

システムズ・レジリエンス

Towards Systems Resilience

丸山 宏† 井上克巳‡ 椿 広計† 明石 裕† 岡田 仁志‡ 南 和宏†
 Hiroshi Maruyama Katsumi Inoue Hiroe Tsubaki Hiroshi Akashi Hitoshi Okada Kazuhiro Minami

†統計数理研究所 ‡国立情報学研究所 ††国立遺伝学研究所

1. はじめに

2011 年 3 月 11 日の東日本大震災とそれに続く福島第一原子力発電所の事故においては、「想定外」という言葉が多く使われた。我々の社会が持続可能なものであるためには、様々な外界の事象に柔軟に対応していなければならぬ。それらの事象の中には、想定されていたものも、想定されていなかったものもあるだろう。そもそも「想定外」とは何だろうか？ そのような事象に対して、我々はどのような備えをすればよいだろうか？

東京大学工学系研究科 緊急工学ビジョン・ワーキンググループ「震災後の工学は何をめざすのか」では、「今回のような震災に立ち向かうためには、災禍の損害から早期の機能回復が可能な技術社会システムを実現するための、レジリエンス工学とも呼ぶべき新分野を確立しなければならない」と述べている[1]。レジリエンスとは、環境の大きな変化に対して、一時的に機能を失ったとしても柔軟に回復できる能力を指す概念であり、生態学等ではよく知られたものである[2,3]。

生物、生態系、国家や企業などの社会システム、人間の心理など、レジリエントな性質を持つシステムは多くある。我々は、これら多様な分野におけるレジリエンスを調べることによって、レジリエントなシステムを構築・運用するための共通な知識体系を構築することを目指し、大学共同利用機関法人 情報・システム研究機構の中に、新たに領域横断型研究プロジェクト「システムズ・レジリエンス」を立ち上げた。

本稿では、このプロジェクトの狙い、方針、それに現在の研究活動について述べる。

2. レジリエンスとは何か

2.1 レジリエンスの定義

レジリエンスをどのように捉えるか、については様々な考え方がある。最も簡潔な定義として、我々は、Logstaff ら[2]による「Resistance と Recovery を組み合わせたもの」という立場をとる。Resistance とは、システムが外界の擾乱に対してその機能を維持すること、すなわちシステムの信頼性を指す。Recovery とは、システムが機能の一

部を失った時に、その障害から回復する能力を指す。

このような能力は定量化できるだろうか？「システムの機能」を何らかの形で定量化することが可能な場合、レジリエンスを「失われた機能を時間軸上で積分したもの」と捉えることにより、定量化する考え方もある[5]。特定の擾乱シナリオを想定し、その際のシステムの機能喪失を予測できれば、このような定量化はある程度可能であろう。一方、想定することが難しい事象、例えばセキュリティシステムに対する未知の攻撃や、システムに対する被害の程度が予測しにくい大規模災害などに対しては、システムのレジリエンスを事前に定量化しておくことは難しい。

一方、レジリエンスの定量化が困難な場合であったとしても、2つのシステムのレジリエンスを相対的に比較できることが望ましい。それが可能であるならば、自分のシステムをよりレジリエントなものにするために、複数ある方策のどれを採用すべきか、の目安になる。

また、レジリエンスがこれまでの信頼性工学と異なるもう一つの側面は、回復したシステムが必ずしも元のシステムと同一の機能を持たなくてもよい、と考えられることである。災害復興などにおいては、現状に復旧するのではなく、むしろより望ましい状態に移行するチャンスと捉えることもできる。このような場合、多様なステークホルダーとの合意形成を考えなければならない。

2.2 システムズ・レジリエンス

レジリエンスはシステムレベルの性質である。個別の要素が機能を失ったり、消滅したり別の要素に置き換わることもあるかもしれない。それでも、システムとしての同一性を維持し、機能を何らかの形で回復させていくのがレジリエントなシステムである。複雑なシステムの各要素が互いに連携することによって、個別の要素の単純な和でない、システムレベルの性質として「レジリエンス」が創発されるものと我々は考える。また、生態系、社会システムなど我々の扱うシステムの多くは、複数のシステムが有機的に結合した、システム・オブ・システムズとなる。我々は、レジリ

エンスのシステム的な理解を明らかにする。

3. 様々な分野におけるレジリエンス

自然界・人工物・社会システムを問わず、レジリエントな性質を持つシステムは多くある。それらの間の共通の性質・原理は何だろうか？ 最初に幾つかの分野において知られているレジリエントなシステムについて考察する。

3.1 生物

地球上に生物が誕生したのはおよそ 40 億年前であるが、この 40 億年の間に、何度も生物の大量絶滅があり、それらは巨大隕石などの希少事象によって起こされたものではないかと考えられている。それにも関わらず、地球上の生物が全滅せずに残っているのは、生物には何らかのレジリエンスのメカニズムを持っているからだと考えられる。

大腸菌は、その DNA の働きがよく知られた生物である。大腸菌にはおよそ 4,300 の遺伝子があり、それぞれに役割があるが、そのうち約 4,000 については、その遺伝子の機能を失わせて（ノックアウトして）も、大腸菌は繁殖しつづけることができる[6]。その遺伝子の失われた機能を他の遺伝子が肩代わりしたり、別の経路によりタンパク質が生成されたりするからである。

ワシントン湖にいる淡水魚のイトヨは、1957 年には鱗が無かったことが知られているが、現在では鱗を持っている。これは、過去 50 年にわたってワシントン湖の透明度が上がったために、捕食者であるマスの捕食圧が上がったためではないかと考えられている[7]。一万年以上前のイトヨはもとも海水魚であり、その時は鱗を持っていた。1 万年間に渡って発現して来なかった表現型を持つ遺伝子、すなわちその間不要な遺伝子であったものが、マスという天敵を存在に対応してただちに発現したものと捉えることができる。

システム生物学者の北野は、生物と工学物のロバストネスを比較し、それらには共通にフィードバック制御 (Control)、代替メカニズム (Alternative, 冗長性・多様性)、モジュール性 (Modularity)、疎結合 (Decoupling) の 4 つの戦略が見られると主張している[8]。

3.2 ビジネス継続計画

企業は刻々と変換するビジネス環境の中で経営を行なっている。これらの変化の中には、東日本大震災やタイの洪水におけるサプライチェーンの喪失など、普段は想定できない事象もあるだろう。多くの企業は、ビジネス継続計画 (Business Continuity Plan) を策定し、リスク管理を行なっている。ビジネス継続計画は、セキュリティや品

質などと同様にマネジメントプロセスの問題として捉える考え方があり、国際標準化団体の ISO/TC223 ではそれらのベスト・プラクティスを標準化しようとしている。例えば ISO22320 では、危機対応に関する要求事項をまとめている[9]。特に強調されているのは、指揮命令系統の確立、情報の共有、それに組織間の協調・連携関係である。

3.3 コンピュータ・システム

IT システムが社会に深く浸透するにつれ、IT システムへの信頼性の要求が高まっている。しかし、100%の信頼性を持つシステムはあり得ない。想定外の事象が起き、システムが損傷を受けることを認めた上で、柔軟な回復を考える必要がある。2003 年に IBM が提唱したオートノミック・コンピューティング[10]は、生態の自律的な回復力にヒントを得た考え方であり、システムに対する擾乱を検知し、対策を選択し、それを適用して効果を測定する、というサイクルを自動的に回すことによってレジリエンスを実現しようとするものであり、このような考え方はコンピュータ・システムにとどまらず多くのシステムで使われている。

信頼性が主にできるだけシステムが壊れないことを目指す、つまりシステムの平均故障間隔 (Mean Time to Failure, MTBF) の最大化を目指すのに対して、UC Berkley の Patterson ら[11]は、システムが壊れた場合の回復時間 (Mean Time to Repair) の最小化を目指す Recovery-Oriented Computing (ROC) という考え方を提唱している。コンピュータ・システムにおける障害はハードウェアの故障だけでなく、ソフトウェアのバグやオペレータの運用ミスなどからも多く引き起こされることから、回復のための手段を予めシステムに用意しておき、それを定期的にテストする、という戦略などが延べられている。

情報セキュリティも、常に「想定外」の脅威にさらされている分野である。セキュリティ上の攻撃手段は、次々と新しいものが生み出されるからである。

3.4 法律

法律もまた、常に「想定外」に対応することを求められるシステムである。1880 年に布告された刑法には「他人の財物を窃取した者は、窃盗の罪とし」とあるが、その後電気が電灯線から盗まれた時に、電気は「モノ」であるかどうかで争われた。刑法定時時には、電気が窃盗の対象として想定されていなかったことが原因である。

3.5 環境

地球温暖化、生物多様性の喪失、森林火災、海産資源の現象など、地球環境の持続可能性も、レ

レジリエンスに関連の深い領域である。これらはいずれも、人類社会における経済活動と地球環境の相互作用によって発生している問題であり、その解決のための枠組として、**Buzz Holling** はレジリエンスという概念を提唱し、その後広く研究されている[12]。

3.6 その他

以上は、レジリエントなシステムのごく一部であるに過ぎない。例えば、金融、流通、交通、エネルギー、医療などの各産業は、それぞれに外部環境の変化に対応してシステムを持続可能にするメカニズムを持っている。我々はできるだけ視野を広く持ち、これらのシステムに共通な原理を探さなければならない。

4 レジリエンス戦略

以上のように複数の分野におけるレジリエンスを調べると、それぞれの分野における特有の戦略もあるが、共通と思われるものも存在する。現在わかっている、いくつかのものを提示する。

- 冗長性 – 人工物に多く見られる戦略であり、同じ機能を持つ複数の部品を用意しておくことによって、一部の部品の故障に対して、代替の部品が肩代わりする。主に **Resistance** の戦略として用いられる。
- 多様性 – 生物によく見られる戦略であり、未知の脅威に対して、多様な要素のどれかが生き残ることによって回復を可能にする。
- 再生 – システムの古くなった要素を、致命的になる前に壊して、新たに作りなおすこと。生態系などでよく見られる。
- 危機対応 – 組織において主に用いられる戦略で、想定外の事象が起きた場合に、その状況を正確に把握し、適切な対応をとることで回復を早めようというものである。

いくつかのレジリエンス戦略と、そのモデル化については、[11]を参照されたい。

5. 研究方針

以上のように、様々な分野においてレジリエンスを観察することができ、レジリエンスのためのいくつかの戦略を見出すことができる。これらのドメインも目的も規模も異なるシステムの間に、どのような関係があるのだろうか？ 共通なモデル化か可能だろうか？ さらに、システムをレジリエントに設計し、運用するための一般的な方略が導けるだろうか？

本プロジェクト「システムズ・レジリエンス」においては、レジリエントなシステムを設計・運用するための知識の体系 (**Body of Knowledge, BOK**) を構築することが最終目標である。我々は、

以下の 3 点について、答えを持たなければならない。

1. レジリエンスとは何か。その定義と評価基準
2. 様々なレジリエンス戦略のカatalogの体系化
3. レジリエントなシステムを設計・運用するための方法論とベスト・プラクティス

本プロジェクトにおいて我々はまず、できるだけ多様な分野におけるレジリエンスの知見を収集し総合する。それによって、レジリエンスとは何かについてより明快な定義とメトリックを導き出すことを予定する。同時に、得られた知見を実行可能な計算モデルとして定式化することで、レジリエンスの本質を解き明かすアプローチをとる。このため、我々のプロジェクトは、当面、以下の 4 つのサブプロジェクトで研究を行う。

5.1 「想定外」の数理

我々が興味を持っているのは、日常の小さな擾乱ではない。小さな擾乱に対しては、制御工学や信頼性工学などのよく知られた方法で対応できるからである。これはレジリエンスの 2 つの側面のうち、**Resistance** の考え方と言える。

一方、東日本大震災など、稀で規模の大きな事象に対しては、**Resistance** の考え方だけではうまく対処できない。**Resistance** のためのコストが極めて大きくなってしまいうからである。例えば、東日本大震災で東北地方を襲った津波に耐えられる高さの防潮堤を建設することは、工学的に可能であったとしても、コスト的には現実的ではないだろう。

経済学者の竹内啓はその著書「偶然とは何か―その積極的意味」において、極めて稀な事象については、起こらないものと仮定し、万が一起きてしまった場合には、その不幸を社会で再分配せよ、と述べている [15]。我々は、**Resistance** と **Recovery** の戦略をどのように切り分ければよいのか、最適なメタ戦略を考えて行かなければならない。

このサブプロジェクトでは、レジリエントなシステムを構築するために、どれだけのコストを **Resistance** と **Recovery** の準備のために割り当てればよいのか、メタ戦略の指標を作ることを目指す。

5.2 生物におけるレジリエンス

生物システムには絶え間ないストレスや繰り返し起きる危機的状況に耐えうるロバストネスを内包する必要がある。我々は生物システムにおける下記の 3 つの互いに一見矛盾する側面に着目して生物における抵抗性と回復性のメカニズムを解明する。

- 生態遺伝学における環境適応

生態系は常に環境の変化や外乱にさらされており、環境への外乱および危機的な状況変化に対する生態系の生存、遺伝的多様性と適応のメカニズムが寄与しているとかんがえられる。我々は生態系とその遺伝子との関係を明らかにすることによって、そのメカニズムの解明を試みる。

- 集団遺伝学における有害突然変異

遺伝子の多様性を生み出すとされる突然変異は、それ自体が生物種にとっての大きな脅威になることもありうる。大規模な集団の遺伝的解析により、様々な生物の遺伝子には恒常的に有害突然変異が発生していることが明らかになっている[16,17]。ある生物種の個体数が比較的小規模である場合、有害突然変異が種全体に広がり、集団の適応度低下をもたらす可能性がある。しかし生物が収獲選滅の法則に従う適応度関数を持つ場合にはそれが有害突然変異に対する防御機構になる可能性があり、その仮説の検証を目指す。

- 極限的な環境での生物システム

必ずしも多様性を持つ生態系だけが安定とは限らない。南極大陸のような生物にとって過酷な環境において、非常に限られた少数の生物種が安定した生態系を維持していることが知られている。我々はそのメカニズムを解明する。

5.3 社会システムの秩序形成

社会システムの秩序形成は、通常国家によってトップダウンに法制度が規定されることによって行われる、とされている。しかし、現代の複雑な社会システムにおいて、より柔軟に想定外の事象に対応するためには、このトップダウンの秩序形成の仮説を見直す必要がある。問題を解決するための最良の知識は当事者のみが有するという認識の下、状況の変化に柔軟に対応可能な、ボトムアップ型のルール形成を取り入れていく必要がある。

我々が着目するのは、近年欧州を中心として重視されつつある、「共同規制 (co-regulation)」という概念である。共同規制とは、新しい社会的問題について規制を行う際、当該分野で活動する企業等の自主規制による対応を優先しつつも、そのリスクや不完全性を政府が補完するという、公私の協調的な制度形成手法を指す[18]。

このサブプロジェクトでは、主にサイバーセキュリティやプライバシー保護等の法制度分野について、レジリエントな社会システムを実現するための、共同規制手法を用いたボトムアップ型秩序形成の方法論を構築することを目的とする。

5.4 レジリエンスの計算モデル

複雑かつ大規模なシステムのレジリエンス性を

評価するためには、汎用的な数理モデル上で様々な動的特性を解明する計算論的手法が不可欠である。我々は特に大規模システムを様々なネットワークモデル (Boolean, Constraint, Bayesian networks 等) として捉え、想定外のイベントに対するシステム構成の動的変化を効率よく表現するモデリング技法を考案する。またネットワークモデルにおいて、1) 外乱及びシステム変数に対する感受性[19]、2) システム状態の予測不可能性[20]、3) 文法的また意味論的なシステム状態間の距離の概念の導入[21]、4) ソフト制約をできる限り多く満たすネットワーク構成の更新、5) マルチエージェントにおける多目的最適化問題 [22] 等のダイナミクスを分析する計算理論の構築を行い、レジリエントなシステムを設計するための一般的原理の解明を目指す。

6. 終わりに

「システムズ・レジリエンス」は、本質的に領域横断型の研究プロジェクトであり、今後も我々が今まで気づいていない、多くの分野の研究者の協力が必要である。本論文で紹介したシステム・レジリエンスの研究に興味を持たれた研究者の方々は今後も積極的に協業し、活発な議論を行う予定である。

謝辞

領域横断型研究プロジェクト「システムズ・レジリエンス」の各メンバーの助言に感謝します。本研究は、情報・システム研究機構／新領域融合研究センターの援助を受けました。

参考文献

1. 東京大学工学系研究科 緊急工学ビジョン・ワーキンググループ 「震災後の工学は何をめざすのか」, <http://www.t.u-tokyo.ac.jp/epage/topics/pdf/vision.pdf>, 2011.
2. Holling, C. S., Resilience and Stability of Ecological Systems. Annual Review of Ecology and Systematics, vol. 4, 1973.
3. Walker, B., C. S. Holling, S. R. Carpenter, and A. Kinzig. Resilience, Adaptability and Transformability in Social-Ecological Systems. Ecology and Society, 9 (2): 5, 2004.
4. Logstaff et al. Building Resilient Communities. Homeland Security Affairs, vol. 6, no.3, 2010.
5. Bruneau, M., et al. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthquake Spectra, 19-4, 2003.
6. Baba, T., et al. Construction of Escherichia coli K-12 in-frame, single-gene knockout mutants: the Keio collection. Molecular

- Systems Biology, 10-1038, 2006.
7. Kitano, J., et al. Reverse Evolution of Armor Plates in the Threespine Stickleback. *Current Biology* 18, 2008.
8. Kitano, H. Biological Robustness. *Nature Review Genetics*, vol. 5, 2004.
9. ISO 22320: Societal security -- Emergency management -- Requirements for incident response. 2011.
10. Kephart, J. and Chess, D. The Vision of Autonomic Computing. *IEEE Computer*, January, 2003.
11. Patterson, D., et al. Recovery Oriented Computing (ROC): Motivation, Definition, Techniques, and Case Studies. *Berkeley Computer Science*, 2002.
12. F. Stuart Chapin III, Gary P. Kofinas, Carl Folke (Eds). *Principles of Ecosystem Stewardship: Resilience-Based Natural Resource Management in a Changing World*. Springer, ISBN-13: 978-0387730325, 2009.
13. Kazuhiro Minami and Hiroshi Maruyama. *Resilience Engineering: State of the Art and Research Challenges*. Forum on Information Technology (FIT), September, 2012.
14. Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, ISBN-13: 978-0141034591, 2008.
15. 竹内啓. 偶然とは何か—その積極的意味, ISBN-13: 978-4004312697, 2010.
16. Hiroshi Akashi. Inferring weak selection from patterns of polymorphism and divergence at “silent” sites in *Drosophila* DNA. *Genetics* 139, 1067–1076, 1995.
17. Hiroshi Akashi, Naoki Osada, and Tomoko Ohta. Weak selection and protein evolution. *Genetics*, Accepted for publication.
18. 生貝直人. 情報社会と共同規制—インターネット政策の国際比較制度研究. 勁草書房, ISBN-13: 978-4326402700, 2011.
19. Chan, H. and Darwiche, A. On the Revision of Probabilistic Beliefs Using Uncertain Evidence. *Artificial Intelligence*, 163(1):67–90, 2005.
20. Chiaki Sakama and Katsumi Inoue. Abduction, Unpredictability and Garden of Eden. *Model-Based Reasoning in Science and Technology (MBR 2012)*, Sestri Levante, Italy, June 2012.
21. Sébastien Konieczny, Pierre Marquis, Nicolas Schwind. Belief Base Rationalization for Propositional Merging. *Proc. 22nd International Joint Conference on Artificial Intelligence (IJCAI-11)*, page 951-956, 2011.
22. Tenda Okimoto, Yongjoon Joe, Atsushi Iwasaki, Toshihiro Matsui, Katsutoshi Hirayama and Makoto Yokoo. Interactive Algorithm for Multi-Objective Constraint Optimization. *Proceedings of 18th International Conference on Principles and Practice of Constraint Programming (CP 2012)*, 2012. Accepted for publication.