

〈2〉サイバーバイオセキュリティ： 生命と情報を越境する知に向けて

大阪大学大学院 医学系研究科 医の倫理と公共政策学教室 准教授 吉澤 剛

1 はじめに

生命科学は生命現象を探究し、生物学や化学、物理学などの基礎的知識を統合した学問である。いや、「あった」と言うべきか。生命の設計図と言われるDNA（デオキシリボ核酸）は遺伝情報を記録する物質であり、4種類の塩基が二重螺旋の形状に配列されている。生物が正常な生命活動を保持するのに必要な1セットの遺伝情報をゲノムと呼ぶ。ゲノム情報はゲノムの配列データの中で意味を有するものであり、そのなかでも遺伝情報は子孫へ受け継がれるものを指す。次世代シーケンサー（NGS）などゲノム解析技術の目覚ましい進歩によって、最近では生物からこうした情報を取り出すことが非常に安価で容易になり、その情報を意味づけるために生命科学と情報科学との融合が急速に進展しつつある。したがって生物に関する問題は、今日では、もはや情報に関する問題だと言ってよい¹。遺伝情報を解析するゲノム研究の推進においては、研究者間による解析データの公開や共有が重要とされ、データの二次利用によって研究をより迅速に進めることが期待されている。とりわけヒトゲノム研究においては、医療や創薬への応用が強く期待され、個人のゲノム情報を国際的かつ大規模に公開・共有する体制が整えられてきた。その一方で、データ公開・共有がもたらす社会の影響度は増し、プライバシーや

機密性といったセキュリティ対策が求められるようになってきている²。ゲノムデータは改正個人情報保護法における「個人識別符号」であり、ゲノム情報についても、要配慮個人情報に相当すると位置づけられている³。

医療や創薬に期待されるのはゲノム情報ばかりではない。わが国では、国民の医療健康情報の電子化とその管理・活用を通じて、個人の体質や特性に合った診断・治療や医薬品開発、保健指導のあり方が検討されている。こうしたサービスの個人化は健康推進や予防医療につながり、国民の健康寿命を延伸するとともに、国家的な課題である国民健康保険医療費を削減する狙いもある。政府の健康・医療戦略推進本部では、2015年に次世代医療ICT基盤協議会を設置し、マイナンバー制度施行にともない、医療・介護・健康分野のデータの収集と利活用を円滑に行う基盤の構築を推進してきた。

ゲノム情報や医療情報の共有や利用は、住民票や戸籍、社会保障、クレジットカード利用の情報といった取り扱いに機微を要する他の要配慮個人情報と比べて、一般市民にとって心理的抵抗が相対的に高いものの⁴、セキュリティ対策としては、程度の違いであって質の違いが要求されるようには映らない。しかし、こうした理解は正しいのだろうか。要配慮個人情報の一つとしてゲノム情報や医療情報をとらえるだけでは、生命科学の営みの多面性、そし

¹ Carlo Caduff, "The Semiotics of Security: Infectious Disease Research and the Biopolitics of Informational Bodies in the United States," *Cultural Anthropology*, Vol. 27 Issue 2, May 2012, pp.333-357.

² 三成寿作「パーソナルゲノム時代の解析データの共有—データ公開・共有方針と倫理的対応—」『医療・生命と倫理・社会』12, 2015.3.30, pp.105-114.

³ ゲノム情報を用いた医療等の実用化推進タスクフォース「改正個人情報保護法におけるゲノムデータ等の取扱いについて（意見とりまとめ）」2016.1.22. <http://www.mhlw.go.jp/file/05-Shingikai-10601000-Daijinkanboukouseikagakuka-Kouseikagakuka/160122_torimatome.pdf>

⁴ 橋本泰成「医療情報の共有・利用における現状と課題—医療情報共有における一般市民の意識調査—」『医療・生命と倫理・社会』12, 2015.3.30, pp.67-87.

てそれが情報技術との様々な交錯において立ち現れるセキュリティ面での特異性が捨象されてしまう。本稿ではそれを三つの視点から論じてみたい。

2 生命から情報を抽出する

ヒトの生命に関わる情報には大きく分けて医療情報、健康情報、ゲノム情報、生体情報があり（表1）、基礎研究から臨床応用、公衆衛生、社会福祉から民間ビジネスにいたるまで多方面への利活用が考えられる。いったい、こうした情報は誰のものか。情報の保有者である個人か、研究者か、医療従事者か、政策立案者か、民間企業か、国家か、あるいは国際機関か。もちろん情報は単一の主体だけに帰属することは少なく、また、情報の取得手段や内容の専門性によって変わりうる。したがってセキュリティのあり方は、誰が情報に責任を負い、誰とどのように共有するのかといった課題とともに考えなければならない。

表1. 人の生命に関わる情報

- 医療情報
 - 診療明細書（レセプト）及び調剤情報
 - 診療録情報（検査データ、読影レポート、本人提供用退院サマリ等）
 - 健診情報
- 健康情報
 - バイタル（脈拍、心拍、血圧、血流等）
 - 生活情報（運動、食事等）
- ゲノム情報：ゲノムの配列データの中で意味を有するもの
 - 遺伝情報：子孫へ受け継がれるもの
- 生体情報
 - 身体的特徴（指紋、掌形、網膜、虹彩等）
 - 行動的特徴（筆跡、まばたき等）

2-1 責任あるデータの共有主体

ゲノム解析は大学や公的研究機関のみならず、民間企業が熱心に参入を図っている領域でもある。個々の患者の体質や病気の特徴に合った医療を進める個別化医療のためには、大量のゲノムデータを蓄積し、個人の遺伝子特性および治療や薬剤に対する効果などを明らかにする必要がある。このデータの蓄積は安全性やコスト、データの共有しやすさの点から、それぞれの組織が行うよりも、クラウドを利用する方がよいと考えられている。クラウドとは、自分のコンピューターとは物理的に別の場所にあるサーバーにデータやソフトウェアを置き、必要に応じてそれらに自由にアクセスできるサービスを指す。利用者はネットワーク経由でアクセスするため、データやソフトウェアの所在を意識しない。雲のようにつかみどころがないため、「クラウド」という名がついたとされる。米国国立がん研究所（NCI）では、情報基盤コストの削減やデータ解析の品質向上と均一化を目指して、Cancer Genomics Cloud（CGC）という3つのパイロットプロジェクトを実施した。プロジェクトのうち2つはグーグル、1つはアマゾンのクラウド基盤を活用し、がん研究コミュニティに対してクラウド環境を試験的に提供、ゲノムデータや臨床データを管理しながら運用上の課題を洗い出した。これを踏まえ、2016年6月にGenomic Data Commons（GDC）と呼ばれるデータ共有基盤と解析環境を提供するクラウドを正式に立ち上げてサービスを開始した⁵。情報産業の最大手であるグーグルとアマゾンのどちらもクラウドサービスを介して遺伝子ビジネスに参入していることから、彼らの将来市場に寄せる期待と次世代産業の覇権を争う意気込みが強く感じられる⁶。

クラウドでは、データとサーバーのバックアップは容易に設定できる。また、システム管理とデータやソフトウェアの管理を完全に分けるので、セキュリティ対策としては望ましい。どこに置かれようとも、インターネットに接続した機械は数多くの攻撃に対して脆弱であり、データ流出の危険性は変わら

⁵ 三菱総合研究所『平成27年度国内外における遺伝子診療の実態調査報告書：海外訪問調査』2016.3.31 <http://www.amed.go.jp/content/files/jp/program/0401_h27report-09.pdf>

⁶ 「グーグルとアマゾン、『DNA解析』を巡って熱戦—クラウドの最先端で起きていること」『東洋経済ONLINE』2015.6.7. <<http://toyokeizai.net/articles/-/72391>>

ない。したがって、クラウドにより生じる新たなリスクは、そのコストや利便性よりも重要でないと見る向きもある⁷。だが、クラウドはデータの移動を自由にする一方で、データ保管場所の管理や監視を難しくする。さらに、大企業による限定的な賠償責任の保険契約ゆえに、データ損失・盗難・破壊の場合に責任の所在が不明確になりやすい⁸。このため、大規模な個人情報を用いた医学系研究は政府の支援によるクラウドを用いて進めるべきだという提言もなされている⁹。医療データとの統合も勘案すれば、なおさらだろう。

いずれにせよ、一つの研究室や研究機関でデータを管理するよりクラウドに移した方がセキュリティは高まることは間違いない。逆に言えば、大学や研究機関のセキュリティは穴だらけという現状が問題として浮かび上がってくる。ここでクラウド環境を整備し、個別の大学や研究機関の有するゲノムデータや臨床データを統合・活用しようとする動きが立ち現れてきた。それは「ゲノミクスと健康のためのグローバル・アライアンス」(GA4GH: Global Alliance for Genomics and Health) と呼ばれるネットワーク団体で、2012年に設立されて以来、現在では41ヶ国の400を超える組織が参加している。そこでは、あらゆるデータを最初から全て共有することが前提ではなく、共有できるデータや相手をそれぞれの参加機関が決定できるよう自主性が尊重される¹⁰。データ共有にかかる基本理念¹¹の作成はその一環であり、グローバル・アライアンスそのものが参加組織に対するクラウド的存在として、共有可能な情報の範囲を最大にしながらデータアクセスを確保すべ

く、新たなセキュリティ概念と制度の構築に取り組んでいる。

2-2 アクセスコントロール

ゲノム情報は、たとえ匿名化されたとしても、その情報自体に個人識別可能性を有していることがある。したがって、公開されたゲノムデータベースにある匿名化データを用いて、他の情報と突き合わせることで、個人を識別できてしまうおそれがある。実際に匿名化データから個人を再識別した実証研究も報告されており、多様な主体による各種の個人情報の取得とビッグデータの利活用の進展にともない、今後こうした再識別可能性はますます高まると考えられる。同じ属性を持つと考えられる人がk人未満に絞り込めないようにした匿名加工情報(k-匿名性)によって再識別可能性を低め、プライバシー保護を確保するという考え方もある¹²。しかし、現実の運用方針は多様である。米国ではデータへの一般公開ではなく、アクセス制限を課して、データの利用者を限定する方針が主流である。他方、解析データの一般公開や、解析データの匿名化を推奨しないプロジェクトも登場しており、プライバシー上のリスクとデータ利活用にかかる資源節約とのトレードオフという構図を呈している¹³。同様に、データではなく生体試料を物理的に保管するバイオバンクにおいても、アクセスコントロールの維持や試料・データの識別可能性、ユーザー認証などセキュリティ面での考慮すべき点は共通して見られる¹⁴。

バイオセキュリティの教訓では、ならずもののア

⁷ Arnon Rosenthal, Peter Mork, Maya Hao Li, Jean Stanford, David Koester and Patti Reynolds, "Cloud Computing: A New Business Paradigm for Biomedical Information Sharing," *Journal of Biomedical Informatics*, Vol. 43 No. 2, April 2010, pp.342-353.

⁸ Gratien Dalpé and Yann Joly, "Opportunities and Challenges Provided by Cloud Repositories for Bioinformatics-Enabled Drug Discovery," *Drug Development Research*, Vol. 75 No. 6, September 2014, pp.393-401.

⁹ Dov Greenbaum, Andrea Sboner, Xinmeng Jasmine Mu and Mark Gerstein, "Genomics and Privacy: Implications of the New Reality of Closed Data for the Field," *PLoS Computational Biology*, Vol. 7 Issue 12, e1002278, December 2011.

¹⁰ Global Alliance for Genomics & Health Website <<http://genomicsandhealth.org/>>

¹¹ 「ゲノム及び健康関連データの責任ある共有に関する枠組み」2014.9.10. <https://genomicsandhealth.org/files/public/Framework_Japanese_20141008_interlinear.pdf>

¹² Latanya Sweeney, "k-Anonymity: A Model for Protecting Privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 10 Issue 5, October 2002, pp.557-570.

¹³ 三成, 前掲論文.

¹⁴ Elaine M. Sedenberg and Deirdre K. Mulligan, "Public Health as a Model for Cybersecurity Information Sharing," *Berkeley Technology Law Journal*, Vol. 30 Issue 3, May 2016, pp.1687-1739; Raymond Heatherly, "Privacy and Security Within Biobanking: the Role of Information Technology," *Journal of Law, Medicine & Ethics*, Vol. 44 No. 1, March 2016, pp.156-160.

ウトサイダーによる非国家主体の活動よりも、医者と科学者などインサイダーによる犯行が大きなリスク要因となりうる¹⁵。ゲノムデータや診療データを保管するデータベースにおいても、データの解釈に要する専門性の高さゆえに、アクセス権を与えられた利用者のアクセス監視と定期的なスクリーニングが必要と考えられる。

2-3 電子的同意

今やPCやスマートフォンを使って利用者が自身のバイタルを計測したり生活情報を入力することは珍しくない。事業者がそれをビッグデータとして管理し、利用者にフィードバックを行うアプリケーションも多く存在している。ところが、こうした事業と異なり、人を対象とする医学系研究の場合、必ずしも参加者に対して直接的に有益な成果が還元されるわけではなく、それを理解した上での自発的な意思に基づく参加が求められる。参加者に対しては十分なインフォームド・コンセント（説明同意）が必要とされ、文書や口頭による実施が一般的に普及している。ここでも、研究者と研究参加者の双方にとっての利便性を高めるため、オンラインでのインフォームド・コンセントが広まりつつある。これは文書による従来型の手法と実質的に差異はないと見られ¹⁶、参加者である市民にとっても受け入れられやすいとされる¹⁷。政府のゲノム医療実現推進協議会においても、諸外国での先行例をもとに検討が進められている¹⁸。

そのなかでも、研究参加者が自身の提供する情報の利用者や利用方法をいつでも自由に決定でき、ウェブサイト等を通じて同意内容を柔軟に変更できる同意手法のことを「ダイナミック・コンセント」

と呼ぶ¹⁹。ダイナミック・コンセントでは、医療健康情報や生体試料を収集する際に同意を取得し、さらにその情報や試料を利用する際に再同意を取得する。はじめに一度しか同意を取得しない「静的な」包括同意や広範同意などに対して、ダイナミック・コンセントは、同意内容の変更や撤回がしやすいように研究参加者と継続的に接点を持つようになっており、この意味で動的（ダイナミック）な同意である。情報通信技術の活用によって、研究者と研究参加者とのやり取りの手間を軽減することができる。加えて、研究に関する通知を頻繁に受けとることで、患者や一般市民が研究に触れる機会が増え、研究への関心や理解を深めることにつながりうる²⁰。一方で、倫理審査委員会による研究計画の承認のあり方に見直しを迫るとともに、研究参加者に対して倫理的責任を押しつける反面、研究者の倫理的な自律を妨げるおそれがある。また、研究結果の返却についての要求が高まることで研究の遂行が妨げられる、といった批判も見られる²¹。特に遺伝情報を扱う研究では、参加者本人ばかりでなく、家族やコミュニティによる同意や意思表示も実務上必要になることがある。この場合、オンラインでの取り組みだけでは限界があるかもしれない。オンラインとオフラインでの対話を上手に使いわけながら、研究者と研究参加者、家族やコミュニティがそれぞれ適切な役割と責任を分担する仕組みが必要である。

ダイナミック・コンセントについて、セキュリティの観点から見ると情報の不可逆性が課題であり、いったん同意内容を緩やかにした後に同意内容を限定するよう変更しても、すでに各主体に情報が利用・拡散されていて、同意事項を遵守できないおそれがある。また、研究参加者が自ら提供した情報は同一サーバー内に保管されるため、情報破棄にか

¹⁵ 古川勝久「安全保障政策とバイオセキュリティ—安全保障の観点から見た科学者の社会的責任について—」四ノ宮成祥・河原直人編著『生命科学とバイオセキュリティ—デュアルユース・ジレンマとその対応—』東信堂, 2013, pp.123-180.

¹⁶ Connie K. Varnhagen et al., "How Informed is Online Informed Consent?" *Ethics & Behavior*, Vol. 15 Issue 1, 2005, pp.37-48.

¹⁷ Fiona Wood, Jenny Kowalczyk, Glyn Elwyn, Clive Mitchell and John Gallacher, "Achieving Online Consent to Participation in Large-Scale Gene-Environment Studies: A Tangible Destination," *Journal of Medical Ethics*, Vol. 37 No. 8, August 2011, pp.487-492.

¹⁸ 「ゲノム医療実現推進協議会中間とりまとめ」2015.7. <http://www.kantei.go.jp/jp/singi/kenkouiryoku/genome/pdf/h2707_torimatome.pdf>

¹⁹ Jane Kaye et al., "From Patients to Partners: Participant-Centric Initiatives in Biomedical Research," *Nature Review Genetics*, Vol. 13 No. 5, May 2012, pp.371-376.

²⁰ 森田瑞樹「患者中心の情報管理とそれを可能にする新しいインフォームドコンセント」『情報管理』57（1）, 2011.4, pp.3-11.

²¹ 増井徹「バイオバンクプロジェクトの開始と終了に向けて検討すべきELSI」『個人の遺伝情報に応じた医療の実現プロジェクト（オーダーメイド医療実現化プロジェクト）ELSI委員会活動報告書』2013.3, pp.51-67.

かる取り決めに適切に設定しなければ、ハッキングや事故などによる情報漏洩のリスクの程度は同意内容の広狭に関わらない。他の医療情報等との連結可能性や、目的に応じた個人識別可能性の可否の切り換えをどう担保するか、といった点も技術的な障壁として考えられる。

3 情報から生命を構成する

2011年に投稿されたH5N1亜型鳥インフルエンザウイルスの実験結果に関する二本の学術論文について、米国政府が情報の悪用を懸念し内容の一部削除を勧告したことは国際的に大きな騒動となった。この研究は、もともと鳥を宿主とするウイルスを遺伝子改変して人間を含む哺乳類にも伝搬性を持つウイルスに変えようとする内容だったため、遺伝子を操作して特定の機能を付与・増強させるGOF (Gain of Function) 研究と見なされた。論文はどちらも最終的に全文公開にいたったものの、その後もしばらく研究者の自主的な研究の中断が続けられた。だが、論文出版や研究を控えたところでバイオテロに対する脅威は減少せず、むしろ将来的な感染症の大流行への備えとして重要な知識が欠けるというリスクも指摘される²²。この騒動は研究や研究者の倫理のみならず、資金配分機関や大学、企業、出版社など様々な関係者に関わる問題であることを図らずも露呈した²³。

サイバーセキュリティに関して、一般的な情報がひとたび公開されれば、他の研究者が結果を複製し、研究の詳細を明らかにすることは簡単だとされる²⁴。ただし、人工物と生物は異なる。合成生物学などの急速な発展により、公開されたゲノム情報から致死的な病原体を含む遺伝子が構成されうるといふ、バイオテロへの懸念がしばしば示されてきた²⁵。これ

は生物を扱う研究や技術開発の難しさを過小評価しており、GOF研究や合成生物学の進展が直ちに社会的危険性を及ぼすとか、これに対する十全な対策が求められるということはない。したがって、バイオセキュリティについて、サイバーセキュリティからの類推には慎重を重ねる必要がある。とはいえ、セキュリティ対策として現在の技術的困難性を利用するのは短期的な価値しか持たないというサイバーセキュリティの教訓は生かすべきものであり、将来におけるバイオテクノロジーの飛躍的發展も十分視野に入れておくことが求められる。

4 生命によって情報を媒介する

近い将来に革新的飛躍が考えられるのは、むしろ、生物を情報媒体に用いる技術かもしれない。情報爆発とも言われる現代において、取得できるデータ量の伸びに対し、データを長期間保管するストレージの容量が追いついていない。ストレージの代替技術の一つとして注目されているのは遺伝子の本体であるDNAである。デジタルデータの記録媒体に用いると、1グラムのDNAに1ゼタバイト（10億テラバイト）もの情報量を蓄えられるばかりでなく、何千年にもわたってデータに誤りなく保管ができ、堅牢性にも優れている。70万年前の古代馬の化石からDNAの抽出に成功した研究例もあり、長期間にわたる記録媒体としての信頼性は実証されている。2012年にはハーバード大学のジョージ・チャーチらが5万3000語からなる本1冊の情報をDNAに書き込み、読み出すことに成功している²⁶。マイクロソフトの研究開発部門であるマイクロソフト・リサーチはワシントン大学と共同でDNAストレージの研究を行っており、2016年にDNAの4つの塩基のうち3つをデータとして用い、残りの1つを誤り

²² Sabrina Engel-Glatte, "Dual-Use Research and the H5N1 Bird Flu: Is Restricting Publication the Solution to Biosecurity Issues?" *Science and Public Policy*, Vol. 41 No. 3, June 2014, pp.370-383.

²³ Brett Edwards et al., "From Cases to Capacity? A Critical Reflection on the Role of 'Ethical Dilemmas' in the Development of Dual-Use Governance," *Science and Engineering Ethics*, Vol. 20 No. 2, June 2014, pp.571-582.

²⁴ Bruce Schneier, "Securing Medical Research: A Cybersecurity Point of View," *Science*, Vol. 336 Issue 6088, 22 June 2012, pp.1527-1529.

²⁵ Kathleen M. Vogel, "Framing Biosecurity: An Alternative to the Biotech Revolution Model?" *Science and Public Policy*, Vol. 35 No. 1, February 2008, pp.45-54.

²⁶ George M. Church, Yuan Gao and Sriram Kosuri, "Next-Generation Digital Information Storage in DNA," *Science*, Vol. 337 Issue 6102, 28 September 2012, p.1628.

訂正に使用するアイデアを提案した²⁷。このストレージ向けの研究に使用するため、1000万本もの合成DNAの製造業務をスタートアップ企業であるツイスト・バイオサイエンスに委託している。DNAストレージは極めて高密度で耐久性を備えるものの、データのアクセスには数時間から数日かかると見られているため、現在のフラッシュメモリやハードドライブとは異なる用途を想定しなければならない。

DNAは計算能力を持つ演算素子としても用いられる。これを実証したのはRSA暗号の発明でも有名な南カリフォルニア大学のレオナルド・エイドルマンである。彼は1994年にDNAコンピューターを提唱、これを用いて数学の古典的問題である「巡回セールスマン問題」を解いた²⁸。ストレージや演算素子を含め、センサーやメモリスイッチ、生物時計など、バイオテクノロジーを用いてDNAや細胞にデジタル回路の機能を付与する遺伝子部品の設計が多彩な発展を続けている。最近では、こうした部品を組み合わせて人工遺伝子回路を迅速に設計するプログラミング言語も開発された²⁹。

バイオマーカーによる識別のための特徴選択や疾患分類、生物学的ネットワーク分析などにおいて生命科学への人工知能の応用も模索されているなか³⁰、開発されたシステムに自己組織化や世代継承にかかる機能付与がなされれば、深層学習よろしく自律的な進化を遂げる可能性があり、当初の設計意図から離れて適切なシステム制御を行えなくなるおそれもある。

5 おわりに

システムが多くの機密を抱えるほど、システムは安全でなくなる。機密保持に基づくセキュリティは本質的に脆弱であるという原則にしたがうならば、生命科学に関わるデータそのものは一般公開でないにせよ、適切なアクセスコントロールを設定した上で限られた利用者で共有できるようにすることが望ましい。しかし、大事なことはデータではなく、情報である。ビッグデータの収集や保管、共有が可能になったとしても、それに意味を与え、情報としての価値を高めなければ無用となる。たとえば、ClinVarは臨床的に意義のある遺伝子変異情報を蓄積するレポジトリであり、米国国立バイオテクノロジー情報センター（NCBI）に置かれ、誰でも自由に利用することができる。ClinGenと呼ばれる研究コンソーシアムでは専門家パネルを設け、ClinVarに登録されたデータをレビューして、より正確な情報として選択や整備（キュレーション）を行っている³¹。また、ゲノム解析技術の急速な進展にも関わらず、データの蓄積に比して解析能力が追いついていない問題もある。データ解析のボトルネックは計算資源の拡大でも解決せず、新たなアルゴリズムの開発が必要となる³²。公衆衛生分野では、グローバルな疾病監視システムにおいてオープンソースソフトウェア（OSS）の利用が広まりつつある。データ基盤システムをどのように維持するかは、その多くが時限付きの公的研究資金に依存しているなかでは常に悩ましい問題であるが、少なくともソフトウェアをオープンソースにしておくことで維持コストが最小化されるとともに、ユーザーグループによるソフトウェアの継続的改良によって社会的信頼性の向上が期待される³³。

²⁷ James Bornholt, Randolph Lopez, Douglas M. Carmean, Luis Ceze, Georg Seelig and Karin Strauss, “A DNA-Based Archival Storage System,” *ASPLOS 2016*, pp.637-649.

²⁸ L.M. Adleman, “Molecular Computation of Solutions to Combinational Problems,” *Science*, Vol. 266 Issue 5187, 11 November 1994, pp.1021-1024.

²⁹ Alee A.K. Nielsen et al., “Genetic Circuit Design Automation,” *Science*, Vol. 352 Issue 6281, aac7341, 1 April 2016.

³⁰ Yonghong Peng, Yufeng Zhang and Lipo Wang, “Artificial Intelligence in Biomedical Engineering and Informatics: An Introduction and Review,” *Artificial Intelligence in Medicine*, Vol. 48 Issue 2-3, February-March 2010, pp.71-73.

³¹ Melissa J. Landrum et al., “ClinVar: Public Archive of Interpretations of Clinically Relevant Variants,” *Nucleic Acids Research*, Vol. 44 No. D1, January 2016, pp.D862-D868.

³² Willy A. Valdivia-Granda, “Biodefense Oriented Genomic-Based Pathogen Classification Systems: Challenges and Opportunities,” *Journal of Bioterrorism and Biodefense*, Vol. 3 Issue 1, 113, July 2012.

³³ Erin Hahn, David Blazes and Sheri Lewis, “Understanding How the ‘Open’ of Open Source Software (OSS) Will Improve Global Health Security,” *Health Security*, Vol. 14 No. 1, February 2016, pp.13-18.

バイオセキュリティとサイバーセキュリティに対する考え方やアプローチは、それぞれ偏った部分があり、本稿で試みたように両者にまたがる問題群を照射し、お互いの視点や取り組みを交えることでセキュリティが統合的に強化されるだろう。バイオセキュリティはバイオテロ対策としての国家安全保障に関わる領域でなければ、主として科学者の自己規制に委ねられている。バイオセーフティや公衆衛生という観点からの環境や健康への監視的取り組みは電力や水資源と同様の国家的な公共財であるものの³⁴、そうした眼差しは薄れがちである。だが、国家が関わればよいというものでもない。鳥インフルエンザの論文出版騒動では、研究の潜在的な社会的リスクを評価する国際機関が必要とされたが、その機関が国家のみの参加を前提とするのであれば、このインターネット時代では機能しない。先進国が途上国の生物資源や遺伝資源を利用し、医薬品や食品開発における利益を独占する行為（バイオパイラシー）がしばしば見られる。そのため、インドネシアはかつて新型に変異する鳥インフルエンザウイルスを世界保健機関（WHO）に提供することを拒否した。米国国立衛生研究所（NIH）と英国のウェルカム・トラストが出資しているアフリカでの遺伝学研究（H3Africa: Human Heredity and Health in Africa）でも地域間格差が懸念されることから、ゲノムデータの公開に保留期間（エンバゴ）を設け、他の研究者がデータの二次利用をする前にアフリカの研究者がゲノム解析を進められるよう奨励し、あわせて研究者へのトレーニングも用意した³⁵。こうした事例から看取されるように、厳格なトップダウンによる法制や機密保持は研究の国際協調を阻害するおそれもあり、ボトムアップによる取り組みが必要である。政府機関や民間企業も含む世界中の多様な関係者がそれぞれの自主的な取り組みを尊重しながら進めるグローバル・アライアンスは新たな可能性の一つである。対して、

サイバーセキュリティはますます軍事的な駆け引きのツールとして見なされるようになり、複雑な政治的プロセスの問題として俎上に載せられる。結果、国家がサイバー防衛に資金を投じれば投じるほど、そのセキュリティ上の欠陥が明らかになるというジレンマに嵌まっている。そこでは、サイバー空間の国境管理という国家安全保障が主題となり、市民のプライバシーや言論の自由は抑圧されがちである³⁶。

関心の偏りはあれど、問題は通底している。バイオセキュリティもサイバーセキュリティも、国家による取り組みが問題の主要因になっている反面、安全で開かれた活動は国家の関与なしには実現しない。このジレンマは国家を超えて広がっているために、その解決策は国家間の連携だけに見つかるのではない。むしろ、セキュリティに関心をもつあらゆる関与者を巻き込むあり方が検討されるべきである。こうしたボトムアップによる分散的で脱中心的なネットワークによる協働体制は、事前の十分な備えと、迅速かつ柔軟な危機対応という点においてセキュリティを高める³⁷。あと、人間の安全保障という根柢がしばしば見落とされやすい。サイバーセキュリティではプライバシーや言論の自由といった生活圏にとどまっていたものが、バイオセキュリティでは人間の生命や、それらを取り巻く生物環境や生態系に大きく関わる。医療情報やゲノム情報などについても、そのあり方の検討は専門家に多くが任せられ、情報を提供する当の患者や市民との関わりはまだまだ薄い。対話的な説明同意や適切なアクセスコントロール、キュレーション、オープンソース化のみならず、新たな情報媒体と媒介手法を通じて生命科学を人々の手に取り戻す、主体性の回復が緊要である。それは、生命と情報のネットワークを通じて、個人が家族やコミュニティ、民族、そして国家との関係性を考え直す契機でもある。

³⁴ Stephan Velsko and Thomas Bates, "A Conceptual Architecture for National Biosurveillance: Moving Beyond Situational Awareness to Enable Digital Detection of Emerging Threats," *Health Security*, Vol. 14 No. 3, June 2016, pp.189-201.

³⁵ Jantina de Vries et al., "The H3Africa Policy Framework: Negotiating Fairness in Genomics," *Trends in Genetics*, Vol. 31 No. 3, March 2015, pp.117-119.

³⁶ Myriam Dunn Calvelty, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities," *Science and Engineering Ethics*, Vol. 20 Issue 3, September 2014, pp.701-715.

³⁷ Cf. Elżbieta Rzeszutko and Wojciech Mazurczyk, "Insights from Nature for Cybersecurity," *Health Security*, Vol. 13 Issue 2, April 2015, pp.82-87; Daniel J. Barnett, Tara Kirk Sell, Robert K. Lord, Curtis J. Jenkins, James W. Terbush and Thomas A. Burke, "Cyber Security Threats to Public Health," *World Medical and Health Policy*, Vol. 5 No. 1, March 2013, pp.37-46.