サイバーセキュリティのグローバル・ガバナンス

政策・メディア研究科 政策・メディア専攻
後期博士課程 3年 社会人コース
小宮山功一朗

発表目次

1. 簡単な自己紹介

- 2014年春学期～現在
  - 後期博士課程社会人コース

- 2007年～現在
  - JPCERT/CC(サイバーセキュリティインシデント対応組織)で諸外国の技術コミュニティと協力して問題解決に当たる。年間20000件のインシデントは約70～90カ国との国際連携を要する
- 2014年～2018年
  - インシデント対応組織の国際団体「FIRST.org」の理事
- 2017年～現在
  - サイバー空間の規範を議論する「サイバー空間安定化委員会」の技術リサーチグループの副議長(2017年～現在)

2. 本研究の目的

リサーチクエスチョン

- サイバー空間を支配するのは誰なのか?

派生するリサーチクエスチョン

- サイバー空間は支配できるのか? その条件はなにか?
- 力の拡散が起きているのだとすれば、相対的優位なのは誰か?
- 乱立するガバナンスを模索する議論に法則を見いだせるか?

作業仮説

- サイバー空間における力は民主主義国と権威主義国とグローバルテックカンパニーの3アクターに集約されてゆく。ガバナンスはその3アクターの均衡に立脚するものとなる

3. 用語の定義

- サイバー空間
  - 広がるサイバー空間: 人間、電磁スペクトラム、製品の供給路、文明や文化
  - 本研究におけるサイバー空間は「**『通信端末＋通信回線（有線・無線）＋記憶装置＋データ（土屋2018b）』しかしエラスティック(伸び縮みする)である**」
- サイバー空間における力
  - **望んだときに望んだようにより多くのデータにアクセスできること**
    サイバー空間を構成する各プレーヤーを意識的・無意識的により多くのデータにアクセスするための競争を行っている

4-1. 研究の背景「レジームコンプレックス」

- サイバー空間は、人々のコミュニケーションの手段であるだけでなく、電気水道ガスなどのインフラの神経系であり、あらゆる経済活動の土台であり、軍事行動の新領域である
- 無いもの尽くし
  - サイバー空間の定義、中央管理の仕組み、サイバー戦争の定義(河野2015)、秩序や弱者救済の仕組み(Buchanan 2017)、ルールのエンフォーサー(Raymond 2016)
- 乱立するレジーム
  - 傘ではなくパッチワーク(Choucri 2014)と表現されるようにサイバーセキュリティガバナンスの議論の場は増加の一途
- にも関わらず『サイバーセキュリティをめぐるグローバル・ガバナンスにおいて、決定的な場はいまだ設定されていない(土屋2018a)』

4-2. 研究の背景 「勢力図の変化」

- 軍事力のバランスを変える技術革新
  - 火薬、飛行機、潜水艦、ミサイルと核兵器、宇宙技術
- 情報社会の変容を招く通信技術の革新
  - アルファベット、活版印刷、腕木通信、電信、テレビ
- サイバー空間は2つの点で異質である
  - 「普及のスピードの早さ」と「サイバー空間においてコンテンツを提供しているのはユーザ自身」であること(Deibert 2013)
  - サイバー空間は民主主義国家のみを脆弱にした
    - 技術が導くバラ色のデモクラシー論への懐疑
    - インターネットとソーシャルメディア、大規模データ収集、AIの活用は「自由主義のよくない前兆」(Kagan 2019)
    - パノプティコンの高度な現代版ではないかという疑い(神里2015: 29)

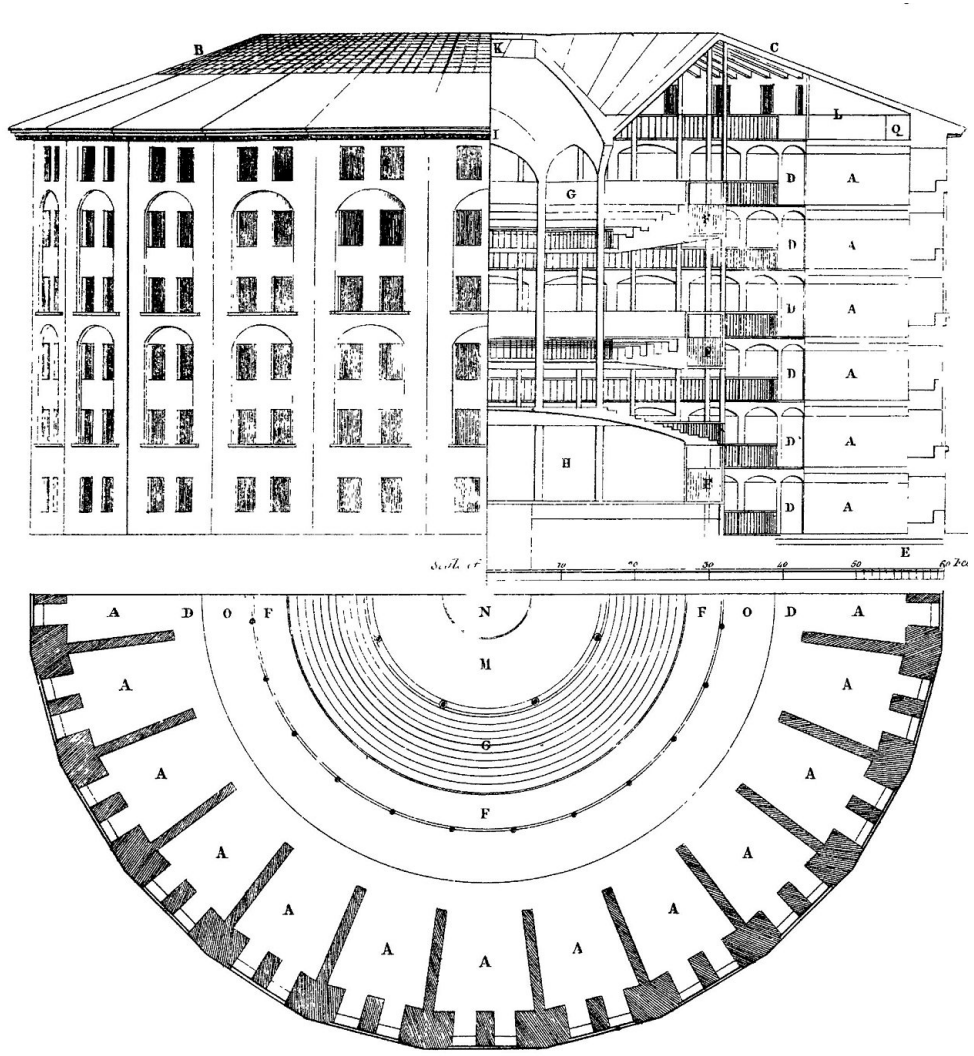


図1: ベンサムによるパノプティコンの構想

5-1. 先行研究

- インターネット・ガバナンスの視座の限界
  - インターネットガバナンスは「インターネット資源管理」、「標準の策定」、「サイバーセキュリティガバナンス」、「相互接続に関する合意形成」、「情報仲介の政策的役割」、「システム化された知的財産保護」の集合 (Denardis 2015)
  - 「官・民・市民社会の対等な参加」 で「自律・分散・協調」のインターネットを保持できるか?
- サイバー空間のガバナンスに期待されるもの
  - 『多様なアクターの分散されたパワーの集合が、結局の所、既存の力関係(パワーダイナミクス)を強化してしまう(Carr 2015) 』
  - 『人間は自由だけを希求するわけではない(Kagan)』。身体の安全、家族の安全、民族の安全、宗教の安全は言論の自由と同等に重要であることを軽視

5-2. 先行研究

- 安全保障論・国際関係論におけるサイバー空間の研究は、国家の戦略・能力・責任にフォーカス
  - 冷戦、核兵器の不拡散、生物化学兵器の制限のアナロジー
  - 『国際的なパワーの源泉は武力であり、政府が武力行使の唯一のエージェント』(Lewis 2018)
- 民間企業の力が死角になっている
  - データの量
    - アメリカの3社(グーグル、フェースブック、マイクロソフト)と中国の1社(テンセント)が10億人以上のユーザを獲得(シュワブ 2019)
    - 米国家安全保障局(NSA)のユタデータセンター(約12エクサバイトを保存)、グーグル社のデータセンター(約15エクサバイトを保存) (シュナイアー 2016)
  - 物理、地理的制約からの独立
    - アカマイ社は世界の通信の30%をコントロール(小川 2014)

6. 先行研究の課題と本研究の意義

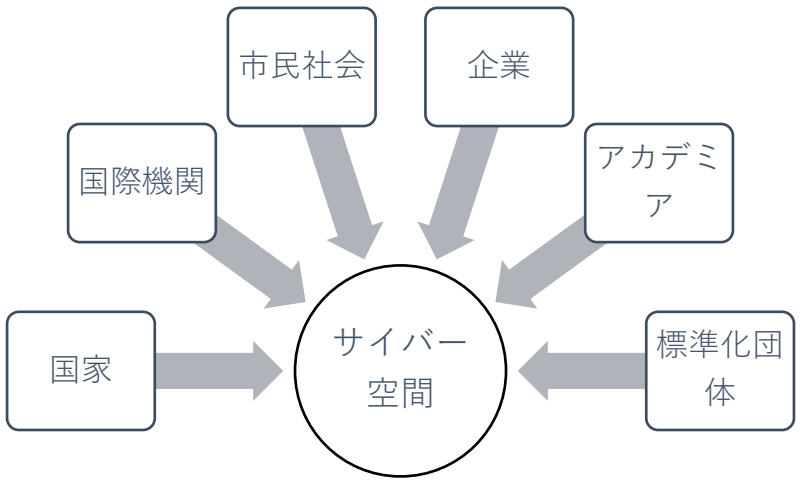


図2: インターネットガバナンス論におけるサイバー空間のイメージ

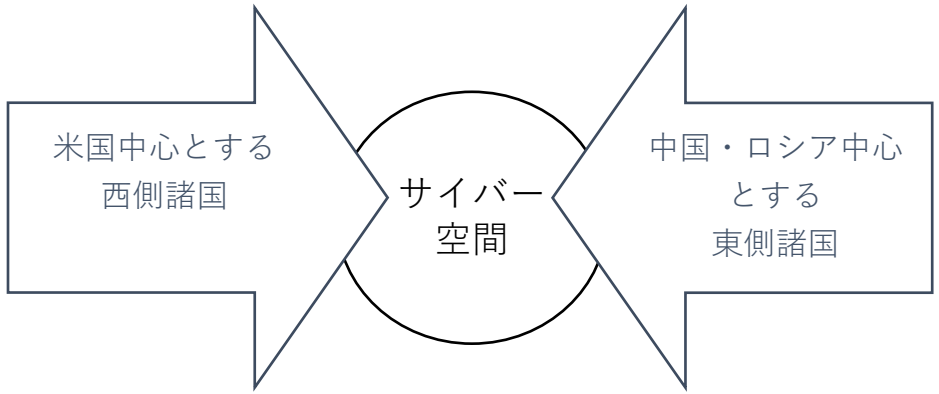


図3: 国際関係論におけるサイバー空間のイメージ

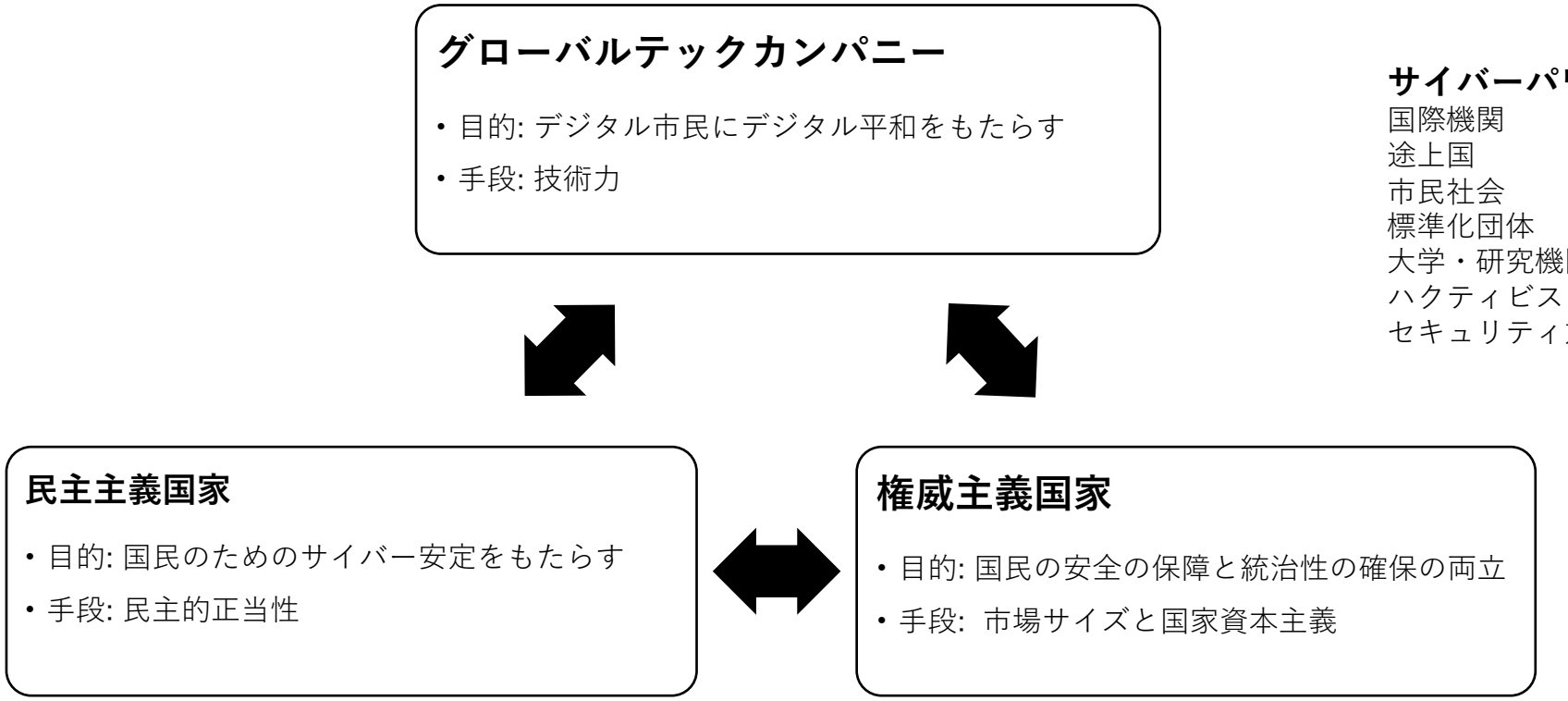
先行研究の課題

- インターネットのガバナンスの仕組みをサイバーセキュリティ・ガバナンスに敷衍することは難しい (図2)
- いわゆる冷戦の構図をサイバー空間にあてはめると、民間企業のサイバーパワーが考慮されない(図3)

本研究の意義

- 独自のモデルを用いて、サイバーセキュリティのグローバル・ガバナンスを論じる
- 「多様なアクター」「パワーの分散」というサイバーセキュリティに顕著な現象への過剰なフォーカスを捨て、3つのアクターによってサイバー空間が支配されることを主張
- 見過ごされていたプライベートテックカンパニーのサイバーパワーへの着目
- 社会人としての経験を活用した「理論と現実の対話」(後述)

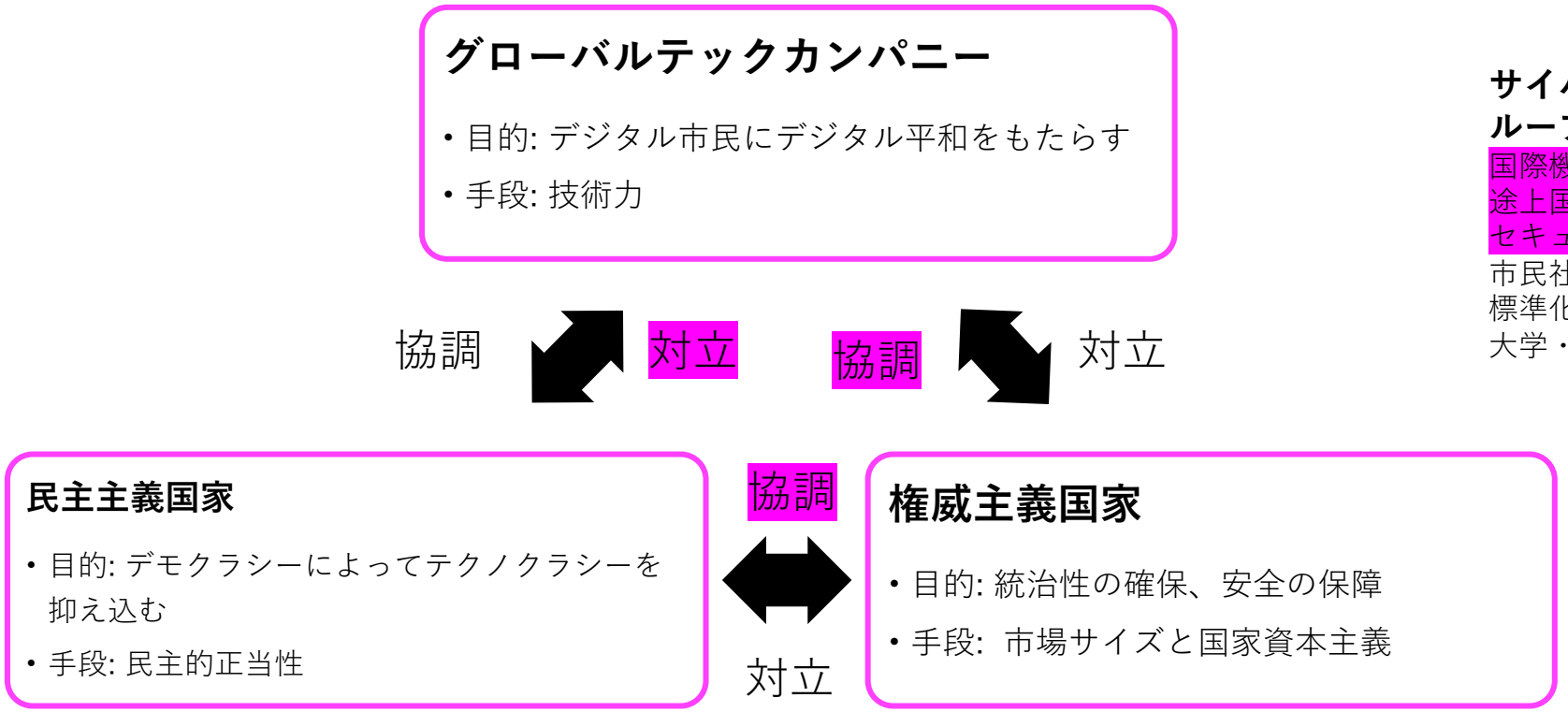
7. 分析の枠組み



サイバーパワーを失っていくグループ
国際機関
途上国
市民社会
標準化団体
大学・研究機関
ハクティビスト
セキュリティ対策組織(CSIRT)

- 3アクターの協調と対立の均衡が「サイバー空間の安定」である

8. 博論における重点と研究手法



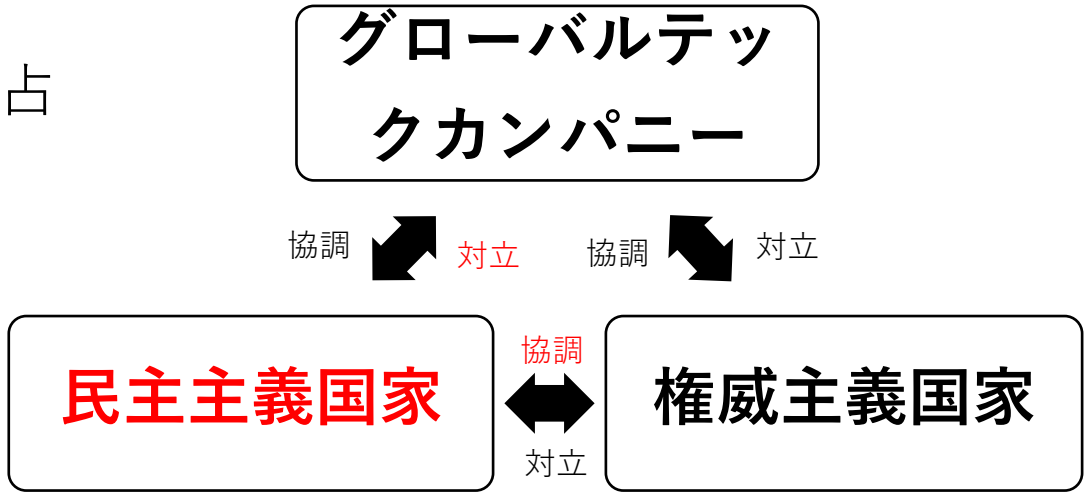
サイバーパワーを失っていくグループ
国際機関
途上国
セキュリティ対策組織(CSIRT)
市民社会
標準化団体
大学・研究機関

1. 3アクターの構成、構造、細かな違いを克服する共通の利害を明らかにする
2. 民主国家とテックカンパニー間の対立、民主国家と権威国家間の協調、テックカンパニーと権威国家間の協調という、これまで検討されてこなかった関係を描く
3. パワーを失いつつあるアクターの考察を通して、主3アクターを浮き彫りにする

用いる手法: 文献調査(サイバーセキュリティ戦略や関連研究)、参与観察(国際CSIRTコミュニティ、各種会議)、インタビュー

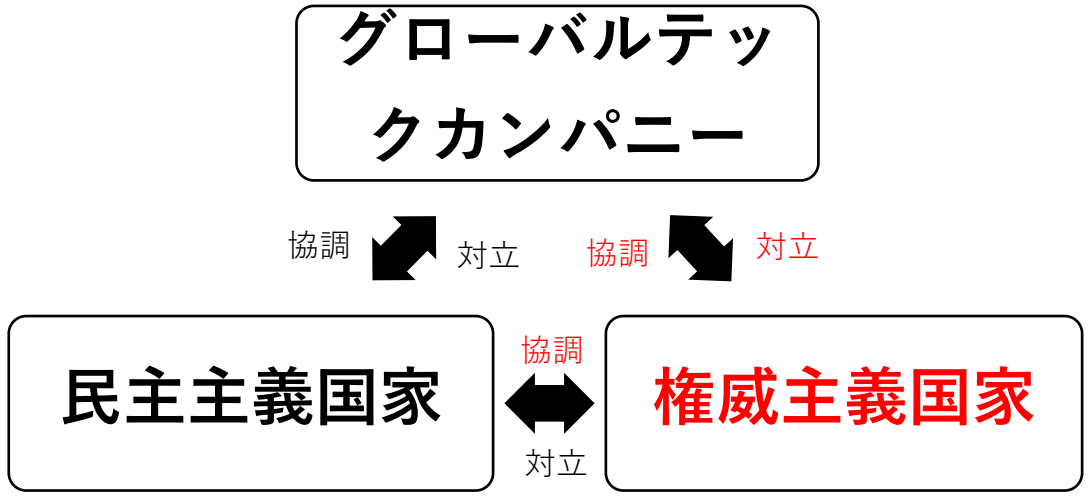
9-1. 民主主義国家

- 例: G7加盟国+α
- かつてのサイバー空間の覇者は力を失いつつあり、民主主義の正当性への不信に苦しむ
- テックカンパニーとの間の対立
  - 技術への規制
  - 税制の不均衡
- 権威主義国家との間の協調
  - サイバー攻撃能力保有の相互承認および独占
    - 民間企業によるサイバー攻撃を禁じる規範
  - 立場の維持
    - サイバー空間への国際法の適用の合意



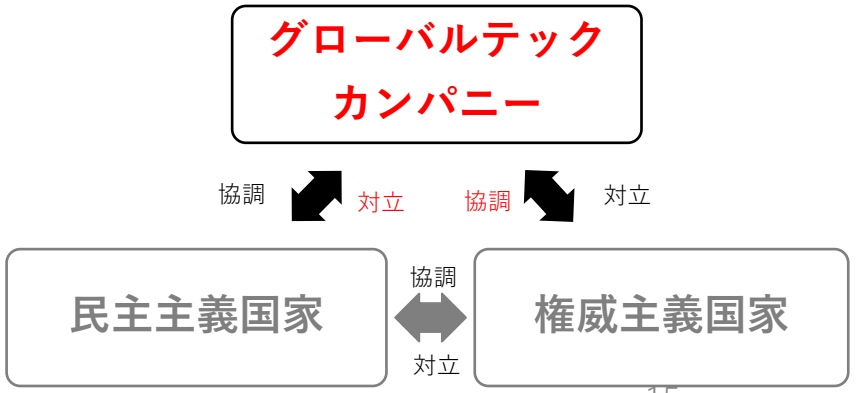
9-2. 権威主義国家

- 例: 中国、ロシア、中東イスラム諸国
- 権威主義体制を維持したまま、資本主義市場で成功 (Bremmer 2010)
- テックカンパニーとの協調
  - サーベイランス活動の土台
  - 市場の誘惑
- テックカンパニーとの対立
  - ファーウェイと中国政府の緊張
- 民主主義国家との協調
  - サイバー攻撃能力保有の相互承認および独占(再掲)



9-3. グローバルテックカンパニー

- 具体例: グーグル、アマゾン、マイクロソフト、アリババなど
- ツイッターは外交の、フェースブックは選挙活動のプラットフォーム。既にサイバー空間において准政府機能を担う(Eichensehr 2017, Kilovaty 2019)。インフラの提供をはじめる
- 雇用を生まないが、生活に欠かせない
- 権威主義国家との間の協調
  - 構造の類似性: テックカンパニーと利用者の関係は封建制
  - 市場の誘惑。Google社の中国版検索エンジン
- 民主主義国家との対立
  - 技術への規制(再掲)
  - 税制の不均衡(再掲)



9-4. その他の変容を迫られるアクター

- CSIRT
  - サイバーセキュリティガバナンスにおけるレジームのうち、目的に「被害者救済と復旧」を掲げ、機能として「インシデント対応能力」を備え、かつ文化として「互恵主義」を信条とする組織群のこと
  - 3アクターの協働で成立した数少ないコードとプラクティスの1つ
  - トランスナショナルな意思決定を助ける知識共同体の性質が強かった。しかし近年急速に国家の枠組みに組み込まれつつある
- 実験
  - CSIRTが一堂に会する場で、脱国家化の提案を行う。そこからの成果、もしくは失敗の教訓は現時点で明らかではないが、直接的な働きかけを通して「理論と現実の対話」を行う(期間: 2019/6-11)

10. まとめ

- サイバー空間を支配するのは誰なのか?
  - 有権者が存在しないサイバー空間に直接のガバナンスは発生し得ない。支配するものという時に連想される単一のアクターによる管理は理論的にありえない
- 力の分散が起きるサイバー空間において相対的優位なのは誰か?
  - 「グローバルテックカンパニー」「民主主義国家」「権威主義国家」
  - およびその中間に位置するレジーム
- 議論に法則を見いだせるか?
  - 各アクターの内側での行動の違いがある (GDPR, 中露のプライベートセクターへの接し方)
  - それらは「各アクターの目的」の裏に言語化されていない別の目的があると仮定すれば説明可能である
    - 民主主義国家は現状維持、権威主義国家は体制の安全、テックカンパニーは利益最大化

11. 博論の章立て案と予定

1 はじめに

2 分析の枠組み サイバーセキュリティ・ガバナンスのトリレンマ理論
- 「先進国家」と「権威主義国家と途上国家」と「プライベートセクター」

3 トリレンマの実態
3.1 先進国家
- サイバーセキュリティ戦略にみる各国の思惑 (※1を再構成)

3.2 権威主義国家
- 主権の確保と統治性を優先するドクトリン
- 北朝鮮のサイバー政策 (※2を再構成)
- 権威主義国家のプライベートセクター

3.3 プライベートセクター
- 市場に導かれたサイバー空間の強制力
- 経済と安全保障

3.4 協調と対立と離間のケーススタディ
- 先進国家 vs プライベートセクター
- 先進国家 vs 権威主義国家と途上国家
- 権威主義国家と途上国家 vs プライベートセクター

4 CSIRT
- レジーム複合体の中のCSIRT (※3を再構成)
- 共同体の信条を再定義する実証実験

5 考察

6 おわりに

- 謝辞、参考文献

今後の予定

2019/5-6 文献調査

2019/6-9 CSIRTに関するフィールドリサーチ

2019/9 執筆

博士候補要件の充足状況

- 外国語: TOEFL iBT 94
- 新規授業計画企画書、技法科目、教育体験: 免除

- 査読付き原著論文

  ※1 小宮山功一朗, 土屋大洋. 2018. “サイバーセキュリティ戦略の国際比較 : 目的と対象範囲に基づく四類型.” グローバル・ガバナンス 3(4).

  ※2 小宮山功一朗. 2019. “北朝鮮の情報通信技術産業 -金正日がもたらしたいびつな成功と労働力余剰-.” InfoCom REVIEW 72: 17–29.

  ※3 (2019年3月1日に情報通信学会投稿済み、査読中) 小宮山功一朗. サイバーセキュリティにおけるインシデント対応コミュニティの発展

- 学会発表
  - 小宮山功一朗. “サイバー空間における信頼醸成措置の実現にむけて.” グローバル・ガバナンス学会第4回研究大会・同志社大学. 2014/4/18.
  - Koichiro Komiyama. 2014. “Confidence Building Measures in Cyberspace.” 2014 TPRC | 42nd Research Conference on Communication, Information and Internet Policy Poster Session. 2014/9/12
  - 小宮山功一朗. 2018. “北朝鮮のIT政策 ―半導体、ソフトウェア開発、ネットワークそして人材育成―." 2018年度秋季（第39回）情報通信学会大会アーリーバードの部. 2018/11/17.

12-1. 参考文献 (英語)

Bremmer, Ian. 2010. *The End of the Free Market: Who Wins the War Between States and Corporations?* Kindle Edi. Portfolio.

Broeders, Dennis. 2017. “Aligning the International Protection of ‘the Public Core of the Internet’ with State Sovereignty and National Security.” *Journal of Cyber Policy* 2(3): 366–76. https://doi.org/10.1080/23738871.2017.1403640.

Buchanan, Ben. 2017. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford University Press.

Carr, Madeline. 2015. “Power Plays in Global Internet Governance.” *Millennium: Journal of International Studies* 43(2): 640–59.

Choucri, Nazli, Stuart Madnick, and Jeremy Ferwerda. 2014. “Institutions for Cyber Security: International Responses and Global Imperatives.” *Information Technology for Development* 20(2): 96–121.

Cuihong, Cai. 2018. “China and Global Cyber Governance: Main Principles and Debates.” *Asian Perspective* 42(4):647–62.

Denardis, Laura . 2015. *The Global War For Internet Governance*. Yale University Press.

Deibert, Ronald J. 2019. “The Road to Digital Unfreedom: Three Painful Truths About Social Media.” *Journal of Democracy* 30(1):25–39.

Eichensehr, Kristen E. 2017. “Public-Private Cybersecurity.” *Texas Law Review* 95: 469–538.

Kagan, Robert. 2019. Brookings Policy Brief The Strongmen Strike Back. https://www.washingtonpost.com/news/opinions/wp/2019/03/14/feature/the-strongmen-strike- back/?utm_term=.79c297a85d53&wpisrc=pw_ret_kaganopinions_031519.

Kilovaty, Ido. 2020. “Privatized Cybersecurity Law.” *UC Irvine Law Review*. (注: 2020 Forthcomingとある論文をhttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=3338155から取得)

Kramer, FD, SH Starr, and LK Wentz. 2009. *Cyberpower and National Security*. Kindle Edt. Potomac Books, Inc.

Lewis, James Andrew. 2018. *State Practice and Precedent in Cybersecurity Negotiations*. Washington, DC. https://www.csis.org/analysis/state-practice-and-precedent-cybersecurity-negotiations (January 9, 2019).

Healey, Jason. 2012. *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*. Atlantic Council Issue Breif.

Maurer, Tim, and Robert Morgus. 2014. *Compilation of Existing Cybersecurity and Information Security Related Definitions*. New America.

Maurer, Tim. 2017. “Contested Governance: Internet Governance and Cybersecurity.” In *Innovations In Global Governance - Peace-Building, Human Rights, Internet Governance and Cybersecurity, and Climate Change* -, The Council on Foreign Relations, 29–32.

Morgus, Robert, Isabel Skierka, Mirko Hohmann, and Tim Maurer. 2015. National CSIRTs and Their Role in Computer Security Incident Response.

Nocetti, Julien. 2015. “Contest and Conquest: Russia and Global Internet Governance.” *International Affairs* 91(1):111–30.

Nye, Joseph S. 2010. “Cyber Power.” *Belfer Center for Science and International Affairs* (May):1–31.

Raymond, M. 2016. Managing decentralized cyber governance: the responsibility to troubleshoot. *Strategic Studies Quarterly,* 10(4), 123-149.

Skierka, Isabel, Robert Morgus, Mirko Hohmann, and Tim Maurer. 2015. CSIRT Basics for Policy-Makers -The History, Types & Culture of Computer Security Incident Response Teams-.

Stevens, Timothy, and David Betz. 2013. “Analogical Reasoning and Cyber Security.” *Security Dialogue* 44(2): 147–64.

12-2. 参考文献 (日本語)

小川晃通. 2014. *アカマイ―知られざるインターネットの巨人*. KADOKAWA.

加藤朗. 2015. “サイバー空間の安全保障戦略.” 戦略研究 15: 3–24.

神里達博. 2015. “第1章 リスク社会における安全保障と専門知.” *シリーズ日本の安全保障7 技術・環境・エネルギーの連動リスク*, 19–48.

加茂具樹. 2013. “中国共産党の挑戦 一党体制を維持するための政治構造とその動揺.” *JRIレビュー* 3(4):60–76.

河野桂子. 2015. “サイバー・セキュリティに関する国際法の考察 ータリン・マニュアルを中心にー.” *戦略研究* 15: 25–46.

神田英宣. 2018. “海底ケーブルの海洋管轄権 － サイバー空間における防御機能の追求 －.” *防衛大学校紀要(社会科学分冊)* 117.

小宮山功一朗, 土屋大洋. 2018. “サイバーセキュリティ戦略の国際比較 : 目的と対象範囲に基づく四類型.” *グローバル・ガバナンス* 3(4).

小宮山功一朗. 2019. “北朝鮮の情報通信技術産業 -金正日がもたらしたいびつな成功と労働力余剰-.” *InfoCom REVIEW* 72: 17–29.

塩原俊彦. 2015. “サイバー空間と国家主権.” *境界研究* (5): 29–56.

朱紅穎. 2018. “中国のサイバー戦略をめぐる国内政治.” 慶應義塾大学大学院修士論文(未公刊).

原田有. 2015. “グローバル・コモンズのガバナンスが抱える難題―海洋とサイバー空間を事例として―.” *防衛研究所紀要* 18(1):31–54.

藤巻裕之. 2018. “旧ソ連圏における多国間主義とサイバーセキュリティ.” *東海大学紀要政治経済学部* 50(1–14).

ブルース・シュナイアー. 2016. *超監視社会: 私たちのデータはどこまで見られているのか?* 草思社.

クラウス・シュワブ. 2019. “デジタル世界に即した統治システムを ー 社会・経済のデジタル化を恩恵とするには.” *フォーリン・アフェアーズ・レポート 3月号*: 6–14.

土屋大洋. 2007. *ネットワーク・パワー ―情報時代の国際政治*. NTT出版.

土屋大洋. 2018a. “第11章 サイバーセキュリティ.” *グローバル・ガバナンス学II.* グローバル・ガバナンス学会編. 渡邊啓貴・福田耕治・首藤もと子責任編集. 法律文化社. 203-220.

土屋大洋. 2018b. “サイバーに関する安全保障上の課題.” 首相官邸ホームページ. Retrieved April 15, 2019 (https://www.kantei.go.jp/jp/singi/anzen_bouei2/dai2/siryou3.pdf).

持永大., 村野正泰., and 土屋大洋. 2018. *サイバー空間を支配する者 -21世紀の国家、組織、個人の戦略-*. 日本経済新聞出版社.