレンツェのアメリゴ・ヴェスプッチに「新大陸」探検を依頼（01～02） コロンブス、西女王イサベルの援助を受けバハマ諸島サンサルバドル到着（1492）[62]	

[62] 葡：ポルトガル、西：スペイン

16C	豊臣秀吉 南蛮貿易 朝鮮出兵（文禄の役（1592)、慶長の役（96～98)）			イヴァン4世,「ツァーリ（皇帝)」として正式に即位	ヘンリ8世(位1509～47）首長法制定、英国国教会成立（1534） エリザベス 1世（位1558～1603)、統一法制定（59）	フランソワ 1世（位1515～47） アンリ 4 世即位，ブルボン朝 （1589～1792，1814～30）	宗教改革 マルティン・ルターの『95か条の論題』公表（1517） 神聖ローマ皇帝カール 5 世（位 1519～56）	大航海時代（「スペイン黄金世紀」西カルロス1世、葡マゼランに航海命令、マゼラン、比到着、死亡(1521)、同船団世界周航完成（19～22） コルテス、アステカ帝国征服（1521)、ピザロ、インカ帝国征服（33） メディチ家、フィレンツェ共和国大公（1530） スイス、カルヴァンの宗教改	オスマン帝国セリム1世(位1512～20)、シリア、エジプト併合(17) スレイマン 1世（位 20～66)、ウィーン包囲（29)、プレヴェザの海戦（38）

								革	
17C 前半	島原の乱（1637～38） 「鎖国」政策		清朝（1616～1912）	ミハイル・ロマノフ即位，ロマノフ朝（～1917）	ステュアート朝	ルイ 13 世の宰相リシュリュー枢機卿 外務省設置（1624） 大航海時代 イギリス東インド会社設立 ジェームズ 1 世，ヴァージニア植民地建設 ピルグリム・ファーザーズ，メイフラワー号で渡米 ニューイングランド植民地形成 三十年戦争	大航海時代 フランス東インド会社設立 三十年戦争	大航海時代 オランダ，連合東インド会社，西インド会社設立，ニューアムステルダム建設 グロティウス『海洋自由論』，『戦争と平和の法』 オランダの覇権	
					勢力均衡（ウェストファリア体制）				

17C 後半			ネルチンスク条約（1689）	ピョートル 1 世（大帝）（位 1682～1725） ネルチンスク条約		ルイ 14 世（太陽王，位 1643～1715），絶対王政の絶頂期			
					ピューリタン革命 第 2 次英仏百年戦争（本国：ファルツ戦争，スペイン継承戦争，オーストリア継承戦争，七年戦争。植民地：ウィリアム王戦争，アン女王戦争，ジョージ王戦争，フレンチ＝インディアン戦争）	第 2 次英仏百年戦争（本国：ファルツ戦争，スペイン継承戦争，オーストリア継承戦争，七年戦争。植民地：ウィリアム王戦争，アン女王戦争，ジョージ王戦争，フレンチ＝インディアン戦争）			

					英蘭戦争				
18C 前半				北方戦争 ニスタット条約 ペテルブルク建設，遷都	グレートブリテン連合王国成立 ジョージ 1 世，ハノーヴァー朝創始 スペイン継承戦争	スペイン継承戦争 ユトレヒト条約 ルイ 15 世（位 1715～74）	スペイン継承戦争 プロイセン王国成立		
18C 後半		13 植民地，独立宣言 パリ条約（英国，独立承認） 合衆国憲法制定 ワシントン初代大統領 「代表なくして課税なし」		エカチェリーナ 2 世（位 1762～96） 露土戦争 キュチュク＝カイナルジャ条約	ナポレオン戦争 七年戦争 パリ条約 三角貿易 産業革命 資本主義制度成立 交通革命 印紙法制定 対仏大同盟	ルイ 16 世（位 1774～92） 七年戦争 パリ条約 仏軍，北米から撤退 フランス革命（民衆の身分制への不満，啓蒙思想の普及，バスティーユ牢獄襲	外交革命 七年戦争 フベルトゥスブルク条約 ピルニッツ宣言 対仏大同盟		

					外務省設置（1782）	撃，人権宣言採択，ルイ16世処刑，全国三部会→国民議会→立法議会→国民公会→（ロベスピエールの恐怖政治→テルミドール9日のクーデター→）総裁政府 ナポレオン，ブリュメール18日のクーデター，統領政府を樹立，第1統領） ナポレオン戦争			
19C前半			アヘン戦争	第3回対仏大	グレートブリ	アミアンの和	ライン同盟結	ウィーン体制	

			アロー戦争	同盟 アウステルリッツの戦い ウィーン体制	テン及びアイルランド連合王国成立 アミアンの和約 第3回対仏大同盟 トラファルガーの海戦 ワーテルローの戦い（15） ウィーン体制 アヘン戦争 アロー戦争	約 トラファルガーの海戦，アウステルリッツの戦い テイルジット条約 ウィーン体制	成，神聖ローマ帝国滅亡 ウィーン議定書、ウィーン体制		
19C後半	日米和親条約（54） 日英修好通商条約（58） 外務省設置（69） 日清戦争（94～95） 「大日本帝国」	日米和親条約（54） モンロー主義（孤立主義，不干渉主義） 米西戦争 ベル、電話発明	日清戦争 北京条約	クリミア戦争	日英修好通商条約締結 クリミア戦争 欧州協調 「世界の工場」	普仏戦争 クリミア戦争	普仏戦争 ドイツ帝国（1871～1918） ヴィルヘルム2世（位1888～1918）	イタリア王国建設	
				三国協商			三国同盟		

1900 年代	日英同盟 日露戦争			日露戦争 ロシア革命	日英同盟				
1910 年代	韓国併合（～45） 第一次世界大戦 パリ講和会議 ヴェルサイユ体制	ウィルソン政権（任 1913～21） パリ講和会議 ヴェルサイユ条約 「14 か条の平和原則」	辛亥革命 中華民国成立，清朝崩壊	第一次世界大戦	第一次世界大戦	第一次世界大戦 ヴェルサイユ体制	第一次世界大戦 ドイツ革命，ワイマール共和国成立		
1920 年代	 アジア主義 国際連盟 パリ不戦条約	パリ不戦条約 大恐慌		ソ連成立	アイルランド独立		国際連盟脱退 ヒトラーによるナチズム 東方生存圏構想	ファシズム	
					国際連盟	国際連盟		国際連盟	
1930 年代	国際連盟脱退 満州事変 日中戦争	ルーズベルト政権（任 1933～45） ニューディール政策	日中戦争		チェンバレン政権（37～40）		ラインラント進駐 ヴェルサイユ条約破棄宣言（35） 墺、併合（38）	エチオピア侵略	

				独ソ不可侵条約、ポーランド侵攻（39）	ミュンヘン会談（宥和政策）		ズデーテン地方割譲要求、ミュンヘン会談で併合（38） 独ソ不可侵条約、ポーランド侵攻（39） WWII 開戦		
1940 年代前半	近衛内閣、大東亜共栄圏構想 日独伊三国同盟 日ソ中立条約（41） 真珠湾攻撃 アジア太平洋戦争（第 2 次世界大戦）	大西洋憲章調印（41） 真珠湾攻撃 アジア太平洋戦争（第2次世界大戦） ダンバートン・オークス会議	第 2 次世界大戦	日ソ中立条約（41） 第 2 次世界大戦 独ソ戦 対日参戦	チャーチル政権（任 40～45、51～55） 大西洋憲章（41） 第 2 次世界大戦	第 2 次世界大戦	日独伊三国同盟 独ソ戦（第2次世界大戦）	日独伊三国同盟 第2次世界大戦	第 2 次世界大戦
1940 年代後半	広島，長崎原爆投下 降伏，第二次世界大戦終結	ヤルタ会談 トルーマン政権（任 45～53） ポツダム会談	中華人民共和国成立、毛沢東国家主席（任 49～59）	ヤルタ会談 ポツダム会談 経済相互援助	ヤルタ会談 ポツダム会談 労働党のアトリー政権（任	第四共和政（1946～58）	降伏 東西分断（ベルリンの壁構築）	（以降，欧州全般の歴史） ブリュッセル	国連憲章発効，国際連合設立

	吉田ドクトリン	トルーマン・ドクトリン（共産主義封じ込め，介入主義） マーシャル・プラン 国家安全保障会議設置		会議（COMECON）結成	45～51） インド、パキスタン独立（47） アイルランド、英連邦離脱（49）			条約、西欧同盟 北大西洋条約発効、北大西洋条約機構（NATO）設立（原加盟国：白、加、丁、仏、氷、伊、盧、蘭、ノルウェー、葡、英、米）(49)	
1950 年代	サンフランシスコ講和条約 日米安全保障条約 日華平和条約 日ソ共同宣言 国連に加盟（56）	日米安全保障条約 米韓相互防衛条約 マッカーシズム アイゼンハワー政権（任 53～61） ARPA（高等研究計画局）を国防総省に設置	中印国境紛争 周恩来首相、平和共存五原則	日ソ共同宣言 ワルシャワ条約機構設立 ハンガリー動乱 フルシチョフ時代（任 1953～64） 史上初の人工				パリ条約発効、欧州石炭鉄鋼共同体（ECSC）設立（52）（現加盟国：仏、独、伊、蘭、白、盧[63]） 希、土 NATO 加盟（52）	印、ネルー首相、平和五原則 バンドン会議，平和十原則採択（55） 米州機構（OAS）設立

[63] 白：ベルギー、盧：ルクセンブルク

				衛星スプートニク 1 号打ち上げ				西独 NATO 加盟（55） ローマ条約発効、欧州経済共同体（EEC）, 欧州原子力共同（EURATOM）設立（58）	
1960 年代	日米地位協定 日韓基本条約	日米地位協定 キューバ危機 ベトナム戦争 米ソ・ホットライン開設 ニクソン・ドクトリン（アジアに対する過度な介入の抑制） ARPANET 開発（米国内の大学研究所にある 4 台の	中印国境紛争（62） 文化大革命 中ソ国境紛争（69）	ガガーリン, 人類初の宇宙飛行 キューバ危機 米ソ・ホットライン開設 ブレジネフ時代（1964～82） ブレジネフ・ドクトリン（制限主権	レソト独立（66）	セネガル独立（60）、アルジェリア独立（62）	西独ブラント首相、東方外交	ブリュッセル（併合）条約発効、ECSC, EEC, EURATOM 統合, 欧州共同体（EC）発足（67） 関税同盟完成（68）	「アフリカの年」 非同盟運動 東南アジア諸国連合（ASEAN）設立：原加盟国尼、馬、比星、泰[64]（67）

[64] 尼：インドネシア、馬：マレーシア、星：シンガポール、泰：タイ

		コンピュータを電話回線で接続、インターネットの起源)		論) プラハの春への軍事介入					
1970 年代	沖縄返還 日中平和友好条約 福田ドクトリン(対東南アジア基本方針) 北朝鮮による拉致	ベトナム戦争 カーター政権の人権外交 ニクソンショック 第1次石油危機 DARPA のカーンとスタンフォード大のヴィントン・カーフ、TCP/IP 開発	改革・開放 日中平和友好条約 中越戦争	アフガニスタン侵攻	EC 加盟 サッチャー政権	ランブイエ会議(第1回主要国首脳会議)		英国、アイルランド、デンマーク EC 加盟(73) 欧州通貨制度(EMS)導入(79～99)	欧州安全保障協力会議(CSCE)ヘルシンキ宣言 東南アジア友好協力条約(TAC)
1980 年代		レーガン政権(1981～89) ネオリベラリズム,スターウォーズ計画 中距離核戦略(INF)全廃条約		ブレジネフ死去後,アンドロポフ,チェルネンコ其々1年余で死去 ゴルバチョフ時代(1985～	フォークランド紛争			希、EC 加盟(81) 西 NATO 加盟(82) 西、葡 EC 加盟(86) 単一欧州議定	湾岸協力理事会(GCC)設立 東欧革命

		ブッシュ（父）政権（任 1989～93） マルタ会談 ARPANET から軍事部門（MILNET）を分離 ARPANET に代わり TCP/IP を使用 モリスワーム拡散 DARPA、CERT/CC をカーネギーメロン大学に設立		91），新思考外交 チェルノブイリ原発事故 ペレストロイカ（立て直し・再編） 中距離核戦略（INF）全廃条約 アフガニスタン撤退 マルタ会談				書発効（87） 欧州原子核研究機構（CERN）のティム・バーナーズ・リー、HTML 開発（89）	
1990 年代前半	インターネット商用利用開始（93）	湾岸戦争		ワルシャワ条約機構，COMECON 解消 バルト三国，独立宣言 ロシア連邦誕生，エリツィン初代大統領		欧州安全保障協力機構（OSCE）	東西ドイツ統一	域内市場統合完成（92） マーストリヒト条約発効，欧州連合（EU）に改称（93） 共通外交・安全保障政策（CFSP）	ASEAN 地域フォーラム（ARF）開始 ボスニア紛争

				（任 1991～99） ロシア連邦，ウクライナ，ベラルーシ，独立国家共同体（CIS）創設 ソ連消滅 集団安全保障条約調印				欧州経済領域（EEA）発足（94） CERN のリー、ワールドワイドウェブ（WWW）開発（世界初のウェブサイト）	
1990 年代後半				チェチェン紛争				墺、スウェーデン、芬[65]EU 加盟（95） ポーランド、チェコ、ハンガリーNATO 加盟（99） ユーロ導入（99） アムステルダ	アジア金融危機

[65] 芬：フィンランド

								ム条約発効（99）	
2000 年代前半		ブッシュ（子）政権（任 2001～09） 9.11 同時多発テロ ブッシュ・ドクトリン（善悪二元論，先制攻撃，単独行動主義，介入主義，新保守主義） 「テロとの戦い」 アフガニスタン戦争 イラク戦争 国土安全保障省設置	上海協力機構（SCO）設立。 印との戦略的・協力的パートナーシップ 胡錦濤政権（任 2003～13）	プーチン政権（任 2000～08） 集団安全保障条約機構（CSTO）発足。				ニース条約発効（03） エストニア、ラトビア、リトアニア、ポーランド、チェコ、ハンガリー、スロバキア、スロベニア、マルタ、キプロス EU 加盟（04） エストニア、ラトビア、リトアニア、スロバキア、スロベニア、ブルガリア、ルーマニア NATO 加盟（04）	

2000 年代後半	宇宙基本法	リバランス政策 ティーパーティー運動					メルケル政権（任 2005～）	ブルガリア、ルーマニア加盟（07） リスボン条約発効、CFSP を CSDP に改名、外務・安全保障政策上級代表ポスト創設（09） アルバニア、クロアチア NATO 加盟（09）	北朝鮮の核実験（2006, 09） BRICS の台頭
2010 年代前半	第二次安倍政権 地球儀を俯瞰する外交 国家安全保障会議設置		習近平政権（任 2013～） 一帯一路	第 2 次プーチン政権（任 2012～） クリミア「併合」				欧州対外行動庁（EEAS）発足（11） クロアチア、EU 加盟（13）	第 1 回 GCCS（2011、於：ロンドン）、第 2 回 GCCS（2012、於：ブダペスト）、第 3 回 GCCS（2013、於：ソ

									ウル) アラブの春 北朝鮮，金正恩時代（任2011～）核実験
2010 年代後半	安全保障法制成立 国家安全保障戦略, サイバーセキュリティ戦略 積極的平和主義	トランプ政権（2017～，アメリカ第一主義，単独行動主義，保護主義）	アジアインフラ投資銀行（AIIB）設立		国民投票により EU 離脱決定	パリ同時多発テロ マクロン大統領（任 2017～）		モンテネグロ、NATO 加盟（17）	第 4 回 GCCS（2015､於:ハーグ） 第 5 回 GCCS（2017､於:ニューデリー） 北朝鮮の核実験（2016 年 1 月, 9 月, 2017 年 9 月）

2.2 伝統的安全保障とサイバーセキュリティ

本節では，伝統的な「安全保障（security）」概念を整理したうえで，これと比較することによって，本論文の研究対象であるサイバー外交の目的の一つであり，サイバー外交によって確保すべき「サイバーセキュリティ（cybersecurity）」あるいは「サイバー安全保障」概念の特色を明らかにする。

2.2.1 伝統的安全保障

一般的な安全保障概念として，広辞苑によれば，安全保障とは「外部からの侵略に対して国家および国民の安全を保障すること」である[66]。

米国の国際政治学者のジョセフ・ナイは、安全保障は「酸素のようなものである。失ってみて初めて気付くもので、失うと他に何も考えられなくなる。」という有名な言葉を残している[67]。

国際関係・安全保障用語辞典において慶應義塾大学の神保謙は安全保障を次のように整理する。すなわち，安全保障とは，「『脅威の不在・脅威からの自由』を示す一般概念であるとともに，『行為主体が，獲得した価値を，それを剝脱しようとする脅威から，独自あるいは他者との協力によって守る』政策概念でもある。これまで，この価値を剝奪しようとする最大の脅威は，国家による軍事力の行使＝戦争であった。したがって，古くより『国家が他の国家からの侵略を軍事力によって守る』という概念（＝国防〔defense〕）こそ，安全保障の中心概念でありえた。しかし現代の安全保障の概念は，より多元的・多義的に展開している。」と説明する[68]。

ここから，安全保障概念を構成する四つの重要な要素があることがわかる。すなわち，「行為主体（誰が守るのか）」，「守るべき価値（何を守るのか）」，「脅威（何から守るのか）」及び「守る手段・方法（如何にして守るのか）」の四要素である。

第一に，行為主体について，「国家の役割は依然として支配的であるが，国際機構・地域・企業，非政府組織（NGO）・個人の役割も増大している」とする。第二に，守るべき価値については，「国家を構成する多元的要素（国土，国民の生命，財産，政治体制，経済，文化，アイデンティティ，環境・生態系・保健衛生）が複雑に交錯して議論が展開されるよ

---

[66] 新村出編『広辞苑第五版』（岩波書店，1998 年）
[67] Foreign Affairs: East Asian Security: The Case for Deep Engagement (https://www.foreignaffairs.com/articles/asia/1995-07-01/east-asian-security-case-deep-engagement)（最終アクセス日：2017 年 12 月 18 日）
[68] 小笠原高雪等編集『国際関係・安全保障用語辞典』（ミネルヴァ書房，2013 年）

うになった」と説明する。第三に，脅威について，「国家による軍事力の行使という伝統的脅威の他に，国際テロリズム，大規模災害，経済摩擦，金融危機，環境破壊，公衆衛生問題などの非伝統的脅威の台頭が顕著な現象となってきた」とする。そして，守る手段について，「伝統的な同盟関係に加えて，多国間安全保障協力，アドホックな協力関係（有志連合），国連等の国際機関の役割，さらには民軍協力や省庁間協力など，多くの連携・協力の形態を捉える必要が浮上した」として，「軍事力を中心とするハードパワーのみならず，制度や規範を形成する力（ソフトパワー）や高度な情報通信技術とその運用が，安全保障政策の重要な側面となってきている」と述べている[69]。

また細谷教授は、国際秩序の展開として、第一に、勢力均衡（バランス）の体系、第ニに、協調（コンサート）の体系、第三に、共同体（コミュニティ）の体系があると主張する[70]。

[69] ibid.
[70] 平成 22 年度外務省国際問題調査研究・提言事業報告書「将来の国際情勢と日本の外交―20 年程度未来のシナリオ・プラニング―」第 1 章　国際秩序の展望―「共通の利益と価値」は可能か―

2.3 陸，海，空，宇宙，そしてサイバー空間

米国はサイバー空間を「第 5 の戦場」と認識していることは第 1 章で既に述べた。本節では，この点について，サイバー空間の「第 5 の戦場」としての特殊性を，その他の 4 つの戦場，すなわち陸，海，空及び宇宙空間と地政学的な視点から比較して概説する。

サイバー空間は，従来の物理的な空間，すなわち，陸，海，空及び宇宙空間とは異なり，人が情報通信技術を利用して開発した人工的な空間である。

陸，海及び空には，それぞれ領土，領海及び領空という国家の排他的な支配権，すなわち領域主権が及ぶものとして，国際法上確立されている。国家は，その領域を，他国に損害を与えるような仕方で自ら使用したり，私人に使用を許可したりしてはならないという「領域使用の管理責任」という原則も 1941 年のトレイルスメルター事件仲裁判決においてうち立てられている[71]。

人類の活動領域は，陸海空宇宙そしてサイバー空間に拡大していった。人類の活動範囲の拡大に従い，国家等の国際社会の主体の利害関係の調整や安全･安定の確保の必要から，国際法の適用範囲も広がっていった。

2.3.1 陸：第 1 の戦場

まず陸については，その地（国家の領土）にある人，物，行為に対して主権を有する国家の管轄権（立法管轄権，執行管轄権及び司法管轄権）が及び，原則としてその国内法に服するものとされる。陸に関する条約としては，ハーグ陸戦法規などがある。また，南極大陸については，1959 年に日米英仏ソ連等 12 か国により南極条約が採択され，2018 年 1 月現在，53 か国が締結している。同条約が定める主な内容として，南極地域（南緯 60 度以南の地域）の平和的利用（軍事基地の建設，軍事演習の実施等の禁止），科学的調査の自由と国際協力の促進，南極地域における領土権主張の凍結，条約の遵守を確保するための監視員制度の設定，南極地域に関する共通の利害関係のある事項について協議し，条約の原則及び目的を助長するための措置を立案する会合の開催などがある。また，陸固有に適用されるルールではないが，核軍縮や不拡散，原子力の平和的利用，生物・化学兵器の禁止，通常兵器の軍縮及び過剰な蓄積禁止のための国際枠組みが存在する。

---

[71] 松井芳郎等『国際法』116 頁（有斐閣，1988 年）

2.3.2 海：第２の戦場

次に，海については，大航海時代の 15 世紀末にスペインとポルトガルが世界の大陸と海洋を二分して支配するようになった時期があった。17 世紀前半にはオランダのグロティウスが，海の大部分は自由な空間としておくことが万人の利益に合致するという考え方（『自由海論』等）を主張し，英国のセルデンが英国の海に対する支配を正当化するため，海洋領有を主張したが，グロティウスの考えが主流であった。そして，大航海時代以降のの世界においては，国家の権利が及ぶ狭い「領海」と，いずれの国家にも属しない広い「公海」の考え方（公海自由の原則）が一般的になった[72]。しかし，この考えは，現実には海洋利用能力に優れた先進国に有利に機能しても，その能力に乏しい途上国の利益を十分保護するものではないという批判とともに，海洋科学技術の急速な進歩によって新たな法規制の対象とすべき問題が増大したことを踏まえ，1982 年に国連海洋法条約が採択され，1994 年に発効した[73]。同条約は，2017 年 3 月現在，168 の国等が締結している[74]。海の国際法で特徴的なルールは，無害通航権である。すなわち，「全ての国の船舶は，領海において，無害通航権を有する」（国連海洋法条約 17 条）。沿岸国の平和，秩序又は安全を害さない通航であれば，いかなる国の船舶も沿岸国の領海を通行することができるというルールである。海洋に係る国際的な紛争を解決する機関として，1996 年，ドイツのハンブルクに国際海洋法裁判所（ITLOS）が設置されている。また，海上の安全保障という観点から，アジア海賊対策地域協力協定（ReCAAP），海洋法に関する国際シンポジウム，海洋安全保障に関する G7 ハイレベル会合，ARF 海上安全保障会期間会合，日シンガポール海上安全保障対話等の国際枠組みがある[75]。

2.3.3 空：第３の戦場

空について，まず，20 世紀初頭に発明された航空機の出現を契機とし，領土と領水（内水（河川，運河，湖沼，湾，内海，港）と領海）の上空一帯である領空とそれ以外の空域に区分されるようになり，1919 年の国際航空条約（パリ条約）は，航空機が軍事的に活用された第一次世界大戦の経験を踏まえ，国家がその領域において「完全かつ排他的な主権」，

---

[72] 外務省　海の法秩序と国際海洋法裁判所 http://www.mofa.go.jp/mofaj/press/pr/wakaru/topics/vol61/index.html
[73] 21 132 頁。国連海洋法条約の前に，1958 年の第 1 次海洋法会議で領海条約，公海条約，漁業資源保存条約，大陸棚条約を採択。国連海洋法条約は 1973 年から審議が開始された第 3 次海洋法会議の末，これらの 4 つの条約に代わるものとして採択されたものである。
[74] 外務省　海洋の国際法秩序と国連海洋法条約：http://www.mofa.go.jp/mofaj/gaiko/kaiyo/law.html
[75] 海上の安全保障：http://www.mofa.go.jp/mofaj/gaiko/kaiyo.html

すなわち領域主権を有することを認め，同条約に代わるものとして 1944 年に締結された国際民間航空条約（シカゴ条約）においても引き継がれ，一般国際法上すでに確立されたルールとなっている[76]。2016 年現在，国際民間航空条約の締約国は，191 である[77]。領海とは異なり，領空を飛行しようとする外国航空機は，安全確保の重要性から，下土国の許可を原則として得る必要がある。外国の軍用航空機が領域国の領空に無許可で侵入した場合，領域国は，強制着陸又は退去を命じることができ，命令に従わない場合は，武器の使用も認められるとされてきた。領空以外の空域は，公海同様全ての国の航空機の自由な飛行が認められている。なお，空の国際法をまとめる機関として，国際民間航空条約に基づき，国連の専門機関として国際民間航空機関（ICAO）が設置され，国際航空運送業務やハイジャック対策をはじめとするテロ対策等のための条約の作成，国際航空運送に関する国際標準・勧告方式やガイドラインの作成等を行っている[78]。

2.3.4 宇宙空間：第４の戦場

宇宙空間へ人類の活動範囲が広がったのは，1957 年，当時のソ連による人工衛星スプートニク 1 号の打上げ成功が起源とされる。

1959 年の第 14 回国連総会において，その常設委員会として，宇宙空間平和利用委員会（COPUOS）が設置された。2018 年現在，COPUOS 加盟国は日本を含む宇宙技術を有する 84 か国である[79]。宇宙技術の特性は，民生にも軍事にも使える軍民両用（dual use）という点にあり，宇宙空間に関する人類の活動は，民生利用（科学目的の宇宙探査等），商業利用（商業衛星打上げ活動等）及び軍事利用（軍による情報収集等）に分類できる[80]。宇宙空間に関する主な国際法としては，1966 年に国連総会で採択された宇宙法の基本原則を定めた宇宙条約，宇宙救助返還協定（1968 年），宇宙損害責任条約（1972 年），宇宙物体登録条約（1975 年）及び月協定（1979 年）などの条約や，宇宙空間自由の原則（宇宙条約 1 条で明文化）及び宇宙空間占有禁止の原則（宇宙条約 2 条で明文化）などの国際慣習法が存在する。すなわち，すべての国は，月その他の天体を含む宇宙空間の探索及び利用を，すべての国の利益のために，国際法に従い自由に行うことができ，また，月その他の

[76] ibid.159 頁。
[77] ICAO member states: http://www.icao.int/MemberStates/Member%20States.English.pdf
[78] 外務省　国際民間航空機関（ICAO）　http://www.mofa.go.jp/mofaj/gaiko/page22_000755.html
[79] Members of the Committee on the Peaceful Uses of Outer Spacehttp://www.unoosa.org/oosa/en/members/index.html
[80] 高屋友里「宇宙空間における安全保障と国際宇宙法」: https://www.usss.kyoto-u.ac.jp/uchugaku/seminar/2015/20150713_takaya.pdf

天体を含む宇宙空間の領有は禁止されている。また，宇宙空間の平和的利用という観点から，核兵器その他の大量破壊兵器を運ぶ物体を地球を回る軌道に乗せてはならず，これらの兵器を宇宙空間に配置し，又は天体に設置することが禁止され，天体における軍事基地・軍事施設の設置，兵器実験及び軍事演習の実施も宇宙条約によって禁止されている。宇宙空間に係る主な課題としては，①宇宙空間利用に関する国際的な規範作り，②宇宙空間をめぐる国際協力の推進及び③宇宙の安全保障（スペース・デブリ問題等への対処）の確保がある[81]。宇宙空間の課題に取り組むための国際枠組みとしては，二国間等協力では，例えば日本の場合，日米宇宙協力，日米豪宇宙協力，日 EU 宇宙協力，日仏宇宙協力，ARF 宇宙セキュリティワークショップ等がある。これらの枠組みを通じて，相手国・機関との政策調整や協力を検討し，かつ，透明性の向上や相互理解の促進等信頼醸成を行い，宇宙空間の安全保障の促進に努めている。また，宇宙に関する国際的な規範作りの枠組みとして，COPUOS 法律小委員会等がある。

米国が運用し、爆撃機の安全保障やパトカーの捜査活動等危機管理目的、航空・船舶・鉄道・車両・農機・建機等の交通・運転ナビゲーション目的、スマートフォンのパーソナルナビゲーションや消防車の緊急通報、民間警備会社等の個人ナビゲーション目的、金融取引や機器制御の時刻参照目的、公共・民間・地籍測量目的等のために用いられる全地球測位システム（Global Positioning System、「GPS」）は、国際社会にとって重要性が増している。

2.3.5 サイバー空間：第５の戦場の特殊性

これら四つの領域・範囲に比べて，サイバー空間は唯一，人工的な空間であるゆえの特徴がある。四つの領域との共通点としては，サイバー空間も「領域」としての性格を観念できる点が挙げられる。南極や海洋や宇宙との共通点として，国際公共財（グローバル・コモンズ）という性質があることを主張する者もいる[82]。しかし，サイバー空間における脅威とその対処については，他の空間との相違点が際立っている。まずはその領域性である。領域としての性格を観念できると述べたが，他の４つの領域は，領空と宇宙空間の境目がどこかという点の決着はついていない点，宇宙空間の限界等はあるが，原則として，

[81] 外務省 宇宙に係る外交政策の推進：http://www.mofa.go.jp/mofaj/gaiko/space/pdfs/seisaku.pdf
[82] 日本国際問題研究所　グローバル・コモンズ（サイバー空間，宇宙，北極海）における日米同盟の新しい課題 http://www2.jiia.or.jp/pdf/resarch/H25_Global_Commons/10-Rising_Challenges_for_the_Japan-US_Alliance_in_the_Global_Commons.pdf

その領域が目に見える形で存在しており，それは「観念できる」ものではない。サイバー空間の場合は，情報通信技術を利用したインターネット等の仮想空間であり，それはコンピュータや携帯電話等という媒体を通じてあたかもそこに存在しているかのように「観念できる」人工的な空間である。また，その脅威形態も，陸海空等においては，犯罪組織・テロリスト，通常兵器，化学兵器・生物兵器，核兵器等の大量破壊兵器，宇宙においては，スペース・デブリ，人工衛星や隕石等物理的な脅威であるのに対し，サイバー空間における脅威はマルウェアの送付やインターネットを通じた大量データの送信，不正アクセス等情報通信技術を利用した非物理的なリスクである。さらに，空間の脅威の特性として，攻撃が行われた場合の①効果の即時性（ミサイルや魚雷，核兵器の発射等と異なり，攻撃を実行した場合に極めて高速・瞬時に効果を及ぼすことができる），②攻撃主体等の多様性（艦艇や航空機，核兵器等国家のみが入手・使用可能な装備品とは異なり，サイバー攻撃用のツールさえあれば，インターネット等にアクセスする環境であれば世界中どこから，誰でも攻撃が可能），③匿名性（国家によるミサイル等の発射，テロリストによるテロ行為等と異なり，誰が実行したかについて，技術的に隠蔽・偽装することが容易である），④隠密性（大量破壊兵器の使用等と異なり，マルウェアの埋め込み等被害が露見するまで防御側が攻撃の存在を察知し難いものなどがある），⑤攻撃側の優位性（核兵器やミサイル等と異なり，攻撃手段を入手することが比較的容易であり，ソフトウェアの脆弱性を完全に排除することが困難であること，攻撃側は相互連接するネットワークの最も脆弱なポイントをついて攻撃すればよいこと，攻撃源の特定が困難であること等から，防御側に対して圧倒的な優位にある）及び⑥抑止の困難性（「懲罰的抑止（耐え難い打撃を与える威嚇に基づき，敵のコスト計算に働きかけて攻撃を断念させること）」については，攻撃するおそれのある者に対し，「サイバー攻撃を行えば，同等或いはそれ以上の被害をもたらすような報復を行う」意思を明示したとしても，例えば，その者が非国家主体であり，防御側による報復の対象となることを恐れる資産を保有していない場合には，攻撃を断念させるという抑止効果は働かないと思われる。）。また，「拒否的抑止（特定の攻撃的行動を物理的に阻止する能力に基づき，敵の目標達成可能性に関する計算に働きかけて攻撃を断念させるもの）」については，「サイバー攻撃を行っても効果が得られない」という心証を与える必要があるが，攻撃側の優位性に鑑みれば，サイバー攻撃を完全に思いとどまらせる高いレベルにま

で防御水準を高めることは困難である。））が挙げられる[83]。

[83] ②から⑥は「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」（平成 24 年 9 月）を参照。

3. 国連における GGE の取り組み

本章では，第 1 節で国連サイバーGGE の起源と第 1 回会合から第 5 回会合を概説し，第 2 節で GGE の意義と第 5 回会合の「失敗」の理由について考察する。

3.1. 国連サイバーGGE の発展

3.1.1. 国連サイバーGGE の起源（1998）

国連サイバーGGE は，ロシアが 1998 年に国際連合総会第一委員会に提出した情報セキュリティの問題に関する決議案「国際安全保障の文脈における情報電気通信分野の進展（Developments in the field of information and telecommunications in the context of international security)」を起源とする情報セキュリティの脅威とその国際的な対応策について国連加盟国の専門家グループが議論を行う会合である[84]。上記決議案は，国連総会において，決議 53/70（A/RES/53/70 : 付属資料参照）として投票なしで採択され，以来，毎年情報セキュリティの問題に関する国連加盟国の見解を求める決議が出されている[85]。2001 年の総会決議 56/19 では，2004 年に GGE の会合を設置することを事務総長に要請した。

その後の概要は，下記表 1 のとおりである。

表 3. 国連サイバーGGE の概要

	時期	参加国	成果
1	2004 年～05 年	P 5[86]，ベラルーシ，ブラジル，ドイツ，インド，ヨルダン，韓国，マレーシア，マリ，メキシコ，南アフリカ（計 15 カ国，議長国は露）	合意なし。A/60/202 で会議を行った旨の報告のみ。

[84] ここで「情報セキュリティ」の問題の議論であるにもかかわらず国連「サイバー」GGE と称しているのは，ロシアや中国が考えるセキュリティの問題と日本や米国，西側諸国が前提としているセキュリティとでその対象の認識の相違に由来する。すなわち，GGE の創案者であるロシアや中国が議論の対象としたいのは，情報のコンテンツを含む「情報セキュリティ」であるのに対し，日本や西側諸国がセキュリティの対象とすべきは情報のインフラ（ネットワークやサイバー空間）であり，情報の内容（コンテンツ）ではないという見解の不一致である。この見解の相違があるが，本研究では，便宜上，また，日本や西側諸国が実務上用いる国連サイバーGGE（UN Cyber GGE）という語を使うことにする。

[85] A/RES/54/49, A/RES/55/28, A/RES/56/19, A/RES/57/53, A/RES/58/32, A/RES/59/61, A/RES/60/45, A/RES/61/54, A/RES/62/17, A/RES/63/37, A/RES/64/25, A/RES/65/41, A/RES/66/24, A/RES/67/27, A/RES/68/243, A/RES/69/28, A/RES/70/237, A/RES/71/28

[86] 国連安全保障理事会常任理事国（米国，英国，フランス，中国，ロシア）

2	2009 年～10 年	P５，ベラルーシ，ブラジル，エストニア，ドイツ，インド，イスラエル，イタリア，韓国，カタール，南アフリカ（計 15 カ国，議長国は露）	報告書（A/65/201）。
3	2012 年～13 年	P５，アルゼンチン，豪州，ベラルーシ，カナダ，エジプト，エストニア，ドイツ，インド，インドネシア，日本（計 15 カ国，議長国は豪）	報告書（A/68/98）
4	2014 年～15 年	P５，ベラルーシ，ブラジル，コロンビア，エジプト，エストニア，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，スペイン（計 20 カ国，議長国はブラジル）	報告書（A/70/174）
5	2016 年～17 年	P５，豪州，ボツワナ，ブラジル，カナダ，キューバ，エジプト，エストニア，フィンランド，ドイツ，インド，インドネシア，日本，カザフスタン，ケニア，メキシコ，オランダ，韓国，セネガル，セルビア，スイス（計 25 カ国，議長国はドイツ）	合意なし。

3.1.2. 第１回 GGE 会合（2004－2005）

第１回 GGE の概要は，次のとおりである。

国連総会決議 56/19，57/53 及び 58/32 に基づき，サイバー空間の現在及び潜在的な脅威とそれに対処するための協力的措置を検討するために，衡平な地理的配分に基づき決定された 15 カ国（P５，ベラルーシ，ブラジル，ドイツ，インド，ヨルダン，マレーシア，マリ，メキシコ，韓国，南アフリカ）の専門家グループによる第１回 GGE の第１セッションが 2004 年 7 月 12 日から 16 日までニューヨークの国連本部で，第２セッションが 2005 年 3 月 28 日から 4 月 1 日までスイスのジュネーヴで，第３セッションが同年 7 月 11 日から 22 日までニューヨークで開かれた。議長には，ロシア代表のアンドレイ・クルツキフ氏が任命された。

2005 年に会合の成果として，報告書（A/60/202）が発表されたが，わずかA４用紙４頁でその内１頁目は表紙で題名と目次のみ記載し，最後の２頁は１５カ国の専門家の一覧で，実質はわずか１頁であり，その内容も根拠決議，構成国，会合実施時期及び場所など手続的な事項のみであり，「問題の複雑さのため，最終的な報告書を作成するコンセンサスを得られなかった」と本文の末尾にあるとおり，１５カ国の専門家グループ間で見解の不一致があったため，国家間のサイバーセキュリティに関する認識の相違が浮き彫りになる苦い幕開けとなった。

ロシア，中国，ブラジル及びベラルーシが，国家の無制約の情報セキュリティを確保する権利と新しい国際レジームの導入を推す一方，米国や欧州諸国は軍縮に関するいかなる言及も拒否したとされる[87]。また，安全保障の観点から，国境を越える情報のコンテンツ（内容）を規制すべきという主張に関して特に見解の不一致があったとされる[88]。どの国がそのような主張を行ったかは定かではないが，ティック＝リンガスの記事や実際の運用から中露等が国家による情報内容統制を奨励したと考えるのが自然であろう。また途上国に対するキャパシティビルディング及び技術の移転の提案についても見解の不一致が見られた[89]。

3.1.3. 第２回 GGE 会合（2009－2010）

第２回 GGE の概要は，次のとおりである（報告書の主な内容の和訳は付属資料参照。）。

国連総会決議 60/45，61/54，62/17，63/37 及び 64/25 に基づき決定された１５カ国（Ｐ５，ベラルーシ，ブラジル，エストニア，ドイツ，インド，イスラエル，イタリア，韓国，カタール，南アフリカ）の専門家グループによる第 2 回 GGE 会合は，第 1 セッションを 2009 年 11 月 24 日から 26 日までジュネーヴ，第 2 セッションを 2010 年 1 月 11 日から 15 日までを国連本部，第 3 セッションを 2010 年 6 月 21 日から 25 日までジュネーヴ，第 4 セッションを同年 7 月 12 日から 16 日まで国連本部で開催された。議長は前回同様ロシアのクルツキフ氏が務めた。

成果として，報告書（A/65/201）が 2010 年に発表された。

---

[87] Developments in the Field of Information and Telecommunication in the context of International Security: Work of the UN first Committee 1998-2012www.ict4peace.org/wp-content/.../Eneken-GGE-2012-Brief.pdf
[88] UNODA Fact Sheet Developments in the Field of Information and Telecommunication in the context of International Security: https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf
[89] ibid.

3.1.4. 第３回 GGE 会合（2012－2013）

第 3 回 GGE の概要は次のとおりである（報告書の主な内容の和訳は付属資料参照。）。

第 3 回 GGE 会合（2012 年～2013 年）の開催背景として，2011 年，国連総会は，フォローアップ GGE を要請した決議 66/24 を全会一致で可決した。これにより 2012 年から 2013 年にかけて 3 回，1 週間の会議が行われた。議長国は豪州（デボラ・ストークス）である。

第 3 回 GGE の報告書(A/68/98)は 2013 年 6 月，国連総会に提出された。

専門家グループは，次に掲げる事項に合意した。

- 国際法，とりわけ国連憲章は，サイバー空間に適用され，かつ，オープン，安全，平和的かつアクセシブルな ICT 環境に必要不可欠である。
- 国家主権は，国家の ICT 関連活動及びその領域内の ICT インフラに対する管轄権に及ぶ。
- ICT のセキュリティに対処するための国家の取り組みは，人権及び基本的自由の尊重と同一歩調で行わなければならない。
- 国家は，プロキシを国際違法行為に利用してはならず，また，その領域が非国家主体の ICT の違法行為に利用されないようにしなければならない。
- 国連は，加盟国間の対話の促進において重要な役割を果たすべきである。

3.1. 5. 第４回 GGE 会合（2014－2015）

第 4 回 GGE の概要は，次のとおりである（報告書の主な内容の和訳は添付資料８．４参照。）。

2013 年 12 月 27 日，国連総会は，第 3 回 GGE（2012 年～2013 年）の成果に留意し，事務総長に 2015 年に国連総会で報告する新たな GGE を設置することを要請する決議 68/243 を全会一致で可決した。

2014 年 7 月から 2015 年 6 月まで 20 カ国（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，ロシア，スペイン，英国及び米国。議長国はブラジル）の専門家が，4 回の会議を開催した。

専門家グループは，2015 年 6 月，全ての国家に広く適用可能なサイバー空間における国家の責任ある行動に関する規範，規則及び原則や 信頼醸成措置，国際協力及びキャパシティビルディングの実質的なコンセンサスレポート（A/70/174）に合意した。報告書は，国際法が如何に ICT の利用行為に適用されるかについても取り組み，また，今後の作業についての提言も行った。

このような成果から，第 4 回 GGE 会合は，これまでの GGE のうちで最も充実した内容が提言されたといえるであろう。合意した主な事項は次のとおりである。

- 国家は，ICT の利用の際に，国家主権，平和的手段による紛争解決，他国の内政不干渉その他の国際法の原則を遵守しなければならない。
- 既存の国際法上の義務は，国家の ICT の利用に適用され，国家は，人権及び基本的自由を尊重し，保護する義務を遵守しなければならない。
- 国家は，ICT を用い国際違法行為を行うためにプロキシを利用してはならず，また，その領域が，非国家主体によって右行為が行われないように努めなければならない。
- 国連は，国家の ICT の利用におけるそのセキュリティに関する対話の促進及び国際法の適用並びに責任ある国家の行動に関する規範，規則及び原則についての共通認識の醸成において主導的役割を果たすべきである。

3.1.6. 第５回 GGE 会合（2016－2017）

第５回 GGE の概要は，次のとおりである。

第５回 GGE は，国連総会決議 70/237[91]に基づき設置された。議長はドイツのカルステン・ガイアーが務めた。会合は４回開催され（第１回：2016 年 8 月 29 日から 9 月 2 日（於国連本部），第 2 回：2016 年 11 月 28 日から 12 月 2 日（於ジュネーヴ），第 3 回：2017 年 2 月 20 日から 24 日（於ジュネーヴ），第 4 回：2017 年 6 月 19 日から 23 日（於国連本部）），これまでの GGE で最多の 25 ヵ国が参加した。

そのマンデートに従い，前回の GGE から引き続き，現在及び潜在的脅威，キャパシティビルディング，信頼醸成措置，責任ある国家の行動規範，規則及び原則，情報通信技術の利用に係る国際法の適用について幅広い議論が行われ，前回の勧告よりさらに具体的な内容に合意することが期待されたが，西側諸国の主張によれば，サイバーオペレーションに関する国際法の適用，とりわけ対抗措置及び自衛権の行使について，ロシア，中国及び

キューバが反対したことなどもあり合意に達せず，報告書も纏められずに終結した[92]。

本会合において 25 か国のコンセンサスを得ることができなかった理由は，サイバー GGE の事務局的役割を担う UNODA（国連軍縮部）においては触れられておらず，国連の公式な発表はないが，全５回の GGE 会合で全て米国政府代表を務めたミシェル・マーコフ国務省サイバー問題副調整官は，2017 年 6 月，GGE の終結を受けて，次のような見解を述べている。

「2016-2017 年 GGE を通じて，国際人道法，国家固有の自衛権を規律する国際法及び国家責任法を含む個別具体的な国際法が国家の ICT を利用する行為にいかに適用するかについて明確かつ直接的なステートメントを追求してきた。私は，国際平和及び安全のために，国際法の枠組みが，国家に対し，国家が直面するサイバーインシデントに対しいかに対処し，又は対処し得ないのかという点について安定した見通しを立てることにより紛争のリスクの低減の一助となり得る行動の拘束力ある基準を提供するという強い確信に基づき，そのようなステートメントを追求した。報告書最終案はこれらの問題について十分に対処していない。本 GGE が，国家の ICT の利用へのこれらの個別の国際法の適用に関する明確な立場を取らず，ましてや ICT の利用に国際法のルール及び原則がいかに適用されるかについて研究するという国連総会から本グループが受けたマンデートを履行できない報告書を提出することは，問題を抱え，かつ，不安定化を示す虞があると考える。

長年にわたる議論と研究にもかかわらず，複数の参加国(some participants)は，そのような決断を下すのは時期尚早と頑なに主張し続け，それどころか，むしろこれまでの GGE 報告書でなされた前進から後退することを欲しているようにも思えた。これらの国際法のルール及び原則の適用を是認しようとしない国々は，その政治的目的を達成するために，何の制限も制約もなくサイバー空間において又は右空間を通じて自由に行動することができると考えているという残念な結論に達した。これは，危険で支持できない見解であり，私はこれを全面的に否定する。

私は，本 GGE において，複数の参加国が，ユス・アド・ベルム（開戦法規），国際人道法及び国家責任法等の国際法の体系の議論は，紛争の平和的解決及び紛争の予防に関して本グループが発すべきメッセージと相容れないということを繰り返し主張していたのを聞いた。これは，吟味に耐え難い誤った二分法である。紛争の平和的解決とそれに関連する概念を論ずるが，国家が直面する悪意あるサイバー活動への国家が選択し得る合法的な手段についての議論を除く報告書は，国家がその活動の不安定化を抑止することができなく

なる虞があるのみならず，国際社会に向けて，そのような悪意あるサイバー活動への国家の対処が国際法によって制約されているという安定化のためのメッセージを伝えることをもできなくなってしまう。

私は本 GGE を楽観的に取り組み始め，交渉の大部分の生産的かつ真摯な内容に勇気づけられた。少数の参加国が国際法の問題のマンデートについて真摯に取り組もうとせず，本 GGE がこれらの重要な課題についての国連加盟国間の共通理解の目標を推し進めることができた報告書のコンセンサスを得ることを妨げてしまったことは不運である。これは，本グループが本セッションにおいて，サイバー空間における責任ある国家の行動に関する自発的な非拘束的規範及び信頼醸成措置を含む安定化措置の実施についての共通理解に達するために行った作業を考えると，特に不本意である。議長の素晴らしい努力にもかかわらず，我々の作業は無駄になってしまった。国際平和と安全にとって非常に重要なこれらの取り組みを他の方々と引き続き行うことを期待している。全ての GGE 参加国に，今後，本件を真摯に受け止め，国際法（の適用）を重点的に取り組むことを求める。[93]」

米国が，報告書をまとめることができなかった失望感を表し，特定の参加国によって合意に達することができなかったことを厳しく批判する内容になっている。批判の対象となった「参加国」が具体的にどの国かは明らかにしていないが，NATO CCDCOE では，前述のとおり，ロシア，中国及びキューバが国際法の適用の議論を拒否したとある[94]。なお，信頼醸成措置についてはコンセンサスを得られたとも捉えられる記述があるが，キャパシティビルディングについては特に触れられていない。

3.2 国連サイバーGGE の意義と失敗

かくして 2016 年から 2017 年にかけて行われた第 5 回国連サイバーGGE は，これまでの会合で最も多い 25 カ国が参加し，第 4 回会合で合意された報告書の勧告をさらに具体化し，国際法の適用や国家の行動規範，信頼醸成措置，キャパシティビルディング等を含めたサイバー空間の脅威に対する国際協調策を提言することが期待されたが，各国のコンセンサスを得ることができず，報告書を纏めずに幕を閉じた。欧州のシンクタンクである

[93] Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security：https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm（最終アクセス日：2017 年 12 月 18 日）
[94] Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly：https://ccdcoe.org/back-square-one-fifth-un-GGE-fails-submit-conclusive-report-un-general-assembly.html（最終アクセス日：2017 年 12 月 18 日）

欧州外交評議会（European Council on Foreign Relations，以下「ECFR」という。）は，「国連 GGE は終わった（The UN GGE is dead）。前に進む時が来た。」と表現した[96]。また，ECFR は「ルールは拘束力を持ち，違法行為は罰せられ，言葉は何らかの意味をもたなければならない。しかし，国連 GGE はこの三つ全てに失敗した。」と酷評した[97]。そして，国連 GGE は今回で最後になるだろうと予想した上で，今後の展開としては，諜報活動や情報収集活動等の法的に「グレー」な領域に関してのみ新たな国際法を制定するのも一案であるが，この問題は国家の安全保障や防衛に関する問題と同様異論が多いため，新たな法を制定するための合意形成は困難との見解を示した。さらに，グローバルな規範に関する議論を進めるのは重要であり，その内容は別にして，中露等 SCO 加盟国が 2015 年に改正版を策定し公開した「情報セキュリティ国際行動規範（案）」のような，オープンな意見交換と議論の新しい思考を受け入れるべきとした。また，GGE 崩壊後に進むべき方向として，「（GGE とは異なる）他のアプローチを考える時が来た。我々と敵対する者の悪い行動を非難し，コストを強いらせるため，同じ志を持った国の少数のグループと協力していくだろう。また，必要に応じて，二国間協定も追求するだろう」という米国国土安全保障省顧問のトム・ボッサートが GGE 会合後に述べたことを引用している[98]。

国連サイバーGGE は，国連という最も注目される外交の場においてサイバーセキュリティのグローバルな問題を取り上げ，国際社会におけるサイバーセキュリティに対する意識を高め，サイバー空間における国家の行為への国際法の適用を初めて認めた点（A/68/98 第 19 段落。）において極めて重要な意義がある。GGE の議題として取り上げられた国際的なルール作り，信頼醸成措置の推進，そしてキャパシティビルディングは，現在の日本のサイバー外交政策の三本柱となっていることから，GGE は日本がサイバー外交上最も重視していた国際枠組みと言っても過言ではないだろう。GGE に参加した国とそうでない国との間では，サイバーセキュリティの国際的な問題に関する意識と知見が異なり，GGE 参加国が自国の政府関係者，民間企業，研究者や技術コミュニティ等と情報共有し，他の様々な国際会議において，議論をリードしてきた。G7 においても，GGE の取組みを評価する旨の声明が出されていた[99]。まさに GGE は，サイバー外交の最前線であった。1

[96] ECFR: The UN GGE is dead: Time to fall forward (http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance)（最終アクセス日：2017 年 12 月 18 日）
[97] ibid.
[98] ibid.
[99] G7 Principles and Actions on Cyber (www.mofa.go.jp/files/000160279.pdf（最終アクセス日：2017 年 12 月 18 日）

５カ国で始まった会合は，第５回では２５カ国に拡大され，Ａ４用紙２頁足らずの抽象的な指針を示した報告書は１５頁の具体的な提言書となっていった。しかし，その GGE が「失敗した（failed）」あるいは「終わった・死んだ（dead）」のである。では，本当に，サイバーGGE は「失敗」したのか，そして，GGE の会合は開催されず，まさに制度的に「終わった」過去の産物となるであろうか。この点について，本研究の主たるテーマであるキャパシティビルディングが GGE で取り上げられ，国際社会レベルにおいての認知度が飛躍的に向上したことを鑑み，ここで若干の考察を加えることにする。

まず，国連は「失敗」したか否かについては，第２回から第４回会合まで，メンバー国間で様々な意見の対立があった中で，全参加国が同意できる最低ラインの内容を妥協するまで交渉し続け，コンセンサスを得て，漸進的に議論が進められ，報告書をまとめてきたことからすれば，第５回会合でそれが叶わず，国際社会に対して何の議論の成果物も提供することができなかったのは紛れもない「失敗」であったと評価せざるを得ない。特に米国にとっては，サイバー空間を利用した国家の行為に対する対抗措置や自衛権の行使を認容する旨の文言を入れた報告書を取り纏め，国連総会に提出することにより，米国が思い描くサイバー空間の国家の行動の規範について国際世論を味方につけることができなかったのは大きな「失敗」であっただろう。これに対し，対抗措置や国家責任，自衛権（それに関連するサイバー攻撃の「武力攻撃」や「武力行使」該当性の閾値の議論等），国際人道法等の従来の国際法の個別具体的な適用に消極的な姿勢を示してきた中露等からすれば，その適用に係る文言を盛り込もうとしていた報告書の合意形成を阻止したことにより，一定の「成功」を収めたという感触を抱いているとも考えられる。サイバー空間における法の支配を推進し，「サイバーに関する G7 の原則と行動」において，「我々は，一定の場合には，サイバー活動が国際連合憲章及び国際慣習法にいう武力の行使又は武力攻撃となり得ることを確認する。また，我々は，サイバー空間を通じた武力攻撃に対し，国家が，国際人道法を含む国際法に従い，国際連合憲章第５１条において認められている個別的又は集団的自衛の固有の権利を行使し得ることを認識する」[100]ことを確認した立場からすると，日本を含む G7 諸国から見ても，今回の GGE のコンセンサスレポートなしという結果は「失敗」と評価されるだろう。しかし，第 5 回 GGE 会合の合意形成が成就できなかったという点においては，「失敗」であったとしても，前述のとおり，GGE をロシアの提案で

[100]サイバーに関するＧ７の原則と行動 （www.mofa.go.jp/mofaj/files/000160315.pdf）（最終アクセス日：2017 年 12 月 18 日）

設置し，10 年以上にわたりサイバーセキュリティの問題を国連全加盟国が参加する国連総会の場で取り上げ，議論をした過程は決して無駄ではなく，サイバーの安全保障上の問題に関する各国の立場や方針が徐々に明らかになり，サイバー空間の在り方に関するイデオロギーの相違から協力できることと，それが困難な点を特定し始めたという点からすればそれは「成功」と言えよう。むろん，従来の国際法の適用や新たな国際規範の策定等を含むサイバー空間に関する国際的なルール作り，信頼醸成措置，キャパシティビルディングというサイバーセキュリティに係る外交上の問題が何であるかということを洗い出した点も「成功」であった。

次に，第 5 回会合においてコンセンサスを得られなかった GGE は「死んだ」あるいは「終わった」会議体となったのであろうか。現在のところ，次回の GGE 会合の開催は決まっていない。インドとスイスは，1959 年に宇宙空間の問題に関する国際協調の場として設置された国連宇宙空間平和利用委員会（Committee on the Peaceful Uses of Outer Space，以下「COPUOS」という。）のサイバー版の委員会を国連総会に新設することを提案した。他方，ブラジルは，意図的に IT サプライチェーンに脆弱性を組み込み，他国の情報セキュリティを損なうサイバーオペレーションの先制攻撃を禁止する新たな法制度の策定を提案した。また，その他複数の国は，GGE の参加国を大幅に増やしたオープンエンドの国連総会のワーキンググループを提案した[101]。しかし，米国のシンクタンク外交問題評議会（Council on Foreign Relations，以下「CFR」という。）のアダム・シーガル（Adam Segal）が CFR のホームページで指摘しているとおり，これらの選択肢を採るのは困難である[102]。国連総会のオープンエンドなワーキンググループは，各国の自由な発言により，これまで選定してきたサイバーセキュリティの重要な問題から議論が逸脱し，収束がつかなくなる虞がある。COPUOS は，その成果として宇宙に関する 4 つの条約を制定したが，これは米国が長年反対してきたものであり，これと同様な枠組みの設置は米国が参加しないとシーガルは予想する。また，ブラジルの新たな法枠組みの策定について，中露等 SCO 諸国が「情報セキュリティに関する国際行動規範（案）」の共同提案国を模索しているところであるが，これを米国等欧米諸国が支持するのは極めて困難である。これに対して米国は，国連や多国間会議システムでの議論を中止し，自国が思い描く規範の合意形成を促すため，小規模の同志国との「有志連合（Coalition of the Willing）」を推進する動きがある

[101] Council on Foreign Relations: The Year in Review: The Death of the UN GGE Process? (https://www.cfr.org/blog/year-review-death-un-gge-process)（最終アクセス日：2017 年 12 月 18 日）
[102] ibid.

とされる[103]。しかし，仮に米国を中心とする有志連合によってサイバー空間の国際規範を構築したとして，その枠組みの中に中露等が入っていなければ，どれだけ実効性が担保されるかは疑問である。

GGE 再開の目途は立っていないが，これは必ずしも GGE が「死んだ」ことを意味していない。GGE の議論の中心である米国とロシアが水面下で再開の交渉を始めている可能性はゼロではなく，両国の政権が変われば，サイバーに対する考え方に変化が生まれる可能性もある。GGE は，「終わった」のではなく，一時的な「休止」あるいは「停止」状態にあるという表現の方が正確であろう。ただ，GGE の再開を待つだけでは現在のサイバーセキュリティの問題に対処できないため，GGE 再開を検討しつつ，米露日等が参加する ASEAN 地域フォーラム（ASEAN Regional Forum，以下「ARF」という。）等の別の既存の国際枠組みにおいて，信頼醸成措置やキャパシティビルディング等の規範以外の分野について議論を進める可能性は高いと思われる。

第 5 回 GGE 後の国際社会は，サイバー空間を利用した行為に対する国際法の適用や国際規範の策定の議論については，激しい鍔迫り合いを展開し，平行線を辿る米国と「有志連合」対中露等という構図から，米国と「有志連合」が例えば NATO の CCDCoE の専門家が策定した「サイバーオペレーションに適用可能な国際法に関するタリン・マニュアル 2.0」等を基礎に認識を合わせ，これを支持する国を増やすために各国にアプローチし，他方，中露等は「情報セキュリティに関する国際行動規範（案）」を支持する勢力圏を拡大するために，各国に働きかけることが予想される。信頼醸成措置については，多国間外交としては，これまでサイバーの分野も含めて信頼醸成を推進してきた ARF の他，欧州安全保障協力機構（Organization for Security and Co-operation in Europe，以下「OSCE」という。）が引き続き主導的な役割を果たすことが展開される。

また，サイバー版のホットラインを 2013 年に設置した例がある米露[104]の他，米中，日露，日中，欧露対話といった潜在的にサイバー攻撃を行っている可能性がある二当事者間外交も積極的に進められるだろう。

キャパシティビルディングについては，ARF などの枠組みで一部議論されるであろうが，GFCE や従来開発援助を行ってきた国連等の国際機関や二国間援助の当事者である国

---

[103] ibid.
[104] The White House: FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security (https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol)（最終アクセス日：2017 年 12 月 18 日）

家，草の根の援助を行う非政府組織（Non-Governmental Organization，以下「NGO」という。）がサイバー分野の開発にも着手し始めており，さらにはサイバーセキュリティ関連の民間企業が，ビジネスの観点も含め GFCE の枠組み等に参画してきている。

1998 年にロシアが提案して始まり，2017 年の第 5 回会合の「失敗」に終わり，ひとまず「停止」状態になった GGE が残した功績，すなわち GGE 参加国が議論を重ね洗い出したサイバー外交上の課題である国際法の適用・国際規範の検討，信頼醸成の促進，キャパシティビルディングを，別の国際枠組みで推進し，対話を続け，妥協点を見出し，信頼を高めることにより紛争を予防し，支援を要する国を支援し，国際社会の平和と安定の維持に貢献することがポスト GGE における国際社会のサイバー外交に携わる者の使命であると言えよう。

では，次章では，このキャパシティビルディングの観念の誕生から現在までの変遷を開発援助の歴史とともに概観し，伝統的なキャパシティビルディングとサイバーセキュリティ分野におけるキャパシティビルディングとの相違点を比較した上で，各主体が取り組んでいるサイバーセキュリティのキャパシティビルディングを概説する。

4. 各国のキャパシティビルディングの取り組み

4.1. キャパシティビルディング概念誕生までの変遷

キャパシティビルディングは開発協力あるいは開発援助という国家の行為が始まった後にできた行為あるいはプロセスであり，その歴史を理解するには，開発協力の歴史を理解する必要がある。

その動機は,「人道上の動機，外交戦略上の動機，商業的な利害にもとづく動機などの複数の動機が複雑に絡み合っている場合」[107]もある。

1950 年から 1960 年代にかけては, 開発分野において, 制度構築（institution building）の取り組みが重視された。その目標は，途上国に公共投資計画の管理に要する公共部門の基礎的制度を備えさせることにあり，個々の組織の設計とそれが機能することに焦点を当て，より広範な環境又は各セクターに着目していなかった。また，その多くは，途上国から輸入・移植された制度構築モデルを用いて行われた。

1960 年から 1970 年代に入ると，制度構築から制度強化・開発（institutional strengthening/development）への変遷があったが，まだ大局的な見地から開発するというより個々の制度の強化・開発に軸が置かれた。

しかし，1970 年代には，開発管理（development management/administration）という手法が考案され，その目標は，それまで国家から無視されてきた特定の人々や集団に手を差し伸べることにあった。この手法における焦点は，公的な計画や政府の能力が開発の対象となる集団に行き届くための供給システムの構築にあった。

1970 年から 1980 年代にかけて，人材育成（開発）（human resource development）が重視された。「開発とは，ヒトである」という，制度ではなく人中心の開発の発現した時期であり，人の教育，保健，人口問題の重要性を強調した[108]。

次に，1980 年から 1990 年代にかけて，制度派経済学の分野を通じて 1970 年代に出現した新制度主義（new institutionalism）を重視し，開発の焦点をネットワークや外部環境を含むセクターレベル（政府，NGO，民間企業等）へ拡大し，国家の経済活動の形成に着目した。この時期に持続可能性の問題が提起され，プロジェクト集中型の開発からの脱却

---

[107] 大平剛著『国連開発援助の変容と国際政治』（有信堂，2008 年）はしがき，i 頁。

[108] インドの経済学者アマルティア・セン（Amartya Sen。1998 年ノーベル経済学賞受賞。）が提唱した capability approach において人間開発の重要性を強調。センの思想は，1966 年に国連特別基金と国連拡大技術援助計画が統合して発足した国連開発計画（United Nationsl Development Programme，以下「UNDP」という。）が毎年刊行する『人間開発報告書』を通じて広く認知されるようになった。

が図られた。

そして，1980 年代後半から 1990 年代後半にかけて，能力開発（capacity development）が様々な開発のアプローチの集合体として出現した。能力開発においては，技術協力の概念が再評価され，自助努力（ownership）及びプロセスの重要性が強調された。能力開発は，開発手法の「主流」となり，現在まで継続して発展している開発のアプローチである。ここで，キャパシティビルディングではなくキャパシティディベロップメントという用語が用いられているが，この点両者の間にどのような相違点があるのかを簡潔に説明しておく。

4.2. キャパシティビルディングとは

キャパシティビルディングという用語の最広義は，その名のとおり，何らかの主体による何らかの客体の特定の「能力」の「構築」である。この意味で用いられるキャパシティビルディングは，例えば，民間企業による非営利組織のマーケティング力の向上のためのワークショップや経営陣に対する研修等などがある。能力を構築する側の主体も能力の構築を受ける側の客体も制限なく，特定の能力を有する主体がその能力を欠く，又は，その能力が乏しい客体に対して，能力の構築を支援する活動を指す。

古澤嘉朗は,「なんらかの課題に対処する実施主体（個人・組織）の能力向上を図ること」

外務省による経済協力の文脈におけるキャパシティビルディングの定義は,「途上国の能力構築」と，客体を限定的に解する[109]。この意味におけるキャパシティビルディングの例として，特定の主体が途上国に対し，特定の協定についてのセミナーの開催，産業育成・中小企業人材育成としての研修員の受入れや専門家の派遣等の技術支援を行うことによって，途上国が特定の交渉に参加できる能力をつけていくことが挙げられている。

防衛省は，安全保障・防衛関連分野の文脈において，キャパシティビルディングを「能力構築支援」と訳したうえで,「自国が有する能力を活用し，他国の能力の構築を支援すること」[110]と定義している。

そのうえで，その対象を，他国の軍又は軍関係機関，分野であって，人道支援・災害救援，地雷・不発弾処理，防衛医学，海上安全保障，国連平和維持活動等，形態を，自衛官等を一定期間派遣しての教育訓練，自衛官を派遣しての短期間のセミナー，防衛省・自衛

[109] 外務省　用語解説：http://www.mofa.go.jp/mofaj/gaiko/wto/yogo.html（最終アクセス日：2017 年 12 月 18 日）
[110] 防衛省　能力構築支援事業（http://www.mod.go.jp/j/approach/exchange/cap_build/about/）（最終アクセス日：2017 年 12 月 18 日）

隊関連部隊・機関等への研修員の受入れ等とする。またその意義・目的を，①支援対象国が自ら国際安全保障環境の安定化・改善に貢献すること，②支援対象国との関係強化，③米国や豪州をはじめとする他の支援国との関係強化及び④国際社会における我が国の信頼性の向上の４点を通じて，国際安全保障環境の安定化・改善を図り，ひいては我が国の安全の確保を図ること並びに自衛隊の能力の向上を図ること，としている[111]。防衛省では，２０１１年に防衛政策局国際政策課に「能力構築支援室」を新設し，同年，東ティモール，カンボジア，ベトナム，インドネシア，パプアニューギニア，トンガ及びモンゴルに対し現地調査や支援ニーズの把握や分析を行い，翌年以降毎年前述の分野に関し，前述の形態により，支援を継続的に実施している。支援対象国は，前述の７か国に加え，ミャンマー，フィリピン，ラオス，マレーシア，タイ，カザフスタンも加え，拡大している[112]。

なお，防衛省が行う能力構築支援は，あくまで各国の防衛当局からの支援要請に基づいて実施しているものであり，我が国の信頼性の向上や我が国の安全の確保を重視して，我が国のイニシアティブによって強制的に支援を行うような性質のものではないことに留意すべきである。これは，従来の我が国のＯＤＡ供与の原則としても見られた「要請主義」と類似している。すなわち，途上国の自助努力という概念から基礎づけられたもので，開発途上国側から要請があった案件についてのみ，審査して援助を行うという手法を採用するものである。

ＯＤＡに関しては，１９９７年以降は「要請主義」から援助国側も自らの援助方針を示し，開発途上国政府と共同して援助計画と適切な案件を探る「共同形成主義」へ方針を変えており，プロジェクト形成促進調査や開発調査を要請前に行うことがこの現れとして位置付けられている。この点，防衛省がニーズの調査等を要請前あるいは要請後に行っているかは定かではない。しかし，ＯＤＡの供与も要請主義の下でうまく機能しなかった点を踏まえると，支援対象国の自助努力を尊重しつつ，我が国の援助方針を示し，適切な案件の形成を図る共同形成主義的側面も能力構築支援事業には少なからずあると考えられる。いずれにしても，前述のとおり，援助供与側による一方的な援助の押付けではない点は変わらず，援助対象国の自助努力を重視するのは安全保障・防衛関連分野におけるキャパシティビルディングも同様である。

宇宙分野におけるキャパシティビルディングは，「開発途上国の能力構築」として，その

111 ibid
112 防衛省・自衛隊：能力構築支援事業とは.
http://www.mod.go.jp/j/approach/exchange/cap_build/about/index.html（最終アクセス日：2017 年 12 月 18 日）

形態は，ハード面の支援（衛星機材，インフラ等の整備），ソフト面の支援（インフラ整備のための人材育成・知見の提供），衛星を利用した技術協力（地球観測データ提供等），その意義は，①宇宙空間における法の支配の強化，海洋状況把握の強化等を通じた我が国の安全保障環境の向上，②衛星を活用した気候変動対策（森林保護等），防災，食糧安全保障等の国際的な開発課題の解決及び③科学技術協力の強化，我が国の先端技術の利活用促進を通じた各国との連携・商業宇宙市場の開拓にあるとする[113]。宇宙分野においては，これまでＯＤＡを活用して，ＡＳＥＡＮ諸国，ブラジル，アルゼンチン及びブルキナファソ等に支援を実施している。

政府開発援助（Official Development Assistance: ODA）は先進国の政府機関やその実施機関が開発途上国に向けて行う援助のことである。先進国政府の途上国援助のうち，政府開発援助として認められるのは，①公的部門（政府機関ないしその実施機関）から開発途上国あるいは国際機関に供与されるもの，②援助条件の指標であるグラント・エレメント（GE）が一定の水準（25%）を超えているもの，③開発途上国の経済開発若しくは福祉の向上に資するもの，という 3 つの条件を満たすものに限られる。GE 要件が 25%未満のものは，その他政府資金フロー（OOF）と呼ばれる。政府開発援助のうち開発途上国に直接供与されるもの（2 国間援助）は援助条件によって，贈与（無償資金協力ないし技術協力）と借款（有償資金協力）に分類される。日本では従来，無償資金協力の実施は外務省，技術協力は国際協力事業団，有償資金協力（円借款）は国際協力銀行（前身は海外経済協力基金）と役割分担してきたが，ODA 政策見直しの観点から，2008 年に国際協力銀行の海外経済協力業務は国際協力機構（JICA）に統合され，外務省の無償資金協力も一部を除き JICA に移管された。現在は JICA がほぼ一元的に政府開発援助を扱っている。2015 年には，従来の「政府開発援助（ODA）大綱」に代えて「開発協力大綱」が定められた。

無償協力（grant aid）は政府開発援助（ODA）のうち，被援助国に返済義務を課さない資金協力。医療や公衆衛生，初等教育などベーシック・ヒューマン・ニーズの改善に資する事業に対して行われる。具体的には，病院・学校の建設や医療などの関連設備の購入のための資金協力の贈与，災害時の緊急支援，紛争終結国への経済社会基盤支援などがある。開発途上国の中でも，特に所得水準の低い国を援助の対象としている。欧米諸国の ODA が無償資金協力を中心とするのに対して，日本は伝統的に被援助国の自助努力を促すため，

[113] 外務省 総合外交政策局宇宙室 国際協力局政策課「宇宙分野における開発途上国に対する能力構築支援」: www8.cao.go.jp/space/comittee/dai55/siryou4.pdf（最終アクセス日：2017 年 12 月 18 日）

有償資金協力（円借款）による援助の割合が高くなっている。

有償協力（loan aid）は政府開発援助（ODA）のうち，被援助国に対して低金利かつ返済期間の長い緩やかな条件で開発資金を貸し付ける資金協力のこと。有償資金協力では，被援助国の経済政策や経済構造に応じて，「プロジェクト型借款」と「ノン・プロジェクト型借款」という 2 つのタイプの資金協力が行われる。前者には，社会経済インフラの整備のための借款（プロジェクト借款）やプロジェクト実施に先立つ先行調査のための借款（エンジニアリング・サービス借款）が含まれる。校舎は，政策改善・制度改革を目指す開発途上国への開発政策借款や外貨準備難に直面した途上国に対して緊急に輸入決済資金を供与する商品借款，商品借款と同時に特定セクターの政策・制度改善を図るセクター・プログラム借款などに分けられる。開発政策借款では，各国間での援助協調や世界銀行との共同援助など，援助側で政策調整が行われることが多い。日本が行う有償資金協力は円建てで行われることから「円借款」と呼称されている。

円借款は日本政府が行う有償資金協力のことである。日本は有償資金協力での貸付を円建てで行っているため「円借款」と呼称される。被援助国には返済義務が課せられるが，その条件は，平均金利 0.31%，平均償還期間 35.4 年，平均据置期間 9.4 年，グラント・エレメント（GE）82.12%（2015 年度実績）と緩やかなものとなっている。欧米諸国の ODA は無償資金協力の割合が高いのに対して，日本は開発途上国のオーナーシップを促すためとして，返済義務のある円借款による援助を重視している。円借款は①大型の経済社会インフラ整備のための「プロジェクト型借款」と，②「ノン・プロジェクト型借款」（経済政策改善などのための開発政策借款や途上国の経済安定支援のために供与される商品借款など）に大別される。これまでの円借款の主たる対象であった東アジア・東南アジア諸国では，プロジェクト借款によってインフラ整備が進み，その後の経済発展に寄与した。また，近年では「持続可能な開発目標（SDGs）」の実現に向け，貧困削減などの分野への支援も行われている。従来，円借款業務は国際協力銀行（前身は海外経済協力基金）が行ってきたが，08 年からは同行の国際協力部門を統合した国際協力機構（JICA）が ODA 政策を一元的に担っている。

2015 年 2 月，日本政府は ODA 開始 60 周年を契機に，従来の「政府開発援助（ODA）大綱」を改定し，新たに「開発協力大綱」を決定した。「ODA」から「開発協力」と名称を変更したことに示されるように，新しい大綱は貧困対策など途上国への資金面での援助だけではなく，より幅広い国際協力活動を対象としており，開発協力政策を日本の外交資源

としてより戦略的に展開していく方針が明確化された。特筆すべきは，国際社会の平和・安定・繁栄への積極的な貢献を通じて，日本の「国益の確保」に資することを開発協力の目的に明記している点である。また，非軍事的協力による貢献や人間の安全保障の推進等が掲げられていることに加えて，軍事的用途や国際紛争助長への使用を回避するとの原則の下，災害救助や人道支援など他国の軍が関与する非軍事分野の開発協力に対する支援も可能となった。2013 年の「国家安全保障戦略」が掲げた積極的平和主義の立場を踏まえ，開発の基盤として，法の支配や基本的人権，民主化，平和構築，テロ対策といった普遍的価値の共有が示されているのも特徴である。

4.3. サイバーセキュリティ分野におけるキャパシティビルディング

２００７年１１月，リオデジャネイロで行われた国連の管轄下にある IGF（インターネットガバナンスフォーラム）の第２回会合において，「情報セキュリティのキャパシティビルディングに関する国際協力」と呼ばれるワークショップが開かれた。

このセキュリティワークショップのモデレーターを務めたのは，JPCERT/CC の伊藤友里恵氏であり，このパネルを共同提案したのは ISOC（インターネットソサエティ）と日本の経団連であった。ブラジル，ベトナム，ガーナのパネリストから開発途上国における情報セキュリティ対策の課題について見解が述べられ，これに対して，日米のパネリストも交え，国際社会がどう協力し，支援していくことが必要なのかについて意見交換が行われた。

その結果，国際的なサイバーインシデント対処におけるコーディネーションポイントの構築，その運用のためのリソースやツール，ベストプラクティスの共有等の支援のみならず，そのための基盤になる法制度等の政策から，民間企業におけるセキュリティ対策のインセンティブ付与，エンドユーザーへの啓発活動までの，多層的なノウハウの共有が必須との指摘がなされた[114]。これが，サイバーセキュリティ分野のキャパシティビルディングの必要性に言及した国際的な議論の起源と考えられる。

その後，2010 年の国連総会第一委員会のサイバーGGE（国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家会合）報告書（A/65/201）においても，サイバーセキュリティ分野におけるキャパシティビルディングの必要性が共有された。2012 年

[114] JPCERT/CC 活動概要［2007 年 10 月 1 日 ～ 2007 年 12 月 31 日］.
https://www.jpcert.or.jp/pr/2008/pr080001.pdf

にはサイバー空間に関するブダペスト会議において，GCSCC（グローバルサイバーセキュリティキャパシティセンター）を自国に設置することを当時の英国外相のウィリアム・ヘイグが国際社会にアピールし，英国がサイバーセキュリティ分野におけるキャパシティビルディングに関してリーダーシップを取ろうとする動きがあった。

4.4. サイバーセキュリティ分野における国際社会のキャパシティビルディングの取り組み

4.4.1. 米国の取り組み

米国の取り組みの特色は，サイバー空間の国際的なルール作りや CBM 等である。

米国国務省は，アフリカ連合委員会(AUC)及び西アフリカ諸国経済共同体(ECOWAS)とともに，アンゴラ，ブラジル，カーボヴェルデ，ガーナ，ケニア，モーリシャス，モザンビーク，ナイジェリア，ポルトガル及びサントメ・プリンシペの政府職員に対し，サイバー犯罪対策，携帯電話のセキュリティ，インターネットの自由，アクセス及びアフォーダビリティ並びに国家 CERT の構築等アフリカのポルトガル語圏の特定の利益に係る問題を中心にサイバー犯罪及びサイバーセキュリティの広範な問題の対処支援を目的とするサイバーセキュリティ及びサイバー犯罪対策ワークショップを 2015 年 9 月に実施した。

このほか，米アフリカ軍司令部(AFRICOM)がジョージ・メイソン大学国際サイバーセンター，フォート・レズリー・J・マクネアの米国防大学アフリカ戦略研究センター D.C.並びに国土安全保障省，国防省及び国務省等の連邦機関と連携して，アフリカ 9 カ国の武官 10 名に対し，2015 年 7 月，サイバーセキュリティ研修を実施した。

また，官民合同で 2001 年に設立された全米サイバーセキュリティ連盟(NCSA)は，「STOP. THINK. CONNECT」キャンペーン，全米サイバーセキュリティ意識啓発月間(NCSAM)など CS の意識啓発活動を行っている。

4.4.2. 英国の取り組み

英国は，１７世紀初頭以降の大航海時代以降から伝統的に国際政治上のグローバルアクターであり，かつて植民地化し，現在英連邦を構成する国々を中心にサイバーセキュリティの CB を積極的に推進する政策をとっている。

英国では，オックスフォード大学の GCSCC が，国家のサイバーセキュリティ能力成熟度モデル（CMM）を開発し（２０１７年２月に改定版を公表），各国にそのモデルを活用

し，サイバーセキュリティ能力の評価を行い，改善すべき能力を特定するのに役立つよう奨励している。ノルウェーがこれを支持し，世界的に普及されるよう促しているほか，ＯＡＳも価値のあるものと認めて，連携することを表明している。

前述のとおり JPCERT/CC は 2007 年以降 CSIRT 構築運用支援を行っており，CERT コミュニティを中心に早い段階で実質的にキャパシティビルディングと言える活動は行われてきたが，それはまだ技術実務者レベルにおける国際協力であった。

これを政策レベル，閣僚級まで上げ，国際社会全体に CS 分野のキャパシティビルディングの必要性と合理性を明確に提唱したのは英国であった。2012 年 10 月，前年にロンドンで始まったロンドン・プロセスの第 2 回会合であるサイバー空間に関するブダペスト会合において，当時の英外務相ウィリアム・ヘイグが CS 分野のキャパシティビルディングの必要性を主張するとともに，英国政府が資金を投下して英国内に CS 分野の効果的なキャパシティビルディングを研究する GCSCC を設置することを発表した。英国は CS 分野のキャパシティビルディングを提唱したロンドン・プロセス自体の創設のほか，2012 年の GCSCC 設立の発表以降，様々な CS 分野のキャパシティビルディング支援を行っている。GCSCC はサイバーセキュリティのキャパシティを「政策・戦略」，「文化・社会」，「教育・研修・技能」，「法制度・規制枠組み」及び「基準・組織・技術」の５つのカテゴリーに分類し，GFCE と連携し，世界各国・地域で取り組まれているこれらの分野に係るキャパシティビルディングのイニシアティブの概要，動向や今後の予定等を掲載し，情報共有及び意識啓発を行っている。また，「CS 能力成熟度モデル(CMM)」を開発し，それを世界展開することにより各国が自己評価，ベンチマーク，より良い投資及び国家 CS 戦略計画並びにキャパシティビルディングの優先順位をつけることができるように支援している。

FCO は，ブラジルの法執行機関に対し，同国連邦及び国家レベルでの法執行機関の相互運用性の改善，汚職及び資金洗浄防止のための国家戦略の支援のための「サイバーによって可能になった犯罪への対処：ブラジル国家汚職防止及び資金洗浄防止活動」，同国の裁判官等司法機関の構成員に対し，同国司法制度のサイバースキル及び意識の向上及びより安全，オープンかつ民主的なサイバー空間に向けた規制強化のための脅威及び機会の特定を目的とした司法制度のデジタル及びサイバー問題に関する研修を通じたサイバーセキュリティの促進計画のほか国家犯罪対策庁(NCA)と連携して，欧州の法執行機関のスキル及び相互運用性を高めるためのサイバー犯罪対策演習，ウクライナ法執行機関デジタルフォレンジック研修，ジョージア法執行機関ネットフロー分析研修，インド法執行機関へのサイ

バー犯罪対策研修等を実施している。

また，インドの現地シンクタンクと連携して同国の法執行機関間のサイバーセキュリティ能力格差の特定の支援や，スリランカ CERT と連携したスリランカ CERT の強化，ナイジェリア企業と連携して同国の全州司法省サイバー担当検察庁の知識基盤をの拡大を目的としたサイバーセキュリティ法の執行のための研修，英コントロールリスク社と連携して行うナイジェリアの金融セクターのサイバーセキュリティ強化支援と国家機関以外のステークホルダーに対しても幅広くキャパシティビルディングを行っている。

英検察庁(CPS)がガーナの検察官のメンタリング，同国経済・組織犯罪局の能力構築支援を行う例や，英連邦議会協会(CPA UK)が英連邦諸国の国会議員，中央省庁等の政府高官へ強固なサイバー犯罪対策法の構築及び実施支援，国家 CS 戦略の策定及び実行支援，世界各国における強固な CS 基準の採用の促進，国際法及び行動規範の適用の強化，警察・捜査機関の研修及び評価等を促すワークショップや会合を開催している。

さらに，カタールの重要インフラ防護のためのスキルの構築，クウェート政府機関のためのサイバー机上演習，アラブ諸国の CS 構築支援，南アフリカの実務的意識啓発研修及びキャンペーン，英連邦電気通信機構(CTO：非政府組織)によるバングラデシュ電気通信規制機構，ケニア通信局，フィジー政府，バルバドス・エネルギー・移民・電気通信・投資省，カメルーン郵便電気通信省 ，ボツワナ運輸通信省への重要情報インフラ防護(CIIP)ワークショップの実施等，その主体は外交・警察・検察・情報通信技術・議会・非政府組織等，その支援対象範囲は英連邦諸国を中心に全世界，その内容はサイバー犯罪対策，インシデントレスポンス，意識啓発，重要インフラ防護支援，ワークショップ等 CS 分野のキャパシティビルディング提唱国らしく，西側諸国でこの分野をリードしている。
ただ，様々なイニシアティブを開始してはいるものの，これらの活動によって具体的にサイバー攻撃やサイバー犯罪の数が減少したという成果は公表しておらず，こうした活動は，研究センターを設置し，世界中の取り組みをホームページで公開し，積極的に自国の取り組みを世界に発信することにより CS のキャパシティビルディングを通じた英国の外交上のプレゼンスや影響力の向上を第一に狙う国家戦略と捉えることができる。

4.4.3. エストニアの取り組み

CS のキャパシティビルディングを外交戦略上重視している国としては，英国のほかに，2007 年に世界で初めて大規模なサイバー攻撃を受け，NATO サイバー防衛協力センター

(CCDCOE)の設立を提唱し，人口わずか 130 万程の小国ながら CS の分野でイニシアティブを発揮しているエストニアがある。

エストニアはイスラエル，ニュージーランド，韓国及び英国とともに「デジタル 5」というグループを形成し，2014 年以降ベストプラクティスの共有等のための年次会合，ワーキンググループを実施しているほか，同国のシンクタンク e ガバナンス・アカデミー(eGA)が同国外務省等と連携し，アンゴラ，ブラジル，ケニア，モーリシャス，タンザニア，タイ，チュニジア，ウクライナからの代表団に対するエストニアの ICT ソリューションの導入，ナミビアにおける政府の相互運用性ソリューション(X-Road)の設計，アルメニアの司法機関における e ガバナンス・ツールの開発，フェロー諸島の e 政府構築支援，ウクライナの e ガバナンス，ジョージア，サントメ・プリンシペの e ガバナンス強化支援，モルドヴァ裁判所の電子アクセス支援及び CS インデックス評価，モーリシャスのデータ共有ポリシー及びデータアーキテクチャ構築支援等を行っている。

「エストニア＝サイバーセキュリティ」というエストニアの国家としてのセールスポイントの認識は 2007 年の大規模サイバー攻撃を受けて以降，定着している。甚大な被害を受けた経験があるからこそ，途上国に対し同じような被害を受けないようにサポートする使命感という建前とともに，その専門的知見を活かし，CS 分野のキャパシティビルディングを外交の手段としてこれまで歴史的に接点がほとんどなかったアジアやアフリカにアプローチし，その関係を構築，強化し，国際社会における信頼を獲得しつつある。エストニアは，サイバー外交実務者間の最重要枠組みとも言える国連サイバーGGE にも第 1 会期から全会合に参加しており，米，英，日等と連携して，西側諸国による多数派形成活動の一翼を担っている。

4.4.4. 韓国の取り組み

韓国は，２０１３年にロンドン・プロセスの第３回会合をソウルで開催するなど，サイバーの世界におけるグローバルアクターとしてプレゼンスを発揮しており，サイバーセキュリティの強化を国策として重視している。

韓国未来創造科学部(MSIP)及び韓国インターネット・セキュリティ庁(KISA)は，全世界のサイバーセキュリティ関連政府機関，公的団体及び非営利団体を対象により安全なサイバーセキュリティ環境を確保するためのグローバルな協力基盤を構築し，サイバーセキュリティにおける共栄のためのパートナーシップを構築することを目的とした「相互発展の

ためのサイバーセキュリティ連合(CAMP)」を 2016 年 7 月に立ち上げた。具体的な活動としては，メンバー間のインタラクティブな国際コミュニティを構築するための年次会合又はフォーラムが予定されている。

また，KISA は，途上国におけるサイバーセキュリティ専門家を対象に，サイバーセキュリティ戦略及び政策の策定計画の作成，知識及び経験の共有並びにサイバーセキュリティ能力の強化により途上国のサイバーセキュリティ及び経済成長の水準を改善することを目的とする「開発のためのグローバルサイバーセキュリティセンター(GCCD)」を 2015 年 6 月に設置している。招待ベースの研修コースの実施，途上国における共同セミナーの主催，サイバーセキュリティ能力成熟度評価の実施とそれに基づく研修の実施，サイバー防衛のためのオンラインハンズオン研修を主に行っていく予定で，2015 年 9 月に韓国で開かれた「国家サイバーセキュリティ政策研修コース」に 13 カ国から 20 人の政府職員が参加し，同年 11 月，コスタリカ，ペルー，モンゴル，インド及びベトナムにおいて，それぞれの国の個別の議題について共同セミナーを開催するなど，アジアのみならず，全世界を対象とした CS 分野のキャパシティビルディング活動を推進している。

韓国は，この他にも，エストニア等と「デジタル 5」の一員としてキャパシティビルディングを通じたサイバー外交を積極的に展開している。

4.4.5. 中国の取り組み

2015 年 7 月に北京において ARF の枠組みにおいて中国及びマレーシア両政府の共催の CS キャパシティビルディングに関するワークショップを行った以外，中国は GFCE，GCSCC のいずれにもその取り組みを共有していないため，中国が CS 分野のいかなるキャパシティビルディングを行っているかは定かではない

しかし，中国の対外援助については，「中国対外援助白書」等で公開されており，その 2014 年度版では「中国の対外援助供与国は，全世界で計 121 ヵ国である。内訳としては，アフリカ 51 ヵ国，アジア 30 ヵ国，ラテンアメリカ・カリブ 19 ヵ国，大洋州 9 ヵ国，ヨーロッパ 12 ヵ国。アフリカ連合等，地域組織を通じた支援も実施」とあり，また援助の分野別では経済インフラが 44.8%，社会インフラ 27.6%，物資 15%等となっており，特にアフリカやアジア諸国に対して CS に関する何らかの援助を行っている可能性は否定できな

い[115]。また，中国はこれまですべての国連サイバーGGE の会合に参加しており，そのコンセンサス報告書においてキャパシティビルディングへの重要性や具体的な取り組みへの提言が盛り込まれているが，コンセンサスを得ているということはこの点については中国としてもこれには異論がないということである。いずれにしても，中国は現時点における西側諸国との CS 分野のキャパシティビルディングに関する協力には慎重かつ消極的な立場をとる点は明確である。

4.4.6. ロシアの取り組み

ロシアは 2016 年，インドネシアと CS 分野の協力を強化することに合意し，協力の中身としては CS のキャパシティビルディングや情報共有が含まれること明言した[116]。

このほか，中国等と国連に共同提案している「情報セキュリティのための国際行動規範（案)」では，CS 分野のキャパシティビルディングの重要性については認識しており，この点はサイバーGGE においても同様である。

しかし，中国同様，GFCE や GCSCC の枠組みには参加しておらず，西側諸国と情報を共有していない。日露サイバー協議においても，その詳細は公開されていないが，少なくともキャパシティビルディングは議題に挙がっていない点からも，やはり中国と同様，西側諸国とこの分野での協力には消極的な立場をとっていると推察される。

4.4.7. 国連の取り組み

国連サイバー政府専門家会合(GGE)における議論の経緯は，前述したとおりであるが，キャパシティビルディング関係については，次のように概観することができる。

ロシアが 1998 年に国連総会第一委員会（軍縮問題及びそれに関連する国際安全保障問題のみを取り扱う委員会）に提出した情報セキュリティの問題に関する各国の見解と評価を調査するための「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展」決議案に端を発して 2004 年に初めて招集されたサイバー専門家会合(GGE: Group of Governmental Experts[117])の第 2 次会合（2009 年から 10 年に開催）で取り纏められたコ

[115] 中国の対外援助の現状(https://www.mof.go.jp/pri/research/conference/china.../china2014_04_02.pdf)
[116] Russia stresses importance of cybersecurity cooperation with Indonesia (http://www.thejakartapost.com/news/2016/10/03/russia-stresses-importance-of-cybersecurity-cooperation-with-indonesia.html)
[117] 正式名称は Group of Governmental Experts on Developments in the field of information and telecommunications in the context of international security: 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展に関する政府専門家会合。

ンセンサス報告書(A/65/201)において，国家間の CS の格差はグローバルなネットワークの脆弱性を高める危険性があり，その格差是正のためにキャパシティビルディングの必要性と重要性が指摘された。

これを踏まえ 2012 年から 13 年にかけて実施された第 3 次サイバーGGE の報告書(A/68/98)では，引き続き相互にネットワークで接続された世界における脆弱性を軽減するためのキャパシティビルディングの重要性が強調されたほか，「キャパシティビルディング措置に関する提言」と題する章を設けて，国連加盟国が検討すべき 5 つの具体的措置（①法制度，法執行機関，戦略等既存のサイバーセキュリティ強化のための取り組みの支援，②CERT 等インシデントレスポンス強化，③e ラーニングの利用等を通じた CS の研修と意識啓発，④インシデント管理に関する技術支援等及び⑤研究機関及び大学による CS に関する研究・分析の奨励）を提案した。

2014 年－15 年の第 4 次サイバーGGE では，これをさらに敷衍し，8 つの具体的措置（①CERT 強化支援，②重要インフラセキュリティ改善及びベストプラクティスの共有のための研修，③CS 技術支援，④迅速なインシデントレスポンス相互支援手続の創設，⑤重要インフラの脆弱性対処のための国境を越えた協力の円滑化，⑥持続可能な CS・キャパシティビルディングのための戦略の策定，⑦CS の意識啓発及び⑧サイバー犯罪対策等のためのフォレンジックの奨励を推奨した。

4.4.8. 途上国の取り組み

途上国の取り組みは，主に①国際社会への支援の呼びかけ，②地域機関の研修等への参加及び③外交交渉の道具という 3 つの視点から説明できる。

第一に，サイバーセキュリティの能力構築支援を要する開発途上国側は，支援を国際社会に要請する立場であり，その声を国際機関若しくは地域機関又は個別の国家に表明している。例えば GFCE や国連 GGE の場への参加ができるように主催者などに働きかけ，必要に応じてデマルシュを提出する。GGE の参加国が 15 カ国から 20 カ国そして 25 ヵ国に拡大していった背景には，途上国側のキャパシティビルディングの必要等の意見を国際社会に反映させたい狙いがあり，国際社会において圧倒的多数派を形成する途上国は，その存在と支援要請の継続的な主張を行っている。例えば，アフリカでは，ケニアやセネガルなどが GFCE などの場で自国のサイバーセキュリティの問題点を指摘し，支援を要することを表明し，サイバー先進国の国家や民間企業の協力を要請している。

第二に，途上国の政府職員や CERT 職員等は，国連等の国際機関や ARF や OSCE，OAS 等の地域機関や国際 CERT 機関が実施する研修，演習，ワークショップやセミナーに参加し，国際場裏におけるサイバーセキュリティの法制度や政策・戦略等の発展に後れを取らないようにしている。サイバー空間の非国境性という特質から，脆弱な途上国のネットワークは先進国に対するリスクでもあるため，先進国は，自国の安全保障のために途上国のサイバーセキュリティの強化が需要であり，そのため，途上国へサイバーセキュリティに関する演習や研修等の参加を促す機会が多い。

第三に，サイバー空間の在り方，特に従来の国際法の適用を巡り，西側諸国と中露等の間で激しい対立があり，両陣営としては，国際社会における多数派を形成するために途上国に対して自陣に取り込むよう外交的に働きかける必要がある。このような政策的判断を迫られる途上国としては，より自国の必要に適した支援・援助を行う側の政策を支持するという実質的な選択権がある。被支援者という立場にありながら，支援者の真の目的が多数派形成にあるのであれば，途上国側としてもより良い支援を行うのであればそれを受け入れるという外交交渉ができる材料となる。この点，第 5 次 GGE の失敗により，サイバー空間に関する国際的なルール作りは，西側諸国と中露等が歩み寄り国際規範を形成するというよりも，両陣営が個別に理想とするサイバー空間の統治のあり方に基づいてルールを作り，それを支持する国を増やすという方向に進む可能性が高い。途上国としては，支援国がｍ自国が理想とするサイバー空間の統治の在り方かどうかという点とともに，自国が必要とするサイバーセキュリティの能力構築支援をより適確に行えるのはどの国かという点から支援国を選ぶという機会も増えるだろう。

4.4.9. 民間企業の取り組み

AT&T，シスコ，ヒューレット・パッカード，IBM，マイクロソフト，シマンテック，ファーウェイ，ヴォーダフォン等の民間企業は，GFCE のメンバーである。また，マイクロソフト，トレンドマイクロ及びシマンテックは，OAS と連携して，OAS 加盟国への専門的知見を提供している。シマンテックは，アフリカ連合と連携して，アフリカにおけるサイバー脅威の傾向を分析した報告書等を作成している[118]。日本の NEC は，総務省が推進する日・ASEAN 統合基金 2.0(JAIF)の「日 ASEAN サイバーセキュリティ協力ハブ」プロジェクトにおいて，ASEAN 加盟国のサイバーセキュリティ主管庁の職員など約 40 人

[118] https://www.thegfce.com/initiatives/c/cybersecurity-and-cybercrime-trends-in-africa

を対象に，サイバーセキュリティ演習を実施した[119]。

4.4.10. アカデミア・研究機関の取り組み

英国の GCSCC の他に NUPI（ノルウェー国際関係研究所）や ISS（EU セキュリティ研究所）等がサイバーセキュリティのキャパシティビルディングに関するペーパーを作成している。

GCSCC はサイバーセキュリティ能力成熟度モデルを開発し，①サイバーセキュリティ政策・戦略（国家サイバーセキュリティ戦略，インシデント対応，国家重要インフラ防護，危機管理，サイバー防衛，デジタル冗長性），②サイバー文化・社会（サイバーセキュリティの心構え，サイバーセキュリティの意識（アウェアネス），インターネットに対する信頼，オンラインのプライバシー），③サイバーセキュリティ教育，研修及び技能（サイバー教育及び研修に関する国家の可用性，サイバーセキュリティに関する国の教育制度，企業内の研修及び教育的取り組みとの協力，コーポレートガバナンス，知識及び基準），④法規制枠組み（サイバーセキュリティ法制度，法的調査，責任ある公開）及び⑤基準，組織及び技術（基準の遵守，国家インフラの強靭性，サイバーセキュリティの市場）と５つの分野を評点化し，各国のサイバーセキュリティの成熟度を計測して，必要な対策を検討することを提案している[120]。

ISS は，サイバーキャパシティビルディングに関する 10 個の提言として，①サイバーキャパシティビルディングは社会経済発展を支持する長期的なプロセス（チェーンプロセス），②共通認識の必要性（サイバーキャパシティビルディングは軍事的協力ではなく，犯罪との闘い，強靭性の確保，安全な環境の構築という共通認識の醸成），③サイバーキャパシティビルディングは安全保障のみならず世界の社会経済発展のためのものという認識，④サイバーキャパシティビルディングはドナー（支援者）とレシピエント（被支援者）によってその内容が異なること，⑤サイバーキャパシティビルディングの優先順位は全員共通ではないこと（ドナー側の欲しいものリストとレシピエント側の欲しいものリストの洗い出しの必要），⑥キャパシティビルディングの枠組みは全ての者に対して有効ではないが，ほとんどの者に対して有効である（地域的特殊性等もあるが，国家サイバーセキュリティ戦略の重要要素等は汎用性もある），⑦サイバーキャパシティビルディングは国際協

[119] http://jpn.nec.com/press/201710/20171026_01.html
[120] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf

力を要すること（サイバー関連脅威は国境がなく，単一の国家より世界各国の能力を有効活用した方がその技術を提供する機会が増えるため），⑧サイバーキャパシティビルディングは利害関係者の協力を要すること（政府，産業界，技術コミュニティ，NGO，シンクタンク等），⑨サイバーキャパシティビルディングは優先されていないが，優先されるべきである（飢餓，衛生，犯罪，インフラ構築等に比べて，そのリスクが目に見えないため，サイバーセキュリティの問題は軽視されがちだが，その影響は甚大であり，優先的に取組むべき）及び⑩必要性を叫ぶ時からそれを実施する段階に入った（サイバーセキュリティに関する意識啓発，CERT/CSIRT 構築，戦略，産業制御システムの策定・構築，演習の実施等を行わなければならない）を挙げた[121]。

4.4.11. CERT コミュニティの取り組み

各国の CERT は，①コンピュータの不正利用などによるインシデントへの対応の支援，②マルウェアの感染活動の観測をはじめとするインターネット定点観測システムの運用，③ソフトウェア等の脆弱性に関する調整，④コンピュータセキュリティインシデントを未然に防ぐための早期警戒活動及び⑤企業等の組織内におけるコンピュータインシデント対応チーム（CSIRT）の構築・運用支援を行っている[122]。また，各地域ごとの CERT 団体や世界の CSIRT やセキュリティチームの集まりである FIRST (Forum of Incident Response and Security Teams)が CSIRT 同士のサイバー脅威に関する情報交換を行っていたり，サイバー先進国の CERT が途上国の CERT の構築，能力強化・維持支援等を行っている。

また，日本の実質的な国家 CERT である JPCERT/CC はサイバーグリーンプロジェクトを立ち上げ, 英国, アフリカ CERT, APNIC, CSA シンガポール, ITU, ICANN, APCERT, インターネット・ソサイエティ等と連携して，①健全なインターネット利用の妨げとなる各種の「リスク環境要因」を洗い出し，②それぞれのリスク環境要因を，世界各国のセキュリティベンダーなどの協力のもと収集し，③インターネットの健全性レベルなどを，リスク別，国別，地域別に，比較可能な指標で表し，可視化し，また長期的な変化を明らかにし，④各国 CSIRT や ISP などとデータを共有し，連携してインターネットの「クリーンアップ」を行い，⑤これにより，中長期的に，インターネット及びサイバー空間を攻撃

[121] https://www.iss.europa.eu/sites/default/files/EUISSFiles/EUISS_Conference-Capacity_building_in_ten_points-0414.pdf
[122] http://www.jpcert.or.jp/faq.html#q01

や犯罪のインフラとして悪用しにくくすることを目指した活動を行っている[123]。

[123] https://www.jpcert.or.jp/research/cybergreen.html

5. 日本のサイバーセキュリティ分野におけるキャパシティビルディングの取り組み

5.1. 日本のサイバーセキュリティ分野のキャパシティビルディングに関する方針

5.1.1. 基本方針策定の経緯

日本のサイバーセキュリティ分野のキャパシティビルディングに関する方針は，次のような第一～第六の経緯をたどっている。

第一に，2013 年 12 月に閣議決定された「国家安全保障戦略」において，「サイバー空間については，情報の自由な流通の確保を基本とする考え方の下，その考えを共有する国と連携し，（中略）開発途上国への能力構築支援を積極的に行う」との CS のキャパシティビルディングを積極的に取り組むという一般的な方針が示された。

第二に，2015 年 2 月に閣議決定された「開発協力大綱」の重点課題の 1 つである「平和で安全な社会の実現」の施策としてサイバーに関する能力強化，開発途上国の支援が開発関連文書として初めて挙げられた。

第三に，2015 年 9 月に閣議決定された「サイバーセキュリティ戦略」の「5.3. 国際社会の平和・安定及び我が国の安全保障 5.3.2 国際社会の平和・安定(4)サイバー分野における能力構築（キャパシティビルディング）への協力」において，「我が国は，自由と民主主義を基調とする責任ある国際社会の一員として，これまでの経験と蓄積を元に，各国のキャパシティビルディングに積極的に取り組む。国境を越えるサイバー空間の脅威は，世界各国の多様な主体が連携して対処していく必要があり，一部の国や地域において脅威に対処するための能力が不十分であることは，我が国を含む世界全体にとってのリスク要因となる。事実，我が国へのサイバー攻撃は，国外からの攻撃が多く確認されている。また我が国の国民及び企業の活動はグローバル化しており，海外への渡航や企業の海外進出拠点は増加を続けている。その活動は，情報化の進展に伴い，渡航先国・進出先国の管理・運営する社会インフラ及びサイバー空間に依存する。こうしたことから，世界各国における CS 確保のためのキャパシティビルディングに協力することは，当該国への貢献となるのみならず，日本国と世界全体にとっても利益となる。

日本国は，これまで情報通信社会の発展に伴い，CS に関する法令や政策の整備を推進するとともに，政府機関，重要インフラ事業者，その他の組織及び個人における CS の確保やサイバー犯罪対策，CS 人材の育成，CS に関する技術の研究開発に取り組んできた。 我

が国は，これらの経験と蓄積を元に，情報の自由な流通を基本原則とする責任ある国際社会の一員として，引き続き，各国のキャパシティビルディングに積極的に協力していく。このため，政府及び関係機関は一体となってキャパシティビルディングに ついて検討し，その効率的・効果的な実施を図る」と，CS 分野のキャパシティビルディングに積極的に取り組む背景，理由及び方針を示し，「5.3.3 世界各国との協力・連携」では，特に「アジア大洋州地域」のキャパシティビルディングを推進し，その次に「中南米，中東アフリカ」両地域の「共通の価値観を持つ国々」とキャパシティビルディングの「可能性を検討」するとの我が国の CS 分野のキャパシティビルディングの取り組みにおける対象地域の優先順位を明らかにした。

第四に，2016 年 5 月に開催された G7 伊勢志摩サミットで発出された「サイバーに関するＧ７の原則と行動」の「Ｇ７の一致した行動」では，G7 諸国が「サイバー空間における安全及び安定を促進するため，国家の CERT 間の協力，キャパシティビルディング及び意識啓発の促進」等の協力の強化に努める方針が打ち出された。これには，G7 諸国間のキャパシティビルディングを含めた国際連携の強化とサイバー空間のガバナンスの在り方についての共通認識を国際社会に示すことにより，その立場を異にする中露等をけん制するねらいがあることが容易に推測される。

第五に，2016 年 7 月に国連総会において公表されたサイバーGGE 関連文書「A/71/172」において，日本の CS 分野の国際協力を推進する取り組みとして，（１）サイバー空間における法の支配の推進，（２）キャパシティビルディング Ms，（３）キャパシティビルディング措置という三本柱があり，キャパシティビルディングに関して，日本は特に ASEAN 地域の人材育成支援及び技術協力に積極的に取り組んでいる旨を特に具体的な事例を示さず，簡潔に紹介している[124]。

第六に，2016 年 10 月，内閣サイバーセキュリティセンター(NISC)，警察庁，総務省，法務省，外務省，経済産業及び防衛省が共同で発出した「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」では，CS 分野のキャパシティビルディング支援の重要性として，次を挙げている。

（１）国際的なサイバーセキュリティ上の弱点の低減による日本を含む世界全体へのリスクの低減

（２）支援対象国の重要インフラ等に依存する在留邦人の生活や日本企業の活動の安

[124] A/71/172 (http://www.un.org/ga/search/view_doc.asp?symbol=A/71/172)

定の確保

（3）支援対象国への情報の自由な流通や法の支配を基本原則とする日本の立場の理解の浸透

（4）日本の情報通信産業等の現地展開を進める上での基盤の形成可能性

また，キャパシティビルディングの在り方として，キャパシティビルディングの形態を（1）「インシデントレスポンス等の能力の向上支援」，（2）「サイバー犯罪対策支援」及び（3）「サイバー空間の利用に関する国際的ルール作り及び信頼醸成措置に関する理解・認識の共有」の 3 つに大別した。

（1）については，さらに（ア）「途上国政府の態勢作りの支援（アウェアネスの向上，制度・政策面（サイバーセキュリティ戦略の策定・改定支援等），態勢・機構面の知見の提供）」，「（イ）機材・設備の供与」，「（ウ）機材・設備の運用能力の向上支援（技術面の知見の提供，人材育成）」の 3 つに分類している。

その上で，「高度な機材を供与しても，その運用能力が伴わない状態では，支援の効果が十分に発揮されないおそれがある」との理由から，「当面は技術協力を中心に，（ア）及び（ウ）に注力」し，「途上国側の制度・態勢等の整備の進展と並行して，（イ）で供与する機材の高度化を図っていく」とあり，このような方針に基づき，「当面は ASEAN 諸国を中心に，政府開発援助（ODA），その他の政府資金等各種形態の支援の可能かつ適切な連携の下，積極的に支援を進めていく」方向性を示した。

5.1.2. 日本のキャパシティビルディング方針の特色

以上の 6 つの方針等を検討すると，我が国は，CS 分野のキャパシティビルディングの支援対象としては，「ASEAN 諸国」を重視していることが挙げられる。

支援の具体的な活動としては「インシデントレスポンス能力向上支援」，「サイバー犯罪対策支援」及び「国際的なルール作り及び信頼醸成措置に関する認識の共有」の 3 点を重視し，支援の手法としては「技術協力」を中心に積極的に支援を行うとの基本方針である。

それでは，このような方針の下，具体的に我が国はどのような取り組みを行っているのだろうか。以下に，基本方針でもあった 3 つの支援対象分野の順に基づいて，各種の取組の検討を行うこととする。

5.2. 日本のサイバーセキュリティ分野のキャパシティビルディングに関する取り組み

第一に，インシデントレスポンス等能力向上支援について，JPCERT/CC は 2007 年以降，アジア太平洋及びアフリカ地域の CSIRT の構築及び運用支援を実施している[125]。JPCERT/CC によるアフリカ地域の CSIRT 支援は 2009 年に開始し，2016 年 6 月にはその功績を称える AfricaCERT 功労賞を受賞する程その支援活動は評価されている[126]。JPCERT/CC は英外務・英連邦省(FCO)とともに，「サイバーグリーン研究所」を設置し，全世界の CSIRT やネットワーク運営者及び政策立案者を対象に，グローバルな「サイバーエコシステム」の健全性を高めることを支援し，信頼できるサイバー空間のメトリクス，測定及び被害防止に関するベストプラクティスの提供することを目的とした「サイバーグリーンプロジェクト」を推進している。

また，近年 JICA がミャンマーの通信網改善事業[127]を有償資金協力で行っているほか，総務省，経済産業省，NISC 等と連携して同国[128]，インドネシア[129]，ベトナム[130]等の ASEAN 諸国に技術協力として CS 専門家を派遣している。さらに，日 ASEAN 情報セキュリティ政策会議の枠組みによるサイバー防護等に関する短期研修やワークショップ，サイバー連絡演習を実施してきたほか，近年は日本の大学に ASEAN の留学生を受け入れる長期研修の実施も検討している[131]。

この他にも，日 ASEAN 統合基金（JAIF）2.0 を活用した日 ASEAN サイバーセキュリティ協力強化に向けた取組[132]や 2015 年 7 月には外務省をはじめ NISC や JICA 等の政府関係者がベトナムに調査団として派遣され，ベトナム政府関係機関からサイバーセキュリティ分野の現状や人材育成の取組や課題等を聴取するとともに，関連施設の視察等を行っている[133]。これが意図するところは明確ではないが，ODA のプロジェクト型無償資金協力の一環としての準備・現地のニーズ調査とも考えられる。

---

125 JPCERT/CC 活動概要［2007 年 7 月 1 日 ～ 2007 年 9 月 30 日］
https://www.jpcert.or.jp/pr/2007/pr070008.pdf
126 JPCERT/CC 活動概要［2016 年 4 月 1 日 ～ 2016 年 6 月 30 日](https://www.jpcert.or.jp/pr/2016/PR20160714.pdf)
127 事業事前評価表(http://www2.jica.go.jp/ja/evaluation/pdf/2014_MY-P9_1_s.pdf)
128 ミヤンマー国サイバーセキュリティにかかる情報収集・ 確認調査
(https://www2.jica.go.jp/ja/announce/pdf/20150527_150361_1_01.pdf)
129 情報セキュリティ能力向上プロジェクト(https://www.jica.go.jp/project/indonesia/014/outline/index.html)
130 ベトナム国サイバーセキュリティにかかる情報収集・確認調査（一般競争入札（総合評価落札方式））
(https://www2.jica.go.jp/ja/announce/pdf/20151007_150825_1_02.pdf)
131 第 9 回「日・ASEAN 情報セキュリティ政策会議」を開催しました
(http://www.meti.go.jp/press/2016/10/20161024006/20161024006.html)
132 日・ASEAN 統合基金（Japan-ASEAN Integration Fund（JAIF））
(http://www.mofa.go.jp/mofaj/area/asean/j_asean/jaif.html)（最終アクセス日：2017 年 12 月 18 日）
133 ベトナムに対するサイバーセキュリティに関する調査団の派遣
(http://www.mofa.go.jp/mofaj/press/release/press1_000076.html)（最終アクセス日：2017 年 12 月 18 日）

第二に，サイバー犯罪対策支援について，2014 年 5 月に第 1 回目 ASEAN サイバー犯罪対策対話が立ち上げられ，同対話の枠組みを通じて ASEAN におけるサイバー犯罪対策（法執行機関の人材育成及びサイバー関連法制度整備支援等）を支援する方針である[134]。また，我が国は，UNODC（国連薬物犯罪事務所）のサイバー犯罪技術援助プロジェクトへ出資し，ASEAN 諸国のサイバー犯罪対処能力向上を支援している。別の枠組みとして，アジア大洋州地域の治安機関が情報技術の解析に係る知識・経験等を共有し，円滑な情報交換を促進するとともに，各国・地域のサイバー犯罪等の対策に資する解析能力の向上を図ることを目的として，2000 年から警察庁が毎年開催しているアジア大洋州地域サイバー犯罪捜査技術会議[135]や我が国も加盟しているサイバー犯罪に関するブダペスト条約締約国による関連会合（オクトパス会合）もある。さらに，2015 年には，JICA の課題別研修として，インドネシア，コートジボワール，セーシェル，バングラデシュ，パキスタン，パナマ，フィリピン，ボツワナ，ボリビア，ミャンマー，メキシコ及びモンゴルの研修員を受け入れ，サイバー犯罪の捜査手法等についての研修を通じてサイバー犯罪対処能力向上を行った[136]。

第三に，サイバー空間の利用に関する国際的なルール作りや信頼醸成措置に関する理解・認識の共有について，NISC が主導で 2012 年以降，日本は ASEAN と共同で CS の意識啓発活動（ポスターの作成，教材（アニメーション，）の ASEAN 加盟国の母国語への翻訳及び日 ASEAN 間の資料の共有など）を行っているほか，2015 年に開催された「サイバーセキュリティカフェ～日本×ASEAN セキュリティ文化，どう違う？」では日 ASEAN 双方の学生がセキュリティ文化の近いについて意見交換を行った[137]。

この他，ARF 等の多国間枠組みのワークショップや二国間のサイバー協議・対話を通じて国際的なルール作りやキャパシティビルディング Ms に関する共通理解の促進に努めている。また，特に国連サイバーGGE，ロンドン・プロセス，グローバルサイバーサミット，メリディアン会合等の多国間協議の場においてこれらの議題に関する立場が近い米欧等と足並みを揃えるとともに，CS 分野のキャパシティビルディングの支援国と被支援国のマ

---

[134]第 1 回目・ASEAN サイバー犯罪対策対話の開催（結果概要）
(http://www.mofa.go.jp/mofaj/fp/is_sc/page22_001080.html)
[135] 警察庁４ サイバー犯罪捜査への支援(https://www.npa.go.jp/hakusyo/h23/honbun/html/1-toku2_2_4.html) （最終アクセス日：2017 年 12 月 18 日）
[136] 警察庁平成２７年の国際協力等の状況(https://www.npa.go.jp/kokusaikyoryoku/suishin/kyoryokujokyo/H27.pdf)（最終アクセス日：2017 年 12 月 18 日）
[137] サイバーセキュリティカフェ ～日本×ASEAN セキュリティ文化，どう違う？～
(https://www.youtube.com/watch?v=xtCQV0rxgJc) （最終アクセス日：2017 年 12 月 18 日）

ッチング・プラットフォーム兼ベストプラクティス共有の場としてロンドン・プロセスのハーグ会議で 2015 年に立ち上げられた GFCE(Global Forum on Cyber Expertise:サイバーの専門的知見に関するグローバル・フォーラム)のメンバーとなり，これまで日本が ASEAN 等と行ってきた上記の活動等を共有し，その概要を GFCE と密接に連携しているオックスフォード大学グローバルサイバーセキュリティキャパシティセンター(GCSCC)の「ポータル」で公開している。

6. サイバーキャパシティビルディングの在り方に関する考察

以上，3.4 から 4.まで，世界及び日本サイバーキャパシティビルディングの取り組みを概観してきた。これらの取り組みの例の概要は，付属資料「サイバーキャパシティビルディングに関する取組一覧」を参照されたい。サイバーキャパシティビルディングを実施している主体は多々あるが，その中で，主な国家，国際機関，民間企業等の１４４（日本が 5，星が 1，韓国が 2，ASEAN（東南アジア諸国連合）が 2，APEC（アジア太平洋経済協力）が 1，米国が 8，墨が 1，英が 34，エストニアが 13，スイスが 1，メリディアンが 1，仏が 1，白が 1，以が 1，加が 1，ENISA（欧州 ネットワーク情報セキュリティ庁）が 2，欧州評議会が 5，欧州委員会が 1，OSCE（欧州安全保障協力機構）が 1，ユーロポールが 2，フィンランドが 1，ディプロ財団が 1，ICT4Peace が 1，UNIDIR（国連軍縮研究所）が 3，UNODC（国連薬物犯罪事務所）が 2，UNDP（国連開発計画）が 5，UNESCAP（国連アジア太平洋経済社会委員会）が 1，UNECA（アフリカ経済委員会）が 4，ITU（国際電気通信連合）が 11，UNCTAD（国連貿易開発会議）が 5，UNAFRI（国連アフリカ犯罪防止・加害者治療研修所）が 2，OAS（米州機構）が 10，GSMA（GSM アソーシエーション）が 1，世界経済フォーラムが 1，GPEN（グローバル検察官 E 犯罪ネットワーク）が 1, GPD(グローバルパートナーズデジタル)が 1, ナイロビ大学 1, セネガル 1, ANSTeRD（持続可能な技術及び地方開発のためのアフリカ機構）が 1，EC3（欧州サイバー犯罪センター）が 1，インターポールが 2，NATO（北大西洋条約機構）が 2，GFCE（サイバーの専門的知見に関するグローバル・フォーラム）が 1 である。）の取り組みの名称，ドナー，パートナー，レシピエント，対象グループ，主たるテーマ，目的・目標，具体的活動，（想定される）成果・効果及び時期を表にまとめた。

ここで，これらの既存の取り組みを分析し，主な主体のサイバーキャパシティビルディングの在り方について考察する。

6.1 米国型サイバーキャパシティビルディング：ハードパワー安全保障連動型

米国は，支援対象地域としては，アフリカ（米アフリカ軍司令部（AFRICOM）によるアフリカの武官への研修，国務省による西アフリカ諸国に対するサイバー犯罪対策ワークショップの実施等）を重視しており，その他では日本や豪州等と ASEAN 諸国のサイバー犯罪対策に関して共同で UNODC などに資金を拠出しているほか，OAS の構成国として国

際的なサイバーセキュリティの能力構築に関与はしているものの，ジョージ・C・マーシャル欧州安全保障研究センターのサイバーセキュリティ研究プログラムや全米サイバーセキュリティ連盟の取り組みからも分かるように，国内の政府機関や企業，一般大衆等の能力構築，意識啓発を重視しており，サイバーセキュリティのキャパシティビルディングを国家安全保障の延長線上の施策（「安全保障連動型」）として捉えていると考えられる。また，その特徴として，シスコ社当の民間企業と共同で様々なサイバーセキュリティの能力向上を図る研修やキャンペーンを実施している。そして，キャパシティビルディングの理念自体には賛同しているが，サイバー外交において最も重視しているのはサイバー空間を利用した国家の責任ある行動規範を中心とする国際的なルールの確立であり，キャパシティビルディングの重要度は,国際的なルール作り及び信頼醸成措置に劣ると考えられる。米国は，キャパシティビルディングをあくまでサイバー空間の国際ルール作りを行う前提としての付随的な施策にすぎないと考えているとも言えよう。米国は国際規範と重要インフラ防護重視の姿勢を見せているが，その背景には強力な軍事力があり，サイバー空間を第 5 の戦場と称した点からも，サイバー空間を安全保障・軍事上の観点から取り組むべきものとして捉えており，その取り組みの根底には，サイバー空間を利用した他国からの武力行使や武力攻撃が行われた場合には従来の国際法枠組み内で行使できる対抗措置をとることができることを理想としており，第 5 次 GGE の失敗を受け，そうしたルールを，中露等を含めて合意できないのであれば，同志国のみで合意形成を目指し，あるいは信頼醸成措置やキャパシティビルディングを通じた国際平和と安全を模索する可能性もあるが，そこでもキャパシティビルディング重視するとの公式な見解は今のところ出されていない。なお，GGE の交渉失敗を受け，オバマ政権の 2011 年に設置された国務長官直属であった国務省のサイバー問題調整室が，国務長官直属から外れ，経済・企画局に移管されることになった[138]。これを受け，サイバー問題調整官のクリス・ペインター氏も辞職した。これら一連の流れは，トランプ政権下の米国におけるサイバー外交の重要性の低下を示唆しており，米国は元々サイバーキャパシティビルディングに消極的であったが，さらにその優先度が低くなる可能性が高いと考えられる（米国のサイバーキャパシティビルディングの具体例は，付属資料 12 から 20 等を参照）。

なお，この安全保障連動型のキャパシティビルディングには，支援対象国や地域を踏み

[138] http://thehill.com/policy/cybersecurity/346499-state-department-quietly-establishes-new-cyber-office（最終アクセス日：2017 年 12 月 18 日）

台にしたサイバー攻撃を自国が受けているために，当該対象国のサイバーセキュリティの能力構築支援を行うことにより，自国の安全保障を強化する目的を有する場合も含まれよう。

6.2 英国型サイバーキャパシティビルディング：積極的広報外交強化型

英国は，GCCS や GCSCC の創設，別表の数々の取り組みからも分かるとおり，サイバーセキュリティ分野のキャパシティビルディング重視のサイバー外交を展開している。GCSCC の創設などこの分野のパイオニア的な存在であるとともに，支援対象地域は旧植民地諸国（インド，スリランカ，ナイジェリア，南ア等アフリカ諸国やアラブ諸国）や東欧諸国（ジョージア，ウクライナ等）などが多いが，アジア太平洋地域や中南米等に対しても，在外公館職員等と連携を組み，全地域を対象に支援や協力を展開しようとしている。また，他国や国際機関・地域機関が行っている既存の取り組み（サイバーグリーンプロジェクトや GFCE 等）と連携して，自国の存在感を示すなど，キャパシティビルディングを広報外交の一環として活用している側面がうかがえる（「広報外交型」）。その典型的な例は前述の GCSCC であり，GFCE と連携して世界の各地域で行われているサイバーセキュリティのキャパシティビルディングの取り組みを調査し，そのウェブサイト（「ポータル」）で公表しており，GCSCC が開発したサイバーセキュリティ能力成熟度モデルを各国が活用するよう働きかけるなど広報外交のアプローチの道具として積極的にキャパシティビルディングを利用している。また，GCSCC がオックスフォード大に設置している点からも分かるように，学術的・研究の観点からキャパシティビルディングを捉え，それを国が積極的に支援している点も特徴的である（「研究重視型」）。米国のようにサイバー空間を「第 5 の戦場」と称してはいない英国は，ハードパワーをちらつかせるサイバー政策ではなく，21 世紀におけるサイバー空間の重要性に鑑み，積極的なサイバーセキュリティの支援・援助活動等を通じた自国のプレゼンスの向上のためのツールとしてキャパシティビルディングを利用する狙いがあると考えられる（英国のサイバーキャパシティビルディングの取り組みの一例については，付属資料 22 から 55 等を参照）。

6.3 エストニア型サイバーキャパシティビルディング：スモールパワー特化型

エストニアは，人口わずか 130 万，国土面積は九州程度の小国であり，ソ連併合の歴史から独立後は西側諸国との関係を重視し，ＮＡＴＯ及びＥＵ加盟国であり，ロシアからと

思われる大規模なサイバー攻撃の被害の経験から，サイバーセキュリティと IT を国家安全保障戦略上最重視している国である。英国や韓国等と「デジタル５」を創設し，政府の IT 化・電子化の推進を図っているほか，国立 e ガバナンス・アカデミーや外務省が積極的にナミビア等のアフリカ諸国やモルドヴァ等の東欧諸国に対して政府の電子化の支援を行いつつ，サイバーセキュリティの能力強化を支援している。首都タリンには NATO CCDCoE を置き，対ロシア最前線として，地政学的にも重要であり，西側諸国もそのサイバーセキュリティにおけるリーダーシップを期待している。サイバーセキュリティと言えばエストニアを想起する程，そのサイバーセキュリティ分野における存在感は大きく，日本もこれまで 3 回サイバー協議を行っており，今後さらに支援活動を通じて，各国の信頼を今以上に獲得すれば，西側陣営のサイバー外交の中心的存在になる可能性を秘めている（エストニアのサイバーキャパシティビルディングの取り組みの例については，付属資料 56 から 68 等を参照)。

6.4 中露型サイバーキャパシティビルディング：非公表非国際協調型（新サイバー軍事同盟型？）

中国やロシア等は，サイバー空間に関する国際的なルール作り同様，サイバーセキュリティのキャパシティビルディングに関しても西側諸国と歩調を合わせず，GFCE などの西側諸国主導のイニシアティブには参加せず，どのような取り組みを行っているかをほとんど公表していない。中国が ARF の枠組みにおいてサイバーセキュリティのキャパシティビルディングに関するワークショップをマレーシアと共同で開催したことはあるが，それ以外の具体的な取り組みに関する情報は不明である。中露等が西側諸国とサイバーキャパシティビルディングを議論した場としては国連 GGE があるが，中国又はロシアが独自に行っているキャパシティビルディングについては触れられていない。第３回日中韓サイバー協議でキャパシティビルディングは議題に挙がっていたが，その詳細については公開していない[139]。GGE において，理念的にキャパシティビルディングの重要性については賛同するが，西側諸国と共同してキャパシティビルディングを行うことは考えにくい。裏を返せば，中露等のサイバー空間の在り方に関する同志国間でサイバーキャパシティビルディングを行い，自陣への取り込みのための働きかけや支援を行っている可能性は否定できないだろ

[139] http://www.mofa.go.jp/mofaj/press/release/press4_004250.html（最終アクセス日：2017 年 12 月 18 日）

う。その裏付けはないが,「情報セキュリティのための国際行動規範案」を SCO のメンバー国が共同提案しているのは，少なくともサイバー空間の在り方について国家主権中心，国家による強力な統制を重視するという理念を共有していることの表れであり，キャパシティビルディングは，国家安全保障連動型あるいは「新サイバー軍事同盟型」とも言えるサイバー空間の在り方を通じた新たな同盟関係を模索している可能性も否定できないだろう。

6.5 国際連合A型サイバーキャパシティビルディング:国際安全保障強化，国際協力促進型(国際協調促進型)

国連とその機関（総会第一委員会下の GGE，ITU，UNDP，UNODC，UNCTAD，UNIDIR 等）は，「国際の平和と安全を維持し，平和に対する脅威の防止及び除去と侵略行為その他の平和の破壊の鎮圧とのため有効な集団的措置をとること並びに平和を破壊するに至る虞のある国際的の紛争又は事態の調整または解決を平和的手段によって且つ正義及び国際法の原則に従って実現すること」を目的とする（国連憲章 1 条 1 項)。このため，これらの機関の目的はサイバーセキュリティの問題に関しても国際平和と安全の維持，すなわち国際安全保障にある。

また，国連総会の下に設置されたサイバーGGE は，国連総会の目的が，.「政治的分野において国際協力を促進すること並びに国際法の斬新的発達及び法典化を奨励すること」及び「経済的，社会的，文化的，教育的及び保健的分野において国際協力を促進すること並びに人種，性，言語又は宗教による差別なくすべての者のために人権及び基本的自由を実現するように援助すること」にあるため(国連憲章 13 条 1 項),その目的もこの範囲内，すなわち政治・経済分野等に係るサイバーセキュリティにおける国際協力の促進等に限られる。

国連とその機関は，国際安全保障と国際協力の促進を主たる目的とする組織であり，これはサイバーキャパシティビルディングについても当てはまる。国連を中心とする国際機関は，特定の国や地域のみのサイバーセキュリティの能力構築を支援するのではなく，全世界を対象に，サイバーセキュリティの能力の現状を調査，分析し，先進国と比してその能力を欠くか著しく低い国家を支援するために金銭的な援助や技術支援を行う，あるいは各地域機関，国家，民間企業や CERT コミュニティ等と調整して，その支援を要請することが国際機関としての目的に合致する。

国連の主なサイバーキャパシティビルディングのプレーヤーはITUであり，付属資料の103から113までの取り組み等サイバーセキュリティの意識啓発やCIRT構築支援等を原則として各国の要請に基づいて継続的に実施しているところである。全世界的なサイバーキャパシティビルディングを計画し実施できる意思と能力がある主体は限られ，この問題における国際機関が果たすべき役割は大きく，その継続的かつ実効性のある行動が期待される。ただし，付属資料109でもあるように，国連加盟国の3分の1程度しかCIRTの評価が行われていないなど，未だに各国のサイバーセキュリティの現状を把握しきれていない面もあり，より多くの国にサイバーセキュリティの重要性について喚起していくことが今後の課題と言えよう。

なお，国連サイバーGGEもサイバーキャパシティビルディングの具体的な措置を勧告し続けてきたが，主に西側諸国と中露キューバ等のサイバー空間に関する個別具体的な国際法の適用に関する見解の相違に起因すると考えられる第5回会合の失敗を受け，今後はその設置自体が困難な状況であり，これまで勧告してきた措置の実施や発展を他の国際枠組みや各国が継続することが重要となる。今後サイバーGGEが設置されなかったとしても，この枠組みが国連加盟国にサイバーセキュリティ問題を取り上げ，国際社会におけるサイバーの主な問題点を特定し，加盟国にサイバー問題の国際協力を促し，国際協力の具体的な提言を行ってきたことは評価に値し，仮に今後二度とGGE会合が行われなかったとしても国際社会はその遺産を活用し，発展させることがサイバー空間の平和と安定に資すると考えられる。

この国際安全保障や国際協力の強化を重視するアプローチは，一国のアプローチとしてみた場合は，自国の国益のみならず，他国と友好的な外交関係を構築することにより，国際社会で共存することを重視する国際協調主義（internationalism）と言い換えることができる。

6.6 国際連合B型サイバーキャパシティビルディング：開発援助延長型

国連とその機関は，全て国際安全保障と国際協力の促進という目的があり（5.5），また，各国の経済的問題の解決もまたその目的として掲げられている（国連憲章第1条第3項）。経済問題に取り組む国連の機関としては，国連総会とその補助機関（国連貿易開発会議（UNCTAD），国連開発計画(UNDP）等），経済社会理事会，専門機関として世界銀行グループ（国際復興開発銀行(IBRD)，国際投資開発センター（ICSID），国際開発協会（IDA），

国際金融公社（IFC），多数国間投資保証機関（MIGA)）などがある。これらの中で，積極的にサイバー問題に取り組んでいるのは既述の国連総会第 1 委員会の下に設置された政府専門家会合のほか，国連薬物犯罪事務所(UNODC：サイバー犯罪対策支援を実施）や国際電気通信連合(ITU：各国のサイバーセキュリティの状況を調査・分析)などがあるが，この他にも，国連開発計画(UNDP）や国連貿易開発会議(UNCTAD)は，開発援助（含持続可能な開発）や貿易，投資，金融等の分野において途上国の技術支援プロジェクトを実施している[140]。サイバー分野においても，例えば UNCTAD は西アフリカ経済共同体(ECOWAS)諸国やカリブ諸国の電子商取引に関する法制度整備支援を実施している（付属資料 115 から 119 参照）ほか，UNDP はキルギにおける電子医療サービス制度構築支援，グアテマラやアフリカ諸国における電子ガバナンス制度構築支援，西アフリカ諸国における電子政府への市民参加支援等を行っている（付属資料 93 から 97 参照)。このほかにも国連アフリカ経済委員会（UNECA）は，アフリカ諸国における社会経済発展のための ICT の意識啓発のためのワークショップや研修等を継続的に実施している(付属資料 99 から 102 参照)。これらは，サイバー「セキュリティ」という安全保障的性質が強い分野に関し，開発援助の観点から，例えばデジタル・デバイド（情報格差）の是正，サイバーセキュリティ強化による平和・安全な社会の構築支援，開発途上国自身の自発性と自助努力を重視したサイバーセキュリティのインフラ整備や法制度整備支援等のキャパシティビルディングを行い，開発援助・開発協力の延長としてサイバーセキュリティを再構築するものと捉えることができる。

なお，国際機関による開発援助（拠出・出資等）には，国家戦略のように，援助国の安全保障や被支援国・地域における援助国の企業の現地展開に向けた基盤形成等の国益追求という側面ではなく，世界全体のリスク低減や国際協力の促進という国際社会全体の利益追求が主な目的であるが，二国間援助（日本の例で言えば，贈与（無償資金協力及び技術協力）及び政府貸付等（有償資金協力：円借款（政府等向け）及び海外投融資（民間セクター向け））の場合には，被支援国自体の能力構築支援や強化等のほかに，こうした国家戦略が背景にあると考えられる。

二国間による開発援助には「アンタイド援助」と「タイド援助」という二種類に分類す

[140] 国連貿易開発会議（UNCTAD）
United Nations Conference on Trade and Developmenthttp://www.mofa.go.jp/mofaj/gaiko/unctad/gaiyo.html（最終アクセス日：2017 年 12 月 18 日）

ることができる。アンタイド援助とは，物資及びサービスの調達先が国際競争入札により決まる援助のことをいい，タイド援助（紐付き援助ともいう。）とは，これらの調達先が，援助供与国に限定されるなどの条件が付くものを指す[141]。そこでサイバーセキュリティに関する物資（機材）やサービスの提供についても，その調達先を国際競争入札により決めるのか，又は援助供与国に限定するのかで，アンタイド型サイバーセキュリティキャパシティビルディング又はタイド型サイバーセキュリティキャパシティビルディングの二種類が考えられる。援助国の国益重視であれば，タイド型，国際協調の要請を重視すればアンタイド型に当然傾く。また，タイド型の場合，物資及びサービスの調達先が援助供与国に限定されることにより，供与国の経済活動範囲の拡張，市場の開拓など経済効果が得られる反面，被援助国の反発を招きやすいデメリットがある。

6.7 地域機関型サイバーキャパシティビルディング：地域的安全保障・信頼醸成強化型

ARF，OSCE，OAS，AU 等の地域機関は，各地域における独自の特色はあるが，各地域の安全保障を促進・強化することを目的の一つとする点では一致している。

この中で ARF は，1）信頼醸成の促進，2）予防外交の進展，3）紛争へのアプローチの充実，という三段階のアプローチを設定して漸進的な進展を目指す枠組みを確立しており[142]，サイバー問題についてもこの枠組みに乗せて参加国及び機関の対話と協力を通じた安全保障環境の向上を目指した活動を続けている[143]。2018 年 1 月に行われた ARF のサイバーセキュリティに関する会合では，「ARF メンバーの協力を強化し，平和で安全で公正かつ協力的なサイバー環境を発展させ，能力構築を通じた相互の信頼醸成の促進により紛争や危機の防止に寄与する」とあることから，サイバーキャパシティビルディングを通じてアジア太平洋地域の信頼醸成を促進し，右地域における紛争を防止し，安全保障環境を向上させようとしていることが分かる[144]。

また，OSCE は，サイバー空間の利用に起因する紛争のリスクを軽減するための信頼醸

[141] http://www.mofa.go.jp/mofaj/gaiko/oda/shiryo/hakusyo/09_hakusho/honbun/b0/yogo.html（最終アクセス日：2017 年 12 月 18 日）
[142] 外務省：ASEAN 地域フォーラム（ARF）の概要 http://www.mofa.go.jp/mofaj/area/asean/arf/gaiyo.html（最終アクセス日：2017 年 12 月 18 日）
[143] 最も新しい例は 2018 年 1 月に行ったサイバーセキュリティに関する ARF 会期間会合のための第 1 回専門家会合（http://www.mofa.go.jp/mofaj/press/release/press4_005528.html）（最終アクセス日：2017 年 12 月 18 日）
[144] ibid.

成措置を 2013 年の外相理事会で初めて採択し，2016 年にも採択した[145]。この採択された措置の中で，OSCE をその参加国がサイバーセキュリティに関するキャパシティビルディングの情報等に関するプラットフォームとして利用することを明記している[146]。これは，欧州諸国は，第一の拠り所として OSCE が実施するサイバーセキュリティに関するワークショップやセミナー等を通じて，サイバーセキュリティについて学習し，信頼を醸成し合い，地域の安全保障を促進することを狙いとしていると読み取れる（OSCE のサイバーキャパシティビルディングの取り組みについては，付属資料 83 を参照）。

OAS についても，サイバーセキュリティに関するキャパシティビルディングや信頼醸成の重要性が共有され[147]，その理念に基づき，付属資料の 122 から 131 に掲げるサイバーセキュリティに関する意識啓発活動，研修，ワークショップ，演習，戦略策定支援等様々なキャパシティビルディングが継続的に実施されている。

このような地域機関は，サイバー問題に関しても，各地域の能力の構築を支援，強化することにより，国家間の信頼を醸成し，紛争を防止することにより，安全保障を促進するというアプローチを採用しているものと考えられる。

6.8 欧州評議会型サイバーキャパシティビルディング：サイバー犯罪条約普及・法制度整備支援型

欧州評議会（CoE）は，1949 年にフランスのストラスブールに設立された人権，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汎欧州の国際機関であり，一地域機関であるが，CoE が 2001 年に作成し，2004 年に発効したサイバー犯罪条約には，加盟国のうちロシアを除くすべての国が署名し（批准していないのは他にアイルランド，サンマリノ，スウェーデン），CoE 非加盟国の日本（2012 年 11 月発効），米国，豪州，カナダ，チリ，コスタリカ，ドミニカ共和国，イスラエル，モーリシャス，パナマ，セネガル，スリランカ，トンガが批准しており，2018 年現在，56 か国が批准国となっている[148]。

---

[145] DECISION No. 1202 OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES: https://www.osce.org/pc/227281?download=true（最終アクセス日：2017 年 12 月 18 日）

[146] ibid. 第 5 段落。

[147] Confidence Building Measures in Cyberspace　Presentation to the Inter-American Committee Against Terrorism (CICTE) of the Organization of American States http://www.oas.org/en/sms/cicte/Documents/2016/Speeches/JAMES%20LEWIS%20CSIS.pdf（最終アクセス日：2017 年 12 月 18 日）

[148] Chart of signatures and ratifications of Treaty 185 Convention on Cybercrimehttps://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=uqcnzKWF（最終アクセス日：2017 年 12 月 18 日）

CoE は，サイバー犯罪対処のための国際協力促進を目的とする「オクトパス会合」を年次で開催しており，サイバー犯罪条約委員会（T-CY）を設置し，サイバー犯罪条約を批准した国へのワークショップの実施等の支援活動を行い，かつ，法の支配の分野で国際社会の基準策定を主導とあるとおり，サイバー犯罪条約の締約国の拡大を目指し，T-CY を中心として欧州以外の地域や国に積極的に働き掛けている。しかし，人権，民主主義，法の支配等の価値観を重視していない国，欧州評議会という欧州地域の枠組みの主導を好まない国，サイバー犯罪条約第 32 条の「締約国は，他の締約国の許可なしに，次のことを行うことができる。（略） b 自国の領域内にあるコンピュータ・システムを通じて，他の締約国に所在する蔵置されたコンピュータ・データにアクセスし又はこれを受領すること。ただし，コンピュータ・システムを通じて当該データを自国に開示する正当な権限を有する者の合法的なかつ任意の同意が得られる場合に限る[149]」という点について，国家主権平等違反，主権侵害に繋がりかねないとして，サイバー犯罪条約の締結に否定的な国もある[150]。

サイバー犯罪条約の締約国の拡大，ひいてはその普遍化をも目指す T-CY の委員は，サイバー犯罪条約への加盟の意欲とその実施に向け準備を行っている国に対し，サイバー犯罪条約に合致するための国内法制度の整備支援を行っている。日本は 2012 年，アジア地域において初めてサイバー犯罪条約を締約した経験を踏まえ，アジア諸国への同条約の普及に積極的に参画しているが，現在のところ，アジア地域の同条約の締約国は，日本及びスリランカにとどまっている。しかし，前述のとおり，欧州のほぼすべての国は，T-CY の積極的な働きかけと支援もあり，締約国となっている（CoE のサイバーキャパシティビルディングの具体的な取り組みの概要については，付属資料 77 から 81 等を参照）。

6.9 GFCE 型サイバーキャパシティビルディング：支援者・被支援者マッチング・知見共有型

2015 年に行われたサイバー空間に関するハーグ会議（ロンドン・プロセス第 4 回会合）において立ち上げられた GFCE（サイバーの専門的知見に関するグローバルフォーラム：Global Forum on Cyber Expertise）は，サイバーセキュリティ，サイバー犯罪，データ保護，e ガバナンスという四つのテーマに関し，国家，国際機関，民間企業等が主体となり，

[149] サイバー犯罪に関する条約：http://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4a.pdf（最終アクセス日：2017 年 12 月 18 日）
[150] サイバー空間の施策に関するロシアと欧米諸国のアプローチ
佐々木 孝博 日本大学大学院総合社会情報研究科 atlantic2.gssc.nihon-u.ac.jp/kiyou/pdf14/14-001-012-Sasaki.pdf
（最終アクセス日：2017 年 12 月 18 日）

NGO，技術コミュニティ及び学界の協力を得て，サイバーキャパシティビルディングに関するベストプラクティスや専門的知見を共有するための機会を提供するプラットフォームである。各主体が行っている又は行うことを計画しているサイバーキャパシティビルディングの取り組み（initiative）の結果や現況，そこから得られた教訓等に関する情報を共有し，さらに，その取り組みに賛同する主体（支援側・被支援側双方）は，当該取り組みに参画することを歓迎するオープンな仕組みとなっており，国際社会においてどのようなサイバーキャパシティビルディングが行われているかが分からない途上国等の被支援者（recipient）にとっては，支援者（donor）にアプローチをする絶好の機会であり，支援者側も，通常外交関係がそれほど緊密ではない国家等に対しても，このプラットフォームを契機に，新たにキャパシティビルディングを通じて外交関係の拡大，強化を図ることのできる場と捉えることができる。また，ドナーは他のドナーとの関係を強化することもできる。GFCE はその理念に賛同するすべての国家，国際機関及び民間企業がメンバーとして参加することができ，また，これら以外の主体（NGO，研究機関，政府機関等）もパートナーとして専門的知見の共有を行うことができ，年次会合も開催しており，また，オックスフォード大学のサイバーキャパシティポータルとも連携し，右ポータルでは世界各地のサイバーキャパシティビルディングの取り組みの概要をまとめて公開している。

サイバーキャパシティビルディングのドナーとレシピエントの突合せの場とサイバーキャパシティビルディングの専門的知見の共有を継続的に国家のみならず様々な主体が一堂に会して行う場というのは稀であり，GFCE のメンバーやパートナーが増加し，支援者と被支援者が共通認識を醸成し，支援の形態等に合意できれば，二国間や特定の地域間で外交交渉で行うよりも効率的に二国間，多国間，多主体間の様々なサイバーキャパシティビルディングを創造する契機となる可能性を秘めている。ただし，その情報を当事者間以外のものに公開し，また，賛同する者を歓迎するというオープンな性質のため，キャパシティビルディングの内容を秘密裡に行いたい，又は当事者以外の関与を受けたくないという主体はメンバーやパートナーになる可能性は乏しいとも考えられる。しかし，サイバーセキュリティに関する様々な国際枠組みの議論にさえ参加する機会がない途上国等にとっては，サイバーキャパシティビルディングの取り組みに関する知見を習得し，ドナーに働きかける場としてその存在意義は小さくない。事実，GFCE の枠組みを活用し，アフリカ諸国等は欧州諸国とともに地域的な取り組みを開始している（付属資料 137 等を参照）。

7. 結論（提言）：日本型サイバーキャパシティビルディング：安全保障・外交・経済促進・国際協調折衷型

本研究は，第 5 次国連サイバーGGE の失敗を受け，今後のサイバー外交のパラダイムの変革期にある状況において，我が国としては積極的にサイバーセキュリティのキャパシティビルディングを推進すべきとの立場を論じるものである。

2016 年から 2017 年にかけて行われた第 5 次国連サイバーGGE は，サイバー空間を利用した国家の行為に対する国際人道法，自衛権，国家責任及び対抗措置等を含む従来の国際法の適用について西側諸国と中露キューバ等が激しく対立したため，合意が形成できずに失敗に終わった。このサイバー空間に関する国際的なルール作りの論点は，2012 年－13 年の第 3 次 GGE から既に両者の対立が顕著に現れていたため，今回の失敗はある程度予想できた事態ではあった。しかし，国際的な同意形成がなされないからと言っても，国際的なサイバーセキュリティの脅威は日々刻々と明白な危険として存在しており，ここで議論を終結することはできない。そこで，次の重要な論点は，これまで約 20 年近くにわたって進めてきた国連 GGE の議論を今後はどの枠組みで進め，また，どのような方法でサイバーの脅威に国際的に対処していけばいいかという点である。サイバー空間に関する国際的なルール作りとともに GGE でも継続して議論されていた信頼醸成措置とキャパシティビルディングの中で，日本が途上国への開発協力の分野で経験と知見が深いキャパシティビルディングである。日本は 1954 年 10 月 6 日にコロンボ・プランに加盟して以降，戦後補償に始まり，東南アジア諸国を中心に様々な国と地域へ無償資金協力，円借款，技術協力等の国際協力を行い，成功してきた実績がある。その協力では，手法としてキャパシティビルディング又はキャパシティディベロップメントのプロセスを用いたものも数多く存在する。4.で述べたとおり，日本は現在，ASEAN 諸国を中心に，政府開発援助（ODA）その他の政府資金等各種支援を，可能かつ適切な連携の下で技術協力を中心にサイバーセキュリティのキャパシティビルディングを実施している。JPCERT/CC は東南アジアやアフリカ諸国の CSIRT 構築支援及び強化を 2000 年代後半以降数多く行い，これらの諸国の CSIRT 職員や政府関係者等の研修，現地への専門家への派遣等を継続的に行い，技術的なキャパシティビルディングを実施している（日本の主なサイバーキャパシティビルディングの取り組みは付属資料 1 から 5 を参照。）。手法は技術協力が中心であり，途上国政府のサイバーセキュリティ態勢作りの支援（意識啓発，制度・政策面，機構面の知見の提供）

や機材・設備の運用能力の向上支援（技術面の知見提供，人材育成）を展開している。他方，サイバーセキュリティの確保に必要な機材や設備の供与等資金協力には消極的である。確かに，機材や設備の供与には人材育成等に比べて大きなコスト負担を要するが，GGE の失敗を受け，西側諸国と中露陣営双方の途上国の取り込み・働きかけの契機であり，この間に例えばアジア諸国に中国が潤沢な資金によって囲い込みを行い，その影響を受けたサイバー空間の規制，つまり国家主権によるサイバー空間の管理・統制の強化に傾斜してしまう危険性があることは看過できない。また，脆弱な東南アジア諸国の途上国等を経由して行われる日本の政府や企業へのサイバー攻撃が多数確認されているのは事実であり，その脆弱性をなくすためにそれらの国々を支援することは，日本の安全保障に直結するのである。したがって，日 ASEAN 統合基金(JAIF2.0)等を積極的に活用し，5.1 で述べた「安全保障連動型」のサイバーキャパシティビルディングを展開する必要がまずある。この点，2017 年 12 月，薗浦健太郎内閣総理大臣補佐官がベトナムを訪問し，防衛省によるベトナム人民軍に対するサイバー分野の能力構築支援事業の開講式に参加したのはこの方向性に沿うものである[152]。ベトナムに限らず，今後はメコン 5 か国の軍事的能力構築支援を含めたサイバーセキュリティキャパシティビルディングに期待したい。ただし，憲法 9 条等との関連で，軍事的な援助を公に幅広く展開するのは避けるべきであり，水面下での調整・歩調合わせを密に行い，技術支援及び人材育成を継続的に実施しつつ，資金援助も検討すべきと考える。

次に，5.2 に関し，英国型のキャパシティビルディングの積極的な外交的利用の手法も取り入れるべきである。英国は GCCS の創設や GCSCC の設置等により，閣僚クラスの人間がその存在感を誰よりも先にアピールした。サイバーセキュリティ能力の成熟度モデルなど，その手法は必ずしも画期的・斬新なものではないが，最初にそのようなモデルを発表し，それに向けて，各国が注目し，関心を持つようにする外交力に長けている。この点，日本のサイバー外交は後手後手に回っており，サイバーグリーンや CYDER など，取り組んでいるキャパシティビルディングの内容は他国に引けを取らないものであるにもかかわらず，その広報力に乏しい。英国は，大学，在外公館ネットワークやサイバーセキュリティ関連企業，警察組織，議員機構，検察機構等「オールイギリス」によるサイバーキャパシティビルディング政策を推進しており，我が国もこれに習い，日本のサイバーセキュリ

[152] http://www.mofa.go.jp/mofaj/s_sa/sea2/page3_002328.html（最終アクセス日：2017 年 12 月 18 日）

ティ関連企業や学界等の積極的な国際展開を慫慂すべきであり，また，これと連携して日本のサイバー外交を推進すべきと考える。この点，近時 NEC が総務省主催のサイバーセキュリティ演習に協力する動きがあるのは良い方向に向かっていると思われるが，未だに政府主導のサイバー外交が見受けられるため，既に積極的な国際協力・国際展開を行っている JPCERT/CC 等を模範に，今後は真の「オールジャパン」によるサイバー外交の展開による日本のプレゼンスの向上を図るべきである。

5.3 に関し，エストニア型のスモールパワー特化型のキャパシティビルディングは国家規模や他の課題からこれを採用することはできないが，ミドルパワー外交すなわち「軍事力を最終的な拠り所とする「大国」による権力政治の舞台ではなく,,「大国」が規定する国際システムを所与としそれ以外の領域（多国間協力など）に外交資源を投入して影響力を発揮する外交」[153]を参考に，多国間協力によるキャパシティビルディングを展開することは日本の国益に資する。国際的なルール作り等の国際レジームの主導的な役割は米国等の超大国に委ね，それ以外の領域，キャパシティビルディングを通じて，自由主義的かつ民主主義的なサイバー空間の統治を理想とする体制を国際社会の多数派にするための国際協力の担い手となり，欧米諸国中心の自由主義・民主主義の基本的価値とアジア的価値観の双方の特性を有する日本の独自の強みを生かして，両地域の架け橋となることが日本の責務であり，また，日本が目指す方向と考える。

5.4 の点について，中露等の非公表非国際協調型とも捉えられるキャパシティビルディングのアプローチは，国家の政策手段の一つとしては特に規制もなく，認め得るものかもしれないが，国際協調主義（憲法前文，9 条，98 条 2 項等）を採る我が国とは相容れない政策であり，日本が採用することはできない。サイバー空間が世界中のインターネットが国境を越えて繋がっている仮想空間と考えると，サイバーセキュリティの問題は一国のみで対処することは不可能であり，国際協調が不可欠であり，協力には信頼醸成措置や透明性の向上以外にも，専門的知見やベストプラクティスの共有，支援を要する国や地域に対する先進国として義務とも言える援助，オフラインにおいても尊重される表現の自由等の人権や基本的自由はオンラインにおいても尊重されるべきであり，オフラインで適用される従来の国際法はサイバー空間という情報通信技術を利用した行為に対しても適用されるべきであり，これを否定する政策をとることは許されない。ただし，中露等がサイバー問

[153] 添谷 芳秀『日本の「ミドルパワー」外交―戦後日本の選択と構想』2005, 筑摩書房

題全般に関して同盟型とも言える，サイバー空間のあり方に関する価値観について歩調を合わせ，その「味方」を募る手法自体は，採用し得る。我が国の場合は，例えば，サイバー問題に関し，東南アジア諸国へ働きかける際に，情報の自由な流通，マルチステークホルダー・アプローチ，従来の国際法の適用等の立場を推進し，これとは立場を異にする中露等（国家主権に基づく国内管理の優先，国内法に基づくサイバー空間における表現の自由等基本的人権の制限等）の影響力を避けるために，対中露等サイバー同盟とも言えるアプローチは必要であり，キャパシティビルディングを行う際にはそれを常に念頭に置くべきである。

次に，5.5 の国際協調促進型のキャパシティビルディングというアプローチについて，無償資金協力という観点からは，前述のとおり JAIF2.0 等を活用して，機材や設備の供与などを行うのは今後の課題であるが，これを純粋な国際協調と捉えるのは適切ではない。ASEAN 諸国やアフリカ諸国に人道的見地や憐憫の情を持つがゆえに無償資金協力を行うのではなく，被支援国には支援の必要があり，その必要を満たす支援を行い，両国の関係を強化し，別の案件で支援国が被支援国の協力を要する場合に，友好な関係に基づき，「友人」として，協力に応じるような関係性を構築するのは外交上日常茶飯事であり，同盟や友好，協力の裏には常に何らかの真意があり，それは国益の最大化である。サイバーセキュリティはあくまで「セキュリティ」の問題であり，最大の関心事は安全保障である。このため，人道援助等では純粋な国際協調は有り得るかもしれないが，サイバーセキュリティの分野では妥当ではないと考える。しかし，開発協力大綱にもあるように「我が国の平和と安全の維持，更なる繁栄の実現，安定性及び透明性が高く見通しがつきやすい国際環境の実現，普遍的価値に基づく国際秩序の維持・擁護といった国益の確保に貢献する」形での国際協力・開発協力，言い換えると，安全保障を念頭に置いた「積極的平和主義」による国際協調は採用すべきである。アジア太平洋諸国やアフリカ諸国の脆弱なサイバー空間は日本及び世界全体のリスクであり，そのセキュリティの強化支援を行うことは，日本を含む世界全体のサイバーセキュリティリスクを軽減させ，同地域におけるネットワーク等の重要インフラに依存する在留邦人や日系企業の安全保障に繋がるため，この観点からの国際協力は重要である。

5.6 の開発援助延長型の紐付きのキャパシティビルディングを展開するのも日本国の国益に資する。ここで紐付きと言うものの，これを緩和し，援助供与国であるの日本のみに機材やサービスの調達先を限定するのではなく，日本と被援助国に限定という条件にする

のも一案である。すなわち，日本の企業等の現地市場の展開による我が国の経済活動の拡大のみならず，支援国の企業や団体等もその調達先として受け入れることにより，現地自身による能力の構築を促進することは，キャパシティビルディングないしはキャパシティ・ディベロップメントの精神にも合致し，両国がウィンウィンの関係になる。むろん資金力の差で，日本企業ばかりが落札してしまう場合が生じ得るが，それについても，例えば，Ａの案件については両国による入札，Ｂの案件については被支援国の優先的入札権など，一方に偏らないような配慮をすればよい。この開発援助型のキャパシティビルディングは，安全保障連動型と双璧をなす経済面の能力向上として重要である。なお，UNODC 等の国際機関への拠出による間接的な開発援助も従来どおり重要であるが，より日本企業の現地展開を推進し，日本のプレゼンスの向上という観点からは，二国間援助の方が直接的な援助で政策を表しやすく，より効果的であると考えられるため，例えば GFCE の枠組み等を利用した新規支援対象国の開拓等を行うのも一案である。ただし，これまで援助を積極的に行っていない国や地域あるいは外交関係が緊密ではない国や地域から新たに関係を強化し，サイバーキャパシティビルディングを行うのは相当な時間を要する場合もあるため，支援対象国・地域の開拓は重要であるが，それよりも優先的に取り組むべきは既に支援を積極的に行い，良好な外交関係を構築・維持している国や地域へのサイバー分野での新たな支援であり，この観点から，引き続き ASEAN 諸国の人材育成や JAIF 等の基金を活用して，東南アジア諸国を中心とする国への積極的なサイバーセキュリティキャパシティビルディングを展開し，そのセキュリティの強化により，我が国の安全保障を確保するとともに，我が国企業による被支援国の援助事業を促進させ，支援国とともに日本経済の強化を図り，サイバー空間の統制のあり方としては自由で安全かつ開かれたサイバー空間の統治のためにプライバシーや人権が尊重され，法の支配が適用され，経済及び社会の発展のために国際社会の平和と安全及び個々の人々が安心して利用できる情報通信技術の環境を整備することが重要であり，そのための有効的なツールとして，サイバーセキュリティのキャパシティビルディングをオールジャパン体制で積極的に展開することが求められていると考えられる。ここでいう「オールジャパン体制」とは，各省庁や地方公共団体，民間企業，学術・研究機関，技術コミュニティ，NGO，市民社会等の支援主体が個別にそれぞれの方針・戦略に従ってバラバラに支援を行うのではなく，各主体が共通の方針の下に，調整し合い，それぞれの強みを活かして，適切な役割分担を行った上で途上国のキャパシティビルディングを行うことを意味する。このため，そのような調整機能が適切に発揮で

きる日本サイバーキャパシティビルディングセンターのような司令塔の存在が名実共に必要であろう。現在，この機能に最も近いのは内閣サイバーセキュリティセンター(NISC)であるが，その調整権限等の強化のための制度改革も検討すべきであろう。

5.7 のサイバーキャパシティビルディングを通じた信頼醸成も積極的に推進すべきである。特に ARF の枠組みなどを活用し，自国のサイバーセキュリティ戦略等の関連施策動向や脅威認識に関する情報共有や二国間，多国間のサイバー対話の継続的な実施，重要インシデント時のコンタクトポイントに関する連絡体制の整備，サイバー演習の共同実施等を通じて透明性・信頼を高め，相互理解を促進することは，地域の安定・安全保障に資すると考えられる。ただし，自国に対してサイバー攻撃を行っていると思われる国（例えば，ARF の枠内で言えば，中国や北朝鮮等）との機微な情報の共有には注意を要する。これらの国への脅威に関する情報共有等は，むしろ自国の手の内を明かすことにより，安全保障上問題になる虞がある。地域のサイバー空間の安全，安定を脅かす存在との信頼醸成の必要性を常に考え，あくまで安全保障を強化できるための信頼醸成，そしてそのためのキャパシティビルディングを行うべきであり，緊急時の連絡窓口の明確化や定期的な対話等はこれに資すると考えられるが，サイバー演習や脅威情報の共有等には慎重を期する必要があるだろう。

5.8 の法制度整備支援型のキャパシティビルディングは，日本も警察庁，法務省，外務省等が連携して ASEAN 諸国等を中心に積極的に実施している分野であり，今後も継続して行うことがアジア地域の安全，安定と日本の安全保障に資するものである。アジア諸国等がサイバー犯罪条約を締結すると，締約国である日本や欧米諸国等の国境を越えたサイバー犯罪対策が円滑になり，サイバー犯罪に係る犯罪人の引渡し等の国際連携が強化される。国境を越えて行われるサイバー犯罪は一国のみでの対処は困難であり，かつ，迅速な対応が要求されるため，国際捜査共助に係る協力の強化，円滑化は不可欠である。また，このアプローチは，サイバー犯罪条約の普及とそれに基づく法制度整備支援を行うことにより，サイバーセキュリティに関する独自の条約の普及を目論む中露等陣営側に被支援国を取り込まれることをけん制する効果も期待できる。2014 年に引き続き第 2 回日 ASEAN サイバー犯罪対策対話が 2017 年に実施されたのは正にこのアプローチに係るものであり，ASEAN 諸国との関係のさらなる強化とサイバー犯罪条約の普及を実現するために，今後も積極的に取り組むべき手法である。

5.9 の支援者・被支援者マッチング・知見共有型キャパシティビルディングについては，

5.6 でも述べたとおり，GFCE のような枠組みを自国に設置する必要はないが，日本の政府機関や CERT，民間企業等が実施しているサイバーキャパシティビルディングの取り組みを紹介し，パートナーや支援を希望する主体を探す機会として GFCE 自体を有効活用すべきである。特に，ASEAN 諸国に対するキャパシティビルディングについては，ARF 等の地理的に近い枠組みにおいて接する機会があるが，それ以外の国や地域，国際機関等とサイバーキャパシティビルディングについてピンポイントで話し合う場として利用するのに適していると考えられる。また，GFCE のメンバーである日本（政府）は，オールジャパン態勢という観点から，サイバーキャパシティビルディングに意欲がある日本企業等にも積極的に参加するよう慫慂すべきである。ただし，GFCE はあくまでこうした支援者と非支援者を繋ぐプラットフォームの一例であり，GFCE 自体に拘る必要はなく，重要な点はサイバーキャパシティビルディングに参画する意思と能力がある日本企業や日本の政府機関以外の主体が国際場裡において他国のサイバーセキュリティ関連企業との競争に負けないような存在感を発揮できるように日本政府が支援することである。

サイバーキャパシティビルディングを実施する対象として，現在アジア大洋州が，歴史的な関係や基本的価値観の共有，国民相互の往来，経済活動の増加等から「キャパシティビルディングへの協力，情報の収集や発信を強力に推進していく」地域と指定している（サイバーセキュリティ戦略 5.3.3(1)参照）。この点，この方針には賛同する。これまで長年にわたり伝統的なキャパシティビルディング等の開発協力等を通じて，アジア大洋州地域の国々との良好な関係を維持，強化してきた信頼の基盤が構築された上で，新たにサイバー分野における支援を行うことについては，外交関係が希薄で，良好な関係の構築から開始する支援よりも，ARF や年次で行われる日 ASEAN 情報セキュリティ政策会議等を通じて円滑かつ迅速にサイバーキャパシティビルディングを実施できる可能性が高く，実際，日 ASEAN 間のサイバーセキュリティに関する協力は年々強化されており，この流れを今後も重視し，より強固な関係を築くとともに，対中国を念頭においた安全保障アプローチを心掛けるべきである。また，GFCE や TICAD（アフリカ開発会議）の枠組み等を活用し，サイバーセキュリティ戦略において，「キャパシティビルディング等の連携・協力の可能性を検討していく」とされた中南米や中東アフリカ諸国に対する支援の模索を本格化していい時期にあると考える。

以上の提言をまとめると，日本のサイバーキャパシティビルディングとして次のようなアプローチをとるべきである。

第一に，日本国，日本企業，日本国民等の安全保障の強化・促進という目的のために，日本へのサイバー攻撃の踏み台になっているが，歴史的に良好な外交関係を維持し続けている東南アジア地域を中心とする国の脆弱なシステムやネットワークのセキュリティ能力の構築支援のさらなる強化と当該地域との信頼の醸成と強化を技術コミュニティや刑事司法関係者，民間企業等と連携し，かつ，日 ASEAN 統合基金(JAIF2.0)を有効活用し，技術面，金銭面から行い，サイバー空間のリスクの低減に貢献すること。

第二に，国際社会における日本のプレゼンスの向上という目的のために，在外公館ネットワークや GFCE，TICAD 等の枠組みを利用し，東南アジア諸国以外の潜在的に支援対象国となり得る国への働きかけを積極的に展開するとともに，軍事力の間接的な支援等機微な情報以外の既存の又は今後計画しているサイバーキャパシティビルディングの取り組みを国際社会にアピールすること。

第三に，日本企業の現地産業基盤の確立と経済の強化という目的のために，日本企業に積極的に働きかけ，支援を慫慂し，開発協力大綱の方針のような支援国の自発性と自助努力を支援しつつ，被支援国の要請への応対のみならず，積極的な提案を行い，日本と支援国の企業等に限定した緩やかなタイド型開発援助を行い，中国企業等他の支援国との競争に勝てるような関係と態勢を構築すること。

第四に，大国でもなく，小国でもなく，西側諸国とサイバー空間の在り方に関する基本的価値観を共有しつつ，東南アジア諸国とも良好な関係を東西の架け橋とミドルパワーとしての独自の強みを生かすため，キャパシティビルディングを通じた安全保障や経済促進を推し進めつつ，安全保障のための国際法適用一辺倒で大国との対立を深める強硬的なアプローチをとらず，また，表現の自由等基本的人権を軽視し，国家によるサイバー空間の管理の強化をし，サイバー軍事同盟型ともいえる中露等の道は歩まず，各国，各地域の事情を踏まえ，キャパシティビルディングを含む国際協力を強化することにより国家間の信頼を醸成し,紛争を予防するという国際協調路線を維持し,その存在意義を発揮すること。

第五に，真のオールジャパン体制を確立するために，上記のそれぞれの措置を，日本の各ステークホルダーと連携・調整する統一的な機能を持った機関の設置あるいは現存する内閣サイバーセキュリティセンター等の機能・権限を強化することにより，日本のサイバーセキュリティの司令塔的役割を担わせ，各省庁，技術者・研究者コミュニティ，民間企業等の資源を有効活用し，適切な分掌を行わせることにより，支援の重複を避け，効率的かつ実効性のあるサイバーキャパシティビルディングを行える態勢を整備すること。

本研究においては，中国語やロシア語の知識がないせいもあり，中国やロシアのサイバーキャパシティビルディング政策の調査がほとんどできなかったのは痛恨の極みであるとともに，今後の課題である。今後もこれらの国々や日，米，英，国連，ARF，OSCE，SCO，OAS，ITU 等が繰り広げるサイバー外交の展開に注視し，特に我が国の官民学等の連携によるサイバーセキュリティキャパシティビルディングの積極的な進展に期待したい。

さらに、近年、特にサイバー攻撃の対象となっているのは重要インフラ（日本の場合情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット及び石油の 13 分野を想定）であり、その制御ネットワークを如何にして防護するのかが大きな課題となっている。こうした制御ネットワークは、たとえ物理的にネットワークが外部とつながっていなくてもスタックスネットの例があるように、USB メモリ等を経由してサイバー攻撃を仕掛けることは可能である。業務上の関係がある以上、サイバー攻撃のリスクが存在すると考えなければならない。情報セキュリティ大学院大学の後藤厚宏学長・教授が指摘するように、システムの調達や業務のアウトソーシング等のサプライチェーンのリスクの再点検が重要である[154]。途上国を含む外国から調達した機器やシステムにバックドアが仕掛けられていたり、マルウェアが埋め込まれるリスクがある。サイバー攻撃者が、日本政府や日系企業、日本人を狙わず、日本に輸入されるシステム供給者を標的にすることは十分考えられる。このため、輸出先において、こうしたリスク点検の徹底を要求することを義務化し、その点検ができない一定程度の水準以下のセキュリティの国にはその製品を輸出できないようにする国際的な取り決めを途上国に課すことも有益と考えられる。そして、そのような水準のセキュリティに達するまでのキャパシティビルディングを日本が行うべきではないだろうか。

[154] IPACSS2017「講演 2：IoT 時代のサイバーセキュリティ確保に向けて」（https://www.youtube.com/watch?v=9f-BVPRNk8c）（最終視聴日：2018 年 2 月 24 日）

8. 謝辞

本研究は, 2012 年 10 月より筆者が外務省安全保障政策課のサイバー政策専門員として, サイバー外交の実務についた後，2014 年 10 月より情報セキュリティ大学院大学情報セキュリティ研究科に在籍した時から進めたものである。

慶應義塾大学法学部在籍時から 10 年以上お世話になっている指導教員の湯淺墾道教授と林紘一郎教授に深く感謝したい。また， 3 年間サイバー外交実務の最前線を経験させていただいた外務省にも謝意を表したい。

付属資料１．サイバーキャパシティビルディングに関する取組の一覧[156]

※国名は，『外務省記録総目録　戦前期』「主要宛字一覧」を基本として慣行的に使われている略称を用いている。

名称	ドナー（支援主体）	パートナー	レシピエント（支援対象）	対象グループ	主たるテーマ	目的・目標	具体的活動	（想定される）成果・効果	時期
1.「サイバーグリーン」イニシアティブ	サイバーグリーン研究所 （日本）	JPCERT/CC 及び英外務・連邦省 （資金提供）	全世界	サイバーセキュリティインシデントレスポンスチーム（CSIRT），ネットワーク運営者及び政策立案者	サイバーエコシステムの健全性のメトリクス，測定，被害防止	·グローバルな「サイバーエコシステム」の健全性を高めることを支援するのに特化した活動の実施 ·CSIRT，ネットワーク運営者及び政策立案者に信頼できるメトリクス，測定及び被害防止に関するベストプラクティスの提供	·サイバーの健全性測定 ·リスクデータのソーシング ·リスク軽減のための情報センター（クリアリングハウス）の提供 ·キャパシティビルディング ·アドボカシー	システムの機能の浄化の促進，政策策定とキャパシティビルディングがシステミックリスクの軽減を重視する内容であることの確保	2015 年 4 月以降，全世界に公開
2. 日 ASEAN 情報セキュリティ意識啓発イニシアティブ	日本及び ASEAN 加盟国	特になし	ASEAN 加盟国	政府職員，国民	サイバーセキュリティ意識啓発	同左	共同意識啓発ポスターの作成，教育材料の ASEAN 加盟国の母国語への翻訳及び日 ASEAN 間の資料の共有	ASEAN 諸国の政府職員や国民のサイバーセキュリティの意識啓発	2012 年以降毎年
3. 尼の情報セキュリティ能力向上プロジェクト	国際協力機構（JICA） （日本）	情報セキュリティ専門家等	尼	通信情報省	サイバーセキュリティ，情報セキュリティ，インシデントレスポンス	尼通信情報省(MCIT)の情報セキュリティ対処能力の向上	日本側からのインプット： ·JICA 専門家の長期派遣(チーフアドバイザー，情報セキュリティ専門家及びプロジェクト・コーディネーター) ·研修 ·機器，ソフトウェア等 尼側からのインプット：	（想定される）全体成果 1. 情報セキュリティ局の機能強化 2. 政府の各部局におけるセキュアな IT 利用をサポートする仕組みの確立 3. 情報セキュリティ啓発活動の改善	2014 年 7 月 23 日から 2017 年 1 月 22 日

[156] Global Cyber Security Capacity Centre: Cybersecurity Capacity Portal 参照(https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/gfce)（最終アクセス日：2017 年 12 月 18 日）

							·カウンターパート ·事務所等の職場環境	個別成果 1 1.情報セキュリティ局の組織構成と要員スキルの再設計 2.要員の技術スキル向上 3.情報セキュリティ対策の将来トレンドを知るためのネットワークづくり 個別成果 2 1. Index KAMI（尼版 ISO27001）導入支援体制の構築 2. CSIRT 導入支援体制の構築 個別成果 3: 1.啓発対象者への普及方法の確立 2.啓発用教材の開発	
4. サイバー犯罪対策	国際協力機構（JICA） （日本）	警察庁	アジア：孟，印，尼，馬，蒙，緬，パキスタン，比及び錫 アフリカ：ボツワナ，象及びセーシェル ラテンアメリカ：ボ	国家警察のサイバー犯罪対策担当課	サイバー犯罪	法制度，捜査手法・技法及び民間セクターとの協力を含むサイバー犯罪対策に関する日本の知識及び経験を学ぶこと	プレゼンテーション，ディスカッション，講義，実地見学を含むサイバー犯罪に対する対抗措置のために特別に設計されたグループ研修コース	·サイバー犯罪に関する現況及び参加国が実施している対抗措置の共有 ·サイバー犯罪に対する法制度，捜査手法・技能，対抗手段及び日本の民間セクターとの協力についての説明 ·サイバー犯罪の分野における国家警察機関間の効果的な連携及	2015 年 1 月から 2 月

			リビア，墨及びパナマ					び協力のためのネットワークの構築	
5. 日 ASEAN 情報セキュリティ協力	日本及び ASEAN	NEC 等	ASEAN 加盟国	政府職員	サイバーセキュリティ	政府職員のサイバーセキュリティ能力の向上	日 ASEAN 情報セキュリティ政策会議（2009 年以降毎年開催） 演習（CYDER），ワークショップ，研修	脅威に関する情報共有，演習，ワークショップや研修を通じた日 ASEAN 諸国政府の総合的なサイバーセキュリティ能力強化	2009 年以降
6. 星国家サイバーセキュリティ研究・開発プログラム	星国家研究財団(NRF)，防衛省(MINDEF)，内務省(MHA)，国家安全保障調整センター，星情報通信開発庁，サイバーセキュリティ庁及び経済開発庁(EDB) （星）	英 ESPRC（工学・物理科学研究会議）（資金面）	星	政府機関，学界，研究機関及び民間部門	·拡張可能な信頼できるシステム ·レジリエントなシステム ·効果的な状況認識及び攻撃の特定 ·内部者脅威対策 ·脅威検知，分析及び防衛 ·効率的かつ効果的なデジタルフォレンジック	国家の戦略的なセキュリティニーズを満たすサイバーセキュリティの研究及び開発能力を構築すること	5年間で1億3千万星ドルの資金による6つのテーマに関する研究開発	①拡張性があり信頼できるシステムの構築 ②強靭なシステムの構築 ③効果的な状況認識及び攻撃の帰属の確保 ④内部者の脅威対策 ⑤脅威の検知，分析及び防衛 ⑥効率的かつ効果的なデジタルフォレンジックの確保	2016 年以降
7. 相互発展のためのサイバーセキュリティ連合(CAMP)	韓国未来創造科学部(MSIP)及び韓国インターネット・セキュリティ庁(KISA) （韓国）	特になし	全世界	サイバーセキュリティ関連政府機関，公的団体及び非営利団体 会員制：CAMP の会員になりたい者は，事務局へ申請	サイバーセキュリティ，サイバー脅威，キャパシティビルディング，国際協力	より安全なサイバーセキュリティ環境を確保するためのグローバルな協力基盤を構築し，サイバーセキュリティにおける共栄のためのパートナーシップを構築すること（以下，具体的目標） ·双方向型国際社会の形成のためのグローバルなヒトのネットワークの構築 ·最新のサイバーセキュリティの傾向及	·メンバー間のインタラクティブな国際コミュニティを構築するための年次会合又はフォーラム ·メンバー間の非公式会合又はネットワーキングは，特定のサイバーセキュリティ問題の解決策を議論，模索するために自由にアレンジすることができる。 ·サイバーセキュリティ関連ニュース及び	CAMP 準備会合が 2015 年 6 月に開催され，29 のメンバー国候補が参加。 また，サイバーセキュリティに関するグローバルな協力の重要性についてコンセンサスが得られた	2016 年 7 月 13 日以降

				書を提出。会員は書面による請求よって自由に脱会す可能		び戦略的国家政策に追いつくためのサイバーセキュリティ問題に関する情報共有 ·グローバルな場における政治的影響力を強化するためのサイバー問題への集団的対処	最新の問題は，メンバーが頻繁に交流するためにCAMP ウェブサイト又は e メールを通じて共有	ため，正式な立ち上げ前に「CAMP 宣言」が採択された。	
8. 開発のためのグローバルサイバーセキュリティセンター(GCCD)	韓国インターネット・セキュリティ庁(KISA) (韓国)	特になし	全世界	途上国におけるサイバーセキュリティ専門家及び職員	サイバーセキュリティキャパシティビルディング	サイバーセキュリティ戦略及び政策の策定計画の作成，知識及び経験の共有並びにサイバーセキュリティ能力の強化により途上国のサイバーセキュリティ及び経済成長の水準を改善すること	キャパシティビルディング ·招待ベースの研修コース ·途上国における共同セミナーの主催 ·サイバーセキュリティ能力成熟度評価の実施とそれに基づく研修 ·サイバー防衛のためのオンラインハンズオン研修 協議 ·サイバーセキュリティ管理協議 ·サイバーセキュリティ技術評価 ネットワーキング ·国際機関，地球規模の研究所等とのパートナーシップの拡大 ·地球規模の会合及びフォーラムの主催	グローバルレベルな協力と知識の共有に取り組むため，GCCD は一連のプログラムを実施。 ·2015 年 9 月，韓国で開かれた「国家サイバーセキュリティ政策研修コース」に 13 カ国から 20 人の政府職員が参加 ·2015 年 11 月，コスタリカ，秘，蒙，印及び越において，それぞれの国の個別の議題について共同セミナーを開催。	2015 年 6 月 1 日以降
9. ASEAN サイバー大学	東南アジア諸国連合(ASEAN)	ソウル大学	カンボジア，ラオス，ミャンマー，越(CLMV)	学生	教育	1.ASEAN 諸国間の開発格差を解消し，ASEAN の地域統合の取り組みを支援すること 2.教育の協力及び人材交流を促進すること	·CLMV 諸国における e ラーニングセンターの試験的運用 ·ASEAN 韓国サイバー大学の設置：ASEAN e ラーニングポータル及び韓国−CLMV カリキュラムマネジメントの構築	ASEAN 諸国の学生のサイバーセキュリティ能力の強化	2009 年以降

							·ASEAN-韓国サイバー大学の拡張：e ラーニング及び研究の連携を通じた韓国及び ASEAN におけるハブ大学としての出現。 韓国と CLMV 諸国は，e ラーニングセンターを以下の機関に設置することで基本合意した。： カンボジア：カンボジア工科大学(ITC) ラオス：国立ラオス大学(NUOL) ミャンマー：工科大学(UT) 越：ハノイ科学技術大学(HUST)		
10. ASEAN 単一窓口(ASW)プロジェクト	東南アジア諸国連合(ASEAN)	特になし	ASEAN 加盟国	税関当局等	サイバーセキュリティ，オンラインデータセキュリティ，電子アーカイビング，ASW のためのセキュアな送信及び技術アーキテクチャ	目的： ·シームレスで安全な国境を越えるオンライン取引及び e コマース活動が ASEAN 内で行えるような環境を作り出すこと ·各加盟国が国際オープン標準を活用するいかなる貿易相手国ともデータを安全かつ確実に交換できることを確保しつつ，各加盟国単一窓口と国際オープン通信標準との適合性を確保すること ·より単純かつ高速な処理速度を実現し，より透明性が高い営業手法にすること	·ASEAN 内の原産地証明書(ATIGA 様式 D）及び ASEAN 税関申告書(ACDD)を7加盟国間で試験的に交換することを支援し，その後他のデータの交換の拡張を検討 ·非 ASEAN 貿易当事国との原産地証明書の交換を支援し，貨物情報を推進 ·法的相互運用性，ASEAN の政策調和努力(植物検疫措置等)の支持及び加盟国間のデータ交換の理解の深化等漸進的利益の促進 ·制度面として，ASW 運用委員会の設置と技術及び法ワーキンググループの支援 ·民間セクターとの協議及び ASW 持続	ASEAN 加盟国の税関手続の標準化，格差解消等	2013 年以降

						目標: ·経済統合が進む ASEAN 内における貨物通関の迅速化	可能性研究等のその他の付属的イニシアティブ		
11. データプライバシー・パスファインダー計画	アジア太平洋経済協力(APEC)	APEC 参加国・地域	豪州，加，智，中国，日本，韓国，墨，新，秘，台湾，泰，米，越	政府機関等	プライバシー及びデータ保護	目的：APEC 参加国・地域が協力して「APEC プライバシー枠組み」の実行に取り組めるようにすること 目標：·概念的枠組み原則·協議プロセス·実用的な文書·実行·教育及びアウトリーチ	2004 年に APEC 首脳が採択した APEC プライバシー枠組みに合致した越境プライバシー規則(CBPR)制度の構築及び実施	・越境プライバシールールの実施のための枠組みの構築。 ・9つのプロジェクトを実施中。	2007 年以降
12. サイバーセキュリティ及びサイバー犯罪対策ワークショップ	米国務省	アフリカ連合委員会(AUC)，西アフリカ諸国経済共同体(ECOWAS)	アンゴラ，伯，カーボヴェルデ，ガーナ，ケニア，モーリシャス，モザンビーク，ナイジェリア，葡及びサントメ・プリンシペ	政府職員	サイバー犯罪対策，携帯電話のセキュリティ，インターネットの自由，アクセス及びアフォーダビリティ並びに国家 CERT の構築等	アフリカの葡語圏の特定の利益に係る問題を中心に，その他サイバー犯罪及びサイバーセキュリティの広範な問題の対処	ワークショップ	西アフリカ諸国の政府職員のサイバーセキュリティに関する意識啓発，教育	2015 年 9 月に実施
13. サイバーセキュリティ研究プログラム(PCSS)	ジョージ・C・マーシャル欧州安全保障研究センター（米独国防当局）	サイバーセキュリティ専門家	米国内	参加者はサイバー法，政策の策定担当又は影響を及ぼす政府高官に限定。 外交官，立法者，中央省庁職員，政策立案者，軍及び法執行機関職員 その他	·インターネットガバナンス ·サイバーに関する国政術の構築 ·サイバーキャパシティビルディング ·インターネットの自由 ·情報共有 ·プライバシーとセキュリティ	目的：民主的な社会の基本的価値観を忠実に守りながらサイバー環境の多くの課題に取り組むこと 参加者が今日の脅威の性質及び重大性を理解し，公共及び民間サイバーセクター内における語彙，ベストプラクティス及び現在のイニシアティブに関する共通理解を進展すること。また，本プログラムは世界のサイバーセキュリ	·居住者コース(13 日間) ·政府高官 FO/GO/上級幹部職(SES)，議員コース ·非居住者イベント ·サイバーウィークリーニューズレター ·通信教育 ·インターン ·サイバーセキュリティ英語学習コース ·サイバー図書館 ·卒業生プログラム	国家安全保障の強化（米国内の政府職員の総合的なサイバーセキュリティ能力の強化）	2015 年 12 月開始

				·国防省(文民及び武官) ·内務省 ·司法省 ·銀行・金融省 ·非常事態省 ·外務省・外交官 ·法執行機関 ·通信セキュリティ及び情報省等を含む政府機関職員に適している	·知的財産の保護 ·テロ及びサイバー犯罪対策 ·官民パートナーシップ ·重要インフラのサイバー防護に関する全政府的アプローチ	ティのリーダーが講師を務めることから，参加者は他のサイバーの専門家との人脈を形成することができる。 目標: 1. 国際的な及び各国特有のサイバーセキュリティへのアプローチ法についての相互理解の進展 2. 参加者の防衛及びサイバーセキュリティ問題並びに国境を越える問題の把握，分析及び評価を行う能力の強化 3. サイバー問題に関する批判的及び戦略的思考能力の養成 4. サイバーセキュリティの課題の共有に対する協調的アプローチの基盤の強化			
14. サイバーセキュリティ・イベント	米アフリカ軍司令部(AFRICOM) （米国）	ジョージ・メイソン大学国際サイバーセンター，フォート・レズリー・J・マクネアの米国防大学アフリカ戦略研究センター D.C.並びに国土安全保障省，国防省及び	アフリカ	アフリカ 9 カ国の武官 10 名	サイバー犯罪対策，携帯電話のセキュリティ，インターネットの自由，アクセス及びアフォーダビリティ並びに国家 CERT の構築等	アフリカの葡語圏の特定の利益に係る問題を中心に，その他サイバー犯罪及びサイバーセキュリティの広範な問題の対処	参加者は米のサイバーセキュリティへのアプローチを学習するために同国首都地域の複数の政府機関及び学術機関を訪問。	アフリカ諸国の武官のサイバーセキュリティの意識啓発及び教育	2015 年 7 月に実施

		国務省等の連邦機関							
15. データプライバシーの日(DPD)	全米サイバーセキュリティ連盟(NCSA) (米国)	TRUSTe, インテル社, パスコード社, ロッキードマーティン社, Private WIFI, Privacy Ref 社, Mozilla	米	·親 ·10 代及び若年成人 ·企業 ·教育者 ·米国外のプライバシー提唱者・擁護者 ·家庭内暴力の被害者	データ保護, プライバシー	プライバシー及び個人情報の保護の重要性についての意識啓発	·DPD チャンピオン・プログラムは, 組織及び個人が支持を公に示す方法である。チャンピオンは, プライバシーの尊重, データの保護及び信頼の構築に献身した者を代表する。チャンピオンになるのは容易で, 資金の提供も不要。 ·ワークショップ, フォーラム及びツイッターチャット等のイベント ·プライバシーのコツ ·プライバシー図書館 #プライバシーアウェアキャンペーンデータプライバシーデーはすべてのデジタル市民が#プライバシーアウェアになることを奨励する取り組みの一部。年間を通じて NCSA が消費者にオンラインでプレゼンスを得る方法を教育し, 企業に対しプライバシーがビジネスにとって良いものであることを示す	データ保護, プライバシーの受容性に関する意識啓発, 信頼できる商取引の確保	2009 年以降毎年(1 月 28 日)
16. 全米サイバーセキュリティ意識啓発月間(NCSAM)	全米サイバーセキュリティ連盟(NCSA) (米国)	米国土安全保障省	米, 全世界	·消費者 ·中小企業 ·大企業 ·教育機関 ·若年者	サイバーセキュリティ	「STOP. THINK. CONNECT」キャンペーン全体のメッセージを強調し, オンラインの生活の安心, 安全が保たれるようにすること	·全米サイバーセキュリティ意識啓発月間プログラム, キャンペーン, イベント, ツール, リソース(解説画像, 情報誌, 研究論文, クイズ, ゲーム等)	米国内を中心とするサイバーセキュリティに関する意識啓発	毎年 10 月に実施

17. RE:サイバー	全米サイバーセキュリティ連盟(NCSA)及び国家安全保障のための企業幹部(BENS) （米国）	特になし	米	最高経営責任者(CEO)及び中小企業のサイバーセキュリティ・リスクマネジメント幹部	サイバー脅威の傾向，アウェアネスの文化の醸成，サイバーリスク評価及び管理，サイバー規制，法及び政策	最終目標： 企業の CEO 及び役員レベルのリスクマネジメントにサイバーセキュリティを組み入れること サイバーセキュリティのリスクマネジメントを行うことにより，各企業の CEO 及び役員は当該企業を守る責任を果たし，米国の今後の経済を守り，かつ，米国の防衛基盤を支援することができると考える	企業の CEO 及び幹部がその必要に応じたサイバーセキュリティの情報を知り，最新のガイダンスや補足の資源へのリンクとしてウェブサイトがそのファーストストップとしての役割を果たすべき	2017 年 12 月現在ウェブサイトは閉鎖	
18. STOP. THINK. CONNECT.	アンチフィッシングワーキンググループ(APWG) 全米サイバーセキュリティ連盟(NCSA) （米国）	·民間企業，非営利団体及び非政府組織の連合体 ·米国土安全保障省	米，全世界	市民	サイバーセキュリティ意識啓発	STOP. THINK. CONNECT.™はすべてのデジタル市民がオンラインでより安心，安全になるようにすることを手助けするグローバルなサイバーセキュリティキャンペーンである	ヒント，助言を記載したウェブサイト，ポスターの作成，研修，セミナー等	セミナーや研修等を通じてインターネット利用者に，安全なネット利用のための行動習慣の形成に寄与。	2010 年以降

19. グローバルサイバー同盟(GCA)	ニューヨーク群地区検察局，ロンドン市警察及びインターネットセキュリティセンター	米英企業多数，日本のサイバーグリーン等	全世界（米及び英中心）	サイバーセキュリティ関連企業，金融機関等	サイバー犯罪	・部門間を超えたサイバーリスクに対する国際社会の団結 ・システミックなサイバーリスクの緩和及び根絶するための具体的な対策の実施 ・GCA の取り組みの効果の測定及び公表	GCA は 2016 年 3 月に第 1 回 SAC 会合を開催し，TAC が GCA が最初の取り組みと検討すべき 4 つのグローバルなサイバーリスクを提示 1. フィッシング 2. 脆弱な識別及び認証メカニズムから生じるリスク 3. 脆弱で不法侵入を受けたウェブサイトから生じるリスク 4. DDoS 攻撃	DMARC（メール認証ツール） Quad9（DNS サービス）等のサービスの提供	2015 年 9 月 16 日設立
20. 自己ペース型サイバーセキュリティコース	シスコ・ネットワーキング・アカデミー	特になし	全世界（自己ペース）	企業又は顧客システムのセキュリティ及びプライバシーの責任を負う専門家	サイバーセキュリティ入門：サイバーセキュリティの重要性，最もよく見られるリスク及びそれを緩和する方法	サイバーセキュリティの人材育成	サイバーセキュリティの基礎知識のセルフ e ラーニングコースの提供	これまでに 780 万人が受講	コースの時間は 15 時間 1997 年から実施

21. 墨国家サイバーセキュリティ週間の一環としてのサイバー犯罪ワークショップ	墨国家安全保障委員会ー連邦警察 （墨）	米州機構サイバーセキュリティ意識啓発月間の枠組みにおける米州テロ対策委員会 亜，智，墨及びエストニア政府共催	墨	警察機関	サイバー犯罪	米州機構サイバーセキュリティ意識啓発月間の枠組み及び GFCE の OAS 加盟国におけるサイバーセキュリティイニシアティブの一環	·初のサイバー警察の全国会議 ·サイバーセキュリティの経験及びベストプラクティスの交換に関する全国ワークショップ ·高度な攻撃及び標的型攻撃についてのフォレンジック研究ワークショップ ·アメリポール，ユーロポール，西司法長官，OAS 等のメキシコ国内外の専門家の基調講演	サイバー空間において行われている高まる違法行為の予防，検知及び対応のためのツールの改善及びこの惨事に対処するための国家の連携及び国際協調を改善するためのサイバーセキュリティ分野に携わる 140 人以上の職員の研修を実施	2015 年 10 月（5 日間）
22. サイバーによって可能になった犯罪への対処：伯国家汚職防止及び資金洗浄防止活動	英外務・英連邦省（FCO） （英国）	在ブラジリア英大使館，英国家犯罪対策庁	伯	法執行機関	サイバー犯罪	連邦及び国家レベルでの法執行機関の相互運用性の改善，汚職及び資金洗浄防止のための国家戦略の支援	詳細は不明	同左	同左
23. 司法制度のデジタル及びサイバー問題に関する研修を通じたサイバーセキュリティの促進	英外務・英連邦省（FCO） （英国）	リオ技術・社会研究所(ITS：リオデジャネイロの非営利シンクタンク)	伯	裁判官及びその他の司法制度の構成員	サイバー犯罪，サイバースキル，意識啓発	伯司法制度のサイバースキル及び意識の向上及びより安全，オープンかつ民主的なサイバー空間に向けた規制強化のための脅威及び機会の特定	詳細は不明	同左	同左
24. サイバー犯罪対策キャパシティビルディングに関するグローバルな協力の強化	英外務・英連邦省（FCO） （英国）	インターポール	全世界	法執行機関コミュニティ	サイバー犯罪，協調	国際法執行機関コミュニティによるインターポールのサイバーキャパシティビルディングプラットフォームの利用を高めること	詳細は不明	同左	同左

25. スキル及び相互運用性を高めるためのサイバー犯罪対策演習	英外務・英連邦省（FCO） （英国）	英国家犯罪対策庁(NCA)，米連邦捜査局(FBI)	欧州	法執行機関	サイバー犯罪	主要な法執行機関パートナーのサイバー能力の評価及び測定並びに各国の共同及び独立したサイバー犯罪対策オペレーションの支援，推進及び完了能力を強化すること	国際石油会社に大規模なサイバー攻撃が発生した場合を想定した集団的対処方法の演習等	「シルバーパイロット」演習 「シルバーシャドウ」演習 欧州 8 カ国の法執行機関職員に対する演習	2015 年等
26. ウクライナ法執行機関デジタルフォレンジック研修	英外務・英連邦省（FCO） （英国）	英国家犯罪対策庁(NCA)	ウクライナ	法執行機関（NABU：国家汚職対策局）	サイバー犯罪	ウクライナ法執行機関の調査能力の改善	56 万 4 千ポンドを投入し，デジタルフォレンジック研究所及び分析システムの開発支援	ウクライナ当局の同国の高官の汚職の分析及び調査能力の改善	2016 年 7 月から 2017 年 3 月
27. ジョージア法執行機関：ネットフロー分析研修	英外務・英連邦省（FCO） （英国）	英国家犯罪対策庁(NCA)	ジョージア	法執行機関	サイバー犯罪	中度及び高度なマルウェア及びネットワーク・トラフィック分析に関する研修	詳細は不明	同左	同左
28. 印法執行機関へのサイバー犯罪対策研修	英外務・英連邦省（FCO） （英国）	英国家犯罪対策庁(NCA)	印	法執行機関	サイバー犯罪	印法執行機関へサイバー犯罪対策研修を行い，共同作戦の開始を目的に関係を強化すること	詳細は不明	同左	同左
29. 法執行機関間のサイバーセキュリティ能力格差の特定	英外務・英連邦省（FCO） （英国）	オブザーバー研究財団（ORF：印の公共政策シンクタンク）	印	法執行機関	サイバー犯罪	印の州及び連邦法執行機関のサイバーセキュリティの脅威への対処能力を強化すること	研修モジュールの策定 サイバーレンジ（演習）の実施 ハードウェアのセキュリティ確保等8つの取り組み	左の実現による印法執行機関のサイバー脅威対処能力の強化	2016 年にイニシアティブを発表
30. 錫 CERT の強化及び向上	英外務・英連邦省（FCO） （英国）	錫 ICT 庁(ICTA)及び錫 CERT	錫	国家 CERT	サイバーセキュリティ，CERT，インシデントレスポンス	錫のサイバー脅威及びインシデントへの対処能力の強化，女性及び児童のオンライン保護の改善等	詳細は不明	英 FCO による錫 CERT 支援に関する契約を締結。	開始時期は不明だが現在も継続中

31. ナイジェリア「2015 年サイバーセキュリティ法」の実施のための研修	英外務・英連邦省（FCO） （英国）	ナイジェリア企業（ヴォーカル・リソース・アンド・パートナーズ社及びコンチネンタル・プロジェクト・アフェアーズ・アソシエイツ社）	ナイジェリア	全州司法省サイバー担当検察庁	サイバーセキュリティ	全州司法省サイバー担当検察庁の知識基盤を拡大すること	詳細は不明	同左	同左
32. ナイジェリアの銀行セクターのサイバーセキュリティ強化	英外務・英連邦省（FCO） （英国）	コントロールリスク社	ナイジェリア	銀行部門	サイバーセキュリティ	ナイジェリアの銀行部門が直面する具体的なサイバー脅威及び当該部門のサイバーセキュリティ成熟度を評価することにより当該部門のサイバーセキュリティを改善すること及び目に見える改善を実現するためのロードマップを作成すること	詳細は不明	同左	同左
33. サイバー犯罪対策のための電気通信セクターの活用	英外務・英連邦省（FCO） （英国）	英連邦電気通信機構	バングラデシュ，パキスタン	電気通信部門	サイバー犯罪	パキスタン及びバングラデシュのサイバー犯罪に対処するための電気通信部門の能力を構築し，ナイジェリアにフォローアップ作業を提供すること	詳細は不明	同左	同左
34. e-Kawach:全国及び各州のサイバーセキュリティのための e シールド	英外務・英連邦省（FCO） （英国）	サイバー平和財団	印		サイバーセキュリティ，重要インフラ	重要情報インフラの防護	詳細は不明	同左	同左
35. 尼サイバーセキュリティ連携・能力強化	英外務・英連邦省（FCO） （英国）	在ジャカルタ英大使館	尼		サイバーセキュリティ，協調，立法	法律によって下支えされた連携を促進することにより尼のサイバーセキュリティを強化すること	詳細は不明	同左	同左

36. 連邦警察のサイバースキル強化	英外務・英連邦省（FCO）（英国）	BSI グループ，イノバシオネス・テレマティカス社（テレマティック・イノベーション社）	メキシコ		サイバーセキュリティ，サイバー犯罪対策スキル構築	メキシコ連邦警察の CERT(CERT-MX)のための情報セキュリティマネジメントシステムを実施すること	詳細は不明	同左	同左
37. チーヴニング・サイバーセキュリティ・フェローシップ	英外務・英連邦省（FCO）（英国）	チーヴニング・印チーム，在デリー英高等弁務団	印		サイバーセキュリティ，教育	印の中堅サイバーセキュリティ専門家に英国のベストプラクティスを触れさせ，特注の専門スキル向上コースを提供すること	詳細は不明	同左	同左
38. 国家サイバーセキュリティ戦略の策定及び実行	英外務・英連邦省（FCO）（英国）	英連邦電気通信機構	ルワンダ，タンザニア，マラウイ，モザンビーク，ボツワナ，カメルーン及びウガンダ		サイバーセキュリティ，国家戦略策定	英連邦 4 カ国(ルワンダ，タンザニア，マラウィ及びモザンビークを提案)の国家サイバーセキュリティ戦略及び CERT（該当する場合）を含む実行計画を策定し，ボツワナ，カメルーン及びウガンダの国家サイバーセキュリティ戦略の実行を支援すること	詳細は不明	同左	同左
39.「能力成熟度モデル」をフォローアップするための運用ツールボックス	英外務・英連邦省（FCO）（英国）	RAND Europe（シンクタンク）	全世界		サイバーセキュリティ	グローバルサイバーセキュリティキャパシティセンター(GCSCC)の「能力成熟度モデル」によって実施されたサイバー成熟度評価の結果に政策立案者及び意思決定者が対応できるようにすること	詳細は不明	同左	同左
40. 実務的意識啓発研修及びキャンペーン	英外務・英連邦省（FCO）（英国）	Wolfpack	南ア		サイバーセキュリティ，意識啓発，研修	サイバー脅威について情報セキュリティスタッフ及び一般ユーザーを教育するための国の研修及び意識啓発キャンペーンを作成，実施及び管理	詳細は不明	同左	同左

41. 国際重要インフラ・サイバー防衛：対象国のペースに合わせたサイバーリスクの評価	英外務・英連邦省（FCO） （英国）	APM グループ	ナイジェリア，モロッコ，コロンビア及びボツワナ		サイバーセキュリティ，重要インフラ	各国のペースで国家の重要インフラへのサイバーリスクを評価することを支援するために英国防省(MOD)及び国防科学技術研究所(DSTL)により構築されたベストプラクティスの活用	詳細は不明	同左	同左
42. カタールの重要インフラ防護のためのスキルの構築	英外務・英連邦省（FCO） （英国）	在ドーハ英大使館	カタール		サイバーセキュリティ，重要インフラ	カタールのエネルギーセキュリティを強化し，英カタールのサイバーパートナーシップの拡張の支援	詳細は不明	同左	同左
43. 国会議員，大臣及びハイレベル公務員のためのキャパシティビルディングワークショップ	英外務・英連邦省（FCO） （英国）	英連邦議会協会，英連邦事務局，米州機構	アフリカ，アジア太平洋及びカリブ海の英連邦諸国	国会議員	サイバーセキュリティ，研修，政策	一連の地域的国会議員間ワークショップを通じた国会議員のサイバーセキュリティ及びサイバー犯罪問題についての知識及び能力の構築	詳細は不明	同左	同左
44. コンピュータセキュリティインシデントレスポンス能力	英外務・英連邦省（FCO） （英国）	FIRST	全世界		サイバーセキュリティ，インシデントレスポンス	新規の経験が浅い CSIRT に質の高いオンライン又は対面式の研修を提供することによりそのインシデントハンドリング能力を継続して改善すること	詳細は不明	同左	同左
45. アラブ諸国のサイバーセキュリティの構築	英外務・英連邦省（FCO） （英国）	PGI	中東及び北アフリカ		サイバーセキュリティ，政策	アラブ世界中に本計画を広め，サイバーセキュリティ政策問題についての常設会議を設置することにより既存のサイバーPGI-DLA パイパー政策立案者ネットワークに基づく拡張	詳細は不明	同左	同左
46. 政府機関のためのサイバー机上演習	英外務・英連邦省（FCO） （英国）	PGI ／ 在クウェート英大使館	クウェート	政府機関	サイバーセキュリティ，インシデントレスポンス	クウェートの発展すべき分野の特定及び強化を目的としたサイバー攻撃への対処能力をテストすること	詳細は不明	同左	同左

47. コミュニティ脅威情報モデル/官民セクターインシデントレスポンスチームの設置	英外務・英連邦省（FCO） （英国）	ウォルフパック社	南アフリカ	CSIRT，業界団体，公的機関及び民間企業	サイバーセキュリティ，インシデントレスポンス	CSIRT，業界団体，公的機関及び民間企業等南ア及び英のステークホルダーの利益のための脅威情報収集及び共有態勢の改善	詳細は不明	同左	同左
48. グローバルサイバーセキュリティキャパシティセンター(GCSCC)フェーズ 3	英外務・英連邦省（FCO） （英国）	ノルウェー外務省，オランダ外務省，世界銀行，米州機構，英連邦電気通信機構及び国際電気通信連合	全世界	政府，国際機関，地域機関及び民間セクター	サイバーセキュリティキャパシティビルディング	各国が自己評価，ベンチマーク，より良い投資及び国家サイバーセキュリティ戦略計画並びにキャパシティディベロップメントの優先順位をつけることができるようにすること	·「サイバーセキュリティ能力成熟度モデル(CMM)」の策定とその世界展開 ·ベストプラクティスに関する研究の照合 ·サイバーセキュリティキャパシティポータルを通じた連携支援 ·「サイバーハーム（損害）」の研究を通じたメトリクスの改善	GCSCC の取り組みの変革的成長を継続し，その世界へのリーチと影響を著しく高め，その見返りとして，包括的，持続可能，戦略的かつ効果的なサイバーセキュリティキャパシティビルディングのグローバルな共通認識の構築支援	継続中
49. サイバー犯罪対策に焦点を置いたガーナ刑事司法アドバイザー(CJA)	英検察庁(CPS) （英国）	英内閣府，英外務・英連邦省	ガーナ	法執行機関，刑事司法セクター	サイバーによって可能となった犯罪対策，オンライン児童保護	ガーナの刑事司法改革の設計及び実施に寄与することにより刑事司法のサイバー犯罪への対処を改善すること	·検察官のメンタリング，ガーナ経済・組織犯罪局の能力及び知見の構築 ·警察・捜査機関の研修及び評価等	·サイバーにより可能となった犯罪に関する捜査及び訴追の質及び実効性の向上 ·管轄外の証人から証拠を得るためのビデオリンク施設の利用についての司法機関の同意のためのプロセスマップの起案 ·国家サイバーセキュリティ戦略における児童オンライン保護の導入 ·サイバー犯罪に関する裁判における司法の信頼の強化	2014 年 9 月から 2015 年
50. オペレーション・ブラックフィン	英国家犯罪対策庁(NCA) （英国）	ユーロポール欧州サイバー犯罪センター(EC3)，豪州，	豪州，コロンビア，仏，独，イタリア，	一般大衆	デジタルなりすまし，e メールフィッシング詐欺，オンラインバンキ	·重大かつ組織的なサイバー犯罪がもたらす脅威への事前対応策を提供すること	·「追跡」-ストレッサーツールのデプロイヤーに対する「予防」キャンペーンにリンクする活動を提案	ユーロポール及び EC3 が，特にソーシャルメディアのチャネル及び共同サイバー犯罪対策タスクフ	2015 年 10 月に実施

		仏，英，イタリア，コロンビア，蘭，西，米，独連邦刑事局(BKA)，独連邦情報セキュリティ局(BSI)	オランダ，スペイン，英，米		ングにおけるフィッシング，ソーシャルエンジニアリング，携帯機器・スマートフォン，DDoS 攻撃	·大陸間対応の調整を通じてこの活動の「足跡」を増やすこと ·能力をテストし，発展するサイバー犯罪の脅威への 4P（追跡，予防，防御，準備）対策の奨励，調整及び実行すること	·「予防」−若年者に何が違法かを教え，またその行動がどんな結果をもたらすかを伝え，彼らがサイバー犯罪者になる傾向を予防し，正しい道を歩むかどうかの分岐点に立っている若年者の犯罪を抑止するための事前のコミュニケーションキャンペーン ·「防御」−脅威データを活用し，修正されていない脅威がインフラに侵入している企業にその事実を通知 ·「準備」−サイバー犯罪のアウェアネスを高め，犠牲になったときを想定した犠牲者経験の改善。アンチウィルス企業の協力を得て，実施。	ォース(J-CAT)メンバーとの連携を通じて，参加国間の通信の調整を提供	
51.「サイバーで生き抜く術を持とう」キャンペーン	·英内務省，ビジネス・イノベーション・技能省，内閣府と密接に連携 ·国家犯罪対策庁 （英国）	民間セクター及びボランティア	英	消費者及び中小企業	·「あなたのオンラインの機器を安全にしよう」 ·「あなたのオンラインのプライバシーを守ろう」 ·「あなたのオンラインのお金に気を配ろう」 ·「あなたのビジネスを守ろう」	消費者及び中小企業(SMEs)のオンラインの安全行動及び信頼性を測れる程度大幅に改善すること	サイバーキャリア，教育リソース等を記載したウェブサイト，フリーのツール，有益なウェブサイト，ビデオ及びゲームの紹介等		
52. 英連邦サイバーセキュリティ及び	英連邦議会協会(CPA UK)	英外務・英連邦省(資金面)，米州機	アジア，アフリカ及びカリブ地域	英連邦諸国の国会議員約100名，	サイバーセキュリティ，サイバー犯罪，国	目的： 意識向上を通じて英連邦諸国の国会	カリキュラム及び資料の作成，主な国際ステークホルダー，地域ワークショッ	·シニアな国会議員，政府職員及び大臣のためのサイバー犯罪対	·フェーズ1：地域ワ

サイバー犯罪対策プロジェクト	(英国)	構(米州テロ対策委員会), 英連邦事務局, 英下院, CPA 国際, 地域及び支局		中央省庁職員及びハイレベル公務員, 約50の国際機関及び地域機関	家及び国際安全保障, 国際法及び国内法並びに人権	議員(並びに職員及び大臣) が各国内のサイバーセキュリティの実行, 精査及び促進できるようにすること 目標: 国会議員, 大臣及び政府高官が以下の事項を奨励すること ·対象国の強固なサイバー犯罪対策法の構築及び実施支援 ·国家サイバーセキュリティ戦略の交付及び実行支援 ·世界各国における強固なサイバーセキュリティ基準の採用の促進 ·国際法及び行動規範の適用の強化	プの研究及びマッピング, e ハンドブックの起草及び作成, 国家安全保障に関する国際議員会合	策及びサイバーセキュリティカリキュラムの構築 ·重要な国際ステークホルダーがプロジェクトに参加するための調査及びマッピング, マルチステークホルダーネットワークの構築及び維持並びに主催国の議会とのパートナーシップの構築 ·2016 年 7 月から 11 月の間の 3 つの地域ワークショップ(アジア, アフリカ及びカリブ地域)の開催によるサイバーセキュリティ及びサイバー犯罪対策に関する議員の知見及び関与の強化 ·E ハンドブック:作成及び継続的更新 ·サイバーセキュリティに関する 1 日会合	ークショップ(2016 年 7 月から 10 月) ·フェーズ 2:サイバーセキュリティ及びサイバー犯罪対策に関する国際議員の e ハンドブックの作成(2016 年 11 月) ·フェーズ 3:国家安全保障に関する国際議員会合—「サイバーデイ」(2017 年 3 月)

53. サイバーセキュリティ能力の評価及び開発	英，ノルウェー，OAS （英国主導）	グローバルサイバーセキュリティキャパシティセンター（GCSCC）				5 つの分野（dimensions）を用いて各国のサイバーインシデントに対処するために必要な重要要素の概要を示すことにより投資及び開発のための優先順位の理解を支援すること			
54. 重要情報インフラ防護(CIIP)ワークショップ	英連邦電気通信機構(CTO：英非政府組織) （英国）	·バングラデシュ電気通信規制機構 ·ケニア通信局 ·フィジー政府 ·ITU ·バルバドス・エネルギー・移民・電気通信・投資省 ·カメルーン郵便電気通信省 ·ボツワナ運輸通信省	東アフリカ，西アフリカ，南アフリカ，カリブ，太平洋及び南アジア地域	省庁等政府機関，民間及び公的セクター，学界及び市民社会グループ	·P 国家の重要インフラの優先及び重要情報インフラ防護(CIIP)の重要性 ·CIP 枠組みの構築，サイバーセキュリティの課題及び緩和のためのグッドプラクティスの協調 ·国家サイバーセキュリティ戦略立案 ·国家，地域的及び国際協力並びに便地域的及び純地域的サイバーセキュリティイニシアティブ及び会合への参加 ·提言を採用する省庁への技術的助言	インフラ及びそれを通じて流通する情報並びにユーザーの安全，セキュリティ及びレジリエンスの確保	7 つの地域的ワークショップ: ·南部アフリカ地域：ボツワナ ·西アフリカ地域：カメルーン ·東アフリカ地域：ケニア ·カリブ地域：バルバドス ·太平洋地域：バヌアツ ·南アジア地域：バングラデシュ，錫		2014 年 8 月から 2015 年 3 月

55. メキシコ金融セクター：サイバーセキュリティ健康診断	コントロールリスク社 （英企業）	·メキシコ金融機関 ·メキシコ銀行協会 ·メキシコ金融機関組合 ·国家銀行証券委員会 ·連邦警察科学部 ·メキシコ金融機関幹部協会 ·英外務・英連邦省	メキシコ及びラテンアメリカ全域	金融セクター及び関連政府機関（金融規制当局，法執行機関等）	サイバーセキュリティ CNI（金融セクター）	以下によりメキシコの金融セクターのサイバーセキュリティを改善すること a）公的に入手可能な具体的なサイバー脅威の評価書の作成 b）メキシコ金融セクターのサイバー脅威に対する成熟度の評価 c）当該セクターの改善計画（ロードマップ）の策定	·脅威評価(研究・情報収集・分析・報告) ·各国内のインタビュー及びワークショップ ·報告 ·参加者との報告会 ·脅威評価の結果を明らかにする意識啓発キャンペーン ·影響度評価	·公共脅威評価による当該セクターにおけるサイバーセキュリティの意識の向上 ·個別の金融機関がその防御力を高めるための具体的な優先順位をつけた行動計画があること ·当該セクターが当該セクターのサイバーセキュリティへのアプローチを構築するための青写真があること。コントロールリスク社はこれを実現するために当該セクター協会と協力して取り組んでいる。	2015 年以降(フェーズ 1 は 12 カ月）
56. 途上国からの代表団に対するエストニアの ICT ソリューションの導入	エストニア外務省(資金面)及び e ガバナンス・アカデミー(eGA) （エストニア）		アンゴラ，伯，ケニア，モーリシャス，タンザニア，泰，チュニジア，ウクライナ		中央及び地方 e 政府，e サービス，e 民主主義，サイバーセキュリティ	途上国(OECD が提供したリストによる国)からの代表団を歓迎し，e ガバナンス及び e 政府の知識及びベストプラクティスを普及すること	·最低年 10 回の研修，政府の相互運用性及び法制度へのアプローチ，途上国への派遣		2015 年 3 月から 2017 年 3 月

57. ナミビアにおける政府の相互運用性ソリューション(X-Road)の設計及び実行	エストニア e ガバナンス・アカデミー(eGA) (エストニア)	ナミビア政府，ナミビア首相府（資金面），エストニア・サイバーネティカ社	ナミビア		e ガバナンス	·エストニアの X-Road ソリューションに基づいた政府の相互運用性枠組みをナミビアの e 政府相互運用性システムへ導入し，開始すること ·様々な省庁，事務局及びその他の政府機関が利用する e 政府の相互運用性システムに関連する組織の組立，規制枠組み及び基準を構築すること	本プロジェクトは3つのステージに分けて実施 1. 目録評価(現在のシステム，データベース，ICT インフラ，組織の組立，既存の技術（ハードウェア）支援及び効率的かつ効果的な導入を保証するために必要な追加的作業）を完了し，プロジェクトの実行のための詳細プランを作成 2. ナミビア e 政府構築の現在の段階の分析と組織の組立及び法枠組みのための提案の構想 3. サイバーネティカ社とともに相互運用性ソリューションの全面的な実行	ナミビアの公共機関が安全なインターネットを利用した異なる機関からのデータのクロスオーバー及び同国の住民及び企業のための e サービスの構築ができるようにすること	2014 年 10 月から 2016 年 12 月
58. チュニジア政府の e 政府システムの開発支援	エストニア e ガバナンス・アカデミー(eGA) （エストニア）	大統領府 e 政府部	チュニジア	公務員	e ガバナンス		·チュニジアの公務員のエストニアへの 1 週間の研修訪問 2 回 ·エストニアの専門家のチュニジアへの派遣 4 回（共同ワーキンググループの会合に参加し，報告及び分析のためのインプットを収集するため） ·政府枠組み及び個人識別マネジメントに関する提言 ·対象国でさらに発展するデジタル文書のオプション選択支援	·2 国間の技術移転 ·e 政府ツールを利用することにより市民へのサービスの提供の改善し，もって，市民と政府の間の信頼関係を構築するチュニジアのノウハウの強化 ·民主的かつオープンな世界の一員になるために既にチュニジアが行っている取り組みの強化	2013 年 10 月から 2015 年 11 月

59. 国家サイバーセキュリティ・インデックス	エストニア e ガバナンス・アカデミー（eGA） （エストニア）	エストニア外務省	エストニア，モルドバ		中央 e 政府，サイバーセキュリティ	モルドヴァにおける国家サイバーセキュリティ評価手法の構築とその実施	·国家サイバーセキュリティ評価方法論 ·エストニアにおける方法論の導入 ·モルドヴァにおける方法論の試験 ·国家サイバーセキュリティインデックスのためのウェブ環境の構築	国家又はその中心的機能におけるサイバーセキュリティの状態の評価を可能にする普遍的な方法論（インデックス）の構築	2015 年 3 月から 12 月
60. アルメニア司法機関における e ガバナンス・ツールの開発	エストニア e ガバナンス・アカデミー（eGA） （エストニア）	欧州委員会（資金面），VX ソフト（アルメニア企業），GTA アルメニア	アルメニア		e ガバナンス	目的： ·アルメニア司法省が公的サービスの電子提供を行うための能力を強化すること ·国家の内部の効率性を高め，かつ，透明性を向上し，また，利用可能なサービスへの国民のアクセスを高めること 具体的目標： ·e 刑務所制度の構築 ·法人の商業登記制度（e 登記）をアルメニアの e ガバナンスインフラ全体と統合し，近代化すること ·e 公証制度をアルメニアの e ガバナンスインフラ全体と統合し，近代化すること ·開発された e ガバナンス制度のための研修を実施すること	1. e ガバナンス支援活動 2. e サービス開発 3. 研修及び意識啓発活動 4. 法枠組みの強化		2015 年 10 月から 2017 年 10 月

61. フェロー諸島の e 政府構築支援	エストニア e ガバナンス・アカデミー (eGA) (エストニア)	フェロー諸島政府 (資金面)	フェロー諸島	公務員	中央 e 政府	フェロー諸島のための相互運用性及びデジタルアイデンティティの協議及び実装, X-Road の構築	X-Road v5 のデプロイメントのための協議, 研修及び技術支援		2015 年 10 月から 2016 年 6 月
62. ウクライナの e ガバナンスキャパシティビルディング	エストニア e ガバナンス・アカデミー (eGA) (エストニア)	·ウクライナ e 政府の州当局 ·エストニア外務省, USAID (資金面)	ウクライナ	e 政府の州当局職員	戦略的通信活動及び政府内連携能力	e 政府の州当局のキャパシティビルディング支援を中心とするウクライナの e ガバナンス 能力を構築すること	·戦略的通信活動及び国民意識啓発 ·政府内連携能力強化 ·e サービスの構築		2015 年 9 月から 2016 年 9 月
63. ジョージアにおける e ガバナンスの強化支援 II	エストニア e ガバナンス・アカデミー (eGA) (エストニア)	·CSI-ピエモンテ(イタリア), エストニア政府, LEPL (公法法人) ジョージア司法省データ交換局 ·欧州連合 (資金面)	ジョージア	LEPL データ交換局(DEA)職員	1.ジョージアの e 政府及び情報社会に関する法規制枠組み 2. 組織及び制度枠組み 3. 研修能力 4. カスタマイズされたコンサルティング及びベンチマーキング・サービス 5. 大衆へのアウトリーチ及びマーケティング	目的: ·LEPL ジョージア司法省データ交換局(DEA)の制度的組立を強化すること ·DEA のスタッフが EU 基準に沿った e 政府及び情報セキュリティの研修, コンサルティング, ベンチマーキング及び促進を行うために必要なスキル及び知識を向上すること 目標: ·EU 基準に合致するためのジョージアの e 政府法の改定 ·国民が親しみを感じられる総体的な e ジョージア・コンセプトの創造 ·新たに出現している課題に対処するための e ジョージア戦略の考案 ·e サービス提供のためのデジタルアイデンティティの利用の促進	·対面式コンサルティング ·研修コース ·ワークショップ ·研究訪問	·ジョージアの e 政府及び情報社会法規制枠組みが EU 基準を満たすために検証及び改定されること ·e ジョージア戦略において概説された業務の拡大を踏まえた DEA の組織的及び制度的枠組みの改変 ·知識基盤の設置, 評価及び品質保証研修法の導入及び研修資料の構築を通じた DEA の研修能力の強化 ·DEA の政府のパートナーへの注文に応じたコンサルティング及びベンチマーキングサービスの設計, 構築及び提供能力の強化 ·DEA の国民へのアウトリーチ及	2015 年 9 月から 2017 年 3 月

						·DEA のサイバーセキュリティインシデントハンドリング能力の改善 ·DEA の研修コース，コンサルサービス及び国民へのアウトリーチ活動を行う能力の強化		びターゲットマーケティング能力の改善	
64. サントメ・プリンシペの e ガバナンス能力の評価	エストニア e ガバナンス・アカデミー（eGA） （エストニア）	エストニア外務省，サントメ・プリンシペ政府	サントメ・プリンシペ		中央 e 政府	eGA は，サントメ・プリンシペの現状，次に取るべき手段，中期(2 年から 3 年)の行動計画及び同国において e ガバナンスを構築するための関連する技術的 ICT ソリューションを実行するために必要なおおよその予算を記述した分析報告書を作成する	·サントメ・プリンシペの状態及び政府の今後の計画に関する統計及び概要を知るためのアンケートの実施。アンケートには e ガバナンスが政府レベルで現在どのように整備されているか，政府機関の責任はどのように分掌されているかなどに関する質問が含まれる。また，ICT インフラに関連する問題や法律及び戦略文書もアンケートに明記。 ·eGA 専門家のサントメ・プリンシペへの派遣 ·関心があるパートナー及びステークホルダーへのセミナー（eGA 専門家がサントメ・プリンシペが直面する同様の課題に対処したエストニアの経験に関する概要を説明し，派遣団の調査結果を紹介） ·現状，次に取るべき手段，中期(2-3 年）の行動計画及び必要なおおよその予算を記載した分析報告書		2015 年 8 月から 2015 年 9 月

65. モルドヴァにおける判決への電子アクセス	エストニア e ガバナンス・アカデミー(eGA) (エストニア)	モルドヴァ最高裁，下級裁 ·USAID，エストニア外務省(資金面)	モルドヴァ	裁判所職員，一般大衆	中央 e 政府，地方 e 政府	目的: モルドヴァの裁判所の紙ベースのアーカイブ(公文書記録)のデジタル化の試験を行い，下記の事項を可能にすること ·現在のデジタル形式では利用不可能な裁判所の情報への高速かつ簡易なオンラインアクセス ·後で選択及び確認できる複数の付加的基準に基づく訴訟情報の検索 上記の制度により 裁判所の活動の透明性を高め，利用者にとって分かりやすい形で大量の情報及びサービスへのアクセスを可能にすること。	·必要な作業の評価 ·期待される作業についての取決め事項の策定 ·裁判所の判例・裁判例ファイルのデジタル化とそのオンライン公表を行う IT 企業の入札及び請負契約 ·判例・裁判例ファイルのデジタル化の結果のモニタリング及び品質保証 ·デジタル化された判例・裁判例の公表 ·モルドヴァの裁判所職員等についてデジタル化された判例・裁判例の取扱いに関する研修の実施 ·モルドヴァの裁判制度のさらなるデジタル化活動を支援するための持続可能なプロセスの整備支援 ·計画される発展についての一般大衆及び主なステークホルダーの意識向上	·合意に基づく最高裁判所及びニスポレニ地方裁判所の紙ベースの判例・裁判例ファイルのデジタル化とオンライン公表 ·モルドヴァの裁判制度のさらなるデジタル化活動を支援するために適した持続可能なプロセスの整備 ·モルドヴァの裁判制度のさらなるデジタル化活動のためのステークホルダーが同意した活動計画書の形成 ·デジタル化した裁判所の判例・裁判例ファイルの機会及び機能についての一般大衆及びステークホルダーの知見の向上	2015 年 2 月から 2016 年 6 月

66. モーリシャスのためのデータ共有ポリシー及びデータアーキテクチャ	エストニア e ガバナンス・アカデミー(eGA) (エストニア)	ノータル社(資金面)	モーリシャス	公務員，企業及び市民	モーリシャス ICT エコシステムの相互運用性，e ガバナンス	目的: 公務員，企業及び市民のユーザー中心型サービスを可能にするための原則，メカニズム及び要素に重点的に取り組むこと 目標: ·公的サービスの確立を目的とする行政機関間の協力 ·法的要件及び政治的コミットメントを満たすための行政機関間の情報の交換，共有及び再利用 ·市民及び企業へのより良い公的サービスの提供並びに公的サービスの効率的提供による行政機関，企業及び市民のコストの削減		1. データ普及報告書 2. データ共有ポリシー及びデータアーキテクチャの構築	2016 年 7 月から 11 月
67. ノルウェーーエストニア e 政府イニシアティブ	エストニア e ガバナンス・アカデミー(eGA) (エストニア)	ノルウェー・グラント(贈与)プログラム，シードフォーラム・エストニア財団，シードフォーラム・ノルウェー財団，ウォッチコム社	エストニア及びノルウェー	公的及び民間セクターのパートナー	e ガバナンス，サイバーセキュリティ，イノベーション及び事業開発	目的: e ガバナンス，サイバーセキュリティ，イノベーション及び事業開発の分野におけるノルウェー及びエストニアのリーダー間の協力を強化，実行及び発展すること 目標: ·e ガバナンス及びサイバーセキュリティの分野に関するノルウェー及びエス			2015 年 12 月から 2016 年 5 月

						トニアの公的及び民間セクターのパートナー間の将来の連携態勢の構築 ·新しい e 政府イニシアティブのためのタリンのノルウェー・エストニア e 政府研究インキュベーターの共通プラットフォームの締結 · 開発協力地域におけるパートナー間のさらなる再現・反復可能な連携モデルの締結			
68. デジタル 5	エストニア，以，新，韓国及び英		エストニア，以，新，韓国及び英		e ガバナンス，デジタル政府	·ベストプラクティスの共有，各国のデジタルサービスの改善法の特定，共通プロジェクトへの協力及びデジタル 5 の成長するデジタル経済を支援し，擁護することに特化したフォーラムを提供すること ·デジタル技術が持つ潜在的なグローバルパワーを活用し，各国が情報を共有し，学び合うことによりさらに良い高速かつ効率的なデジタル政府になるように支援し合うこと	年次会合，ワーキンググループの設置		2014 年以降
69. ジュネーヴ・インターネット・プラットフォーム(GIP)	スイス連邦外務省(EDA) 及び連邦通信局(OFCOM)	ディプロ財団(Diplo)の運営委員会 5 団体: EDA，OFCOM，DCAF，ETH-Board 及び	全世界	第一次対象グループ: ジュネーヴに政府代表部を置く小国及び途上国並びに限られた資源の	デジタル政策過程，サイバーセキュリティ	使命: 観測所，キャパシティビルディングセンター(オンライン及びオンサイト)及び議論のためのセンター。GIP はジュネーヴより運営。	支援は主な対象グループの個別のニーズに合わせたテーラーメイド方式で行う。以下その例: ·資源を最大限活用するための個別の協議及びオンライン会議 ·テーマに関するウェビナー，デジタル政	·サイバーセキュリティの課題，インターネットガバナンスにおける政府の役割，ビットコイン及びその他の暗号通貨，インターネット時代における裁判管轄権，プライバシー及び監視への地球規模の	継続中

		ジュネーヴ大学によって運営		ためにジュネーヴに代表部を置いていない国 第二次対象グループ: 政府，市民社会，学界，技術コミュニティ及びその他のステークホルダー		目的: 政府，市民社会，学界，技術コミュニティ及びその他のステークホルダーの中でも特に小国及び途上国のデジタル政策及びガバナンスに関連するリソースの調査，デジタル戦略の策定し，他のステークホルダーとの政策協議の実施を支援すること 目標: ·途上国のサイバープロセスへの参加の促進 ·議論及び意見交換のための中立的かつインクルーシブな場の提供 ·既存の政策サイロ（貯蔵庫）を超えたプロセスへの集学的アプローチの促進	策説明会，政策観察活動等のオンライン活動 ·カスタマイズされたテーマに関する主要な外交官が多く集まる世界中の都市で行う（ビットコイン，ダークウェブ等の）ディスカッションパネルや探求セッション等から構成される各国の外交官，政府職員，専門家のための 1 日がかりのイベント(例：サイバーセキュリティ・デー） ·オンサイト及びオンラインのデジタル政策過程の近年の動向に関するエンゲージメント及びキャパシティビルディング活動 ·記事，ブログ等の形式による主なデジタル政策の動向及びイベントのフォロー及び報告を行う政策観察	対応策の構築を目的とするサイバーセキュリティに関する議論 ·太平洋諸島の国々のための重要な資源としてインターネットに関する円卓会議 ·デジタル時代の透明性と人権 ·国際ジュネーヴインターネット会合(概要書：「インターネットガバナンスの強化―ジュネーヴインターネット会合からのメッセージ」） ·毎月主なデジタル政策の展開を要約したオンライン説明会の提供及びオンサイトの同様の議論 ·ジュネーヴの政府代表団内の外交へのインターネットガバナンスの入門オンラインコースの提供 ·1 つの場所に情報及びリソースをフォローし，収集するオンラインプラットフォームと観測所–www.giplatform.org –の設置	

70. 重要情報インフラ防護イニシアティブ	スペイン，スイス，ノルウェー，オランダ メリディアン・コミュニティ（2005 年以降 CIIP 関連国際会議を主催している国家グループ）		メリディアン・コミュニティの加盟国	重要情報インフラ防護(CIIP)担当政策立案者	CIIP	CIIP の責任を負う政策立案者がサイバーセキュリティ問題の含意及び影響を理解し，その最近の動向を継続して認識するために支援すること		2016 年に想定される成果 ·特定の CIIP 関連議題の研究(既存の研究と連携又は新たに始める)。CIIP 成熟度ビルディングブロック研究プロジェクトをメリディアン・コミュニティと連携して構築する。 ·途上国の CIIP 知識のベースラインの構築を目的とするワークショップ。これには基本的な CII セクターの定義，CERT モデル，NCSS，PPP 及び同様のコンセプトが含まれる。 · 蓄積された過去 11 年間のメリディアン会合の様々なセッションの結果及び成果に基づく定期的な議題別セミナー及びワークショップ（オンラインを想定） ·CIIP に関するグッドプラクティスガイドラインの作成等。 2017 年以降に想定される成果 CIIP の個別の問題に適したツールキット又は学習資料(ヴァーチャル・実物)の作成。	

71. ENCYSEC	エクスパティーズ・フランス （仏）	Adetef & Civipol から成るコンソーシアム，EU 安定及び平和への貢献手段（資金面）	マケドニア(サイバー犯罪対策課 情報社会・管理省，電子通信庁-(CERT)，内務省，大学，マケドニア情報通信技術会議所） モルドヴァ(モルドヴァ特別電気通信センター；サイバーセキュリティセンター CERT-GOV-MD，内務省，サイバー犯罪課，e 政府センター/政府 CIO 事務所，国家個人データ保護センター，大学 コソボ(ARKEPー電気通信規制局，組織犯罪捜査局サイバー犯罪捜査課，大統領及び首	CERT，政策立案者	サイバーセキュリティ，インシデントレスポンス	サイバー攻撃及び事故による故障の適切な予防，対応及び訴追のための各地の能力の構築及び訓練することにより受益国の情報通信技術ネットワークのセキュリティ及びレジリエンスを強化すること	CERT キャパシティビルディング ·オペレーショナルな CERT の構築・強化支援 ·共同サイバーセキュリティ演習の円滑化 ·CERT 職員のための特定のカリキュラム・研修コース構築に関する助言 サイバーセキュリティ戦略と意識啓発 ·国家サイバーセキュリティ戦略の策定及び採用に関する助言(政策，財政及び法的影響に関する助言を含む) ·意思決定者のための国内及び国際ワークショップの組立を含むサイバーセキュリティの意識啓発に関する助言 協力の強化：PPP 及び国際協力 ·サイバーセキュリティ及びコンピュータ科学(CS)，科学，技術，工学及び数学(STEM)の学位を含む新しい柔軟な大学課程の構築に関する助言についての政府と民間セクター間の協力の強化 ·サイバーセキュリティの分野に関する国際機関との協力 ·CERT 及び 24 時間コンタクトポイントの		2014 年から 2016 年

			相府，内務省サイバー犯罪対策室，電子・郵便通信規制局（CERT），情報社会庁，国家個人データ保護庁，司法省，大学				サイバーセキュリティに関する国際イベントへの参加の促進		
72. 白におけるサイバーセキュリティ連合	ASBL(白 NPO)サイバーセキュリティ連合 （白）		白	·IT 意思決定者 ·全セクターの企業 ·従業員 ·一般大衆 ·若年者	サイバー犯罪，サイバー攻撃，サイバー防衛	目的：白におけるサイバーセキュリティ・レジリエンスの強化 目標：·知識及び経験の共有 ·具体的なセクター間イニシアティブの開始，整理及び調整 ·市民及び組織間の意識啓発 ·専門性の向上の促進 ·より効率的な政策及び規制のための勧告の発出	·ベルギー連邦サイバー緊急チームである CERT.be のベルギーインターネットセキュリティ会合(BISC)の支援 ·白政府による安全なパスワードに関する全国キャンペーンの支援		2014 年以降
73. 以・英サイバー研究プログラム.	以及び英政府	英工学・物理科学研究会議(EPSRC) ブリストル大学／バル＝イラン大学， ロンドン大学(UCL)／バル＝イラン大学 ケント大学 ／ ハイファ大学	以及び英		アイデンティティ管理，ガバナンス：サイバーセキュリティ規制，プライバシー保証及び認識，携帯及びクラウドセキュリティ，セキュリティの人的側面，利用可能なセキュリティの暗号化技術	英国がオンラインで事業を行い，サービスへアクセスする最も安全な場所の一つになること	·公開市場，オープン標準及びオープンソースに関する情報及び経験の交換 ·各国がデジタル公共サービスを構築できるような能力を持つための協力 ·他の国際連携の方法の構築		2014 年以降

74. サイバーセキュリティ・アクションプラン	加公安省(PS)及び米国土安全保障省(DHS)		米国及び加		サイバーインフラのレジリエンスの強化，運用及び戦略レベルにおける関与，連携及び情報共有の改善，民間セクター及び国民の意識啓発活動	目的: PS と DHS それぞれのサイバーセキュリティの取り組みの一層の統合及び民間セクターとの連携の強化を通じて両国のサイバーセキュリティを強化すること 目標: ·サイバーインシデント管理の強化 ·両国のサイバーセキュリティオペレーションセンターの連携 ·サイバーセキュリティに関する民間セクターとの共同関与及び情報共有 ·既存のサイバーセキュリティに関する国民意識の啓発に関する取り組みについての継続的協力			
75. CERT 研修資料	欧州連合ネットワーク・情報セキュリティ庁(ENISA)		EU 加盟国	CERT メンバー	技術面:アーティファクトのハンドリング及び解析環境の構築，アーティファクトの処理及び保存，アーティファクト解析の基礎，高度なアーティファクトのハンドリング，高度なアーティファクトの解析の基礎，アーティフ		以下を活用 ·よりプロアクティブかつ効率的な CERT 研修を行うための研修方法及びロードマップについてのグッドプラクティスガイド ·教師のためのハンドブック ·学生のためのツールセット ·体験型研修を支援するためのヴァーチャル画像		2008 年に開始。2012 年，2013 年及び 2014 年に新しい演習シナリオを追加

					ァクトの動的解析，静的解析，アーティファクト解析のための対抗措置，共通枠組みの構築，防御能力強化のための指標の利用，電子証拠の特定及びハンドリング，デジタルフォレンジック，携帯脅威インシデントハンドリング（IH），携帯脅威 IH パート II，インシデントの事前検知，IH の自動化，ネットワーク・フォレンジック，ハニーポット，脆弱性ハンドリング等 運用面：重要情報インフラに対する攻撃時の IH，APT 攻撃，標的型攻撃のベクトルとして利用されるソーシャルネットワーク，ICT インシデントの費用，ロールプレイング形式の				

					IH，クラウドにおける IH，大規模 IH 等 CERT の設置：トリアージ・基本 IH，IH 方法のテスト，CERT スタッフの採用，CERT インフラの構築，外部との連絡体制の構築，法執行機関との協力，CERT 及びすべてのステークホルダーとの通信路の評価及びテスト，サイバー犯罪の痕跡の特定及びハンドリング，フィッシングキャンペーン中の IH 及び協力，サイバー犯罪分野における協力，ENISA 第 13 条 a 及び第 4 条上の義務に関連した IH における CERT の参加				
76. 欧州サイバーセキュリティ月間（ECSM）	欧州連合ネットワーク・情報セキュリティ庁(ENISA)，欧		墺，白，クロアチア，キプロス，チェコ共和国，デンマ	欧州市民及び機関	従業員のサイバーセキュリティ研修，職場でのサイバーセキュリ	目的： 市民間のサイバーセキュリティを促進し，データ及び情報セキュリティ，教	情報セキュリティに関する助言，コンテスト，会議，セミナー，グッドプラクティス		2015 年 10 月（毎年）

	州委員会 DG CONNECT（欧州委員会 通信ネットワーク，コンテンツ及び技術総局）		ーク，エストニア，フィンランド，仏，独，ギリシャ，ハンガリー，アイスランド，アイルランド，イタリア，ラトヴィア，リトアニア，ルクセンブルク，オランダ，ノルウェー，ポーランド，葡，ルーマニア，セルビア，スロヴァキア，スロヴェニア，スペイン，スウェーデン，トルコ及び英	ティの文化の醸成，コーディング，クラウドソリューションの理解，デジタル単一市場	育，グッドプラクティスの共有及び競争の促進によりサイバー脅威の認識を変えることを提唱すること 目標： ·サイバーセキュリティについての一般認識の生起 ·ネットワーク・情報セキュリティ(NIS)指令案で取り上げられている NIS に関する具体的認識の生起 ·すべてのユーザーの安全なインターネットの利用の促進 ·ECSM を通じた意識啓発の確固たる実績の確立 ·関連のあるステークホルダーの関与 ·本プロジェクトの欧州及びグローバルな側面を通じた各国メディアの関心の強化 ·政治的及びメディアの調整を通じた情報セキュリティに関する注意及び関心の強化	の共有，意識啓発キャンペーン，ワークショップ等		
77. GLACY（サイバー犯罪についてのグローバルアクション）	欧州評議会（CoE）	欧州連合(EU)，インターポール，ユーロポール欧州サイバー犯罪センター(EC3)，ルーマニ	モーリシャス，モロッコ，フィリピン，セネガル，南アフリカ，トンガ，錫	司法及び法執行機関職員，判事・裁判官，検察官，法執行機関第一応答者の研修指導者，法執行研修	サイバー犯罪，電子証拠，省庁間協力	全体目標： 組織犯罪との闘いと防止 個別目標： サイバー犯罪に関するブダペスト条約に基づくサイバー犯罪対策及び電子	·研修者の研修 ·ワークショップ ·会議 ·研修演習	·成果 1-意思決定者の関与:プロジェクト対象国の意思決定者はサイバー犯罪の脅威及びその法の支配・人権への含意を認識し，サイバー犯罪対策に関する戦略的優先事項を特定した	2013 年 11 月から 2016 年 10 月

		ア CERT（CERT-RO）		機関及びサイバー犯罪対策課の代表，データ保護当局，市民社会，企業及び学界並びに国家及び各部 CERT		証拠についての刑事司法機関の協力の実現 目標： ·国内法執行機関の研修戦略の策定支援 ·欧州サイバー犯罪対策研修・教育グループ(ECTEG)が作成した研修資料へのアクセスの円滑化 ·想定されるサイバー攻撃への CERT のレスポンスのベンチマーキング		·成果 2-法律の調和：国内法をサイバー犯罪条約(CETS 185) に完全に合致し，また，データ保護及び児童オンライン保護に関する法規制を改善するための改正案が出された ·成果 3-司法研修：サイバー犯罪事案及び電子証拠に関する裁判官及び検察官のスキルが強化された ·成果 4-法執行能力：サイバー犯罪の捜査及び電子証拠のための特別の技能及び制度の強化 ·成果 5-国際協力：サイバー犯罪条約に関するブダペスト条約第 3 章に基づきサイバー犯罪対策に関する国際的な法執行及び司法協力が強化された ·成果 6-情報共有：データ保護基準に沿う官民及び省庁間の情報共有の強化 ·成果 7-進捗状況の評価：政府はサイバー犯罪の捜査，訴追，判決についての進捗状況を評価することができる	

78. サイバー犯罪に関するオクトパス会合	欧州評議会（CoE）	欧州連合（EU），エストニア，日本，メキシコ，ノルウェー，ルーマニア及びパナマ政府，フィリピン司法省，米州機構(OAS)，国連アフリカ犯罪防止・加害者治療研修所(UNAFRI)，ECOWAS	亜，智，コロンビア，コスタリカ，ドミニカ共和国，ヨルダン，メキシコ，パナマ，パラグアイ，秘，ECOWAS 地域	法執行専門家，市民社会団体代表，インターネットサービスプロバイダ(ISP 協会を含む)，ソーシャルメディア，クラウドサービスプロバイダ，e コマースのプラットフォーム，メンバー，オブザーバー，立法・司法・行政機関及び民間セクターの代表者	サイバー犯罪法， 電子証拠，児童保護，データ保護	プロジェクト目標： サイバー犯罪に関するブダペスト条約(CETS（欧州評議会条約シリーズ）第185 号)及び関連文書の実施支援 目標： ·年次オクトパス会合の開催 ·メンバー，機能及び会合数が拡大したサイバー犯罪条約委員会の機能の共同出資及び支援 ·ブダペスト条約及びデータ保護及び児童の保護に関する関連文書を実施する準備ができている国への助言及びその他の支援の提供	·オクトパス会合（年 1 回） ·サイバー犯罪条約委員会（T-CY）メンバー及びオブザーバーの委員会会合への参加を支持 ·研究及び分析を通じた T-CY の評価とその他の活動 ·T-CY 会合のロジ支援，翻訳・通訳の資金提供 ·T-CY メンバーの関連するフォーラムへの参加支援 ·最大 15 の国内又は地域ワークショップの設置支援 ·他の組織が開催するイベントへの貢献 ·立法その他についての助言	·サイバー犯罪対策の協力に関するオクトパス会合の実施 ·T-CY の支援 ·各国のブダペスト条約及びデータ保護及び児童オンライン保護に関連する基準の実行支援	2014 年 1 月から 2016 年 12 月 31 日
79. 地域的プロジェクトサイバー犯罪 EAP II	欧州評議会（CoE）	欧州連合(EU)，欧州サイバー犯罪センター(EC3)，ユーロジャスト，ルーマニア，エストニア，独，仏，葡，米	アルメニア，アゼルバイジャン，ベラルーシ，ジョージア，モルドヴァ及びウクライナ	24 時間コンタクトポイント	サイバー犯罪，電子証拠	目的： サイバー犯罪対策及び電子証拠に関する効果的な地域及び国際協力を実現すること 目標： ·サイバー犯罪対策及び電子証拠に関する国際協力のための相互の法的支援の強化 ·24 時間コンタクトポイントの役割の強化	·東方パートナーシップ(EaP)6 カ国及びその他 2，3 カ国の司法共助(MLA)機関の代表からなるワーキンググループ(WG)の設置 ·サイバー犯罪対策及び電子証拠に関する MLA の機能を見直し，その役割と責任を明らかにし，強みと弱点を特定し，かつ，一連の提言を準備，採用するための MLAWG の会合を 3 回開催 ·今後の行動に関する一連の提言の準備及び採用に関する MLAWG の支援 ·上記の活動の結果出された提言の実	·6EaP 諸国の MLA 担当機関はサイバー犯罪対策及び電子証拠に関する国際連携のためのより良い技能及びツール(マニュアル，オンライン資源)を得ることができる ·6EaP 諸国の 24 時間コンタクトポイントの役割が強化 ·6EaP 諸国のサイバー犯罪及び電子証拠に関する MLA の手続及び規則の改正のための提言	2015 年 5 月から 2017 年 10 月 31 日

							行の支援 ·EaP6 カ国の 24 時間コンタクトポイントの代表及びその他の国から 2，3 のコンタクトポイントで構成される WG の設置 ·24 時間コンタクトポイントの機能を見直し，役割と責任を明らかにし，かつ，強みと弱点を特定するための WG 会合を 3 回開催 ·今後の行動に関する一連の提言の準備及び採用に関する 24 時間 WG の支援 ·上記の活動の結果出された提言の実行の支援 ·サイバー犯罪対策及び電子証拠に関する MLA の規則及び手続の詳細な分析の準備		
80. iPROCEEDS	欧州評議会サイバー犯罪プログラム事務所(C-PROC)	欧州連合(IPA II 多国籍アクションプログラム 2014)	アルバニア，ボスニアヘルツェゴビナ，モンテネグロ，セルビア，「マケドニア旧ユーゴスラビア共和国」，トルコ及びコソボ	法執行機関その他の政府機関。 (コソボの例：金融情報課，裁判官及び検察官，コソボ警察，コソボ司法研究所等	サイバー犯罪，東南欧州及びトルコ(IPA 地域)におけるオンライン犯罪による収益を対象とする iPROCEEDS プロジェクト	IPA 地域の当局のサイバー犯罪による収益の捜索，差押及び没収並びにインターネット上の資金洗浄を防止する能力を強化すること 指標には以下の事項が含まれる ·サイバー犯罪及びオンライン犯罪による収益に関連した金融犯罪調査の範囲 ·サイバー犯罪，資金洗浄並びに犯罪	・サイバー犯罪シミュレーション演習 ・電子証拠及びオンラインの犯罪収益に関する司法研修 ・サイバー犯罪に係る没収に関する裁判官及び検察官に対する研修 ・電子証拠の取得及び利用に関するワークショップ	·各受益国のオンライン詐欺及びその他のサイバー犯罪に関する公開報告制度(予防機能を持つ)の改善又は創設 指標：各受益国における報告書の受領及び処理並びに分析結果の公表という観点からの公的報告メカニズムの存在及び実績 ·サイバー犯罪による収益の捜索，差押及び没収並びにインター	42 カ月(2016 年 1 月から 2019 年 6 月 30 日)

						による収益の捜索，差押及び没収についての国際基準(欧州評議会条約ETS185 号及び 198 号)の遵守レベル		ネット上の資金洗浄の防止に関する法律をデータ保護要件に沿う形で強化。 指標：国際基準に沿う形で各受益国に出された法制度の改正案の数と質 ·オンラインの犯罪収益の捜索，差押及び没収についての国内のサイバー犯罪対策課，金融捜査機関及び金融情報部門の協力 指標：各受益国におけるサイバー犯罪捜査とそれに伴う並行的な金融捜査（逆も然り）の関連性の数と度合いの増大 ·オンライン詐欺の予防及び管理並びに金融機関のための犯罪資金フローに関する指針の構築及び普及並びにオンライン資金洗浄の予防のための指標の見直し及び更新 指標：この指針に基づく金融機関の指標の公表の数の増加 ·国内及び地域レベルのサイバー犯罪に関する官民情報共有及びインテリジェンス交換メカニズム	

									の設置又は強化 指標：国内及び地域レベルにおける数多くの金融セクターISACs ·司法研修所によるサイバー犯罪及び電子証拠と関連金融捜査及び資金洗浄対抗措置に関する研修 指標：各受益国における司法研修機関による研修コースの増加 ·サイバー犯罪対策課，金融捜査機関及び金融情報部門(FIU)間並びに司法協力所轄官庁間の国際連携及び情報共有の強化 指標：適時性及び協力の要請の数という観点からの国際連携の実効性の強化	

81.GLACY+	欧州評議会(CoE)及び欧州連合(EU)	実行パートナー：ブカレスト欧州サイバー犯罪対策プログラム事務所(実行全般)，インターポールイノベーションのためのグローバルコンプレックス（法執行要素）	優先・中心国：ドミニカ共和国，ガーナ，モーリシャス，モロッコ，フィリピン，セネガル，南アフリカ，錫及びトンガ	司法及び法執行機関職員，判事・裁判官，検察官，法執行機関第一応答者の研修指導者，法執行研修機関及びサイバー犯罪対策課の代表，データ保護当局，市民社会，企業及び学界並びに国家及び各部CERT	サイバー犯罪，電子証拠，省庁間協力	全体目標： 各国が国際人権基準及び法の支配を遵守しつつ，サイバー犯罪対策及び電子証拠に関する法律を適用する能力を強化し，この分野における効果的な国際協力のための能力を強化すること， 本プロジェクトの3つの要素（1)政策及び戦略，(2) 法執行能力及び(3)刑事司法能力 個別目標： 各国がサイバー犯罪対策及び電子証拠に関する法律を適用する能力を強化し，この分野における効果的な国際協力のための能力を強化すること 目標： ･一貫したサイバー犯罪対策及びサイバーセキュリティ政策及び戦略の推進 ･警察機関のサイバー犯罪捜査能力を高め，効果的な警察間並びに欧州及びその他の地域のサイバー犯罪担当部署と協力できるようにすること ･刑事司法当局が法律を適用し サイ		･少なくとも 16 カ国のサイバー犯罪及びサイバーセキュリティ政策及び戦略の強化(優先国及びその他複数の国)及び他国との経験の共有 ･国際及び地域機関間のサイバー犯罪対策に関する政策対話及び連携の強化 ･優先国の法執行機関の能力の評価・サイバーレビューの実現 ･優先国におけるサイバー犯罪及びコンピュータフォレンジック部門の強化及び他国との経験を共有した ･優先国において ECTEG 研修資料へのアクセスを含む法執行研修戦略が利用可能になった ･少なくとも 500 人の法執行機関職員に対する基礎的サイバー犯罪捜査及びコンピュータフォレンジック並びに関連する法の支配要件に関する研修を実施した ･サイバー犯罪対策及び電子証拠に関する国際警察機関間連携がより効果的になった ･優先国の刑事司法能力の評価	48 カ月（2016 年 3 月から 2020 年 2 月）

						バー犯罪及び電子証拠の事案を訴追し，判決を出し，国際協力を行うことができるようにすること		が可能になった ·ブダペスト条約，法の支配及び人権基準に従い優先国のサイバー犯罪対策及び電子証拠に関する法律が強化され，その他の国でも改定作業が開始 ·少なくとも 10 カ国の司法研修所はその一般課程の一環としてサイバー犯罪対策及び電子証拠に関する研修が実施され，他国とその経験を共有 ·少なくとも 10 カ国においてサイバー犯罪対策及び電子証拠に関連する国際司法協力の制度が強化され，手続が改善され，他国とその経験を共有	
82. e 犯罪対策	欧州委員会（資金面）	欧州 8 カ国からの 10のパートナー：トライラテラル・リサーチ＆コンサルティング社，デルフト工科大学，ローザンヌ大学，インスブルック大学，ウォーリック大学，イプソス社，フロー	欧州連合(EU)加盟国		·非 ICT セクター，加盟国及び多種多様なステークホルダーコミュニティ内及びその間におけるサイバー犯罪の観測可能な展開及び効果のマッピング ·既存の対抗措置の評価 ·非 ICT セクターに対	目的： ·政策立案者の意識向上 ·企業のクライムプルーフ（注：犯罪によって得たものではないことが証明済みの意）アプリケーションの提供を支援すること ·サイバーアプリケーションの利用に関する EU 市民の信用及び信頼を向上すること ·EU のセキュリティ雇用プログラムの	主たるテーマと同じ	·サイバー犯罪者がサイバー犯罪を行っている時に取った行動と被害者の行動を提示するジャーニーマップの作成。このマップは，サイバー防御活動の適用が最大の効果を得る共通のピンチポイントを特定することができる。 ·政策及び執行対応を含む現在の対抗措置に関する報告書の作成 ·既存のサイバー犯罪技術及びベ	2014 年 4 月から 2017 年 3 月

		ニンゲン大学，グローバルサイバーセキュリティセンター(GCSEC)，タリン工科大学，インターポール			するサイバー犯罪の経済的影響の評価・測定 ·サイバー犯罪に対処するための具体的なセクター間及びセクター内のソリューションの構築	効果へ寄与すること 目標: 1. 非 ICT セクター（運輸，エネルギー，金融，医療等）へのサイバー犯罪の経済的影響を測定・分析し，当該犯罪の背後にある犯罪構造及び経済組織を分析すること 2. 想起される犯罪の抑止及び当該犯罪の魅力を劇的に減らすための具体的な措置及び方法の構築		ストプラクティスの評価書の作成 ·様々なサイバー犯罪及び非 ICT セクター内の犯罪者ネットワークに関する目録の作成	
83. 信頼醸成措置（CBM）	欧州安全保障協力機構（OSCE）	OSCE 加盟国，国際機関	欧州，中央アジア及び北米の57参加国	政府，政府機関，法執行機関	重要インフラ防護，国際協力，情報共有，意識啓発	·情報通信技術(ICT)の利用から生じる紛争のリスクを軽減すること ·国家間の協力，透明性，予測可能性及び安定性を強化すること ·ICT の利用から生じ得る誤解，エスカレーション及び紛争のリスクを軽減すること	地域及び準地域レベル等におけるワークショップ，セミナー及びラウンドテーブル		初回: 2013 年 第 2 回: 2016 年

84. サイバー犯罪意識啓発及び防止	欧州刑事警察機構（ユーロポール） 欧州サイバー犯罪センター（EC3）	EU 加盟国の法執行機関	EU 加盟国	一般大衆，立法者	サイバー犯罪，オンライン児童性的搾取，決済詐欺	·加盟国のサイバー犯罪との闘いにおける予防能力の強化及び加盟国の法執行機関がサイバー犯罪者の一歩先を行くために支援すること ·早期警戒，サイバー犯罪脅威評価及び意識啓発の方法を専門に追求すること ·既存の意識啓発イニシアティブを促進し，主なテーマの分野に関する新しいイニシアティブの構築，交付及び提携に寄与し，また，可能であれば NGO，民間セクター及び学界のパートナーも関与させること	·犯罪予防に関する助言 ·安全なインターネットの日 ·立法者への予防措置の提供 ·脆弱性及び手続的格差のスキャニング ·予防イニシアティブの促進及び資金調達		
85. サイバー犯罪対策研修コース	欧州刑事警察機構（ユーロポール） 欧州サイバー犯罪センター（EC3）	·欧州警察大学校（CEPOL） ·欧州サイバー犯罪研修教育グループ(ECTEG) ·その他 EU 内外の法執行機関に研修を提供するための関連するパートナー	EU 加盟国	EU 加盟国の法執行機関	サイバー脅威及びサイバー犯罪への対処法	急速なペースで発展するサイバー犯罪により欧州の公的サービスの迅速かつ効果的な対応が求められている。しかしながら，加盟国が有するサイバー犯罪対策に関する専門的知見は同等な水準にはないため，他の犯罪のように当該脅威を効果的に対応することができない。EC3 は，サイバー犯罪に効率的に対処するために必要なツールへの平等なアクセスを確保することによりこの不均衡を是正するよう努める。　また，EC3 は様々なサイバー脅威に対処するための最新の手法を	·オープンソース IT フォレンジックに関するユーロポール研修コース ·支払カード詐欺フォレンジックに関するユーロポール研修コース ·インターネット上の児童の性的搾取の撲滅に関するユーロポール研修コース ·支払カード詐欺に関する戦術・技術研修		

						使って法執行機関に研修する。 ·EU 加盟国法執行機関のキャパシティビルディング及び研修の支援			
86. PADOS: 直接民主主義，オープンガバナンス，効率的 e 政府サービス	HAUS フィンランド公的管理機関 （フィンランド）	e ガバナンス・アカデミー，エストニア外交学院，公的サービス開発・研修センター(ATAK)	アルメニア，アゼルバイジャン，ベラルーシ，ジョージア，モルドヴァ及びウクライナ		中央 e 政府，e 民主主義，サイバーセキュリティ	意思決定及びガバナンスの透明性及び開放性を強化し，民主的なガバナンスを支援すること プロジェクトの 3 つの要素： 1. 市民参加，e 民主主義，オープンガバナンス 2. e ガバナンス，サイバーセキュリティ，データ保護 3. 公共管理改革及び複雑な環境における新たなリーダーシップ	·各国の実情調査 ·ワークショップ，セミナー及び研修訪問 ·ニーズ評価，欧州のベストプラクティス分析及び提言		2015 年 2 月から 2016 年 1 月
87. インターネットガバナンス及びデジタル政策キャパシティビルディングプログラム	ディプロ財団 (Diplo)	主：スイス政府 特定のイニシアティブ：マルタ，メキシコ，南アフリカ，印，エジプト，オマーン政府，欧州委員会（EDF 及び FP7），国連(ITU)，欧州評議会，英連邦，DCAF 並びに Hivos, ISOC，ベリサイン社，AT&T	全世界	国際機関，政府，企業，市民社会及び学術界	·インターネットガバナンス及びデジタル政策 ·サイバーセキュリティ ·プライバシーとデータ保護 ·e 外交及び e 市民参加 ·サイバー外交 ·デジタル・プロセス及び主体 ·児童と携帯技術 ·重要インターネット資源及びインフラ	インターネットの将来を決める政策過程に関する小国及び途上国の効果的な参加を支援すること	以下の活動を組み合わせて企業等にカスタマイズされた研修プログラム及びコースの提供 ·インタラクティブなオンラインコース ·講義，討論，シミュレーション，ケーススタディに基づくオンサイト（現場）研修プログラム及び対面ワークショップ ·研修者研修ワークショップ ·スクール（例：2014 年西バルカン及びモルドヴァのためのサイバーセキュリティウィンタースクール） ·意識啓発資料(イラスト，漫画，ビデオ，アニメ)	2005 年以降，サイバーコースとプログラムへ 140 カ国以上（26 の小島途上国及び 39 後発開発途上国を含む)から 1500 人以上が参加：現在は 1600 人以上の政府職員及び専門家からなるグローバルコミュニティ	継続中

		社，アフィリアス，加産業省，GSMA 等 特定の活動の実施：アフリカ連合委員会，NEPAD，太平洋共同体事務局，UNESCWA，アフリカ・太平洋・カリブ地域諸国，欧州委員会，カリブ電気通信連合，UNECA 及びその他の現地パートナー			·政策研究手法 ·ICT 政策及び戦略立案 ·キャパシティ・デベロップメント		·コミュニティの実務の円滑化 ·認可を受けた大学院の学位及びインターネットガバナンスに特化した現代外交修士課程（マルタ大学との協力による）		
88. 国際サイバーセキュリティ交渉のためのキャパシティビルディングプログラム	ICT4 平和財団	プログラム・パートナー： 英，独，スイス，ケニア，蘭，星，加，米国，豪州政府 地域的ワークショップのパートナー：アフリカ連合，クリンゲンタール国際	ASEAN 地域，東アフリカ諸国，ラテンアメリカ地域，アフリカ連合加盟国，ジュネーヴ外交官コミュニティ	外交官，政府職員，学界及びシンクタンクの代表者	サイバーセキュリティ，サイバーセキュリティ外交	長期目標 責任ある国家の行動の国際規範，信頼醸成措置(CMBs)及び国際協力の促進を通じたサイバー領域の権利及びセキュリティに対するリスクの軽減 短期目標 ·世界のすべての地域の公務員・外交官，企業，市民社会の代表のサイバー空間における国際規範，CBM 及び	これまでに実施したコースの一覧 ·ラテンアメリカ諸国のためボゴタにおいて OAS が実施：国際サイバーセキュリティ外交コース(2016 年） ·東アフリカ諸国のためナイロビにおいてケニア政府が実施： 第 1 回国際安全保障及びサイバー空間における外交に関するアフリカ地域研修ワークショップ(2015 年 3 月） ·サイバー空間に関するハーグ会議	·規範及び CBM に関するすべての地域の政府，事業者，学界を含む市民社会のすべてのステークホルダーによるよりインクルーシブな知識ベースの議論，協議又は交渉の実現 ·規範，CBM 及び国際協力に関する二国間，地域及び世界レベルの合意の増加 ·持続的，オープン，繁栄した，信	2014 年から 2016 年

			関係研究所,ジュネーヴ安全保障政策研究所(GCSP), ケニア, シンガポール, オランダ政府, 米州機構及び S.ラジャラトナム国際関係学院(RSIS)			国際協力のより深い理解 ·ロンドン・プロセス, 国連 GGE, OSCE, ASEAN, OAS, EU, AU 及び AP-CERT 等のフォーラムにおける国際議論並びに地域的及び世界的交渉への参加者の拡大 ·地域レベルにおけるサイバーセキュリティ分野の懸念, ベストプラクティス, 政策及び制度的取決めについてのより良い理解 ·世界的, 地域的及び国際的なサイバーセキュリティの議論, 研究及び交渉の今後の展開に関する情報の更新及び交換を行うためのワークショップコースの卒業生, 講師及び専門家のネットワークの構築	(GCCS)においてオランダ政府が実施: 国際サイバーセキュリティ外交(2015 年 4 月) ·ASEAN 諸国のためシンガポール政府と共催: サイバーセキュリティ政策及び外交(2015 年 10 月) ·アフリカ諸国のためアフリカ連合と共催(2016 年 2 月) ·ジュネーヴの外交コミュニティのためジュネーヴ安全保障政策センター(GCSP)と共催(2016 年 3 月) ·中国政府及び国連「サイバー空間のための規範, 規則及び原則の構築:オープン・安全・安定・アクセシブルかつ平和的な ICT 環境の促進」と共催(2016 年 7 月) ·戦略・国際研究所(Institute for Strategic and International Studies)と共催(2016 年 11 月)	頼できる, 安心, 安全なサイバー空間の構築へ向けた進展	
89. 国際安全保障サイバー問題ワークショップ	国連軍縮研究所(UNIDIR)	UNIDIR 主要資金提供者, オランダ及び米国政府	全世界	政府, 国際機関	サイバーセキュリティ, 規範作り, 法的措置及びサイバーツールの悪用に対するアプローチ法	数多くのサイバーセキュリティ問題に関する共通認識及び相違点を特定すること	招待者のみを対象とした専門家ワークショップ 3 回	報告書	2016 年

90. サイバー安定性会議	国連軍縮研究所(UNIDIR)	チャタムハウス, VERTIC, フランコフォニー(仏語圏)国際機関 UNIDIR 主要資金提供者の支援が全ての活動の基礎を提供。 プロジェクトへの資金提供:豪州(2014 年, 2015 年), 独 (2012 年, 2014 年), オランダ(2015 年), スイス(2014 年, 2015 年), 米(2012 年)及びフランコフォニー国際機関(2012 年)	全世界	政府, 国際機関	サイバーセキュリティ, 信頼醸成措置	紛争時のエスカレーションのリスク及び透明性及び信頼醸成措置の実施に特に焦点を置いたより安全で予測可能なサイバーセキュリティ環境の実現のための実利的な手段をいかにとるべきかについてステークホルダーが議論する機会を提供すること	会議	報告書	2012 年以降
91. 国連 GGE(宇宙及びサイバー)支援	国連軍縮研究所(UNIDIR)	UNIDIR 主要資金提供者の支援が全ての活動の基礎を提供。 国連軍縮部(プロジェクトの資金面)	全世界	国連事務総長の政府専門家会合(GGE)	サイバーセキュリティ, 信頼醸成措置	·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展に関するGGE(2009-2010 年, 2012-2013 年, 2014-2015 年, 2016-2017 年)の支援 ·宇宙空間における透明性及び信頼醸	コンサルティング業務	調査報告書	2009 年から 2015 年

						成措置に関する GGE(2012-2013 年)の支援			
92. サイバー犯罪対策に関するグローバルプログラム	国連薬物犯罪事務所 (UNODC)	豪州, 加, ノルウェー, 日, 英及び米等 UNODC 拠出国	中央アメリカ, 東アフリカ及び東南アジア	法執行機関, 検察官, 裁判官, 中央政府, パブリック・アウトリーチ(予防教育を含む)	サイバー犯罪, デジタルフォレンジック及び人権	1. 各地域内の現在のサイバー犯罪対策の理解の促進 2. サイバー犯罪の特定, 対処及び予防のための知識, スキル及び運用能力の強化 3. サイバー犯罪に係る地域協力及び情報交換メカニズムの強化	·法執行機関, 検察官及び裁判官への地域研修 ·サイバー犯罪対策ワークショップ ·国のサイバー犯罪対処能力の評価 ·	·サイバー犯罪の捜査及び訴追に関する地域研修ワークショップ(入門レベル)に 11 人の検察官及び 18 人の法執行機関職員が参加 ·サイバー犯罪の捜査及び訴追に関する地域研修ワークショップ(上級レベル)に 11 人の検察官, 18 人の法執行機関職員及び 1 人の CERT 職員が参加 ·電子証拠に関する地域研修に 16 人の検察官及び 2 人の裁判官が参加 ·5 カ国(ミャンマー, タイ, 越, 比及びカンボジア)におけるサイバー犯罪対策に関する国家の連携及び官民連携ワークショップを開催。各国の法執行機関, 司法機関, 検察機関, 電子通信機関, 金融機関, 専門家が参加 ·8 カ国の国別評価報告書を起案: カンボジア, ラオス, 尼, 馬, 緬, 泰, 比及び越	2014 年 7 月開始 2014 年 7 月から 2017 年 12 月まで

93. キルギスにおける初の e 医療サービス	国連開発計画（UNDP）	国家の医療機関	キルギス	医療従事者	e ガバナンス，e 医療サービス	人命を救う情報を伝達するための e-ヘルス技術の活用	詳細は不明	同左	同左
94. グアテマラにおけるウェブ及びモバイル技術の利用	国連開発計画（UNDP）	グアテマラ政府「ミ・ファミリア・プログレサ」	グアテマラ	親	e ガバナンス，e 医療サービス	5 歳未満の児童の慢性的な栄養失調と闘うためのデータの取得	家族の送金等グアテマラのすべての社会的投資を追跡，監視する国家のウェブベースの情報システムの構築。パイロット版では，貧しいコミュニティへのサービスの提供を改善するために携帯技術を利用し，e ガバナンスが何を達成できるかを模索。		
95. アフリカ e ガバナンスアカデミー	国連開発計画（UNDP）		アフリカ		e ガバナンス	いかに ICT が政府の機能及びサービス並びに行政セクター間の意思疎通を改善することができるかを実証すること		e ガバナンスのための地域機関をミレニアム開発目標(MDGs)に関連したネットワーキング，研修及び研究のハブにすること	
96. ICT がどう議会をエンパワーできるかを評価	国連開発計画（UNDP）	EU	全世界	国会議員	e ガバナンス，ICT	ICT の利用がどうすれば議会及び議員をエンパワーすることができるかを検討すること	実行可能性調査(F/S)		
97. 西アフリカにおける e 参加（電子政府への市民参加）の増加	国連開発計画（UNDP）	パノス研究所	西アフリカ	市民	e ガバナンス及び e 参加	政治過程の透明性の向上，民主的プロセス及び意思決定における市民の直接参加の強化及び意見形成の質の改善（情報及び審議のための新たな場の開設）方法	西アフリカにおける e 参加の手法についての知識の向上及び普及		

98. 女性のエンパワーメントのための e 政府	国連アジア太平洋経済社会委員会(UNESCAP)	国連経済社会局(UNDESA)行政開発管理部のプロジェクト・ガバナンス事務局(UNPOG)		女性	e 政府のジェンダーの側面	目的: ジェンダー格差の是正, UNESCAP は e 政府の女性のニーズに対応し, インクルーシブかつ持続可能な開発のため男女平等を促進する能力を構築するためのツールを開発している。 目標: 政府の女性のニーズに対応できる e サービスの設計, 開発及び実施を支援するための新しいツールを提供すること	関連する問題及びグッドプラクティスに取り組んでいることを確実にするための研修モジュールの大枠の評価(報告)に専門家を関与させるための専門家グループ会合の実施 研究(2017 年上半期)		2016 年以降
99. サイバーセキュリティに関する国家の政策及び法制度整備支援	国連アフリカ経済委員会(UNECA)		ブルキナファソ, ガーナ, ギニア, ケニア, モザンビーク, セーシェル, ルワンダ, タンザニア等		サイバーセキュリティ政策及び法制度	ICT の利用における信頼及び安全性の確保	加盟国の要請に応じて ·サイバーセキュリティに関する助言サービス ·サイバーセキュリティの特定の政策及び法枠組み構築支援		2015 年
100. 調和のとれた ICT 法制度及びサイバーセキュリティ政策の実施	国連アフリカ経済委員会(UNECA)	アフリカ連合委員会(AUC),西アフリカ諸国経済共同体(ECOWAS), 南部アフリカ開発共同体(SADC)	ECOWAS 及び SADC 加盟国		サイバーセキュリティ, 政策及び法制度構築	準地域レベル及び加盟国におけるサイバーセキュリティ法の調和の支援	サイバーセキュリティに関する法制度の調和についての一連のワークショップ		2015 年

101. サイバーセキュリティ及び個人データ保護に関するアフリカ連合条約策定支援	国連アフリカ経済委員会（UNECA）	アフリカ連合委員会，地域経済共同体(REC)	REC 加盟国		e 取引，サイバー犯罪，個人データ保護		キャパシティビルディング及び意識啓発キャンペーン		2014 年から 2015 年
102. アフリカ地域におけるステークホルダー協議及び意識啓発活動	国連アフリカ経済委員会（UNECA）	ITU，UNCTAD，地域経済共同体(REC)（例：SADC 及び ECOWAS），各国政府，アフリカ連合委員会(AUC)，アフリカ開発のための新パートナーシップ(NEPAD)等	ボツワナ，ガンビア，ケニア，ニジェール，ルワンダ，スワジランド，タンザニア，トーゴ，ウガンダ，ザンビア，ECWAS 及び SADC 加盟国	政府，政策立案者，国会議員(e.g. SADC 議会フォーラム)，REC，民間セクター，市民社会，学界等	ICT 関連セキュリティ問題，立法，意識啓発	·意思決定者及びその他のステークホルダーの能力支援 ·より良い政策及び戦略のオーナーシップ並びに効果的なサイバーセキュリティ政策の実施を確保すること ·意識啓発，証拠に基づく政策過程及びキャパシティビルディング活動を支援すること ·社会経済的発展のための ICT の潜在能力を活用できる必要最低限の ICT スキルを構築すること ·安全で安心できる環境において ICT の恩恵を享受できるようにすること	·地域ワークショップ及び研修コース（クラッカー・ハッカー，電話及びパソコン攻撃，CCTLD，サイバーセキュリティ政策） ·ウェブ・ポータル及びオンラインディスカッション ·サイバーセキュリティに関する簡潔な報告書等 ·加盟国の政策，法規制及びインフラの要件を満たす能力を強化するためのケニアにおけるアフリカサイバーセキュリティ戦略プログラム		2013 年から 2015 年
103. CIRT の設置	国際電気通信連合（ITU）	2013 年以降 ITU オマーン地域的サイバーセキュリティセンター，及びプロジェクトによりその他のパートナー	国連加盟 193 カ国	政府機関及び政府機関を通じた技術コミュニティ，法執行機関，民間セクター，市民を含む関連する主体	サイバーセキュリティ（技術面）	国家 CIRT の計画，実行及び運用	計画，場所の特定及び準備，機材及びソフトウェアの調達，設置及びテスト，人材の配置，人事研修 （国家 CIRT は，当該国が全期間集中して準備を行えば 11 カ月間で実行可能）	国際的に認められる機能的な国家 CIRT 12 の国家 CIRT が実行され，現在 3 つが準備中。	2012 年以降，要望に基づき実施

104. CIRT の実行	国際電気通信連合（ITU）	ITU-IMPACT イニシアティブの下の ITU オマーン地域的サイバーセキュリティセンター（2013 年以降）	国連加盟 193 カ国; ·国家 CIRT を創設した11カ国：ブルキナファソ，象，キプロス，ガーナ，ジャマイカ，ケニア，モンテネグロ，タンザニア，トリニダード・トバゴ，ウガンダ，ザンビア ·CIRT を実行中の 4 カ国：バルバドス，ブルンジ，ガンビア，レバノン ·CIRT 強化中の国：ケニア	政府機関及び政府機関を通じた技術コミュニティ，法執行機関，民間セクター，市民を含む関連する主体	サイバーセキュリティ（技術面）	国家 CIRT の計画，実行及び運用	計画，場所の特定及び準備，機材及びソフトウェアの調達，設置及びテスト，人材の配置，人事研修 （国家 CIRT は，当該国が全期間集中して準備を行えば 11 カ月間で実行できる）	国際的に認められる機能的な国家 CIRT 12 の国家 CIRT が実行され，現在 3 つが準備中	2012 年以降，要望に基づき実施
105. 人のキャパシティビルディング	国際電気通信連合（ITU）	2013 年以降 ITU オマーン地域的サイバーセキュリティセンター，ITU アカデミー及び ITU センターオブエクセレンス	国連加盟 193 カ国	政府機関及び政府機関を通じた技術コミュニティ，法執行機関，民間セクター，市民を含む関連する主体	サイバーセキュリティ	各国の要請に応じたサイバーセキュリティの主体への特定の分野の研修	必要に応じて対面及びオンラインワークショップ，研修及び演習	参加者の認証と研修分野のノウハウの強化	要請に応じて継続中

106. 技術協力	国際電気通信連合(ITU)	2013 年以降 ITU オマーン地域的サイバーセキュリティセンター，協力の内容によりその他のパートナー	国連加盟 193 カ国	政府機関及び政府機関を通じた技術コミュニティ，法執行機関，民間セクター，市民を含む関連する主体	サイバーセキュリティ	·個別のサイバーセキュリティ技術評価(脆弱性評価，内部・外部ペネトレーションテスト，ウェブアプリケーション評価)を実施すること ·技術的インシデント管理サービス(脅威分析，警戒・警報，インシデントレスポンスハンドリング，リアルタイムネットワーク監視，ログの保存・管理，データ漏洩防止，ハニーネット)を実施	·機材・ソフトウェアのインストール及びテスト ·ワークショップ ·研修 ·ハッカソン ·演習	参加者の技術支援の性質に従い提供される新しいツールの使用法に関する技術的知見の強化	2010 年以降要請に応じて継続中
107. 地域的サイバー演習	国際電気通信連合(ITU)	2013 年以降 ITU オマーン地域的サイバーセキュリティセンター，イベントによりその他のパートナー	国連加盟 193 カ国(これまで 100 カ国が参加)	政府機関特に国家 CIRT	サイバーセキュリティ，技術能力	·国際基準及びグッドプラクティスに調和した国家 CIRT の効果的なインシデント管理の確保 ·国家 CIRT 間の技術レベルの協力の促進	サイバー演習は 5 日間のイベント(参加者無制限のワークショップ(2-3 日間)及び 2 日間の国家 CIRT の技術スタッフのためのサイバー攻撃シミュレーション演習	·参加者の特に攻撃の検知，解析ハンドリング及び調整等のインシデント管理に関する技術知識の強化 ·これまで 13 のサイバー演習を実施	
108. ITU サイバーセキュリティ意識啓発	国際電気通信連合(ITU)	2013 年以降 ITU オマーン地域サイバーセキュリティセンター，及び要請に応じてその他のパートナー	国連加盟 193 カ国	政府機関	サイバーセキュリティ	·地域及び国際的なサイバーセキュリティのイベントの主催及び参加を通じて対話及び意識啓発を促進すること ·ITU セクターのメンバーに専門的な報告書及び情報を広めることを通じてサイバーセキュリティ及び国，地域及び国際レベルの現在及び将来の状態に関する質の高い情報をメンバーに,提供するために同メンバー及び産業界のパートナーを活用すること ·ITU 加盟国を ITU-D 研究グループ 2	·ワークショップ ·アドボカシー・意識啓発キャンペーン ·要請に基づく地域的意識啓発イベント ·ウェビナー(オンラインセミナー) ·研修 ·WSIS(アクションライン C5)，テレコムワールド，規制者のグローバルシンポジウム(GSR)等の具体的な年次会合 ·年 2 回の研究グループ ·年 6 回のオンライン児童保護イベント ·年 2 回の出版	参加者のサイバーセキュリティ及びオンライン児童保護の意識の向上	具体的な活動に記載

						課題 3（グローバルなサイバーセキュリティ文化の構築のためのベストプラクティス）に参加することを促し，その内容に寄与すること ･オンライン児童保護について国レベルの意識啓発を行い，行動を呼びかけること			
109. CIRT 評価	国際電気通信連合（ITU）	ITU オマーン地域的サイバーセキュリティセンター	国連加盟 193 カ国；評価済 65 カ国： ･アフリカ：アンゴラ，ボツワナ，ブルキナファソ，ブルンジ，カメルーン，チャド，コモロ連合，コンゴ民主共和国，コンゴ共和国，象，ジブチ，ガボン，ガンビア，ガーナ，ケニア，レソト，リベリア，モーリタニア，ニジェール，ルワンダ，セネガル，スーダン，スワジランド，タンザニア，トー	政府機関及び政府機関を通じた技術コミュニティ，法執行機関，民間セクター，市民を含む関連する主体	サイバーセキュリティ（技術面）		CIRT 評価は，国家レベルのサイバーセキュリティ問題を認識し，国家 CIRT の運用をより良く理解するための初のワークショップを含む 5 日間の実地視察の際に通常行われる その後の分析及び報告書の作成はオフサイトで行われ， 対象国へ最終報告書を提出することで完了する。	各国の国家 CIRT の実行のためのそれぞれにカスタマイズされた詳細なロードマップの策定。 65 の評価を実施済	2010 年以降要請に基づき継続中

				ゴ，ウガンダ，ザンビア，ジンバブエ ·アジア太平洋：アフガニスタン，バングラデシュ，ブータン，カンボジア，キプロス，フィジー，ヨルダン，ラオス，レバノン，　モルディブ，緬，ネパール，パレスチナ，バヌアツ，越 ·中南米：アンギラ，アンティグア・バーブーダ，バルバドス，ボリビア，ドミニカ，ドミニカ共和国，エクアドル，グレナダ，ホンジュラス，ジャマイカ，スリナム，セントクリストファーネーヴィス，セントルシア，セントヴィンセント及びグレナディーン諸島，トリ						

			ニダード・トバゴ ・欧州：アルバニア，アルメニア，マケドニア，モナコ，モンテネグロ，セルビア						
110. ITU グローバルサイバーセキュリティインデックス（GCI）	国際電気通信連合（ITU）	GCI バージョン1の共同作成者：ABI リサーチ社。現行の GCI バージョン 2 については 13 のパートナーに拡大	国連加盟 193 カ国（うち 105 カ国が回答済）	政府機関	サイバーセキュリティのあらゆる側面（法的，技術的，組織的，キャパシティビルディング，協調体制）	各国のサイバーセキュリティへの関与度を測定することによってサイバーセキュリティの分野において改善すべき点を特定するのを助け，また，各国のランキングを上げるために行動をとる意欲を起こすことによって世界全体のサイバーセキュリティの底上げを支援すること	・政府機関へのオンラインアンケート ・世界の地域及びテーマごとの結果（法的，技術的，組織的，キャパシティビルディング，協調体制）から構成される自由な GCI インデックスの公表 ・自由な特定及び共有されたベストプラクティス ・次の GCI バージョン(2016)は特定の地域又はテーマに関する定性分析を行う予定	ランキング及び弱点分野を特定された各国の政府がサイバーセキュリティにおける的を絞った正しいキャパシティビルディングを行い改善するよう努めること	2016 年以降は 2 年ごとに作成予定（第 1 版は 2013 年に開始，2014 年完了），新版は 2015 年 1 月開始，2017 年上半期に完了予定）

111. 国家サイバーセキュリティ戦略ツールキット	国際電気通信連合(ITU)	14 のパートナー(GCSCC を含む)との新規プロジェクト	国連加盟 193 カ国	政府機関及び政府機関を通じた技術コミュニティ，法執行機関，民間セクター，市民を含む関連する主体	·国家のサイバーセキュリティ管理責任 ·国家の情報セキュリティ枠組み ·重要情報インフラ防護 ·国家のインシデントレスポンス ·研究及びイノベーション ·国家の意識啓発及び人員育成 ·国際連携 ·法制度及び法執行 ·国防及びインテリジェンス	ツールキットはレファレンスガイド及び評価ツールから成る ・レファレンスガイドは，各国が国家戦略の目的及び内容，戦略策定手法，関連するモデル及び利用可能な資源並びに様々な組織から受けることができる支援等を含む当該イニシアティブに関連があるすべての側面についての明確な理解を得るための唯一のソースとなる ・評価ツールは各国がその現在のすべてのサイバーセキュリティの戦略的分野の成熟度を評価し，改善の余地がある分野を特定し，必要に応じてその状態の再評価をできるようにする。	·ツールキットの作成 ·すべての国への普及・啓発セッション ·各国のオンライン評価 ·ワークショップ，研修棟を含む国家戦略の策定又は見直しのための各国の要請に応じた支援	本プロジェクトの成果として国家戦略を持つ加盟国の数が大きく増えるべき	2015 年 6 月，ツールキットの作成開始，国家戦略サービス及びオンラインツールは 2017 年上半期に利用可能予定

112. アラブ地域のためのサイバーセキュリティイノベーションセンターの設置	国際電気通信連合(ITU)	ITU と対サイバー脅威国際多国間提携パートナーシップ(IMPACT)の枠組み内（ITU-IMPACT イニシアティブ）及び 2012 年 12 月 15 日オマーン情報技術庁と ITU 間で締結された行政協定の規定に従う	アラブ地域:; サイバーセキュリティイノベーションセンターはオマーンのマスカットにある OCERT が主催		サイバーセキュリティ	オマーン情報技術庁(ITA)を代表するオマーン CERT(OCERT)の支援を受け，アラブ地域のサイバーセキュリティイノベーションセンターを設置すること		アラブ地域への ITU のサイバーセキュリティ関連イニシアティブの理解を深めるのみならずアラブ地域におけるサイバーセキュリティ，重要インフラ防護及びヒトのキャパシティビルディングの分野の能力，機能，準備態勢，技能及び知見の強化が期待される。	2013 年から 2016 年
113. CIRT 強化	国際電気通信連合(ITU)	2013 年以降 ITU オマーン地域的サイバーセキュリティセンター，プロジェクトによりその他のパートナー	国連加盟 193 か国	政府機関及び政府機関を通じた技術コミュニティ，法執行機関，民間セクター，市民を含む関連する主体	サイバーセキュリティ（技術面）	国家 CIRT の強化された機能の見直し，企画，実行及び運用	企画，機材及びソフトウェア調達，設置・インストール・テスト，人材の配置及び研修	1 つの国家 CIRT の強化。	2015 年以降要請ベースで継続中
114. サイバー犯罪及び電子証拠に関する東アフリカ刑事司法ネットワーク	英連邦サイバー犯罪イニシアティブ(CCI)後援の国連薬物犯罪事務所(UNODC)及び英連邦事務局	当該ネットワークとその運営員会(網羅的ではない)へ助言を行う役割を有する国際機関及び地域機関: ·国連薬物犯罪事務所(UNODC)	·現在の委託事項（TOR）採択時の東アフリカ共同体(EAC)加盟国: ブルンジ，ケニア，ルワンダ，タンザニア及びウガンダ ·東アフリカ地域の	EAC 加盟国及びその他のアフリカ諸国の刑事司法職員及び主なステークホルダー並びに政府間及びその他の関連組織の代表	サイバー犯罪及び電子証拠	1. サイバー犯罪との闘いに関する問題についての加盟国の刑事司法及び法執行機関のカウンターパート間の情報交換の促進 2. 刑事司法及び法執行部門とその他の主なステークホルダー間の仕事上の関係の円滑化	開始:サイバー犯罪対策及び電子証拠に関する東アフリカネットワーキング会合(2015 年 8 月 19-20 日於ナイロビ）－本ネットワークの取決め事項の採択 2016 年 4 月 －サイバー犯罪捜査及びデジタルフォレンジック基本研修:3 日間の法執行捜査機関及び検察官のた	本ネットワークは下記の加盟国の当局間の連携を促進する。 ·サイバー犯罪及び関連事項の問題に関する国家のコンタクトポイントに（法又は行政命令により）任命された事務局又は人 ·既存のインターポールの専門家グループを考慮し，サイバー犯罪	

		·英連邦サイバー犯罪イニシアティブ(CCI)後援の英連邦事務局 ·インターポール ·東アフリカ警察長機構(EAPCO) ·アフリカ連合(AU) ·国際電気通信連合(ITU) ·欧州評議会	その他の国:ジブチ，エリトリア，エチオピア，ソマリア及び南スーダン 他国，地域機関又は国際機関の参加又はアドホックなパートナーシップ並びに地域的又はテーマ別のネットワーク又はプラットフォームは，その参加が当該ネットワークに有益かどうかに基づいて当該ネットワークの運営委員会が決定する。				めのサイバー犯罪捜査及びデジタルフォレンジック基本研修ワークショップ(ウガンダ，カンパラ於)	の検知及び捜査を担当する法執行機関職員(各加盟国から 2 名) ·サイバー犯罪の訴追権限を持つ検察官(各加盟国から 1 名) ·司法機関(各加盟国から 1 名) 司法共助，犯罪者引渡し及びその他の国際協力の要請の執行を受理，処理及び促進することを指定された中央政府機関(各加盟国から 2 名) ·電気通信事項担当省・政府機関(各加盟国から 1 名) ·本ネットワークの実効性を確保するため，各加盟国より加盟国内の前述の国家機関間の調整を円滑にする任務を受託する政府の特定の事務局の者から「国家フォーカルポイント」を 1 名指名する	
					3. サイバー犯罪対策に関する加盟国間の公式及び非公式の国際協力の円滑化と促進 4. サイバー犯罪と闘うための国際協力の分野におけるベストプラクティス，国内法の調和及び技術協力のニーズについての情報の交換 5. サイバー犯罪事例のデータベースの構築及び各地域におけるサイバー犯罪のパターン及び傾向についての情報の整理 6. 加盟国のための研修及びキャパシティビルディング活動の促進及び調整 7. 電子証拠を含むサイバー犯罪に関する法的問題についての協力の促進 8. 加盟国のニーズ及びネットワーク自体に有益と考えられるその他の形式の協力の促進及び円滑化			

115. ECOWAS におけるサイバー法の調和に関する地域セミナー	国連貿易開発会議（UNCTAD） E コマース及び法改革プログラム	·ECOWAS 委員会 ·フィンランド政府 ·国連開発アカウント 特定の活動：欧州評議会 その他：アフリカ連合委員会，ITU，国連国際商取引法委員会（UNICITRAL）等	ECOWAS 諸国：ベナン，ブルキナファソ，カーボヴェルデ，象，ガンビア，ガーナ，ギニア，ギニアビサウ，リベリア，マリ，ニジェール，ナイジェリア，セネガル，シエラレオネ及びトーゴ	政策立案者，立法者，法執行機関職員（警察及び判事）	E コマース法：e 取引，データ保護，サイバー犯罪及びサイバーセキュリティ，オンライン消費者保護，オンラインコンテンツ及びドメイン名規制	ECOWAS 地域におけるサイバー法の現況評価及び地域レベルで採用された次の文書に記載のある e 取引，データ保護及びサイバー犯罪の分野におけるサイバー犯罪の調和プロセスを進展する最良の手法を議論するための代表団の能力及び専門性を強化すること: ·個人データ保護に関する補足法 A/SA.1/01/10 ·電子取引に関する補足法 A/SA.2/01/10 ·サイバー犯罪に関する 2011 年 8 月 19 日指令 C/DIR/1/08/11 これらの分野を超え，消費者保護，オンライン規制及びドメイン規制等のその他の問題も e コマースの発展に影響を与えるため統合された。	2013 年から 2015 年にかけて UNCTAD は ECOWAS にキャパシティビルディングプログラムを実施。 315 人の政策立案者及び立法者への e コマースの法的側面についてのオンライン研修セッション 2 回，ECOWAS 加盟国から集まった 69 人の代表への地域ワークショップ 3 回。うち 1 回は欧州評議会と連携して開催。 その他アフリカ連合委員会，ITU 及び UNICTRAL が協力。	·384 人の ECOWAS の代表への研修 ·対面ワークショップは，加盟国代表間のグッドプラクティスの交換を実現し，特に今まで法律を制定していない者の助けとなった。	2013 年から 2 年間
116. e コマースの強化のためのサイバー法規制に関する専門家会合	国連貿易開発会議（UNCTAD） E コマース及び法改革プログラム	·ASEAN ·英連邦事務局 ·国際消費者 ·東アフリカ共同体(EAC)事務局 ·e ベイ社 ·西アフリカ諸国経	政府間専門家会合	70 カ国の政策立案者，立法者，法執行機関職員，民間セクター及び市民社会代表者計 250 名	e 取引，データ保護，サイバー犯罪，オンライン消費者保護，地域的サイバー法整備	各国が法枠組みを見直し，経験を共有し，互いに学び合うためのプラットフォームとしての機能を果たすこと 初の世界の e 取引，消費者保護，データ保護及びサイバー犯罪分野の法律のマッピング結果を示した	ケーススタディ等を含む e コマースの促進のためのサイバー法と規制専門家グループ会合	サイバー法に関するベストプラクティスの特定及び e コマースを促進するための法枠組みに関する提言	2015 年 3 月 25 日から 27 日

		済共同体 (ECOWAS) ·欧州委員会 ·フィンランド政府 ·国際電気通信連合(ITU) ·ジュミア(ナイジェリア企業) ·経済協力開発機構(OECD) ·国連国際商取引法委員会 (UNCITRAL) ·国連開発アカウント ·国連西アジア経済社会委員会 (ESCWA) ·国連薬物犯罪事務所(UNODC) ·米国 ·万国郵便連合 (UPU) ·米連邦取引委員会 ·世界銀行				(unctad.org/cyberlawtracker 参照) あらゆる開発レベルにある国の政策立案者及び立法者並びに民間セクターが直面する課題の検討. ASEAN, EAC, ECOWAS, ラテンアメリカ・カリブ地域経済機構(SELA)及びラテンアメリカ統合連合(LAIA) 等の地域機関に国内及び国境を越えるｅコマースを支援することができる法枠組みの調和に関する協力の範囲を模索する機会を提供			

117. ラテンアメリカ e コマース法の調和：通信教育研修及び対面ワークショップ	国連貿易開発会議（UNCTAD）	·カリブ諸国連合（ACS） ·エクアドル外務貿易省 ·フィンランド政府 ·ラテンアメリカ・カリブ地域経済機構（SELA）	亜，ベリーズ，ボリビア，コロンビア，コスタリカ，キューバ，エクアドル，エルサルバドル，グアテマラ，ハイチ，ホンジュラス，ジャマイカ，メキシコ，ニカラグア，パナマ，パラグアイ，秘，ドミニカ共和国，ウルグアイ及びベネズエラ	ラテンアメリカ及びカリブ地域 20 カ国の政策立案者及び立法者，法執行機関職員，民間セクター代表者計 40 人	グローバル，地域的及び各国の e コマースの傾向，e 取引，データ保護及びオンラインのサイバー犯罪からの消費者保護，and 各地域における地域的サイバー法整備のベストプラクティス	e コマースの法的側面に関する UNCTAD の通信教育研修の参加者に e 取引，消費者保護， IPRs，サイバー犯罪，データ保護及び情報の自由の議題に関する理解を深める機会の提供	·300 人の参加者への UNCTAD 通信教育研修 ·e コマース法の調和に関する地域的ワークショップ	·カリブ地域の e コマース関連法のマッピング ·e コマース法に関するグッドプラクティスの共有及び当該地域における e コマースを促進する規制枠組みを可能にする方法についての議論 ·カリブ地域の e コマース法の調和に関する比較地域研究	2014 年 6 月，2014 年 9 月 16 日から 19 日(4 日間)
118. カリブ諸国 e コマース法の調和：通信教育研修及び対面ワークショップ	国連貿易開発会議（UNCTAD） E コマース及び法改革プログラム	·カリブ諸国連合（ACS） ·フィンランド政府 ·トリニダード・トバゴ政府 ·ラテンアメリカ・カリブ地域経済機構（SELA） ワークショップへの貢献者： ·カリブ共同体・共同市場	アンティグア・バーブーダ，バハマ諸島，バルバドス，コスタリカ，キューバ，エルサルバドル，ジャマイカ，セントルシア，スリナム及びトリニダード・トバゴ	政策立案者，立法者，法執行機関職員，民間セクター代表者．ワークショップには 10 カ国から計 35 人の代表が参加。通信教育研修には 140 人が参加。	グローバル，地域的及び各国の e コマースの傾向及び法的課題等 個別トピック：e 取引，データ保護及びオンラインのサイバー犯罪からの消費者保護及びオンラインコンテンツ	e コマースの法的側面に関する UNCTAD の通信教育研修の参加者に研修コースで取り扱った議題に関する理解を深め，法の採用及び実施に関する経験を共有する機会を提供	·140 人の参加者への UNCTAD 通信教育研修 ·カリブ諸国における e コマース法の調和に関する地域ワークショップ	·カリブ地域の e コマース関連法のマッピング ·e コマース法に関するグッドプラクティスの共有及び当該地域における e コマースを促進する規制枠組みを可能にする方法についての議論 ·カリブ地域の e コマース法の調和に関する比較地域研究	2015 年 3 月・4 月及び同年 9 月 29 日から 10 月 2 日(4 日間)

		(CARICOM)事務局 ·TriniTrolley（カリブ地域の最大の e コマース事業者） ·国連国際商取引法委員会（UNCITRAL） ·国連ラテンアメリカ・カリブ経済委員会(UNECLAC) ·国連薬物犯罪事務所(UNODC) ·米司法省 ·米連邦取引委員会 ·世界銀行等								
119. 万人のための e トレード	国連貿易開発会議(UNCTAD)が調整するマルチステークホルダーイニシアティブ	e コマースに関与している政府，国際機関及び民間企業の代表	全世界	途上国	1.e コマース即応態勢評価及び戦略策定 2.ICT インフラ及びサービス 3.取引のロジスティックス及び促進 4. 支払ソリューション 5.法規制枠組み(サイバーセキュリティ等）	·途上国とりわけ後発開発途上国の e コマースを利用し，恩恵を受ける能力を改善すること ·対象国の e コマース特有の機械，課題及び制約に関する意識を啓発すること ·優先プロジェクトの実行のためにその課題及び制約に取り組むための利用	e コマースの発展に特に関連のある 7 つの政策テーマに関して様々なパートナーから提案されたキャパシティビルディングプログラムの透明性向上のためにオンラインプラットフォームが設計された。次の UNCTAD e コマース週間(2017 年 4 月 24 日から 28 日)中に正式に立ち上げ予定。	·e コマースの発展の支援のためのリソースの向上 ·パートナー間の連携の強化	2016 年 7 月に行われた UNCTAD の 4 年に 1 回開催される総会で立ち

					6.e コマーススキル構築 7. 資金調達へのアクセス	可能な財源及び人的資源を動員し，合理化すること ·途上国における e コマースの利用及び利益を推進するためにパートナーの活動間の一貫性及び相乗効果の強化	「万人のための e トレード」イニシアティブのパートナー会合及び民間セクター評議会は次の UNCTAD e コマース週間(2017 年 4 月 24 日から 28 日)中に開催予定。		上げられた
120. ウガンダ国家サイバー犯罪対策タスクフォースに対する技術協力	国連アフリカ犯罪防止・加害者治療研修所（UNAFRI）		ウガンダ	他のステークホルダー及び一般大衆へリーチアウトするマンデートを負う国家のタスクフォースの主要メンバー 国家のタスクフォースを構成する組織： ·警察(サイバー犯罪対策課，インターポール，地域警察課及び刑事捜査部(CIID) ·国家情報技術庁(NITA) ·ウガンダ通信委員会(UCC) ·市民権・入国管理	サイバー犯罪		·キャパシティビルディング ·規制メカニズム，権利に基づいた法執行，サイバー問題のマネジメントにおける協力の強化及び相互支援の方法についての情報共有		2015 年 5 月以降

				局 ·外務省 ·国内治安機構(ISO) ·UNICEF ·ウガンダ青少年育成リンク ·公訴局(DPP) ·ジェンダー・労働・社会開発省児童支援センター ·教育・スポーツ省					
121. オンライン児童性的虐待防止国家調整ワーキンググループ支援	国連アフリカ犯罪防止・加害者治療研修所（UNAFRI）		ウガンダ	オンライン児童性的虐待防止ワーキンググループ	サイバー犯罪，児童虐待	オンライン児童性的虐待の本質及び範囲及び犯罪組織が児童を性行為を行うように誘い込むテクニックの越境性についての理解を生み出すこと	·技術援助 ·当局が児童性的虐待の被害者を支援するために採用できる様々な措置に関する研修並びに専門的知見の共通性及び共用資源に基づく連携を通じた介入戦略の策定		2015 年 5 月以降

122. OAS 意識啓発	米州機構（OAS）	·USUARIA 及び SEGURINFO –エンドユーザー ·WEF PCF – ビジネスリーダー ·トレンドマイクロ ·シマンテック ·オックスフォード大学グローバルサイバーセキュリティキャパシティセンター ·アンチフィッシングワーキンググループ(APWG) ·STOP. THINK.CONNECT	OAS 加盟国	エンドユーザー，ビジネスリーダー		·加盟国間のサイバーセキュリティの取り組みに関する連携を改善すること ·サイバーセキュリティ教育及び個人ユーザーレベルの意識啓発に関するベストプラクティスを共有することにより加盟国を支援すること	·意識啓発ツールキットの提供 ·会議 ·報告書 ·ビデオ ·ポスター ·IANA 監督管理責任の移管プロセスに関する情報シート		継続中

123. サイバーセキュリティ研修及びワークショップ	米州機構（OAS）	FIRST，インターネットガバナンスに関するサウス・サマースクール	OAS 加盟国	国家のサイバーセキュリティの強化又は調整の監督又は技術的責任を直接負う職員：法執行機関，インシデントレスポンス，技術要員，民間セクターのステークホルダー，政策立案者等		·加盟国間のサイバーセキュリティの取り組みに関する連携を改善すること ·サイバーセキュリティ教育及び個人ユーザーレベルの意識啓発に関するベストプラクティスを共有することにより加盟国を支援すること	·高度産業制御システムに関する技術研修 ·サイバーセキュリティの国際外交 ·重要インフラ防護 ·ISO 27001 情報セキュリティマネジメント ·捜査実務 ·フォレンジック ·インシデントレスポンス ·CIRT 構築及び運用	法執行機関職員のためのサイバーセキュリティ特別研修である「サイバーセキュリティ技術コロキウム」等毎年 1,200 以上の職員に研修を実施	継続中
124. OAS 国家サイバーセキュリティ戦略策定	米州機構（OAS）	オックスフォード大学グローバルサイバーセキュリティキャパシティセンター	コロンビア(2011 年)，パナマ(2012 年)，トリニダード・トバゴ(2013 年)，ジャマイカ(2015 年)，ドミニカ，パラグアイ，スリナム，コスタリカ，秘(策定中)	政府代表者，民間セクター，市民社会及び学界を含むサイバーセキュリティの主なステークホルダー		OAS 加盟国が国家サイバーセキュリティ政策枠組みを構築し，採用するように支援すること	1. 円卓討論 2. 広いサイバーセキュリティコミュニティにおける議論のための OAS による戦略の起案 3. フィードバック及び改定プロセスの促進	国家のサイバーセキュリティ政策の策定	継続中

125. CSIRT 構築及び半球ネットワーク	米州機構（OAS）	英外務・英連邦省	OAS 加盟国				·技術支援 ·地域における CSIRTs のリアルタイム通信及び情報共有の促進及び各国が任命したサイバーインシデントレスポンスの正式なコンタクトポイントがあることを追求する CSIRTs のヴァーチャル半球ネットワーク	CSIRT 構築の促進及び支援（最近 10 年で 4 から 18 まで増加）	継続中
126. 危機管理演習	米州機構（OAS）		OAS 加盟国	国家の様々なステークホルダー及び国家 CSIRT		サイバーセキュリティインシデントハンドリングについての調整及びコミュニケーションの強化	サイバーセキュリティ危機管理演習の実施に関する最先端モバイルサイバーラボの活用	8 つの国及び 2 つの地域の危機管理演習	2012 年以降継続中
127. サイバーセキュリティ技術協力ミッション	米州機構（OAS）		OAS 加盟国				タスクフォース又は緊急時の支援等特定のサイバーセキュリティの懸念に対処するためのテーラーメイドの技術援助	現地視察，政策，法制度枠組みの見直しを含む 10 カ国への派遣を 2014 年に実施	要請に応じて実施
128. サイバーセキュリティに関する専門的知見へのアクセス	米州機構（OAS）	·民間企業(マイクロソフト，トレンドマイクロ，シマンテック)， ·学界(グローバルサイバーセキュリティキャパシティセンター) ·非営利団体（世界経済フォーラム(WEF)，ラテンアメリカ・カリブ地域ネ	OAS 加盟国				·サイバーセキュリティ政策の策定，実行及び技術的評価の支援 ·ベストプラクティス，経験及び技術研修活動へのアクセス	公式報告書の作成及び複数の共同イニシアティブ（研修，ワークショップ，円卓会議等）がまとめられた	要請に応じて実施

		ットワーク情報センター(LACNIC), ICANN							
129. e 政府プログラム	米州機構（OAS）	オープンデータのためのラテンアメリカイニシアティブ (ILDA), MuNet (透明かつ効率的な地方自治体), ラテンアメリカ及びカリブ地域 e 政府首脳ネットワーク (Red GEALC), 政府調達米州ネットワーク(INGP), カダストロ・イニシアティブ	OAS 加盟国		e ガバナンス	・米州の各イニシアティブ及びパートナーシップを通じて e ガバナンスを促進をするための米州の情報センター（クリアリングハウス）になること ・キャパシティビルディング, 対話及び e 政府政策のための中心になること ・Red GEALC の技術事務局として機能を果たすこと	・水平的協力 ・戦略的提携 ・20 のオンラインコース	・14,000 人以上の公務員への研修 ・15 の e 政府ワークショップ（550 以上の市長及び地方の首長を対象） ・民間セクターパートナーシップモデルによるカリブ地域の土地台帳制度の近代化	要請に応じて実施

130. サイバー犯罪に関する米州協力ワーキンググループ及びポータル	米州機構（OAS）	米州テロ対策委員会(CICTE)	OAS 加盟国	サイバー犯罪対策分野又は捜査及び訴追のための国際連携の責務を負う OAS 加盟国の政府専門家	サイバー犯罪対策法及び電子証拠	·米州司法大臣その他主務大臣・法務長官会合(REMJA)から受けたマンデート（委託命令）を検討し，実行すること ·マンデートの達成状況を REMJA に報告すること ·情報及び経験の交換を円滑にすること ·参加した当局間の協力を強化すること ·OAS 加盟国間並びに国際機関及びメカニズムとの協力の促進及び強化のための提言を行うこと 「ポータル」は主としてサイバー犯罪対策分野又は捜査及び訴追のための国際連携の責務を負う OAS 加盟国の政府専門家間の協力及び情報交換の促進及び能率化のために作られた。	·サイバー犯罪に関する政府専門家会合 ·サイバー犯罪に対する半球的協力の促進及び強化のための特定の提言の構築 ·各国のサイバー犯罪及び電子証拠に関する立法及び手続的措置の構築能力を強化することを目的とするサイバー犯罪対策及び電子証拠に関する立法及び手続的措置に関する地域及び国際研修ワークショップ ·米州サイバー犯罪対策協力「ポータル」：サイバー犯罪対策分野又は捜査及び訴追のための国際連携の責務を負う OAS 加盟国の政府専門家間の協力及び情報交換の促進及び能率化を主たる目的に作られた。 これは，OAS 加盟国のサイバー犯罪の分野に関する国の法令に関する情報並びに OAS 内で取り組まれている活動で特に地域及び国際研修ワークショップ，ワーキンググループの会合及びその他の技術協力プログラムに関連する情報等の公的要素を含む。 また，パスワードで保護された専らサイ	·1999 年以降 8 つのサイバー犯罪対策に関する政府専門家会合 ·OAS 加盟 28 カ国から計 181 人を研修	1999 年以降

							バー犯罪対策分野又は捜査及び訴追のための国際連携の責務を負う OAS 加盟国の政府専門家の利益のための情報を含む私的要素がある。 さらに，「ポータル」は，サイバー犯罪関連のリンク(例：条約，法令，組織，ガイド及びマニュアル，ニュース及びサイバー犯罪に関する一般情報，犯罪報告メカニズム，電子記録，文書及びサイバー犯罪対策研修へのアクセス，ドメイン等)を提供する。		
131. OAS ヴァーチャルキャンパス	米州機構（OAS）		OAS 加盟国	電子政府プログラム: e 政府の地方自治体の首長及び役員 CapaciNet プロジェクト: 公務員	電子政府計画，土地登記計画及び CapaciNet プロジェクト 電子政府プログラム: 地域レベルの e 政府戦略を通じた地方自治体の近代化への寄与 地域の社会経済的発展に貢献するための制度的能力を強化するための地方自治体における情報通信技術を促進	電子政府計画: ·地方の効率性及び透明性の向上 ·税制度の運用，記録，許認可等の近代化に貢献すること 土地登記計画: ·対象国の土地登記制度の近代化支援 ·人的及び制度的能力強化。土地管理入門者から地理情報システム(GIS)の技術を利用する高度なレベルの参加者まで対応 CapaciNet プロジェクト: ·ラテンアメリカ及びカリブ地域の数千	電子政府計画 ·地方の e 政府戦略の策定のための技術支援 ·技術移転の促進：e 政府アプリケーション，地方の e-Muni（注：Municipal の略）のパッケージ：MuniPortal(地方自治体ポータル)，MuniCompra（地方自治体調達），MuniServi(市民のための地方自治体サービス)及び MuniParticipa(オンライン市民参加) ·コース： 1. 電子政府戦略策定入門 2. e 政府戦略の設計及び実行 3. 電子政府の規制的側面 4. 相互運用性		継続中

							人の公務員の研修という制度的キャパシティビルディングを通じた民主的ガバナンスの改善に貢献すること ·10 のオンラインコースの設置による米州の政府機関の能力の向上 ·米州諸国の政府機関の国家の優先事項の責任ある，効果的かつインクルーシブな構築の準備態勢を向上する能力の強化	5. e 政府プロジェクトマネジメント 6. 公共調達マネジメント 土地登記計画 ·土地管理入門コース ·土地管理における GIS 技術の利用コース ·土地管理の近代化コース ·土地管理及び登記の近代化を支援するツールキット CapaciNet プロジェクト コース： ·戦略的地方統合観光マネジメント ·効果的な制度的通信戦略 ·行政のマネジメント及び品質保証，競争力ツール ·電子（市民）参加戦略の策定 ·地方分権化と市民参加戦略 ·透明性及び統合性促進メカニズムと戦略 ·育児戦略 ·カリブ地域における政治指導者 ·米州の貿易と環境 ·e 議会と立法機関の近代化		

132. プライバシー，インターネットガバナンス及び「児童と携帯技術」コース	GSMA	対面コースは，各地域のパートナー(学術，政府間研修機関，地域的規制グループ及び各国規制当局)と共同で実施	全世界	規制者及び政策立案者	消費者への携帯サービスの提供を促進する最良の方法を検討する上での世界の規制当局が直面する最も差し迫った問題に関する実用的な情報及び重要な洞察	・世界の規制当局が直面する最も差し迫った問題に関する実用的な情報及び重要な洞察を提供すること ・専門家によって作成され，指導を受ける本コースはキャリアのすべての段階にある専門家に適している	以下の事項の対面型及びオンラインコース ·プライバシー：モバイルインターネット及びコンバージドサービスの成長は個人情報の利用と保護， リアルタイムの地理的国境を越えた多数当事者間のデータの流通に関連する新たな問題を生み出している。本コースはモバイルプライバシーの現状を調査し，消費者のプライバシーに対する態度に関する研究を浮き彫りにし，世界の現在及び新たな規制を検討する。本コースはまた，GSMA の普遍的なモバイルプライバシー原則，アプリケーション開発者のためのプライバシーデザインガイドライン 及び消費者にその情報の利用方法に対するコントロールを強化する業界のイニシアティブを評価する。 ·インターネットガバナンス：インターネットガバナンスはインターネットの進化及び利用を形作る共有原則，規範，規則，意思決定手続及び計画の構築。インターネットガバナンスに係る政策及び過程は近年注目され，インターネット問題にかかわるすべてのステークホルダ		継続中

							一の関心事である。本コースはインターネットガバナンスの概要を，その歴史，制度，過程及び人を通じて提供する。本コースは，国，地域及び世界レベルでインターネットガバナンスとして採用又は提案されているマルチステークホルダーモデルを含む異なる政策アプローチの現況又は潜在的重要性を議論及び分析する。 ·児童と携帯技術：児童及び若年者は携帯技術の最も熱烈なユーザーであり，この技術はかれらの生活に多大なプラスの影響を与えることができる。しかしながら，すべてのツール同様，携帯技術は害を及ぼすために利用されることも可能であり，親，政府及び産業界は右技術に接続している子供の保護及び支援する役割を担っている。本コースは，子供の携帯機器の利用に関する文化的相違，児童オンライン保護等を含む様々な角度からこの問題を眺め，規制が必要かどうかを検討する。		
133. サイバーレジリエンスの強化	世界経済フォーラム	世界経済フォーラムのメンバー企	全世界	政府機関，民間セクター	サイバーレジリエンス	目的： サイバーレジリエンスを事業及び国家戦略に効果的に組み入れるためのツ	2016 年世界各地において世界経済フォーラムのメンバー及び被招待者のためのワークショップを開催	·リスク，影響を受けた産業及び技術の種類の区別を助ける定量的リス	2015 年から 2016 年	

		業，内閣・省庁職員				ールの導入及びパートナーシップの締結について企業，組織及び政府を支援すること 目標： ·サイバー戦略に取り組み，本フォーラムの「サイバー原則及び役員のためのツール」の採用を奨励する役員及び幹部職員のネットワークの構築； ·本フォーラムの原則及びツールを繰り返し行い，サイバーレジリエンス戦略の成功事例に関するケーススタディの収集のためのシステムの構築 ·公共セクター及び政府の幹部へ適応させるための有効なツールの順応 ·サイバーにおける国家行為及び合意された責任基準値等の議題についての官民対話の開始 ·公共及び民間セクターの明確に定義された役割（重要インフラ又は責任基準値等）等についての企業幹部と政策立案者の持続的な対話のためのプロセスの構築 ·サイバーリスクの軽減の標準化及び支援するための保険業界及び政府の幹部との連携の促進		·戦略的意思決定者のための戦略的リスク枠組み	

134. グローバル検察官 e 犯罪対策ネットワーク(GPEN)	グローバル検察官 E 犯罪ネットワーク(GPEN)（国際検察官協会(IAP)の下に立上げ）	英外務・英連邦省（FCO）（研修プログラム）	全世界	サイバー犯罪に係る検察官	サイバー犯罪	目的: 検察官がサイバー犯罪に効果的に対処できるツールを有することができるようにすることによってすべての国が，ユーザーが安全で安心なオンライン環境を構築するのを支援すること 目標:: ·すべての加盟国に有益な e 犯罪分野における国際協力の強化 ·情報交換の改善，作業の重複の削減及び国境を越えた分析及び訴追能力の大幅な強化 ·効果的な訴追を支援し，サイバー犯罪条約を促進するすべての管轄区域における e 犯罪対策のための協調的アプローチの構築。提案されたネットワークは 24 時間プロトコル又は通常の刑事共助と競合しない。各国のコンタクトポイントに指名されえた e 犯罪対策の専門家がすべての必要な国内のリエゾンの責任を負う ·世界中の資源及び専門的知見を用いたグローバルな研修フォーラムの開催。e 犯罪事案を起訴するための検察官の研修はサイバー犯罪対策のため	·e 犯罪対策研修コース及びプレゼンテーションのデータベースを含む「ヴァーチャル・グローバル e 犯罪検察官カレッジ」 ·国の立法及び法的ガイダンス等 e 犯罪対策資料のオンライン図書館 ·質問及び助言の交換のためのディスカッションフォーラム(メッセージ・チャット版) ·e 世界各国のフェローに指名された e 犯罪検察官の連絡先データベース ·サイバー犯罪法に関する研修プログラム（ウェビナー及びワークショップ）	世界各国の検察官のサイバー犯罪に係る研修コース，ベストプラクティスの提供	2008 年以降

						の国際的な取り組みにおける優先事項である。本ネットワークは検察官が同僚に対しても研修できるように検察官に対して適切な研修コースを開発する。 ·世界中の検察官が重要な情報及びデータを迅速かつ効率的に交換できるようにすること			
135. インクルーシブなサイバー政策立案過程を促進するためのグローバル計画	グローバルパートナーズデジタル（GPD）	オランダ外務省	尼，ケニア及び智	グローバル・サウス（南の途上国）の市民社会主体	世界のサイバー政策過程をよりインクルーシブなものにすること	・グローバル・サウスにおける市民社会の主体が国家，地域及び国際レベルのサイバー政策の議論に効果的に関与するための能力を構築すること ・サイバーセキュリティについての政策及び意思決定過程への国家のマルチステークホルダーの参画枠組みを試験すること	サイバーキャパシティ及びアドボカシースキルの構築，サイバー政策の議論のための新たな場の創設及び権利を尊重するサイバー政策の策定に関するより強固な協調関係を促進するための幅広い活動に関しアフリカ，アジア及び南米のパートナーと密接に連携	本プログラムは，現在のサイバー政策の議論において幅広く認識されている傾向である市民社会的側面の不足への対応策として考案された。 これにより，市民社会の多様な進歩的な声をエンパワーし，人権を保障及び推進するサイバー政策を具体化することが期待される。	2016 年 1 月開始 期間：2 年間
136. C4DLab ナイロビ － サイバーセキュリティ研修	ナイロビ大学(C4D 研究所) （ケニア）	ICT 庁(ICTA)	ケニア	情報セキュリティ専門家，IT セキュリティマネージャー，クラウドセキュリティ専門家，IT アーキテクト及びアドミニストレーター，リスク評価専門家，データベー	·情報セキュリティの基礎及びそのマネジメント ·情報セキュリティに関するケニア及び国際的な課題 ·脅威及び攻撃認識 ·攻撃の防止及び検知	参加者が情報セキュリティとそのマネジメントを構成する幅広い分野の知識と理解を得ること コースに無事合格すると参加者は次の分野に関する知識と理解を得ることが期待される：情報セキュリティとそのマネジメントに関連する概念の知識，情報セキュリティマネジメントに影響を	理論的要点，ハンズオン的要素及び現実世界の攻撃のシナリオを含む講義，個別指導及び演習	セミナー，ワークショップ等の開催。詳細は不明。	2015 年

				ス及びウェブデベロッパー，セキュリティ監査及びコンプライアンスマネージャー，ネットワーク及びシステムアドミニストレーター，現実世界の IT 攻撃及び防衛に関心のある政府及び情報機関，デジタルフォレンジック調査官等情報セキュリティについてより深く学習する意欲のある政府及び民間セクターの IT 専門家	·コントロール及びレスポンス技術	与える現在の国家の政策及び法制度の理解， 情報セキュリティのマネジメントを促進する国家及び国際基準，枠組み及び組織の構築の認識，攻撃，侵入，検知，携帯（電子）マネーセキュリティ及び USB 機器のハッキング等情報セキュリティに関連する技術的側面に関する理解，異なる種類及び性質のコントロールの分類，運用及び実効性の知識			
137. セネガル及び西アフリカにおけるサイバーセキュリティの進展	セネガル及び蘭	国連薬物犯罪事務所（UNODC）	セネガル及び広域西アフリカ地域	セネガルのダカールにおける専門家会合への技術コミュニティ，市民社会，学界，民間セクター及び政府参加者	サイバーセキュリティの脅威，国家サイバーセキュリティ戦略，サイバーセキュリティ・インシデントレスポンス，サイバーセキュリティ教育及びサイバーセキュリティ法制度	セネガル及びその他の西アフリカ諸国全般のサイバーセキュリティの強化	·セネガル政府が能力投資分野の優先順位をつけることができるようにするためのグローバルサイバーセキュリティキャパシティセンター(GCSCC)が実施するセネガルのサイバーセキュリティ能力評価 ·西アフリカ地域に関する課題に対処するための 2 つのサイバーセキュリティ専	予想される成果 2016 年 4 月に行われた最初のサイバーセキュリティ専門家会合では，西アフリカ地域におけるサイバーセキュリティの優先事項が特定され，問題を理解するために現在進行中の課題や教訓を検討し，またステークホルダーのセクタ	

							門家会合 成功しそうなサイバープラクティスの交換	一間コミュニケーションによりサイバーセキュリティ政策，計画及びアプローチの策定を支援した。 本イニシアティブの一部として，GCSCC は 2016 年 1 月にセネガル郵便・電気通信省の協力の下，同国のサイバーセキュリティ成熟度評価を行った。GCSCC の専門家は政府，学界，法執行，民間セクター，NGO 等のステークホルダーと会った。当該評価報告書は，セネガルが戦略的に投資し得る能力の分野に関する優先順位付けを可能にする。	
138. 地方開発のためのデジタルデバイドの是正	持続可能な技術及び地方開発のためのアフリカ機構(ANSTeRD)	ジンバブエ情報通信技術連合 (ICTAZ)	アフリカ	地方コミュニティ及び治安部隊	サイバーセキュリティ及び e ガバナンス	·サイバーセキュリティ問題及び e ガバナンスに関する地方コミュニティの意識啓発及び自覚の促進 ·当該コミュニティのサイバー空間，ICT 機器及び e 活用へのアクセシビリティの促進 ·コミュニティのメンバーの ICT ツールの効果的利用及び日々の経済，社会及び環境保護活動への活用についての研修及び能力の構築	·アドボカシー及び意識啓発ワークショップ ·研修及びキャパシティビルディングプログラム	·携帯電話によるサイバー犯罪活動の報告書 ·サイバー犯罪活動の傾向及び動向の更新の要請 ·サイバー空間を利用する市民の信頼及びサイバー犯罪の要素を選別できるようになること	2016 年 1 月から 2020 年 1 月

139. 航空詐欺対策グローバルアクション	欧州サイバー犯罪センター(EC3)，インターポール・シンガポール総局（イノベーションのためのグローバルコンプレックス:IGCI)，加及び米国法執行機関後援のアメリポール， ユーロジャスト（欧州司法機構)，欧州国境沿岸警備機関(Frontex)	43 カ国，75 航空会社及び 8 オンライン旅行代理店が参加	世界の 189 の空港	航空会社，オンライン旅行代理店，ペイメントカード企業の代表者等，ペルセウス及び国際航空運送協会(IATA)	サイバー犯罪，オンライン詐欺	疑わしい取引を特定し，空港に配置された法執行機関職員に確認情報を提供すること	航空会社，オンライン旅行代理店，ペイメントカード企業の代表者等，ペルセウス及び IATA が EC3 の専門家と協力して疑わしい取引を特定し，空港に配置された法執行機関の職員に確認情報を提供	本オペレーション中，350 の疑わしい取引が報告された。その結果，警察が 193 人を拘束し，その搭乗を拒否し，尋問を行い，刑事告訴した。捜査は継続中。複数の者は，詐欺によって取得した航空券を使いラテンアメリカから欧州へ離着陸を頻繁に行い薬物を密輸しようとしたところで逮捕された	2016 年から毎年 5 日間
140. サイバー犯罪対策グローバル同盟	国際刑事警察機構（インターポール）イノベーションのためのグローバル・コンプレックス(IGCI)	カスペルスキー社	インターポール加盟 190 カ国	法執行機関	サイバー犯罪，デジタルセキュリティ	世界最大の警察機構とそれに加盟する190カ国へ同社の製品，情報及び継続的な支援を提供すること	·脅威情報並びにハードウェア及びソフトウェアを IGCI のサイバーフォレンジック研究所に提供 ·インターポールの職員に対する研修セッションの実施	サイバー脅威インテリジェンスの情報共有等によるサイバー犯罪対策の協力の強化。 2015 年 4 月，ボットネット Simda の閉鎖等の実績。 2017 年 4 月，約 9000 台のボttネット指令サーバー(C2)を特定	2014 年から 2017 年

141. サイバーフュージョンセンター（CFC）	国際刑事警察機構（インターポール）イノベーションのためのグローバル・コンプレックス（IGCI）	サイバーディフェンスインスティテュート，カスペルスキーラボ，LAC，NEC，SECOM，トレンドマイクロ，南オーストラリア大学及びワイカト大学（新）	インターポール加盟国	法執行機関	サイバー犯罪	実行可能な脅威情報の共有及び運用上の対応の構築するために 法執行機関，民間セクター及び学界が連携して取り組むための中立的なグローバルプラットフォームを提供すること ·情報共有，サイバー脅威の軽減についての研修及び意識啓発並びに公的機関及び民間企業に対するサイバーレジリエンスの強化についての実行可能な提言を通じてサイバーセキュリティについての共同取り組みを正式なものにし，これを拡大すること	CFC は法執行の専門家及び産業専門家を結集させるマルチステークホルダー環境である。CFC は加盟国におけるサイバー犯罪活動へ効果をもたらすことができる実施可能なインテリジェンスを発出するために利用可能なすべての情報をフル活用するための革新的な技術を使用する。 CFC はダイナミックなサイバー運用活動への支援を管理及び促進する専門的知見及びインフラを供給する。 CFC はデジタル犯罪捜査支援（DIS）ユニット及びインターポール加盟国と連携して運用活動を調整及び提供する機能を果たす。 スタッフは警察及びインターポール CFC のその他の専門家と共に効果的な情報共有及び差し迫った脅威への対応を可能にするために常勤で業務に従事している。	マルウェア解析情報の加盟国への公開，レポートによるアラートの提供	2014 年以降

142. サイバー防衛に関する協力	北大西洋条約機構(NATO)	勃政府	勃	政府機関等	サイバー防衛	目的: 勃のサイバー防衛努力を支援し，多国籍プロジェクト，教育，研修，演習及び情報交換等を通じたサイバー防衛協力を促進すること 目標: ·サイバー脅威及びベストプラクティスについての情報共有の促進 ·サイバーインシデントの予防の改善 ·勃のサイバー脅威に対するレジリエンスの増強 ·NATO 及びブルガリアのサイバー防衛当局間の支援の促進(必要な場合)	研修，演習，情報交換等(詳細は非公表)	勃政府のサイバーセキュリティ能力の総合的強化	2016 年 10 月 MoU 締結
143. NATO 高速対応チーム	北大西洋条約機構(NATO)加盟国	特になし	NATO 加盟国	技術協力又はサイバー攻撃に起因するインシデントへの対処をするために NATO の施設・サイト	サイバーセキュリティ，サイバー攻撃，技術協力，インシデントレスポンス	サイバー攻撃を受けている NATO 諸国又は施設の援助	国家レベルの重大なサイバー攻撃が行われた場合に加盟国の要請に応じた援助を行う	サイバー攻撃を受けている NATO 加盟国の被害の極小化	2015 年以降

144. GFCE インベントリ：サイバーキャパシティビルディングに関する世界的及び地域的取り組みの主要評価基準	GFCE （蘭政府主導，サイバー空間に関する国際会議（GCCS）の枠組み）	ディプロ財団，FIRST（インシデント対応セキュリティチーム・フォーラム），GCSCC，メリディアン・コミュニティ，ニューアメリカ，UNODC	全世界（すべての国や地域等に開かれている）	政府機関，民間企業，研究機関等	サイバーセキュリティ政策・戦略，サイバーセキュリティ文化・スキル，インシデント管理・インフラ防護，サイバーセキュリティ基準，サイバー犯罪，	国家の政府，大企業又は国際機関内の政策立案者及びサイバーセキュリティ戦略家によるグッドプラクティスの特定及び協力の手段の模索を支援するための現在の国際及び地域イニシアティブ，プログラム及びプロジェクトの主要評価基準を提供すること	主要評価項目として次のカテゴリーに分類する： ·組織（主体） ·パートナー ·対象国・地域 ·対象グループ ·主なテーマ ·目的・目標 ·具体的活動 ·成果・効果 ·時期 ·連絡先 s ·情報（リンク先，文書等）	世界の支援主体が既存の二国間，多国間，多主体，地域及び国際サイバーセキュリティ能力の格差を特定，是正し，世界のサイバーセキュリティキャパシティビルディングの効果及び効率を促進すること 2017年12月現在の主な成果文書としては，「サイバーキャパシティ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」がある。	2015 年 4 月の設置以降

付属資料２．ＧＧＥに関する外交文書

付属資料２．１．Ａ／６０／２０２[157]

国連総会

A/60/202

配布:一般

2005 年 8 月 5 日

第 60 会期

暫定議題 87

国際安全保障の文脈における情報電気通信分野の進展

国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ

事務総長報告書

目次

Ⅰ. 序文

1.「国際安全保障の文脈における情報電気通信分野の進展」と題する 2003 年 12 月 8 日の決議 58/32 において，総会は事務総長に対し情報セキュリティの分野における既存及び潜在的な脅威とそれに対処するための協力的措置を検討するよう要請した。また，総会は，事務総長に対し，衡平な地理的配分に基づき事務総長が任命する政府専門家グループの支援とともに，グローバルな情報電気通信システムのセキュリティの強化を目的とする国際概念を検討し，第 60 回総会にその検討結果に関する報告書を提出することも要請した。

Ⅱ. 組織事項

2. 本決議の条件に従い，事務総長はベラルーシ，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，英国及び米国の 15 カ国の政府専門家グループを任命した。専門家の一覧は添付文書に記載。

[157] 原文は A/60/202 (undocs.org/A/60/202)（最終アクセス日：2017 年 12 月 18 日）

3. 政府専門家グループの会合は 3 回実施された。第 1 回は，2004 年 7 月 12 日から 16 日まで国連本部において，第 2 回は 2005 年 3 月 28 日から 4 月 1 日までジュネーヴにおいて，第 3 回は 2005 年 7 月 11 日から 22 日まで国連本部において行われた。第 1 回会合において，本グループは満場一致でロシアのアンドレイ・V・クルツキフを議長に選任した。

4. 軍縮部のモニタリング・データベース・情報室が本グループの事務局を務めた。

5. 決議 58/32 記載のマンデートに従い，本グループは国際安全保障の文脈における情報電気通信分野の進展について包括的で詳細な意見交換を行った。また，本グループは，其々「国際安全保障の文脈における情報電気通信分野の進展」と題する 1998 年 12 月 4 日の総会決議 53/70，1999 年 12 月 1 日の決議 54/49，2001 年 11 月 29 日の決議 56/19，2002 年 11 月 22 日の決議 57/53，2003 年 12 月 8 日の決議 58/32 及び 2004 年 12 月 3 日の決議 59/61 に対する国連加盟国の回答において表明された見解並びに本グループの各メンバーから入手した寄書（contribution）や背景資料（background paper）を考慮した。しかしながら，関連する問題の複雑さにより，最終報告書の作成にむけてコンセンサスを得ることはできなかった。

添付文書

国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ メンバー一覧表

ベラルーシ
ヴァレリー・V・ツェプカロ（Valery V. Tsepkalo）ベラルーシ大統領補佐官

ブラジル
ムリーロ・マルケス・バルボーザ（Murilo Marques Barboza）国防大臣特別顧問

中国
王群(Wang Qun)外交部軍控司審議官
呉海濤(Wu Haitao)外交部軍控司参事官（第 1 回会合）

フランス
ステファニー・シェーアー（Stéphanie Schaer）国防事務総局（担当官）

ドイツ
トーマス・シェーファー（Thomas Schäfer）外務省通常兵器管理部長・一等参事官

インド
アルビン・グプタ（Arvind Gupta）国家安全保障会議次官補
サンジブ・ランジャン（Sanjiv Ranjan）国連インド代表部一等書記官（第 1 回会合）

ヨルダン
ビシェル・アル・カサウネ（Bisher Al-Khasawneh）在ジュネーヴ・ヨルダン代表部一等書記官（第 1 回会合）
アッザム・アラメディン（Azzam Alameddin）在ジュネーヴ・ヨルダン代表部二等書記官

マレーシア
モハメッド・シャア・ヌリ・ビン・モハメッド・ザイン（Md. Shah Nuri bin Md. Zain）首相府国家安全保障局技術開発・情報技術課長（第 2 回会合）
モード・アズラン・ザハルディン（Mohd Azlan Zaharudin）首相府国家安全保障局技術開発・情報技術課長補佐

マリ

シェクナ・ケイタ（Cheickna Keita）国連マリ代表部一等参事官（第 1 回会合）
カリル・ドゥンビア（Kalilou Doumbia）国連マリ代表部一等参事官

メキシコ
ホルヘ・アントニオ・エスピノーサ・デュラン（Jorge Antonio Espinosa Durán）連邦予備警察情報セキュリティ官

韓国
ル・クワンチュル（Lew Kwang-chul）国連韓国代表部公使参事官

ロシア
アンドレイ・V・クルツキフ（Andrey V. Krutskikh）外務省軍縮・安全保障部長補佐

南アフリカ
アシュウィン・C・ヒューリバンス（Ashwin C. Hurribunce）少将・国防省情報システム部最高司令官

英国
ジェフ・スミス（Geoff Smith）貿易産業省情報セキュリティ政策部長

米国
ミシェル・マーコフ（Michele Markoff）国務省政治・軍事局国際重要インフラ防護調整官

（筆者訳）

付属資料２．２．Ａ／ＲＥＳ／５３／７０[158]

A/RES/53/70
配布:一般
1999 年 1 月 4 日

第 58 会期
検討項目 63

総会によって採択された決議
[第一委員会の報告書(A/53/576)について]

53/70. 国際安全保障の文脈における情報電気通信分野の進展

国連総会は,
国際安全保障の文脈における科学技術の役割に関する決議を想起し, とりわけ, 科学技術の進展は民生, 軍事双方に応用することができ, 民生用の科学技術の進歩は維持され, 奨励される必要があることを認識し,

最新の情報技術及び電気通信手段の進展及び応用により相当の進歩を遂げてきたことに留意し,

この過程においてさらなる文明の発展のための最も幅広いポジティブな機会, 全ての国家の公共の利益のための協力の機会の拡大, 人類の創造能力の促進及び国際社会における情報の流通の付加的改善が見られることを認識し,

これに関し, 1996 年 5 月 13 日から 15 日にかけて南アフリカ・ミッドラントで開催された「情報社会と開発」会合において概説されたアプローチ及び原則を想起し,

1996 年 7 月 30 日にパリで開催されたテロリズムに関する閣僚会議の結果とそこで出された提言に留意し,

情報技術及び手段の利用及び普及は国際社会全体の利益に影響を与え, その最適な有効性は幅広い国際協力によって高められることに留意し,

これらの技術や手段は国際的な安定及び安全の維持という目標と相反する目的のために利用され, また, 国家の安全保障に悪影響を及ぼすおそれがあることを憂慮し,

[158] 原文は A/RES/53/70 (https://undocs.org/A/RES/53/70) （最終アクセス日：2017 年 12 月 18 日）

犯罪又はテロ目的の情報資源又は情報技術の不正利用又は悪用の防止の必要を考慮し,

1. 加盟国に対し, 多国間レベルで情報セキュリティの分野における現在及び潜在的な脅威の検討を促進するよう呼びかける。

2. すべての加盟国に対し, 次の質問に対する見解と評価を事務総長に通知するよう呼びかける。
(a) 情報セキュリティの問題の全般的理解
(b) 情報電気通信システム及び情報資源に対する不正な妨害又は不正利用を含む情報セキュリティに関連する基本概念の定義
(c) 世界の情報電気通信システムのセキュリティを高め, 情報テロ及び情報犯罪との闘いに寄与する国際的な原則の策定の妥当性

3. 事務総長に対し, 第 54 回総会に報告書を提出するよう要請する。
4. 第 54 回総会の暫定的な議題に「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展」と題する検討項目を含めることを決定する。

第 79 回本会議
1998 年 12 月 4 日
（筆者訳）

付属資料２．３．Ａ／６５／２０１[159]

国際連合
総会

A/65/201
配布:一般
2010 年 7 月 30 日
原文:英語

第 65 会期
暫定議題 94
国際安全保障の文脈における情報電気通信分野の進展

国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ

事務総長によるノート

事務総長は，ここに，「国際安全保障の文脈における情報電気通信部屋の進展に関する政府専門家グループ」の報告書を伝達する栄誉を有する。本グループは総会決議 60/45 の第 4 段落に従い設置された。

[159] 原文は A/65/201 (https://undocs.org/A/65/201) （最終アクセス日：2017 年 12 月 18 日）

国際安全保障の文脈における情報電気通信部屋の進展に関する政府専門家グループの報告書

要約

情報セキュリティの領域における現在及び潜在的な脅威は二十一世紀の最も深刻な課題の一つである。脅威は多様な発生源から生じ，個人，企業，国家のインフラ及び政府を等しく対象とする破壊（disruption）活動として表れる。その効果は，公共の安全，国家の安全及びグローバルに繋がった国際社会全体の安定に重大な危険を招く。
重要インフラにおける情報通信技術（ICT）の利用の増加は新たな脆弱性と破壊の機会を創出する。電気通信及びインターネットの複雑な相互接続性により，いかなる ICT デバイスもますます巧妙化する不正利用の発信源又は対象となり得る。ICT は本質的に軍民両用のものであるため，堅固な電子商取引を支援する同じ技術が国際的な安全と国家の安全保障を脅かすためにも利用され得る。

破壊の発信源，加害者の正体又は動機を突き止めるのは困難な場合がある。そのような活動の加害者は，しばしばその対象，効果又はその他の状況証拠のみによって推測され，また，事実上どこからでも行うことができる。これらの特性が，ICT が破壊活動に利用されるのを容易にしている。帰属に関する不確実性及び共通認識の欠如が不安定さと誤認のリスクを引き起こす。

国家が ICT を戦争や諜報の道具，また政治的な目的のために開発しているという報告が増えている。懸念が高まっているのは，個人，グループ又は犯罪組織等が 他の者に代わりプロキシ（代理）として破壊的なオンライン活動に従事していることである。犯罪活動の巧妙化と規模の高まりが有害な行動の可能性を高めている。テロリストが破壊的な作戦を実行するために ICT を利用しているという指標は少ないが，将来これが増える可能性がある。

二十一世紀の課題への取り組みは志を同じくするパートナーとの協力の成功にかかっている。国家間，国家，民間部門及び市民間の連携が重要であり，情報セキュリティ改善策を効果的にするためには幅広い国際協力が必要である。政府専門家グループの報告書は，リスクを低減し，国家及び国際的なインフラを防護するための国家間のさらなる対話を勧告する。

目次

Ⅲ. 協力策

Ⅳ. 勧告

添付文書

事務総長による序文

情報技術及び電気通信が我々の日常生活に深く溶け込み，又は，我々がここまで依存することを10年前は予想できなかった。これらの技術はグローバルに繋がった国際社会を作り出し，この繋がりは計り知れない利益をもたらすが，他方，脆弱性やリスクももたらす。この新しい技術の影響に対処するため，これまで相当な進展があった。しかし，それは多大な労力を要する作業であり，我々はこの新しい情報環境に必要な規範，法及び協力の方法を策定し始めたばかりである。

これを念頭に置き，この領域における既存の及び潜在的な脅威とその対処法を検討するため15カ国の政府専門家グループを任命した。グループの議長及び専門家に感謝する。この問題と考えられる次の措置についての簡潔な声明である本報告書の作成を遂げたグループの議長及び専門家の勤勉かつ慎重な作業に感謝する。

総会は，情報技術及び電気通信を国内及び国際的により安全なものにするプロセスにおいて果たすべき重要な役割がある。加盟国間の対話は共通認識を形成する上で不可欠になる。ベストプラクティスを共有し，情報を交換し，途上国の能力を構築し，国際社会のサイバー空間における大規模なインシデントを管理する能力を妨げる可能性がある誤解のリスクを削減するために実践的な協力もまた重要である。

これは今後の作業のための検討すべき議題である。本報告書は，この新たな技術が必要とする安全及び安定のための国際的な枠組みの構築に向けたはじめの一歩としての役割を果たすべきものである。私はその分析及び勧告を加盟国とより広範な世界の読者に託すこととする。

伝達状

2010 年 7 月 16 日

私はここに「国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ」の報告書を提出する栄誉を有する。本グループは総会決議 60/45 の第 4 段落に従い 2009 年に設置された。本グループの議長として，本報告書についてコンセンサスを得られたことを謹んで報告する。

「国際安全保障の文脈における情報電気通信分野の進展」と称する決議において，総会は，衡平な地理的配分に基づき，情報セキュリティの領域における既存及び潜在的な脅威とそれに対処するために考えられる協力策及びグローバルな情報電気通信システムのセキュリティの強化を目的とする概念を引き続き検討するために，2009 年に政府専門家グループを設置することを要請した。事務総長は，第 65 会期総会において，右検討結果についての報告書を提出するよう要請された。

当該決議の条件に従い，専門家はベラルーシ，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，英国及び米国の 15 カ国から任命された。専門家の一覧は添付文書に記載されている。

政府専門家グループは 4 回実施された。第 1 回会合は 2009 年 11 月 24 日から 26 日までジュネーヴにおいて，第 2 回は 2010 年 1 月 11 日から 15 日まで国連本部で，第 3 回は 2010 年 6 月 21 日から 25 日までジュネーヴ及び第 4 回は同年 7 月 12 日から 16 日まで国連本部において開催された。

本グループは国際安全保障の文脈における情報電気通信分野の進展に関する包括的で詳細な意見交換を行った。また，本グループは，「国際安全保障の文脈における情報電気通信分野の進展」とそれぞれ題する総会決議 60/45，61/54，62/17 及び 63/37 に対して加盟国から受領した回答において表明された見解並びに本グループの各メンバーによる寄稿及び背景報告書を考慮に入れた。

本グループは，本グループのコンサルタントを務め，ジェームズ・ルイス及びケルスティン・ヴィニャーによって代表される国連軍縮研究所の貢献に謝意を表明したい。本グループは，本グループの事務局を務めた国連事務局軍縮部情報支援部情報オフィサーのイーウェン・ブキャナン及び本グループを支援したその他の事務局員にも謝意を表明したい。

（*署名*）アンドレイ・V・クルツキフ

I. 序論

1. 情報セキュリティの領域における既存の及び潜在的な脅威は二十一世紀の最も深刻な課題の一つである。これらの脅威は経済並びに国家及び国際の安全に重大な損害をもたらす可能性がある。脅威は多種多様の発生源から生じ，個人，企業，国家のインフラ及び政府を一様に対象とする破壊活動として現れる。これらの結果は，公共の安全，国家の安全及びグローバルに繋がった国際社会全体の安定に重大な危険を招く。

2. 情報通信技術(ICT)は国家及びその他の利用者が脅威に対処するのを困難にする固有の特性を有する。ICT は遍在(ユビキタス)しており，広く利用可能である。ICT は元々本質的に民用又は軍用ではなく，その置かれる目的は主に利用者の動機によって決まる。多くの場合，ネットワークは民間部門又は個人によって所有され，運用される。電気通信及びインターネットの複雑な相互接続性により，いかなる ICT 機器もますます巧妙化する不正利用の発信源又は対象となり得る。ICT の悪意ある利用は容易に隠すことができる。破壊(disruption)の発信源，加害者の正体又は動機を突き止めるのは困難な場合がある。そのような活動の加害者は，しばしばその対象，効果又はその他の状況証拠のみによって推測される。脅威の主体は事実上どこからでも実際に罰を受けることなく(活動を)実施できる。これらの特性が，ICT が破壊活動に利用されるのを容易にしている。

3. これらの国際安全保障の進展の示唆を鑑み，国連総会は，事務総長に，政府専門家の支援とともに，グローバルな情報通信システムのセキュリティを強化するために考えられる協力策を提案するために情報セキュリティの領域における脅威とそれに関連する国際概念の双方を検討するよう依頼した。

II. 脅威，リスク及び脆弱性

4. ICT のグローバルネットワークは破壊活動の舞台となっている。破壊の動機は，単に優れた技術の腕前を見せつけることから，金銭若しくは情報の窃取又は国家の紛争の延長線など千差万別である。これらの脅威の発信源は，犯罪者又は今後可能性があるテロリスト等の非国家主体並びに国家自身などである。ICT は情報資源及びインフラに損害を与えるために利用され得る。ICT は本質的に軍民両用のものであるため，堅固な電子商取引を支援する同じ技術が国際的な安全と国家の安全保障を脅かすためにも利用され得る。

5. 多くの悪意あるツール及び方法論は，犯罪者及びハッカーの取り組みに由来する。犯罪活動の一層の巧妙化と規模の高まりは有害な行動の可能性を高める。

6. テロリストが，ICT インフラを危険にさらし，若しくは機能不全にする又は ICT を利用した作戦を実施しようとするテロリストの試みを示唆する指標は，将来は高まるおそれがあるが，これまでのところは少ない。現在テロリストは，主に通信，情報収集，採用活動，編成，思想及び活動の普及及び資金調達のために ICT に頼っているが，いずれは攻撃を行うために ICT を利用する可能性がある。

7. 国家が ICT を戦争や諜報の道具，また，政治的な目的のために開発しているという報告が増

えている。帰属に関する不確実性及び許される国家の行動に関する共通認識の欠如は不安定と誤解のリスクを招く可能性がある。

8. 懸念が高まっているのは，個人，グループ又は犯罪組織等が他の者に代わりプロキシ（代理）として破壊的なオンライン活動に従事していることである。このような代理主体は，経済的利益又は他の理由によって動機付けられようと，国家及び非国家主体に数々の悪意あるサービスを提供することができる。

9. 重要インフラにおける ICT の利用の増加は，携帯通信機器及びウェブ運営型サービスの利用の増加と同様，新たな脆弱性と破壊の機会をもたらす。

10. 国家は，ICT のサプライチェーンが，ICT の通常，安全及び信頼できる利用を妨げる形で影響を受け，又は弱体化する可能性があることも懸念している。ICT への悪意ある隠れた機能の埋め込みは，商品やサービスの信頼を損ない，取引の信用を失墜させ，国家の安全保障に影響を及ぼす可能性がある。

11. 国家間の ICT 能力（capacity）及びセキュリティの程度の差は，グローバルネットワークの脆弱性を高める。国家の法律や慣行の相違は，安全かつ強靭なデジタル環境を達成する上での課題をもたらす可能性がある。

Ⅲ. 協力策

12. グローバルに繋がったネットワークに係るリスクには，協奏的な対処が必要である。過去 10 年，加盟国は犯罪者による情報技術の不正利用と闘い，グローバルなサイバーセキュリティの文化を創出し，リスクを軽減するその他の重要な対策を促進するための ICT セキュリティの領域における脅威に対する国際協力の必要を再三にわたり確認してきた。

13. 過去 10 年間にわたり，サイバー犯罪の脅威と闘うための取り組みを，とりわけ上海協力機構，米州機構，アジア太平洋経済協力フォーラム，東南アジア諸国連合(ASEAN)地域フォーラム，西アフリカ諸国経済共同体，アフリカ連合，欧州連合，欧州安全保障協力機構及び欧州評議会内で，また，二国間の取り組みを通じて，国際的に行ってきた。

14. 国境を越える懸念の非犯罪領域は適切な配慮を受けるべきである。これには，大規模のインシデントの場合には危機管理に影響を及ぼし得る国家の ICT の利用に係る国際規範に関する共通理解の欠如に起因する誤解のリスクが含まれる。これは，可能な協力の強化を目的とする対策

の精緻化を訴える。このような対策は，ベストプラクティスの共有，インシデントの管理，信頼の醸成，リスクの軽減並びに透明性及び安定性の強化の目的とすることもできる。

15. 情報通信技術を利用した破壊活動がより複雑かつ危険になるため，いかなる国家もこの脅威を一国のみで対処できないのは明らかである。この二十一世紀の課題への取り組みは志を同じくするパートナーとの協力の成功にかかっている。国家間，国家，民間部門及び市民間の連携が重要であり，情報セキュリティ改善策を効果的にするためには幅広い国際協力が必要である。従って，国際社会は協調行動及びメカニズムの必要を検討すべきである。

16. 既存の合意には国家によるICTの利用に関連する規範が含まれる。ICT 固有の特性に鑑み，時間をかけて追加的な規範が策定される可能性がある。

17. キャパシティビルディングは，途上国の重要情報インフラのセキュリティを強めるための取り組みを支援し，ICT セキュリティにおける現在の格差を是正し，グローバルなICT セキュリティの確保を達成するために極めて重要である。ICT のセキュリティ対策において支援を必要とすると考えられる国家の能力を構築するためには密接な国際協力が必要となる。

IV. 勧告

18. 情報セキュリティの分野における既存及び潜在的な脅威，リスク及び脆弱性を踏まえ，政府専門家グループは，信頼醸成及び ICT の破壊から生じる誤解のリスクを軽減するためのその他の措置の構築のための（次に掲げる）さらなる手段を勧告するのが有益と考える。

(i) 集団的リスクを削減し，国家及び国際的な重要インフラを防護するための国家の ICT の利用に係る規範を議論するためのさらなる国家間の対話

(ii) 国家の ICT の利用の影響に取り組むための紛争における ICT の利用に関する国家の意見の交換を含む信頼醸成，安定及びリスク軽減措置

(iii) 国の法律及び国の情報通信技術セキュリティ戦略及び技術，政策及びベストプラクティスについての情報交換

(iv) 開発途上国におけるキャパシティビルディングを支援するための対策の特定

(v) 総会決議 64/25 に関連する共通の用語及び定義の精緻化の可能性の模索

添付文書

国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループメンバー一覧表

ベラルーシ
ウラジミール・N・ゲラシモヴィッチ（Vladimir N. Gerasimovich）外務省国際安全保障・軍備管理局長
アレクサンドル・ポノマレフ（Aleksandr Ponomarev）在ジュネーヴ国連事務所ベラルーシ政府代表部参事官（第 3 回会合）

ブラジル
アレクサンドル・マリアーノ・フェイトーザ（Alexandre Mariano Feitosa）国防省戦略・国際業務事務局海軍政策ブラジル海兵隊中佐

中国
李松（Li Song）外交部軍控司（外務省軍備管理局）局長補佐（第 1 及び第 2 回会合）
康勇（Kang Yong）外交部軍控司（外務省軍備管理局）局長補佐（第 3 及び第 4 回会合）

エストニア
リンナー・ヴィーク（Linnar Viik）エストニア IT カレッジ准教授

フランス
アイメリク・シモン（Aymeric Simon）国防国家安全保障事務総局国家情報システムセキュリティ庁国際関係管理官

ドイツ
グレゴール・クーベル（Gregor Koebel）外務省通常兵器管理課長

インド
B・J・スリナス（B. J. Srinath）情報技術省インド・コンピュータ緊急対応チーム(CERT)シニアディレクター

イスラエル
ロディカ・ラディアン＝ゴードン（Rodica Radian-Gordon）外務省軍備管理課長

イタリア

ヴィンチェンツォ・デッラ・コルテ（Vincenzo Della Corte）閣僚評議会通信安全保障部長（第 1 及び第 3 回会合）
ウォルテル・メッキア（Walter Mecchia）閣僚評議会通信安全保障部（第 2 及び第 4 回会合）

カタール
ラシッド・A・アル＝モハンディ（Rashid A. Al-Mohannadi）陸軍通信局アミリ通信部隊司令官
サード・M・R・アル＝カービ（Saad M. R. Al-Kaabi）国防省中佐（技官）（第 1 回会合）

韓国
ルー・グワンチョル（Lew Kwang-chul）外務貿易省大使

ロシア
アンドレイ・V・クルツキフ（Andrey V. Krutskikh）外務省新規課題脅威省課長補佐

南アフリカ
パレサ・バンダ（Palesa Banda）通信省インターネットガバナンス課長補佐（第 1 回会合）
マリオ・シルヴィーノ・ブラッツォーリ（Mario Silvino Brazzoli）少将・国防省政府情報技術官

英国
ギャヴィン・ウィリス（Gavin Willis）国家情報保証技術庁(CESG：電子通信安全局) 国際関係チーム担当官

米国
ミシェル・G・マーコフ（Michele G. Markoff）国務省サイバー事務局シニア政策顧問

（筆者訳）

付属資料２．４．Ａ／６８／９８[160]

国際連合

総会

A/68/98*

配布:一般

2013 年 6 月 24 日

原文:英語

第 68 会期

暫定議題 94**

国際安全保障の文脈における情報電気通信分野の進展

国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ

事務総長によるノート

事務総長はここに「国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ」の報告書を伝達する栄誉を有する。本グループは総会決議 66/24 の第 4 段落に従い設置された。

国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ報告書

要約

情報通信技術(ICT)は国際安全保障環境を作り変えた。ICT は計り知れない経済的社会的利益をもたらす。ICT は，近年，犯罪及びその他の破壊活動に利用されるなど，顕著なリスクの増加があり，国際平和及び安全と両立しない目的のためにも利用されることがある。しばしば罰せられることなく ICT を運用する主体による悪意ある ICT の利用は隠すことが容易であり，特定の加害者へ責めを帰するのは困難である。これは，ますます巧妙化するエクスプロイトのための ICT の利用を促進する環境を形成している。

加盟国は，ICT の悪意ある利用がもたらす脅威に対する協力策の必要を度々確認してきた。リスクを削減し，セキュリティを強化するには国際協力が不可欠である。国際レベルの協力のさらなる進展には平和，安全，オープンかつ協調的な ICT 環境の促進のための行動が必要となる。安

[160] 原文は A/68/98 (https://undocs.org/A/68/98) （最終アクセス日：2017 年 12 月 18 日）

定性及び安全を強化できる協力策には，国家による責任ある行動の規範，規則及び原則，国家間の透明性，信頼及び信用を高める自主的な措置並びにキャパシティビルディングが含まれる。国家がこれらの取り組みを主導しなければならないが，効果的な協力は民間部門及び市民社会の適切な参加から恩恵を受けることができる。

この課題の広範性を認識し，既存及び潜在的な脅威を考慮し，2010 年 7 月の「国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ」の報告書(A/65/201)に含まれる勧告を踏まえ，政府専門家グループは，本報告書において国家の ICT の利用における平和及び安定の促進のための勧告を提案する。

本報告書は国家による ICT の利用に関連する既存の国際法から派生する規範の適用は国際平和，安全及び安定に対するリスクを軽減するために不可欠であることを認識する。本報告書はこのような規範が国家の行動及び国家による ICT の利用にどのように適用されるかについての共通理解を促進するためにさらに検討することを勧告する。ICT 固有の特性に鑑み，本報告書は時間をかけて追加的な規範が策定される可能性があることに留意した。

本報告書は国際法とりわけ国際連合憲章は適用され，平和及び安定を維持し，オープン，安全，平和的かつアクセシブルな ICT 環境の促進に不可欠であるという本グループの結論を反映する。本グループは国家主権とそれから派生する国際規範及び原則は国家の ICT 関連活動に適用され，国家の領域内の ICT インフラに関する管轄権に及び，国家はその責めに帰する国際違法行為に関する国際義務を果たさなければならないという結論も下した。本報告書は信用，透明性及び信頼を構築するための自主的な措置及び特に途上国の ICT セキュリティの能力を構築するための国際協力についての提言を含む。本グループは，これらの措置を推進するために，これらの問題についての国際連合主催の定期的な制度的対話及び他のフォーラムにおける定期的な対話を行うことを勧告する。加盟国は本報告書を積極的に検討し，さらなる進展と実施のためにこれらの勧告をどのように取り扱うかを評価すべきである。

目次

事務総長による序文

情報通信技術(ICT)は 日常生活の中に溶け込んでいる。全ての国が ICT の多大な恩恵を評価する一方，その不正利用が国際平和及び安全にリスクをもたらすことも広く認識されている。

本報告書は，国家とそのプロキシ（代理）又は非国家主体の ICT の利用を通じた既存及び潜在的な脅威に対処するための 15 カ国の政府専門家グループが策定した勧告を含む。本報告書は，規範についてのさらなる作業，信頼を高める方法及びキャパシティビルディング措置の必要を含んだ過去の専門家グループの 2010 年の勧告を基礎にする。

私は国際連合憲章及び国際法の中心性並びに国家が責任を果たすことの重要性に焦点を合わせる報告書を評価する。本勧告は，国際関係を規律し，国際平和及び安全の基礎を築く既存の国際法制度及び国際理解において ICT セキュリティを定着するための方向性を示す。

本グループが留意するように，国際連合は ICT の利用におけるセキュリティの問題についての加盟国間の対話を促進し，さらにこの分野における国際協力を発展させる上で重要な役割を果たす。

私は本グループの議長及び専門家の勤勉な作業に感謝する。本報告書は ICT の利用における安全及び安定の強化のための今後の取り組みの健全な基盤をもたらす。私はこの勧告を，ICT の価値を最大化する一方でそれに関連するリスクを最小化するためのグローバルな取り組みにおける重要な一歩として，総会に託す。

伝達状

2013 年 6 月 7 日

私はここに「国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ」の報告書を提出する栄誉を有する。本グループは総会決議 66/24 の第 4 段落に従い 2012 年に任命された。本グループの議長として，本報告書においてコンセンサスを得られたことを謹んで報告する。

総会は，決議「国際安全保障の文脈における情報電気通信分野の進展」において，衡平な地理的配分に基づき，情報セキュリティの領域における既存及び潜在的な脅威と 情報空間に関する国家の責任ある行動規範，規則又は原則及び信頼醸成措置並びにグローバルな情報電気通信システムのセキュリティの強化を目的とする概念等それに対処するために考えらえる協力策を引き続き検討するために政府専門家グループを 2012 年に設置することを要請した。本グループは過去のグループの評価及び勧告（A/65/201）を考慮に入れることも求められた。事務総長は検討結果に関する報告書を第 68 会期総会に提出するよう要請された。

右決議の条件に従い，専門家はアルゼンチン，豪州，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，英国及び米国の 15 カ国から任命された。専門家の一覧表は添付文書に記載されている。

政府専門家グループは，国際安全保障の文脈における情報電気通信分野の進展に関する包括的で詳細な意見交換を行った。本グループは 3 回会合を実施した（第 1 回は 2012 年 8 月 6 日から 10 日まで国連本部において，第 2 回は 2013 年 1 月 14 日から 18 日までジュネーヴにおいて，第 3 回は同年 6 月 3 日から 7 日まで国連本部において実施）。

本グループは，本グループのコンサルタントを務め，ジェームズ・ルイス，ケルスティン・ヴィニャー（第 2 回及び第 3 回セッション）及びベン・ベイスリー＝ウォーカー（第 1 回セッション）によって代表される国連軍縮研究所の貢献に謝意を表明したい。本グループは，本グループの事務局を務めた国連軍縮部のイーウェン・ブキャナン及び本グループを支持したその他の事務局員に謝意を表明したい。

（*署名*） 議長 デボラ・ストークス

I. 序論

1. 情報通信技術(ICT)の利用は，国際安全保障環境を再形成した。ICT は計り知れない経済的社会的利益をもたらすが，国際平和及び安全と両立しない目的のためにも利用され得る。近年 ICT は犯罪及び破壊活動に利用され，そのリスクが顕著に増加している。

2. リスクを軽減し，セキュリティを強化するために国際協力は不可欠である。このため，総会は，

事務総長に， 政府専門家グループの支援の下，既存及び潜在的な脅威に対処するために考えらえる協力策（決議 66/24）を引き続き検討し，第 68 回総会に報告書を提出することを要請した。本報告書は，本議題を調べ，今後の作業のための提言をした過去の政府専門家グループによる 2010 年報告書(A/65/201)を基礎とするものである。

3. 2010 年報告書は集団的リスクを軽減し，国家及び国際的な重要インフラを防護するために国家による ICT の利用に係る規範についての国家間のさらなる対話を勧告した。右報告書は，紛争における ICT の利用についての国家の意見交換並びに国家の法律，ICT セキュリティ戦略，政策，技術及びベストプラクティスに関する情報交換を含む信頼醸成，安定及びリスク軽減措置を求めた。2010 年報告書は，ICT のセキュリティに取り組む上で支援を要すると考えられる国家の能力構築の重要性を強調し，共通の用語及び定義を精緻化するための追加的な作業を提案した。

4. 2010 年以降の数多くの二国間，地域的及び多国間のイニシアティブは，ICT のセキュリティ及びその利用の安全の強化，公共の安全に対するリスクの軽減，国家の安全の向上並びにグローバルな安定性の強化の重要性の高まりを際立たせている。平和目的の ICT 利用を推進することは全ての国家に利益にかなう。国家は ICT の利用から生じる紛争を予防することにも関心を持っている。国家による ICT の利用に適用される規範，規則及び原則に関する共通理解並びに自主的な信頼醸成措置は平和及び安全の推進において重要な役割を果たすことができる。国際平和及び安全への挑戦に対処するための国際社会の作業は初期段階にあるが，責任ある国家の行動規範，規則及び原則に関するいくつかの措置をさらに検討するために特定することができる。

脅威，リスク及び脆弱性

5. ICT は（軍民）両用の技術であり，正当な目的のためにも悪意の目的のためにも利用することができる。いかなる ICT 機器も不正利用の発信源又は対象になることができる。ICT の悪意ある利用は容易に隠すことができ，特定の加害者に責めを帰することは困難であり，多くの場合罰せられることなく ICT を悪用する主体のエクスプロイトのさらなる巧妙化を可能にする。ICT ネットワークのグローバルな繋がりはこの問題をさらに悪化させる。グローバルな繋がり，脆弱な技術及び匿名性の組合せは破壊活動のための ICT の利用を促進する。

6. 個人，企業，国家のインフラ及び政府に対する脅威はより深刻になり，これらに対するインシデントはより大きな損害をもたらしている。これらの脅威の発信源は，国家及び非国家主体の双方から成る。また，個人，グループ，犯罪組織を含む集団は，国家のプロキシ（代理）として，悪意ある ICT 行動を起こす可能性がある。国家又は非国家主体によるボットネット等巧妙な悪意あるツール及び技術の開発及び普及の潜在性は，誤った帰属及び意図しないエスカレーションのリスクをさらに高めるおそれがある。ICT の利用に関して許される国家の行動についての共通認識の欠

如は国際平和及び安全に対するリスクを高める。

7. テロ集団は通信，情報収集，採用活動，編成，攻撃の計画及び調整，思想及び活動の普及並びに資金調達のためにICTを利用している。テロ集団が攻撃ツールを得た場合，破壊的なICT活動を行う可能性がある。

8. 国家は，ICTへの有害な隠れた機能の埋め込みは，安全で信頼できるICTの利用並びに製品及びサービスのICTサプライチェーンに悪影響を及ぼし，取引の信用を失墜させ，国家の安全に損害を引き起こすような方法で利用され得ることを懸念している。

9. 重要インフラ及び産業制御システムにおけるICTの利用の拡大は，新たな破壊の可能性を生み出す。携帯通信機器，ウェブサービス，ソーシャルネットワーク及びクラウドコンピューティングサービスの利用の急速な増加はセキュリティの課題を拡張する。

10. 国家間のICTセキュリティの能力のレベルの相違は 相互に連結された世界における脆弱性を高める。悪意を持った主体はどこからでもネットワークをエクスプロイトする（弱点を突く）。この脆弱性はICTの利用に関連する国の法律，規制及び慣行の格差によって拡大する。

II. 平和的，安全，強靭かつオープンなICT環境のための協力の構築

11. 加盟国は，ICTの悪意ある利用がもたらす脅威に対する協調行動の必要を再三にわたって確認してきた。国際レベルにおける協力のさらなる進展のためには，平和的，安全，オープンかつ協調的なICT環境を促進するための一連の行動が必要になる。国際平和，安定及び安全を強化することができる協力策を検討すべきである。この策には，国家の責任ある行動に関連する国際法とそれから派生する規範，規則及び原則の適用に関する共通理解が含まれる。

12. 国家がこれらの課題の対処を主導しなければならないが，効果的な協力は民間部門及び市民社会の適切な参画から恩恵を受けることができる。

13. 国際連合は，ICTのセキュリティ及びその利用の安全に関する共通理解の発展，地域的取り組みの慫慂，信頼醸成及び透明性措置の促進並びにキャパシティビルディング及びベストプラクティスの普及の支援のための加盟国間の対話の促進において主導的な役割を果たすべきである。

14. 国際連合体制の作業に加え，国際機関及びアフリカ連合，東南アジア諸国連合(ASEAN)地域フォーラム，アジア太平洋経済協力フォーラム，欧州評議会，西アフリカ諸国経済共同体，欧州連合，アラブ連盟，米州機構，欧州安全保障協力機構(OSCE)及び上海協力機構等の地域機関によ

って尽力されている。ICT の利用の安全保障に関する今後の作業は，これらの努力を考慮に入れるべきである。

15. 課題の広範性を認識し，既存及び潜在的な脅威，リスク及び脆弱性を考慮し，2010 年 7 月の「国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ」報告書に含まれる評価及び勧告を踏まえ，本グループは，次の措置を勧告する。

III. 国家の責任ある行動規範，規則及び原則に関する勧告

16. 国家による ICT の利用に関連する既存の国際法から派生する規範の適用は国際平和，安全及び安定に対するリスクを軽減するために不可欠な措置である。国家の行動及び国家による ICT の利用に対してそのような規範がどのように適用されるかについての共通理解は，さらなる検討を要する。ICT の固有の特性に鑑み，時間をかけて追加的な規範を策定する可能性がある。

17. 本グループは，総会決議 64/25，65/41 及び 66/24 に含まれる総会からの呼びかけに対する回答として提供された加盟国の国際安全保障の文脈における情報電気通信分野の進展に関する見解及び評価並びに決議 55/63，56/121，57/239， 58/199 及び 64/211 に含まれるその他の措置を検討した。

18. 本グループは，中国，ロシア，タジキスタン及びウズベキスタン政府代表部の要請により事務総長が配布し，後にカザフスタン及びキルギスが共同提案した情報セキュリティのための国際行動規範案を含む国連文書 A/66/359 に留意した。

19. 国際法とりわけ国際連合憲章は適用され，平和及び安定を維持し，オープン，安全，平和的かつアクセシブルな ICT 環境を促進するために不可欠である。

20. 国家主権及び主権から派生する国際規範及び原則は，国家の ICT 関連活動に適用され，その領域内の ICT インフラに対する管轄権に及ぶ。

21. ICT のセキュリティに対処するための国家の取り組みは，世界人権宣言及びその他の国際文書に規定されている人権及び基本的自由の尊重と両立したものでなければならない。

22. 国家は，犯罪者又はテロリストの ICT の利用に対する協力を強化し，必要に応じて法的アプローチを調和し，各国の法執行及び検察機関間の実践的な連携を強化すべきである。

23. 国家は，その責めに帰する国際違法行為に関する国際義務を果たさなければならない。国家

は，国際違法行為を行うためにプロキシ（代理）を利用してはならない。国家は，その領域が，非国家主体の ICT の不正行為のために利用されないように努めなければならない。

24. 国家は，ICT 製品及びサービスのサプライチェーンセキュリティを含む ICT のセキュリティ及び ICT の利用の安全の向上のための適切な役割を果たすよう民間部門及び市民社会に奨励すべきである。

25. 加盟国は，民間部門及び市民社会団体が果たし得る役割を含む上記の責任ある行動規範及び原則の実施を協力する最善の方法を検討すべきである。これらの規範及び原則は，国際連合及び地域的機関の作業を補完し，信頼及び信用を醸成するための今後の作業の基盤である。

Ⅳ. 信頼醸成措置及び情報の交換に関する勧告

26. 自主的な信頼醸成措置は，予測可能性を高め，誤解を減らすことにより，国家間の信用及び信頼を促進し，紛争のリスクを軽減する一助となることができる。右措置は，国家の ICT の利用に対する各国の懸念を払拭するために大きく寄与することができ，国際安全保障の強化への重要な一歩となり得る。国家は，次に掲げるものを含む透明性，予測可能性及び協力を強化する一助となる実践的な信頼醸成措置の構築を検討すべきである。

(a) 自主的な国家戦略及び政策，ベストプラクティス，意思決定プロセス，関連する国家機関及び国際協力を改善するための措置についての意見及び情報交換。当該情報の範囲は提供する国家が決定する。この情報は，二国間，地域機関又はその他の国際フォーラムにおいて共有することができる。

(b)，国家の ICT の利用から生じる破壊的なインシデントをどのように防止するか，又，これらのインシデントがどのように開発され，管理され得るかについての国家の審議を練磨するためのワークショップ，セミナー及び演習を伴う信頼醸成のための二国間，地域的及び多国間協議枠組みの構築

(c) 適時対応，回復及び緩和行動のための ICT インシデントに関連する情報の受領，収集，分析及び共有を目的とする既存のチャネル（ルート）のより効果的な利用又は適切な新しいチャネル及びメカニズムの構築を含む ICT セキュリティインシデントに関する国家間の情報共有の強化。国家は，既存の危機管理用通信チャネルの拡大及び改善並びに早期警戒メカニズムの構築の支援のために，国のコンタクトポイントに関する情報交換を検討すべきである。

(d) 政治及び政策レベルの対話を支援するための二国の国家コンピュータ緊急対応チーム(CERT)間，CERT コミュニティ内及びその他のフォーラムにおける情報交換及びコミュニケーション

(e) ICT 対応(ICT-enabled)産業制御システムに依存する ICT 又は重要インフラに悪影響を及ぼし得るインシデントに対処するための協力の増加。これには，非国家主体が行う破壊行為に対する国家間のガイドライン及びベストプラクティスなどが考えられる。

(f) 敵意ある国家の行動と誤解され得るインシデントを軽減するための法執行機関の協力メカニズムの強化は国際安全保障を改善するだろう。

27. これらの信頼醸成の初期の取り組みは，実践的経験を与え，今後の作業を有効的に導くことができる。国家は，二国間及びアフリカ連合，ASEAN 地域フォーラム，欧州連合，アラブ連盟，米州機構，OSCE，上海協力機構等の地域機構を含む多国間で行われてきた進展を奨励し，基礎にすべきである。これらの取り組みを基礎として，国家は，国家及び地域間の差異を考慮し，措置の補完性及びベストプラクティスの普及を促進すべきである。

28. 国家が信頼醸成措置の構築を主導しなくてはならないが，その作業は，民間部門及び市民社会の適切な関与から恩恵を受けることができるだろう。

29. ICT の発展の速度及び脅威の範囲を鑑み，本グループは，共通理解の促進及び実践的協力の強化の必要があると考える。この関連で，本グループは，国際連合主催の広範な参加者による定期的な制度的対話並びに二国間，地域的及び多国間フォーラム及びその他の国際機関を通じた定期的な対話を勧告する。

V. キャパシティビルディング措置に関する勧告

30. キャパシティビルディングは，ICT とその利用の安全を確保する効果的かつ協調的なグローバルな取り組みにとって極めて重要である。国家によっては，重要 ICT インフラのセキュリティの改善，責務を果たすための技術力及び適切な法律，戦略及び規制枠組みの構築並びに ICT 及びその利用のセキュリティの格差の是正に関する取り組みにおいて支援を要する場合がある。

31. この点，国連機関を含む国際機関及び民間部門と協働する国家は，ICT セキュリティとその利用の能力を構築するための技術的な支援及びその他の支援を必要とする国とりわけ開発途上国にどのように支援をするのが最善かを検討すべきである。

32. キャパシティビルディングに関する決議 64/211 を含むこれまでの国連の決議及び報告書の作業を基礎にし，国家は次に掲げる措置を検討すべきである。
(a) ICT の利用及び ICT インフラの安全の確保，国の法制度，法執行能力及び戦略の強化，犯罪及びテロ目的の ICT の利用との闘い及びベストプラクティスの特定及び普及の支援をするための二国間，地域的，多国間及び国際的なキャパシティビルディングの取り組みの支援
(b) CERT を含むインシデント対応能力の構築及び強化並びに CERT 間協力の強化
(c) デジタルディバイド（情報格差）を解消する一助となり，かつ，開発途上国が国際的な政策の進展に遅れずについていけるようにするための ICT セキュリティに関する e ラーニングの開発及

び利用，研修並びに意識啓発の支援
(d) 特に開発途上国との ICT セキュリティインシデント管理のための協力並びに知識及び技術の移転の増強
(e) ICT セキュリティ関連事項についての研究機関及び大学によるさらなる分析と検討の奨励。国連加盟国及び国際社会を支援する固有のマンデートに鑑み，国家は，これに関して関係のある国連の研究機関及び研修機関がどのような役割を果たせるかを検討すべきである。

33. 本グループは，キャパシティビルディング等を通じた ICT の利用の安全確保の進展は，ミレニアム開発目標 8「開発のためのグローバルなパートナーシップの推進」の達成に寄与することを認識した。

VI. 結論

34. 国家の ICT の利用に関する国際安全保障の進展は，各措置がその前の措置を基礎とする反復的なものになる。変化と新しい ICT 利用者の数の着実な増加によって形成される技術環境がこの反復的な取り組みを必要にさせる。本報告書は過去の作業を基礎にする勧告を含む。その実施と改良は全ての利害関係者間の信頼を高める一助となる。本グループは，加盟国が本報告書を積極的に検討し，これらの勧告のさらなる発展と実施のためにどのように取り扱うことができるかを評価することを勧告する。

添付文書

国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループメンバー一覧表

アルゼンチン
アルフレド・モレッリ（Alfredo Morelli）大使　外務・宗務省エネルギー・技術部調整官

豪州
デボラ・ストークス（Deborah Stokes）外務貿易省第一次官補

ベラルーシ
ウラジミール・N・ゲラシモヴィッチ（Vladimir N. Gerasimovich）外務省国際安全保障軍備管理局長

カナダ
マイケル・ウォルマ（Michael Walma）外務国際貿易省政策企画課長

中国
王雷（Lei Wang）外交部軍控司（外務省軍備管理局）課長（第 1 及び第 2 回会合）
董志華（Zhihua Dong）外交部軍控司（外務省軍備管理局）参事官（第 3 回会合）

エジプト
シェリフ・ハシェム博士（Sherif Hashem）通信情報技術省通信情報技術大臣上級サイバーセキュリティ担当顧問

エストニア
リンナー・ヴィック（Linnar Viik）エストニア IT カレッジ・ディレクター代理

フランス
ジャン＝フランソワ・ブラレル（Jean-François Blarel）外務省事務次長・サイバー事務調整官

ドイツ
デトレフ・ヴォルター（Detlev Wolter）外務省通常兵器管理・信頼安全保障措置総局長

インド
ハーシュ・K・ジェイン（Harsh K. Jain）外務省次官補兼 E ガバナンス・情報技術課長

インドネシア
フェブリアン・A・ルッドヤード（Febrian A. Ruddyard）外務省国際安全保障・軍縮課長（第 1 回会合）
アンディー・ラミアンド（Andy Rachmianto）インドネシア・在ニューヨーク国連政府代表部公使参事官（第 3 回会合）

日本
篠塚保外務省国際テロ対策・組織犯罪対策協力担当大使兼サイバー政策担当大使（第1回会合）
今井治外務省国際テロ対策・組織犯罪対策協力担当大使兼サイバー政策担当大使外務省（第 2 及び第 3 回会合）

ロシア
アンドレイ・V・クルツキフ（Andrey V. Krutskikh）特命大使兼外務省 ICT の利用に関する政務特別調整官

英国
ニコラス・ヘイコック（Nicholas Haycock）内閣府サイバーセキュリティ情報保証局国際安全保障局長補佐

米国
ミシェル・G・マーコフ（Michele G. Markoff）米国国務省国務長官室サイバー問題副調整官

（筆者訳）

付属資料２．５．Ａ／７０／１７４[161]
国際連合

A/70/174

総会

配布:一般
2015 年 7 月 22 日
原文:英語

第 70 回会期
暫定議題 93*
国際安全保障の文脈における情報電気通信分野の進展

国際安全保障の文脈における情報電気通信部屋の進展に関する政府専門家グループ

事務総長によるノート

事務総長は，ここに，「国際安全保障の文脈における情報電気通信部屋の進展に関する政府専門家グループ」の報告書を伝達する栄誉を有する。本グループは総会決議 68/243 の第 4 段落に従い設置された。

国際安全保障の文脈における情報電気通信部屋の進展に関する政府専門家グループの報告書

要約

情報通信技術(ICT)は，国際社会に計り知れない機会を与え，重要性が高まり続けている。しかし，国際平和及び安全に対するリスクを引き起こす不穏な傾向がある。このリスクを軽減するためには国家間の効果的な協力が不可欠である。

2015 年の「国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ」は，国家による ICT の利用がもたらす既存及び潜在的な脅威を調べ，規範，規則，原則及び信頼醸成措置等その脅威に対処するための措置を検討した。また，本グループは国家による ICT の利用に国際法がどのように適用されるかを検討した。過去のグループの作業を基礎に，本グループはこれらの分野において重要な進展を遂げた。

本報告書は規範に関する議論を大幅に拡張する。本グループは，国家が，有害な ICT 慣習を

[161] 原文は A/70/174 (https://undocs.org/A/70/174) （最終アクセス日：2017 年 12 月 18 日）

防ぐために協力し，その領域が ICT を用いた国際違法行為に利用されることを了知しながら認めるべきではないと勧告した。本グループは，テロ及び犯罪者による ICT の利用を起訴するための情報の交換及び支援の強化を求めた。そうすることで，本グループは，国家はプライバシー及び表現の自由を含む人権の全面的な尊重を保障するべきと強調した。

一つの重要な勧告は，国家は，重要インフラの利用及び運用に意図的に損害を与え，又は害する ICT 活動を行い，又はそれを了知しながら支援するべきではないというものであった。国家は，また，ICT の脅威からその重要インフラを防護するための適切な措置を講じるべきである。国家は他国の権限が付与された緊急対応チームの情報システムを害し， 又は当該チームを悪意ある国際活動に従事させるべきではない。国家は，ICT の脆弱性の責任ある報告を奨励し，サプライチェーンの完全性を確保するための適正な措置を講じ，悪意ある ICT ツール，技術又は有害な隠れた機能の拡散を防止すべきである。

信頼醸成措置は協力及び透明性を高め，紛争のリスクを軽減する。本グループは，透明性を高めるための幾つかの自主的な信頼醸成措置を特定し，国家が，協力を強化するための追加的な措置を検討することを提案した。本グループは，国連主催の，及び二国間，地域的及び多国間フォーラムを通じた広範な参加者による定期的な対話を求めた。国家が安全かつ平和的なICT 環境を維持する一義的な責任を負うが，国際的な協力は民間部門，学界及び市民社会の適切な参画から恩恵を受けることができると考えられる。

キャパシティビルディングは協力と信頼醸成に不可欠である。専門家グループの 2013 年報告書（A/68/98 参照）は，国際社会に，重要 ICT インフラのセキュリティの改善支援，技術力の構築支援及び適切な立法，戦略及び規制に関する助言をするよう求めた。本グループは，この結論を改めて表明し，全ての国家は脅威とその効果的な対処について他国から学ぶことができることを強調した。

本グループは，国家による ICT の利用におけるセキュリティの強化の基盤としての国際法，国連憲章及び主権原則の重要性を強調した。本グループは，さらなる検討が必要なことを認識するとともに，国際法に合致し，国連憲章で認められた措置を取る国家固有の権利に留意した。本グループは，人道，必要性，均衡性及び区別原則を含む適切な確立された国際法原則にも留意した。

今後の作業のため，本グループは，総会が新たな政府専門家グループを 2016 年に開催することを検討するよう提案した。

本グループは，加盟国がグループの勧告を積極的に検討し，そのさらなる発展と実施のためにどのように取り上げるかを評価することを求める。

目次

Ⅱ. 既存及び潜在的な脅威
Ⅲ. 国家の責任ある行動のための規範，規則及び原則
Ⅳ. 信頼醸成措置
Ⅴ. ICT セキュリティにおける国際協力及び援助並びにキャパシティビルディング
Ⅵ. ICT の利用にどのように国際法が適用されるか
Ⅶ. 結論及び今後の作業の勧告
添付文書

事務総長による序文

経済，社会及び国際関係を再形成する上で，情報通信技術(ICT)ほど強力であった技術はほとんどない。サイバー空間は我々の生活のあらゆる面に関係がある。その利益は莫大だが，リスクもまた伴う。サイバー空間は国際協力を通じてのみ安定かつ安全なものにすることができ，この協力の基礎は，国際法及び国際連合憲章の原則でなければならない。

本報告書は20カ国の政府専門家が国際平和及び安全を脅かし得る国家及び非国家主体一様の ICT の利用がもたらす既存及び新しい脅威に対処するために策定した勧告を含む。専門家たちは，2010 年及び 2013 年に発表されたコンセンサスレポートに基礎を置き，規範設定，信頼醸成，キャパシティビルディング及び国際法の適用に関するアイディアを提供する。

新たに出現した複雑な問題の一つに過激派，テロリスト及び組織的犯罪集団による悪意ある ICT の利用の増加がある。本報告書は，この気がかりな傾向の対処の一助となり，私の来るべき暴力的な過激主義を防止するための行動計画の策定に寄与する提案を行う。

全ての国家はサイバー空間をより安全なものにすることに関心がある。この分野における我々の取り組みは，オープン，安全かつ平和的なインターネットを促進するための地球規模のコミットメントを守らなければならない。そうした精神から，私は，ICT 環境を安全にする重要な取り組みへの決定的な貢献として，総会及び幅広く世界の人々への本報告書を託す。

伝達状

2015 年 6 月 26 日

私は，ここに，「国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ」の報告書を提出する栄誉を有する。本グループは国際安全保障の文脈における情報電気通信分野の進展についての総会決議 68/243 の第 4 段落に従い 2014 年に設置された。本グループの議長として，本グループについてコンセンサスを得られたことを謹んで通知する。

総会は，その決議において，衡平な地理的配分に基づき，共通理解の促進を目的として， 情報セキュリティの領域における既存の，及び潜在的な脅威とそれに対処するために考えられる国家の責任ある行動規範，規則又は原則，信頼醸成措置等の協力策，紛争における情報通信技術の利用及び国家による情報通信技術の利用にどのように国際法が適用されるかという問題並びにグローバルな情報電気通信システムのセキュリティの強化を目的とする概念を検討し続けるために政府専門家グループを 2014 年に設置することを要請した。本グループは，過去のグループの評価及び勧告（A/68/98 参照）を考慮することも求められた。事務総長は第 70 会期総会において検討結果に関する報告書を提出するよう要請された。

総会決議の条件に従い，専門家は，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，グレートブリテン及び北アイルランド連合王国及びアメリカ合衆国の 20 カ国から任命された。専門家の一覧は添付文書に記載されている。

本グループは，国際安全保障の文脈における情報電気通信分野の進展に関する包括的で詳細な意見交換を行った。本グループは 4 回会合を行った（第 1 回は 2014 年 7 月 21 日から 25 日まで国連本部において，第 2 回は 2014 年 1 月 12 日から 16 日までジュネーヴ，第 3 回は 2015 年 4 月 13 日から 17 日まで，第 4 回は 2015 年 6 月 22 日から 26 日まで国連本部において開催）。

本グループは，報告書案に関する議論のファシリテーターを役割を果たした専門家のフローランス・マンガン（フランス），キャサリン・ゲタオ（ケニア），ウサフ・アリ（パキスタン），リカルド・モル（スペイン）及びオリビア・プレストン（英国）に感謝したい。

本グループは本グループのコンサルタントとして役割を果たし，ジェームズ・ルイス及びケルスティン・ヴィニャーによって代表される国連軍縮研究所の貢献に謝意を表明したい。また，本グループの事務局長を務めた国連軍縮部のイーウェン・ブキャナン及び本グループを支援したその他の事務局員にも感謝の意を表明したい。

（*署名*）議長　カルロス・ルイス・ダンタス・コウティーニョ・**ペレズ**

I. 序論

1. 国際安全保障の文脈における情報電気通信分野の進展に関する総会決議 68/243 に従い，事務総長は，衡平な地理的配分に基づき，共通理解の促進を目的として，情報セキュリティの領域における既存及び潜在的な脅威と，国家の責任ある行動に関する規範，規則又は原則，信頼醸成措置，紛争における情報通信技術（ICT）の使用の問題，国家による ICT の使用にどのように国際法が適用されるか，グローバルな情報電気通信システムのセキュリティの強化を目的とした関連する国際概念等を含む当該脅威に対処するための可能な協力策を継続して検討するための政府専門家グループを設置した。

2. オープンで，安全，安定的，アクセシブルかつ平和的な ICT 環境は，全ての者にとって不可欠であり，国際平和及び安全に対するリスクを削減するための国家の効果的な協力が必要である。本報告書は，「国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ」の勧告を反映し，過去のグループの作業（A/65/201 及び A/68/98 参照）を基礎とする。専門家グループは，そのマンデートに関連する国際概念及び可能な協力策を検討した。当該グループは，ICT の使用を平和目的の ICT の利用とその利用から生じる紛争を防止することを促進するが全ての国家の利益になることを再確認した。

II. 既存及び新たな脅威

3. ICT は，社会経済発展の計り知れない機会を提供し，国際社会において重要性が増し続けている。しかしながら，国家及び非国家主体による ICT の不正利用を伴うインシデントの劇的な増加等グローバルな ICT 環境において不穏な傾向がある。この傾向は，全ての国家にリスクを作り出し，ICT の不正利用は国際平和及び安全を害する可能性がある。

4. 複数の国家は，軍事目的の ICT 能力を開発している。将来の国家間の紛争における ICT の利用の可能性が高まっている。

5. ICT を用いた最も有害な攻撃は，国家の重要インフラ及び関連情報システムに対する標的型攻撃等である。重要インフラに対する有害な ICT 攻撃のリスクは，現実的かつ深刻なものである。

6. 採用，資金調達，訓練及び扇動を超えた ICT に対する又は ICT に依存するインフラに対するテロ攻撃等テロ目的の ICT の利用の可能性は高まっており，もしこれが対処されないままでいると，国際平和及び安全を脅かす可能性がある。

7. 犯罪集団及びテロリストを含む悪意ある非国家主体の多様性，その異なる動機，悪意ある ICT の行為が発生する速度及び ICT インシデントの発生源の帰属の困難性は全てリスクを高める。国家は，不安定化を招く誤解の危険性，紛争の可能性及びその国民，財産及び経済を害される可能性を当然ながら懸念している。

8. 国家間の ICT セキュリティの能力のレベルの相違は，相互に連結された世界における脆弱性を高めるおそれがある。

III. 国家の責任ある行動規範，規則及び原則

9. ICT 環境は，国家の ICT 関連活動に規範，規則及び原則がどのように適用されるかを決める上で，国際社会に機会と課題の双方を与える。目標の一つは，さらに責任ある国家の行動の自主的な非拘束的規範を特定し，グローバルな ICT 環境の安定性及び安全性を高めるために共通理解を強めることである。

10. 自主的で非拘束的な責任ある国家の行動規範は国際平和，安全及び安定性に対するリスクを軽減することができる。従って，規範は，国際法に合致する行動を制限又は禁止しようとするものではない。規範は，国際社会の期待を反映し，責任ある国家の行動の基準を設定し，国際社会が国家の活動及び意図を評価できるようにする。規範は，ICT 環境における紛争の予防の一助となり，グローバルな社会経済発展を高めるICTの完全実現を可能にする平和的利用に寄与する。

11. 専門家グループの過去の報告書は，既存の国際規範及び公約から導かれる ICT のセキュリティ及び利用に関する責任ある国家の行動についての新たな合意を反映した。本グループの前に課された任務は，共通理解の促進を目的として，責任ある国家の行動規範を引き続き検討し，既存の規範をどこで ICT 環境に適用されるようまとめるかを決め，規範がより広く受容されるよう奨励し，ICT の複雑さ及び特性を踏まえた追加的な規範の策定が必要かどうかを確認することであった。

12. 本グループは，中国，カザフスタン，キルギス，ロシア，タジキスタン及びウズベキスタンの情報セキュリティ国際行動規範案（A/69/723 参照）に留意した。

13. 既存の及び新たな脅威，リスク及び脆弱性を踏まえ，過去のグループの 2010 年及び 2013 年の報告書に盛り込まれた評価及び勧告に基づき，本グループは，オープン，安全，安定的でアクセシブルかつ平和的なICT環境の促進を目的とする自主的で非拘束的な責任ある国家の行動規範，規則又は原則を各国に検討してもらうよう，次のことを提案する。

(a) 国際平和及び安全の維持を含む国際連合の目的と両立するよう，国家は，ICT の利用における安定性及び安全性を高めるため，国際平和及び安全に有害と認められ，又は，これらを脅かすおそれがある ICT の慣行を防ぐための方策の策定及び適用に関し協調すべきである。

(b) ICT インシデントが発生した場合，国家は，当該事象のより大きな文脈，ICT 環境における帰属（アトリビューション）の課題及び結果の性質及び範囲を含む関連する全ての情報を考慮すべきで

ある。
(c) 国家は，その領域が ICT を用いた国際違法行為に使用されることを了知しながら認めるべきではない。
(d) 国家は，情報交換，相互支援，テロリスト及び犯罪者による ICT の利用の訴追及びこれらの脅威に対処するための他の協力策の実施の最善の協力方法を検討すべきである。この点に関し，国家は，新しい対策を構築する必要があるか検討しなければならないかもしれない。
(e) 国家は，ICT の安全な利用を確保する上で，表現の自由を含む人権の完全な尊重を保障するため，インターネットにおける人権の促進，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権に関する総会決議 68/167 及び 69/166 を尊重すべきである。
(f) 国家は，国際法上の義務に反して，故意に重要インフラに損害を与え，又は一般市民にサービスを提供する重要インフラの使用及び運用を阻害する ICT 活動を行い，又はそれを了知して支援してはならない。
(g) 国家は，サイバーセキュリティのグローバル文化の創造及び重要情報インフラの防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，その重要インフラを ICT の脅威から防護するための適切な施策を講じるべきである。
(h) 国家は，その重要インフラが悪意ある ICT 行為を受けている他の国家からの適切な支援要請に応じるべきである。 国家は，主権への正当な配慮を踏まえ，その領域から発せられる他の国家の重要インフラを対象とする悪意ある ICT 活動を軽減するための適切な要請にも応じるべきである。
(i) 国家は，エンドユーザーが ICT 製品のセキュリティを信頼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対策を講じるべきである。国家は，悪意ある ICT ツール及び技術並びに隠された有害な機能の利用の拡散を防ぐよう努めるべきである。
(j) 国家は，ICT の脆弱性の責任ある報告を慫慂し，ICT 及び ICT に依存したインフラへの潜在的な脅威を抑え，又は除去するため，当該脆弱性に有効な救済策に関する情報を共有すべきである。
(k) 国家は，他国の権限が付与された緊急対応チーム（しばしばコンピュータ緊急対応チーム（CERT）又は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もの。）の情報システムを害する活動を行い，又はそれを了知して支援すべきではない。国家は，権限が付与された緊急対応チームを悪意ある国際的な活動に従事するために利用すべきではない。

14. 本グループは，このような対策が，オープン，安全，安定的でアクセシブルかつ平和的な ICT 環境の促進に不可欠なものかもしれないが，これを，とりわけ開発途上国が，適切な能力（キャパシティ）を得るまでは，直ちに実施するのは可能ではないかもしれないことを確認した。

15. ICT の固有の特性に鑑み，時間をかけて追加的な規範が策定される可能性がある。

Ⅳ. 信頼醸成措置

16. 信頼醸成措置は，国際平和及び安全を強化する。信頼醸成措置は，国家間の協調，透明性，予測可能性及び安定性を高めることができる。国家は，平和的なICT環境を確保するための信頼醸成の作業において，1988年に軍縮委員会により採択され，また，総会において，決議43/78（H）により全会一致で支持された信頼醸成措置に関するガイドラインを考慮に入れるべきである。信頼及び協力を強化し，紛争のリスクを軽減するため，本グループは，国家が，次に掲げる自主的な信頼醸成措置を検討することを提言する。

(a) 重大な ICT インシデントに対処するための政策及び技術レベルの適切なコンタクトポイントの特定及び当該コンタクトポイントの名簿（ディレクトリ）の作成，

(b) 国家間の信頼醸成及び ICT インシデントから生じ得る誤解，エスカレーション及び紛争のリスクの軽減のための必要に応じた二国間，地域的，準地域的及び多国間協議のメカニズム及びプロセスの策定及び支援

(c) 信頼を高め，今後の作業を周知させる必要に応じた二国間，準地域的，地域的及び多国間レベルの自主的な透明性の慫慂。これには，などが考えられる。ICT 及びその使用に対する国内及び国境を越える脅威の様々な側面，ICT製品の脆弱性及び特定された有害な隠れた機能，ICTセキュリティの最良慣行（ベストプラクティス），地域的及び多国間フォーラムにおいて策定された信頼醸成措置及び ICT セキュリティに関連する国家機関，戦略，政策及び計画等に関する国家の見解及び情報の自主的な共有などが考えらえる。

(d) 国家が重要とみなすインフラの類型についての国家の見解とデータ及び ICT を利活用したインフラの防護のための国家の法律及び政策に関する情報を含むそれを防護するための国家の取り組みに関する国家による自主的な提供。国家は国境を越える重要インフラの脆弱性に対処するための国家間の協力を円滑にするよう努めるべきである。この対策には次に掲げるものが考えられる。

(i) データ及び ICT を利活用したインフラの防護のための国家の法律及び政策のレポジトリ（貯蔵庫）とこの法律及び政策の配布に適切とみなされる資料の公表

(ii) ICT を利活用した重要インフラの防護に関する二国間，準地域的，地域的及び多国間協議のためのメカニズム及びプロセスの構築

(iii)ICT 関連の要請に対処するための二国間，準地域的，地域的及び多国間ベースの技術的，法的及び外交的メカニズムの構築

(iv) インシデントに関する情報の交換を円滑にすることを目的としたインシデントの規模及び深刻さの観点からの ICT インシデントの分類のための自主的な国家の取極の採用

17. 国家は，二国間，準地域的，地域的及び多国間ベースの協力を強化する追加的な信頼醸成措置を検討すべきである。 これには，国家による次に掲げる事項の自主的な合意が考えられる。

(a) 必要に応じたインシデント対応及び法執行等の分野における人材交流の検討並びに研究及び学術機関間の交流の奨励を含む ICT セキュリティインシデントに対処する関連機関間の協調的メカニズムの強化と ICT インフラ関連の要請に対処するための追加的な技術的，法的及び外交的メカニズムの構築
(b) 悪意ある ICT の使用に関する情報交換のためのフォーカルポイントの構築及び捜査における支援の提供を含む協力の強化
(c) 国家のコンピュータ緊急対応チーム若しくはサイバーセキュリティインシデント対応チームの設置又はこの役割を果たす機関の公式な指定。国家は右のような機関をその重要インフラの定義の範囲内において考慮する必要がある。国家は，このような対応チーム及びその他の権限が付与された機関の機能及び協力を支援し，円滑にすべきである。
(d) 脆弱性，攻撃パターン及び対応の調整，演習の企画，ICT 関連インシデントの対応の支援並びに地位的及び部門ベースの協力の強化を含む攻撃緩和のためのベストプラクティスについての情報交換等必要に応じたコンピュータ緊急対応チームとサイバーセキュリティインシデント対応チームの協力の実践の拡大及び支援
(e) 国内法及び国際法に合致する形での他国からの ICT 関連犯罪若しくはテロ目的の ICT の利用の捜査又はその領域から発せられる悪意ある ICT 活動を緩和するための要請への協力

18. 本グループは，ICT の発展の速度及び脅威の範囲を鑑み，共通理解を深め，協力を強化する必要があることをあらためて表明する。この関連で，本グループは，国際連合主催の広範な参加者による定期的な制度的対話並びに二国間，地域的及び多国間フォーラム及びその他の国際機関を通じた定期的な対話を提言する。

V. ICT セキュリティに関する国際協力及び支援とキャパシティビルディング

19. 国家は，ICT 環境においても，国家の安全保障及び国民の安全に関し，一義的な責任を負うが，一部の国はその ICT ネットワークを保護するのに十分な能力（キャパシティ）を欠く場合があり得る。能力の欠如は，国民及び当該国の重要インフラを脆弱にし，又は図らずも悪意ある主体の温床（隠れ場所）にするおそれがある。国際協力及び支援は，国家が ICT の安全を確保し，その平和的利用を確保する上で重要な役割を果たすことができる。ICT セキュリティの分野における能力構築支援は，国家の協調と集団的な行動の能力を改善することにより，国際安全保障にとっても重要である。本グループは，キャパシティビルディング措置は ICT の平和目的の利用を促進するべきものであることに合意した。

20. 本グループは 2010 年及び 2013 年報告書のキャパシティビルディングに関する提言を支持(endorse)した。2010 年報告書は，国家が開発途上国のキャパシティビルディングを支援するため

の措置を割り出すことを提案した。20103 年報告書は，重要 ICT インフラのセキュリティを改善し，その責務を果たすための技術力，適切な法，戦略及び規制枠組みを構築し，かつ，ICT のセキュリティとその利用における格差を是正するため，国際社会に援助に協力することを求めた。本グループは，全て国家は他国から他国が直面した脅威とその脅威への効果的な対処法について学ぶことができるため，キャパシティビルディングは単に先進国から途上国への知識と技能の移転にとどまらないことも強調した。

21.「サイバーセキュリティのグローバル文化の創造及びの国家の重要情報インフラ防護に関する取り組みの精査」という題名の総会決議 64/211 を含む過去の国連の決議及び報告書を通じて始まった作業に引き続き，国家は，次に掲げる支援を必要とし，要請する国家の ICT の安全を確保する能力を構築するために行う技術及びその他の支援のための自主的な措置を検討すべきである。

(a) 国家のコンピュータ緊急対応チーム及びその他の権限が付与された機関と協調メカニズムの強化を支援すること。

(b) 重要インフラを含む ICT の使用におけるセキュリティの改善のために途上国への支援及び研修を行い，法的及び事務的なベストプラクティスを交換（共有）すること。

(c) ICT セキュリティに不可欠と思われる技術へのアクセスの提供を支援すること。

(d) 迅速な支援のための手続を含むインシデント対応及びネットワークの安全確保における短期間の問題への対処の相互支援手続を構築すること。

(e) 国境を越える重要インフラの脆弱性に対処するために国境を越える協力を円滑にすること。

(f) ICT セキュリティのキャパシティビルディングの取り組みの持続可能性のための戦略を策定すること。

(g) 国家の計画及び予算において ICT セキュリティに関する意識啓発（アウェアネス）及びキャパシティビルディングを優先し，開発援助計画において適した比重を置くこと。この計画には，組織及び個々の市民の教育を目的とする ICT セキュリティ・アウェアネス計画などが考えられる。このような計画は，国連とその専門機関を含む国際機関，民間部門，学界及び市民社会団体と併せて実施することが考えられる。

(h) フォレンジック又は犯罪もしくはテロ目的の ICT の利用に対処するための協調的措置等キャパシティビルディングに関するさらなる作業を奨励すること

22. キャパシティビルディングの地域的アプローチの構築は，特定の文化的，地理的，政治的，経済的及び社会的側面を考慮し，状況に適合したアプローチをとることができるため，有益になると考えられる。

23. ICT セキュリティキャパシティビルディングのために，国家は，確立されたパートナーシップ関係に基づく二国間及び多国間協力イニシアティブの形成を検討してもよいだろう。このようなイニシア

ティブは，ICT インシデントに関する国家間の実効的な相互扶助のための環境を改善する一助となり，これは，国連とその専門機関を含む能力のある国際機関，民間部門，学界及び市民社会団体によってさらに発展することができると考えられる。

VI. ICT の利用への国際法の適用の在り方

24. 2013 年報告書は，国際法，とりわけ国連憲章は適用可能であり，かつ，平和及び安定を維持し，オープン，安全，安定でアクセシブルかつ平和的な ICT 環境を促進するために不可欠であると述べた。本グループは，そのマンデートに従い，国際法が国家による ICT の利用にどのように適用されるかを検討した。

25. 国家による国際法，とりわけ（国連）憲章上の義務の遵守は，その ICT の利用とオープン，安全，安定的なアクセシブルかつ平和的な ICT 環境を促進するために不可欠な枠組みである。この義務が，国家による ICT の利用への国際法の適用の検討の中心となる。

26. 国家による ICT の利用への国際法の適用を検討するにあたり，本グループは，国連憲章及びその他の国際法の原則（主権平等，国際平和及び安全並びに正義を危うくしないような平和的手段による国際紛争の解決，国際関係においていかなる国の領土保全又は政治的独立性に対する，又，国際連合の目的と両立しない他のいかなる方法による武力による威嚇又は武力の行使を慎むこと，人権及び基本的自由の尊重並びに他国の内政不干渉原則）への国家のコミットメントが中心的な重要性を持つことを確認した。

27. 国家主権と主権から派生する国際規範及び原則は，国家による ICT 関連活動に適用され，その領域内における ICT インフラに関する管轄権に及ぶ。

28. 過去のグループの作業を基礎にし，国連憲章及び総会決議 68/243 に記載されたマンデートに従い，本グループは，次に掲げる国家による ICT の利用に国際法がどのように適用されるかについての例示的な（non-exhaustive）考え方を提示する。

(a) 国家は，その領域内に所在の ICT インフラに対する管轄権を有する。

(b) その ICT の利用において，国家は国際法の原則の中でもとりわけ国家主権，主権平等，平和的手段による紛争の解決及び他国の内政不干渉を遵守しなければならない。国家は，人権及び基本的自由を尊重し，保障する国際法上の義務を遵守しなければならない。

(c) 人類の共通の利益のための ICT の平和的利用という国際社会の願望を強調し，国連憲章は全体として適用されることを想起し，本グループは，国際法に合致し，国連憲章で認められた措置に関する国家固有の権利に留意した。本グループは，この件に関し，さらなる検討が必要なことを認識した。

(d) 本グループは，適宜人道原則，必要性原則，均衡性原則及び区別原則を含む確立された国際法原則に留意する。
(e) 国家は， ICTを利用した国際違法行為を行うためにプロキシを使ってはならず，その領域が，非国家主体がそのような行為を行うために利用されないように努めなければならない。
(f) 国家は，国際法上，その責めに帰せられる国際違法行為に関する国際義務を果たさなければならない。しかし，ある ICT 活動がある国家の領域又は ICT インフラから着手等されたという示唆（indication）は，当該活動が当該国家の責めに帰するとするには不十分な可能性がある。本グループは，違法行為を計画し，実施したという理由で国家の責任を問うためには，それが立証されなければならないことに留意した。

29. 本グループは，国家の ICT の利用に国際法がいかに適用されるかについての共通認識は，オープン，安全，安定，アクセシブルかつ平和的な ICT 環境を推進していく上で重要であることに留意した。

VII. 結論及び今後の作業のための提言

30. ICT の悪意ある利用による国際平和及び安全に対するリスクの認識について著しい進展があった。ICTが開発に向けた発展を加速させる原動力になることを認識し，グローバルな連結及び情報の自由かつ安全な流通を維持する必要と整合性を取るため，本グループは，これを含むがこれに限らない，次に掲げる今後の作業のための可能な対策を特定するのが有益と考える。
(a) 法的，技術的及び政策的レベルにおけるICTの利用の国際平和及び安全のための国家の集団的及び個別的な概念のさらなる策定，
(b) ICT の悪意ある利用がもたらす国際平和及び安全への潜在的なリスク及び ICT を利用する(ICT-enabled)重要インフラのセキュリティについての共通理解を醸成するための地域的及び多国間レベルにおける協力の強化

31. 国家が安全かつ平和的な ICT 環境を維持する一義的な責任を負うが，効果的な国際協力は，必要に応じて，民間部門，学界及び市民社会団体の関与のメカニズムを特定することによって恩恵を受けるだろう。

32. さらなる研究や検討が有益な分野としては，国家の ICT の利用に関連する概念などがある。全加盟国に尽力する国連軍縮研究所は，他の関連性のあるシンクタンクや研究機関と同様，関係する研究を引き受けることを要請し得る機関の一つである。

33. 国際連合は，国家によるICTの利用に関するICTのセキュリティについての対話の促進並びに国際法の適用及び責任ある国家の行動のため規範，規則及び原則について共通理解の醸成

に関し，主導的な役割を果たすべきである。次の作業には，ICT セキュリティの問題についての国際的な対話及び交流の取り組み（イニシアティブ）を検討することもあり得る。これらの取り組みは，犯罪者及びテロリストのICTの利用，人権及びインターネットガバナンス等の問題に対処するための他の国際機関及びフォーラムによる現在進行中の作業と重複すべきではない。

34. 本グループは，情報セキュリティの領域における既存及び潜在的な脅威と国家の責任ある行動に関する規範，規則及び原則，信頼醸成措置及びキャパシティビルディング等の脅威に対処するための可能な協力策や国家による ICT の利用にどのように国際法が適用されるかを引き続き検討するために2016年に総会が新たな「国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループ」の開催を検討することの重要性に留意した。

35. 本グループは，ICT セキュリティについて国際機関及び地域機関が尽力してきたことを認識する。国家間の ICT の利用に関するセキュリティに係る作業は，これらの尽力を考慮すべきであり，加盟国は，適切と思われる場合は，対話，協議及びキャパシティビルディングのための新たな二国間，地域的又は多国間のプラットフォームの設置を奨励すべきである。

36. 本グループは，加盟国が，本報告書に記載された オープン，安全，安定的，アクセシブルかつ平和的な ICT 環境の構築方法に関する提言を積極的に検討し，当該提言のさらなる進展と実施のためにどう取り組むべきかを評価することを提案する。

添付文書

国際安全保障の文脈における情報電気通信分野の進展に関する政府専門家グループメンバー一覧

ベラルーシ
アリアクサンドル・チャウスノウスキー（Aliaksandr Chasnouski）外務省国際安全保障・軍備管理局次長（第 3 及び第 4 回会合）
ウラジミール・N・ゲラシモヴィッチ（Vladimir N. Gerasimovich）大使外務省国際安全保障・軍備管理局長（第 1 回会合）
イヴァン・グリネヴィッチ（Ivan Grinevich）在ジュネーヴ・ベラルーシ国連政府代表部参事官（第 2 回会合）

ブラジル
カルロス・ルイス・ダンタス・コウティーニョ・ペレズ（Carlos Luís Dantas Coutinho Perez）外務省政務副次官参謀総長行使

中国
呉海濤(Wu Haitao)外交部サイバー事務調整官（第 3 及び第 4 回会合）
傅聡(Fu Cong)外交部サイバー事務調整官（第 1 及び第 2 回会合）

コロンビア
ホルヘ・フェルナンド・ベジャルノ（Jorge Fernando Bejarno）情報通信技術省情報技術標準・構造課長

エジプト
サメ・アブル・エネイン（Sameh Aboul-Enein）大使，外務省軍縮・国際安全保障・核エネルギー平和利用外務次官補（第 1，第 2 及び第 4 回会合）
アムル・アルジョワイリ（Amr Aljowaily）国連政府代表部公使（第 3 回会合）

エストニア
マリナ・カリュランド（Marina Kaljurand）外務次官・法律顧問

フランス
フローランス・マンガン（Florence Mangin）大使，外務省サイバーセキュリティ調整官
レオナール・ローラン（Leonard Rolland）外務省戦略・安全保障・軍備局（第 1 回会合）

ドイツ
カルステン・ガイアー（Karsten Geier）外務省サイバー政策調整部長

ガーナ
マーク＝オリバー・ケヴォー（Mark-Oliver Kevor）国立通信局理事

イスラエル
イッド・モエド（Iddo Moed）外務省サイバーセキュリティ調整官

日本
岡田隆国連担当大使兼サイバー政策担当大使，外務省総合外交政策局審議官（第 3 及び第 4 回会合）
河野章国連担当大使兼サイバー政策担当大使，外務省総合外交政策局審議官（第 2 回会合）
今福孝男外務省総合外交政策局国際安全保障交渉官（第 1 回会合）

ケニア
キャサリン・ゲタオ（Katherine Getao）情報通信技術省 ICT 担当大臣

マレーシア
ヌル・ハユナ・アブド・カリム（Nur Hayuna Abd Karim）国家安全保障会議サイバー・宇宙安全保障課第一次官補（第 4 回会合）
モハメド・シャア・ヌリ・ビン・モハメド・ザイン（Md Shah Nuri bin Md Zain）国家安全保障会議サイバー・宇宙安全保障課次官（第 1，第 2 及び第 3 回会合）

メキシコ
エドガー・スリタ（Edgar Zurita）メキシコ国家安全保障委員会―連邦警察米国・カナダ大使館アタッシェ

パキスタン
アウサフ・アリ（Ausaf Ali）統合参謀本部戦略計画局技術部長（第 1，第 2 及び第 4 回会合）
カリル・ハシミ（Khalil Hashmi）国連政府代表部公使（第 3 回会合）

韓国
イ・チュル（Chul Lee）外務省国際安全保障課長（第 2 及び第 4 回会合）
ジャン・ヒュンチョル（Hyuncheol Jang）在ベルギー王国及び欧州連合韓国大使館参事官（第 1 及び第 3 回会合）

ロシア

アンドレイ・V・クルツキフ（Andrey V. Krutskikh）特命大使，ロシア連邦大統領情報セキュリティ国際協力特別代表

スペイン

リカルド・モル（Ricardo Mor）外務協力省サイバーセキュリティ特命大使（第 4 回会合）

アリシア・モラル（Alicia Moral）外務協力省サイバーセキュリティ特命大使（第 1，第 2 及び第 3 回会合）

英国

オリヴィア・プレストン（Olivia Preston）内閣府サイバーセキュリティ・情報保証局局長補佐

米国

ミシェル・G・マーコフ（Michele G. Markoff）国務省国務長官サイバー事務調整室サイバー問題副調整官

（筆者訳）