研究プロポーザル

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

研究テーマ

サイバーセキュリティのグローバル・ガバナンス

研究背景と目的

今日のサイバー空間は、単に人々の日々のコミュニケーション手段以上の役割を果たしている。それは、例えば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、軍事活動の新領域であることに議論の余地はないだろう。

歴史を振り返れば、国際関係の変容を迫る技術は、絶え間なく生み出されてきた。火薬、飛行機、潜水艦、ミサイルと核兵器、宇宙技術は、その一例である。通信技術に限定しても、アルファベット、活版印刷、腕木通信、電信、テレビなどを挙げることができる。これらの技術革新とサイバー空間には、2 つの大きな違いが存在している。

まず、サイバー空間は、情報社会の変容を招く。Deilbert(2013)らの指摘を待つまでもなく、「僅か 30 年で世界を席巻した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」であることが、その主たる要因である。次に、サイバー空間は、民主主義国家のみを脆弱にする。かつて、多くの未来学者や情報学者が「技術はバラ色の民主主義社会を実現する」と予測したが、その期待は急速にしぼんでいる。民主主義を助けるどころか、「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)」が生まれたのである。AI やビッグデータの技術が、権威主義国家とそのリーダーにとっての効果的な統治の手段となったからだ(Kagan 2019: 13)。

この新たな分野において、統治と管理の仕組みを模索する議論は、発展の途上にある。既存の研究に繰り返し指摘されるように、サイバー空間には、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)が存在しない。サイバーセキュリティのグローバル・ガバナンスを目指す様々な議論は、「傘ではなくパッチワーク(Choucri 2014)」「レジームコンプレックス(Nye 2014)」と表現されるように、乱立し重複している。

本研究は以上の背景を踏まえて、サイバーセキュリティのグローバル・ガバナンスの有り様を論じていく。この広大なテーマの中で特に着目するのは、今後 10 年 t における議論の基本的な対立の構造を明らかにすることである。先行研究で繰り返された「多様なアクター」や「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(プライベートテックカンパニー、民主主義国家、権威主義国家)によってサイバー空間が支配されることを主張していく。とりわけ見過ごされていたプライベートテックカンパニーの力とそれをめぐる民主主義国家と権威主義国家の駆け引きを描き出す。

用語の定義

サイバー空間

「サイバー空間」に定まった定義はない(塩原 2015、Stevens and Betz 2013、 Maurer and Morgus 2014)。文脈や立場によっては、電磁スペクトラム、製品の供給路(サプライチェーン)、文明や文化もまた、サイバー空間の一部とみなされることもある。そこで、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）」と定義する。しかし、今後この定義が拡張される可能性を念頭に置く。

サイバー空間における力(パワー)

個人、企業、国家などのプレーヤーが、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が、サイバー空間における力(パワー)である。サイバー空間を構成する各プレーヤーは、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。

先行研究と分析の枠組み

先行研究の課題

サイバーセキュリティのガバナンスを論じる上で、本研究が依って立つのは、インターネット・ガバナンス論と国際関係論の 2 つの分野である。両分野における典型的な議論を解説し、その課題を補うことを目指した本研究の分析の枠組みを提案する。

インターネット・ガバナンスの研究分野では、1980 年代に利用が拡大したインターネットをどのように管理するかが論じられてきた。同分野のアジェンダは、「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)である。世界中のコンピューターが、一意の IP アドレス体系を使用するというインターネットの構造は、グローバルな実務的協調とその理論的下支えを必要とした。これまでインターネット・ガバナンス論は、議論の前提として、官・民・市民社会のイコールフッティングが確保された場における自律・分散・協調という 3 つの信条を重視しており、その重み付けは現在も失われていない。

インターネットは、サイバー空間およびサイバーセキュリティにおける重要な要素であり、インターネット・ガバナンスの知見をサイバーセキュリティ・ガバナンスに敷衍するという発想は、研究者や実務家の間で少なからず支持されている。一方で、インターネット・ガバナンス論は、今日のサイバー空間のセキュリティ問題が引き起こす、負のインパクトへの対

処に苦しんでいる。「人間は自由だけを希求するわけではない(Kagan 2019: 7)」。身体や民族や宗教の安全は、インターネットの発展や言論の自由と同等かそれ以上に重要であることを直視する必要がある。

国際関係論および安全保障論におけるサイバー空間の研究は、法の支配の確立、有効なレジームの模索、兵器不拡散の実現などのテーマを中心に、研究が積み重ねられてきた。これらの議論は、押しなべて国家の戦略・能力・責任が主たる論点であり、民間企業や市民社会を従属変数として扱うか、その役割に全く言及しない。「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)」だとすれば、デジタル冷戦、サイバー空間のバルカン化などの冷戦とのアナロジーでサイバーセキュリティ・ガバナンスに突破口が得られる可能性はある。しかしながら、現実には、テックカンパニーやテロリストなど非国家主体のもつ力は多くの国家をしのいでいる、というのが本研究の理解である。

もっとも、国際関係論を振り返れば、民間企業や市民社会の役割の拡大を指摘すること自体に新規性はない(Cross 2013、 ストレンジ 1994)。それらの理論をサイバーセキュリティ・ガバナンスに応用できるかの検討が待たれている。

分析の枠組み

先行研究に見られる死角を補うため、本研究では「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」の三つ巴の争いという叙述の枠組みを用いて、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。

1つ目のアクターは、民主主義国家である。アメリカを筆頭として、G7 各国や一部の国は、サイバー空間の安定という戦略目標を実現しようとしている。民主的正当性を行使し、既存の国際関係のパワーバランスを維持しようとしている。一方で、インフラだけを見れば、アメリカの覇権は縮小傾向(Winseck 2017)であり、サイバー空間における情報操作に最も脆弱である。

2 つ目のアクターは、権威主義国家である。中国やロシアは、国家資本主義(Bremmer 2010)と市場のサイズという手段を用いて、国際安全保障だけでなく、統治性の確保をサイバー空間における戦略目標に掲げる。

3つ目のアクターは、グローバル・テックカンパニーである。GAFA(グーグル、アマゾン、フェイスブック、アップル)や BAT(バイドゥ、アリババ、テンセント)に代表されるテックカンパニーは、自らの利益拡大のために、サイバー空間の平和を求める。既存の空間におけるプライベートセクターの役割(軍産複合体など)とサイバー空間におけるそれは違う。サイバー空間においては、プライベートセクターは、国家を超える技術力とデータにアクセスする力に裏打ちされた、強い強制力を行使できる存在である。

つまるところ本研究は、先行研究に見られるサイバー空間のイメージ(図 1 および図 2)を土台にして、新たなサイバー空間のイメージ（図 3 ）を構築するものである。

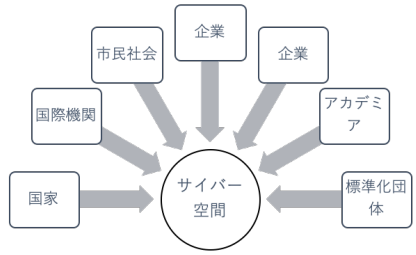

図1: インターネットガバナンス論におけるサイバー空間のイメージ

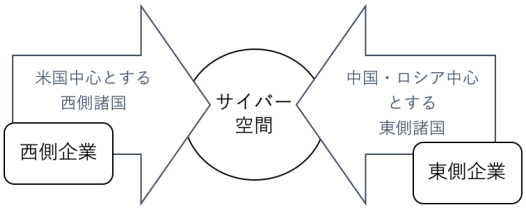

図2: 国際関係論におけるサイバー空間のイメージ

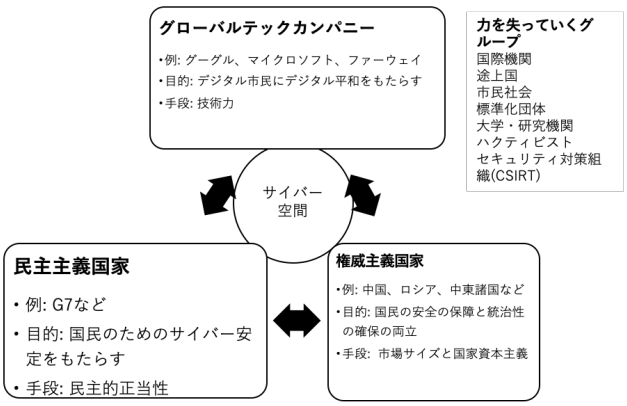

図3: 本研究におけるサイバー空間のイメージ

研究手法

本研究は、文献調査が主となる。既存の学術研究論文だけでなく、サイバーセキュリティ戦略などの公式文書を合わせて検討する。加えて、CSIRT(インシデント対応組織)で勤務する社会人としての経験を活用し、参与観察を行い、研究に厚みを加えていく。

CSIRT は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である。CSIRT の共同体はこれまで 3 つのアクターの中間地点に位置し、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。本研究では、CSIRT が一同に会す機会に、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、参与観察を通して「理論と現実の対話」を行う。

期待される成果

「多様なアクター」や「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 つのアクターのバランスという新たな枠組みを提供するのが、本研究の主たる学術的貢献である。本研究によって得られるサイバーセキュリティ・ガバナンスの理論は、学位取得後に、サイバーセキュリティ・ガバナンスの第一線での業務に関わっていく際の土台として仲間とともに活用したい。

現時点での考察

本研究は未だ途上であるが、分析の枠組みを用いて見えてきたことを、いくつか指摘したい。

冷戦終結後の民主主義国家は、国際関係の秩序構築において、優位な立場を維持してきた。

民主主義国家の比較優位の時代とインターネットが誕生し普及した時代は、符合する。両者は、お互いを補完し合う関係だった。クラウドコンピューティングの普及、ビッグデータ・AI の隆盛は、「分散」時代の終焉を告げ、集約の時代に移り変わっている。サイバー空間における力を決定づけるデータは、もはや分散しておらず、いくつかのプライベートテックカンパニーによる寡占が進んでいる。加えて、2015 年の米大統領選挙、2017 年のフランス大統領選挙、2017 年のウクライナの国民投票を経て、選挙への情報操作の疑いは色濃くなっている。結果、民主主義国家とテックカンパニーの間には、これまで見られなかった緊張が高まっている。

サイバー空間を語る上で、それを支えるインフラが、概ねテックカンパニーの所有・管理するものであることに自覚的である必要がある。海底ケーブルやデータセンターなどがあって、初めて「インターネットを使う」ことができる。サイバー空間の安全保障において、このテックカンパニーの思考回路に着目するものは少ない。多くの研究は、テックカンパニーがインフラを所有・管理する事実を言及するものの、それらの企業が不特定多数の利益のために右から左にデータを受け渡す、対価に応じて平等にサービスを提供する存在としてとらえている。本研究は、サイバー空間をグローバルコモンズと捉えることはできないという立場をとるが、サイバー空間=グローバルコモンズ論を支えるのは、テックカンパニーが中立を保つという幻想である。実際のところ、サイバー空間におけるテックカンパニーの役割は、決定的である。テックカンパニーは、政党のソーシャルメディア上での選挙運動や国家元首のツイッターを使った外交の生殺与奪権を握っている。テックカンパニーが望めば、情報をより多くの人に届けることも、その逆も容易い。

テックカンパニーは、自らのビジネスを保護するために、透明性確保の努力を行っている。しかし、その事自体が立場の不明瞭さを示す一つの証左でもある。例えば、民主主義国家における中国に関する言説は、中国企業のアリババやテンセントを、国家のエージェントとみなしている。一方で、中国政府は「アリババは株式会社であり、最大株主は日本の実業家」であると考え、中国市民は「ファーウェイの創業者は共産党に飼いならされない反逆者」というイメージを持つ。民主主義国家と権威主義国家双方が、プライベートテックカンパニーを対立陣営の一部とみなす、という矛盾した構図である。

そこから導き出されるのは、米政府の 5G 規格を巡る中国ファーウェイ社への圧力は悪手という見方である。三つ巴の争いにおいては、対立グループ内の離間を促し、協力を引き出す必要がある。中国国内において共産党に保護され続けてきた ZTE 社と、ベンチャー企業のファーウェイ社の両者に対して、民主主義国家グループが圧力をかければ、テックカンパニーが共産党との距離を置くことへのインセンティブが消失する。

この点についてロシアは戦略的な動きを見せている。プーチン大統領は「インターネットは米 CIA のプロジェクト」であると公言し、米国政府のインターネット支配を一貫して批判し続けてきた。その一方で、公にマーケットオリエントなインターネット・ガバナンスを批判したことはない(Nocetti 2015)。それは米国政府と米国のテックカンパニーとの離間を

すすめるためのパフォーマンスと捉えることも可能である。

サイバー安全保障のジレンマ理論(Bchanan 2017)は、「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」の 3 つのアクター間に強く当てはまる。どのアクターも、サイバーセキュリティの危機を感じている。ジレンマの解消のためには、攻撃側が防御側に対して圧倒的に有利というサイバー空間の特性、もしくはある行動が攻撃のためのものか防御のためのものかの明確化を含む信頼醸成が必要である。前者に解決の糸口はなく、後者を検討することが、サイバーセキュリティ・ガバナンスの政策的・技術的最大の課題である。

進捗状況

博士論文の目次は、現在のところ、下記を想定している。

1 はじめに

2 分析の枠組み

2.1 サイバーセキュリティ・ガバナンスのトリレンマ理論

2.2「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

- サイバー空間と民主主義
- サイバーセキュリティ戦略にみる各国の思惑（共著論文を再構成）

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（査読付き原著論文を再構成）
- 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（原著論文(査読中)を再構成）
- 共同体の信条を再定義する実証実験(※)

5 考察とまとめ

※ NatCSIRT 2019 での講演などを通じて、R2T(Responsibility to Troubleshoot)を中心としたナショナル CSIRT の規範を実際のナショナル CSIRT コミュニティに提案する

学位要件

学会発表

- 小宮山功一朗. 2014/4/18. “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.
- Koichiro Komiyama. 2014/9/12. “Confidence Building Measures in Cyberspace.” 2014 TPRC | 42nd Research Conference on Communication, Information and Internet Policy.
- 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.

査読論文

※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. 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." (2019 年 3 月 1 日に情報通信学会投稿済み、査読中)

学位要件

- 外国語: TOEFL iBT 94 (2013/9)
- 新規授業計画企画書、技法科目、教育体験: 免除

参考文献(関連文献も含む)

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.

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

Carr, Madeline. 2015. “Power Plays in Global Internet Governance.” *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.*

Davis Cross, Mai'a. 2013. "Re-Thinking Epistemic Communities Twenty Years Later." *Review of International Studies* 39(01):137–60.

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. "The Strongmen Strike Back." *Brookings Policy Brief* 1–19. Retrieved May 5, 2019 (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 SSRN から取得）

Kramer, Franklin, Stuart H. Starr, and Larry Wentz, eds. 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.*

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." *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.

Nye, Joseph S. 2014. "The Regime Complex for Managing Global Cyber Activities." *Center for International Governance and Innovation (CIGI) Publications* (1):1–15.

Raymond, Mark. 2016. "Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot." *Strategic Studies Quarterly* 10(4):123–49.

Segal, Adam. 2018. “When China Rules the Web: Technology in Service of the State.” *Foreign Affairs* (Sept.-Oct. 2018).

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.

Winseck, Dwayne. 2017. “The Geopolitical Economy of the Global Internet Infrastructure.” *Journal of Information Policy* 7(2017):228–67.

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.

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.

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).

スーザン・ストレンジ. 1994. *国際政治経済学入門―国家と市場*. 訳=西川潤、佐藤元彦. 東洋経済新報社.

スーザン・ストレンジ. 2011. *国家の退場 グローバル経済の新しい主役たち (岩波人文書セレクション)*. 訳=櫻井公人. 岩波書店.

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? 訳= 池村千秋. 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. 2018. “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-*. 東京: 日本経済新聞出版社.
山田敦. 2015. “序論 科学技術と現代国際関係.” *国際政治* 179:1–15.
山本達也. 2005. “政府によるインターネット・コントロールとイスラーム.” *KEIO SFC JOURNAL* 4:54–74.