

Nextcom

情報通信の現在と未来を展望する

Vol.43

2020 Autumn

ネクストコム

特集 5G時代の 情報セキュリティ



Feature Papers

特集論文

5Gとサイバー犯罪

湯浅 壘道 情報セキュリティ大学院大学 副学長

特集論文

サイバーセキュリティの未来

——米中対立の先に待ち構える三項対立——

小宮山 功一郎 慶應義塾大学 グローバルリサーチインスティテュート
客員所員

特集論文

5G/IoT時代の情報セキュリティ

杉山 敬三 株式会社KDDI総合研究所 セキュリティ部門 部門長

Paper

論文

サプライチェーン・レジリエンスの再考

——ブロックチェーン・メカニズムの導入による取り組み——

崔 宇 追手門学院大学 経営学部/同大学院 経営・経済研究科 准教授

明日の言葉

安全な時にこそ防御を固めよ。
真に危険を逃れるのはそのような人である。
…… プブリウス・シルス

古代ローマの劇作家であるプブリウス・シルスは、
奴隷身分出身でありながらローマ市民権を得た人物。
多くの箴言^{しんげん}を遺している。

Nextcom ネクストコム

特集

5G時代の 情報セキュリティ

- 2 | **すでに始まってしまった未来について
現実の序列の見直し**
平野 啓一郎 作家
- 4 | 特集論文
5Gとサイバー犯罪
湯浅 壘道 情報セキュリティ大学院大学 副学長
- 14 | 特集論文
**サイバーセキュリティの未来
——米中対立の先に待ち構える三項対立——**
小宮山 功一朗 慶應義塾大学 グローバルリサーチインスティテュート
客員所員
- 24 | 特集論文
5G/IoT時代の情報セキュリティ
杉山 敬三 株式会社 KDDI 総合研究所 セキュリティ部門 部門長
- 32 | 論文
**サプライチェーン・レジリエンスの再考
——ブロックチェーン・メカニズムの導入による取り組み——**
崔 宇 追手門学院大学 経営学部／同大学院 経営・経済研究科 准教授
- 44 | お知らせ
論文公募のお知らせ
2020年度著書出版・海外学会等参加助成に関するお知らせ
- 46 | 情報伝達・解体新書
ネコは自分の名前を知っている
齋藤 慈子 上智大学 総合人間科学部 准教授
- 48 | 明日の言葉
謝って、逃げて、打ち勝つ
高橋 秀実 ノンフィクション作家

すでに始まってしまった未来について——④③

文：平野啓一郎

絵：大坪紀久子

現実の序列の見直し

コロナ禍は、多くの感染者を生み、経済的にも大打撃となったが、他方でリモートワークの拡大など、ライフスタイルや価値観を変えつつある。私も、新聞や雑誌のインタビューは軒並みオンラインとなったが、これで十分となると、なぜ対面の必要があるのかと、元に戻るには、よほどの理由が必要と感じる。

テレビ・カンファレンスにせよ、オンライン飲み会にせよ、今までも可能であったはずだが、一般化はしなかった。

なぜだろうか？

私たちは、五感によって得られる情報量に応じ、現実を序列化しようとする。オンラインでの体験では、嗅覚、触覚、味覚は満たされず、視覚や聴覚も限定的に機能する。だから、物理的な現実こそは真である、と依然として主張しがちである。

しかし、私はこの間、新聞連載中の『本心』という小説の取材で、下半身不随の男性と話をしたのだが、彼に、コロナ禍で非常に多くのレストランがデリバリーやテイクアウトを始めたお陰で、食べることの出来る料理の種類が圧倒的に増えた、と言われてハッとした。オンラインでの活動がますます盛んになれば、色々な事情で外出が困難な人たちは、その分、楽しみが増えるだろう。

その時、私たちは、いや、料理はやはりレストランで食べてこそであり、VRはどこまでいっても偽物で、人には実際に会ってみたいとわからない、と言い続けるだろうか？ 私たちは、この世界の序列化が貧富の差に基づいてなされる時には、強く反発する。一部の大金持ちがプライベート・ジェットでしか行けないようなリゾート地に行って、ここに比べれば、日本の田舎の観光地などはお粗末な偽物だ、などと言おうものなら、忽ち炎上するだろう。しかし、健常者であるという条件に関しては、多くの場合、無自覚である。

コロナ禍は、私たちの世界観を揺さぶったが、実に反省させられることも多い。

Keiichiro Hirano

小説家。1975年生まれ。1999年京都大学在学中に『日蝕』により芥川賞を受賞。以後、『葬送』、『ドーン』、『かたちだけの愛』、『空白を満たしなさい』、『私とは何か—「個人」から「分人」へ』、『透明な迷宮』、『マチネの終わりに』、『ある男』など、数々の作品を発表。最新刊は『カッコいい』とは何か（講談社現代新書）。



特集

5G時代の 情報セキュリティ

2020年、日本でも商用サービスが始まり、5G時代が幕を開けた。
通信速度の超高速化、超低遅延、多数同時接続を可能にする
5Gにより、新たな利用形態の創出が期待されている。
同時に、サイバー攻撃の脅威が想定され、
情報セキュリティの確保が求められている。



5G時代の 情報セキュリティ 1

5Gとサイバー犯罪

情報セキュリティ大学院大学 副学長

湯浅 壘道 Harumichi Yuasa

5Gの普及によってさまざまなサービスが提供され、私たちの生活に恩恵をもたらすことが期待されるが、サイバー犯罪の増加や新たなサイバー犯罪の誘発という問題が発生する恐れがある。また欧州刑事警察機構（ユーロポール）が指摘するように、5Gの技術的特色がサイバー犯罪の捜査を妨げる可能性があり、特に暗号化により解析が困難になる可能性が指摘されている。これに対して、アメリカのカリフォルニア州ではIoTセキュリティ法によりIoT機器にセキュリティ対策を義務付けたほか、オーストラリアでは、暗号化されているデータを復号するために民間事業者への協力を要請する法律が制定されるなど、新たな法整備の動きがある。

キーワード

サイバー犯罪 IoT 暗号 欧州刑事警察機構 オーストラリア カリフォルニア

1. はじめに

いよいよ日本においても、2020年に5G（第5世代移動通信システム）のサービス提供が開始され、5G対応のスマートフォンも発売された。

移動通信システムは、アナログであった第1世代から始まって、新世代の登場に伴って新たなサービスを生み出してきた。5Gには「超高速」「超大容量」「超大量接続」「超低遅延」という四つの技術的要求条件がある。このため、単なる4Gからの技術的な発展ではな

く、「新しい特徴を持つ次世代の移動通信システムであり、本格的なIoT時代のICT基盤」（総務省）¹⁾として位置付けられている。今後、5Gの特色を利用したさまざまなサービスが提供され、私たちの生活に恩恵をもたらすことが期待される。

インターネットとそれに関連する技術・サービスの発展の歴史は、多くのイノベーションを生み出し、国際社会と経済を変革してきた。それと同時に、新たな技術とサービスの普及は、それに呼応する形で、プライバシーの侵害や新たなサイバー犯罪を惹起してきたという一面があることも否めない。国家が背景にあ

るとされる多種多様なサイバー攻撃も行われ、武力紛争にサイバー攻撃が利用される可能性が現実化するに及んで、サイバーセキュリティは安全保障上の課題にもなった。わが国では、サイバーセキュリティ対策は重要インフラへの攻撃や企業や団体等からの個人情報流出や営業秘密の窃取などの問題が中心となっているが、フェイクニュースもサイバーセキュリティの課題であるという指摘がある²⁾。国際的な文脈では、2016年のアメリカ大統領選挙におけるロシア疑惑以来、電子メール窃取とその暴露、個人データ窃取とそれを利用したSNS経由の世論誘導と選挙介入もサイバーセキュリティの大きな課題となっている。

5Gの普及は、プライバシーにとっても脅威となる恐れがある。今後5Gの普及が進み、4Kや8Kのような高解像度の映像(動画)がリアルタイムで伝送されるようになれば、中国が目指しているといわれるように、街頭における国民を監視カメラからのデータと各種の個人データとの突合を通じて瞬時に識別することも容易となり、文字通りの監視国家が実現される可能性がある。政府による監視カメラでの各種の個人データの収集が行われない国であっても、動画の持つ情報量は静止画像よりも圧倒的に多く、動画の伝送が活発になることによって、さまざまな問題を生む恐れがある。

新たな技術とサービスの普及が新たな問題点や犯罪も生み出してきた過去の歴史に鑑みれば、「超高速」「超大容量」「超大量接続」「超低遅延」という5Gの新たな特色が、新たなサイバー犯罪を誘発し、サイバーセキュリティ上の問題を生む可能性は高い。

本稿では、特に5Gの普及によるサイバー犯罪への影響について考えてみることにしたい。

2. 5Gによるサイバー犯罪の増加

2.1. IoTと4IR

5Gの普及によって、実際にサイバー犯罪は増加す

るのか。

この点に関して指摘されているのが、5GによるIoT (Internet of Things)の加速と、第四次産業革命 (Fourth Industrial Revolution = 4IR)³⁾の実現である。4IRは、フィジカル空間、物理空間、バイオロジカル空間との線引きの曖昧化という目的も有しているといわれる⁴⁾。4IRが実現すると、日々の生活はデジタル技術にさらに依存するようになり、生産、マネジメント、ガバナンスに関する現在のパラダイムも変革を余儀なくされるものと予想される。その際に基盤となることが期待されているのが5Gであるが、AI (人工知能)を活用する各種サービス、遠隔医療、自動運転の自動車等において、「超高速」「超大容量」「超大量接続」「超低遅延」という5Gの技術的特色を活用した大量のデータ転送が行われるようになる際、そこにサイバー犯罪が生まれる余地も大きくなるであろう。

ただし、サイバー犯罪の発生という観点から見ると、リスクが存在するのは5Gの「量」ではなく、むしろユーザーによる5Gの利用態様にあると考えられる。

5Gは、インフラのあらゆるレイヤーをカバーしていくようになり、5Gによる通信を介してリアルタイムの制御がなされるようになると予想されるが、5Gによって接続される機器類は、現在私たちが使っているコンピューター類やタブレット、スマートフォン等とは異なり、操作画面やインターフェースすら持たないものが大部分となるであろう。このような5Gによって接続される機器類のOSのアップデートは、誰がどうやって行うことになるのであろうか。また、現在のサイバー犯罪の多くは個人データ、IDやパスワード、設計図、特許情報や営業秘密等の情報の窃取を主たる利益源としているが、5Gが普及してリアルタイム制御が広範に行われるようになった場合、それがサイバー攻撃のターゲットになることが予想される。最悪の場合は制御機能を奪われることになり、企業のビジネスや、政府・自治体の行政行為そのものが継続できなくなる恐れがある。

また、5Gが発展途上国におけるポテンシャルを高めると同時に発展途上国発のサイバー犯罪を増加させる恐れがあることも無視できない。

インターネットの普及初期の段階では、北米の人口は世界の人口の5%程度にすぎないのに対して、北米のインターネット人口は世界のインターネット人口の25%以上を占めていた。しかし、発展途上国においては家庭やオフィスまでの有線の高速通信網の整備を飛び越して移动通信システムが整備されることが多く、それと同時に発展途上国のインターネット人口も急増した経緯がある。

日本も含めた先進国による途上国への能力構築支援の成果もあり、発展途上国においてもサイバーセキュリティ対策が進みつつある。しかし、発展途上国が国際的なサイバー犯罪やサイバーテロの温床となっていることは否定できない⁵⁾。特に、企業や個人などのエンドユーザーのセキュリティ対策の遅れは、発展途上国のコンピューターや情報システムがサイバー犯罪の踏み台として利用されることを招いている。2018年の時点で、アフリカ大陸のユーザーの約4分の1がサポートやアップデートなしに Windows XP を使用し続けており、アフリカ大陸のコンピューターの80%以上がすでにマルウェアに感染しているという報告がある⁶⁾。

先進国や中国の技術支援、財政支援等によって、発展途上国にも5Gは普及していくとみられるが、サイバーセキュリティに対する十分な対策や予算のないままに途上国の企業や個人が5Gに接続できる機器類のユーザーとなった場合、それらがマルウェアに感染し、グローバルに悪用されるボットとなる危険性はか

なり高いとみるべきであろう。

2.2. 欧州刑事警察機構の警告と対策

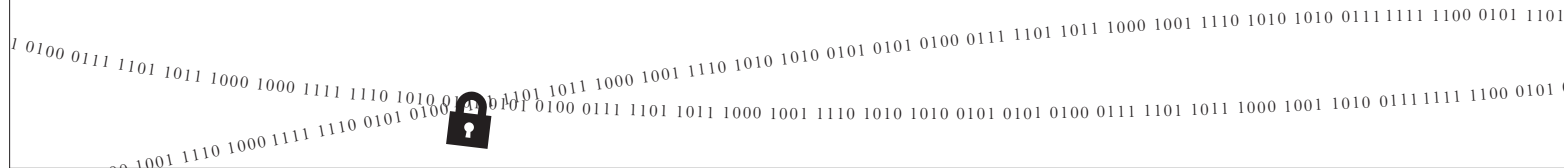
5Gの普及によるサイバー犯罪対策、犯罪捜査への影響について、早い時期から警鐘を鳴らしているのが、欧州刑事警察機構（ユーロポール）である。ユーロポールは、2019年7月に「犯罪者は電気羊の夢を見るか」⁷⁾という報告書を公開した。その中では、5Gによる警察活動への影響について次のように分析している。

・利用者を特定し、探し出す法執行機関の能力に関する潜在的な影響

これまでの世代の移动通信システムは、個別のデバイスに割り当てられる固有の識別子を生成していた。しかし5Gでは、一時的な識別子だけを利用するようになる可能性がある。この場合には、法執行機関がデバイスを識別し探し出すことを可能にする独自の携帯電話カード識別子の使用が困難となるので、捜査機関によるアトリビューションの難易度が格段に上がることになる。その結果、法的に許容される技術的な調査や解析を実施することはもはや不可能になる恐れもある。少なくとも、現在利用されている捜査の手法やツールが時代遅れになることは予想できる。

・合法的な傍受を行う際に必要な情報の入手可能性とアクセス可能性の制限

5Gネットワークは情報が細分化されている。このため、法執行機関が利用できないか、アクセスできない場合が増加する。そのため、国内外の多くのインターネット・サービス・プロバイダー（ISP）の協力が



必要となるが、5G技術の特徴として、デバイスがオペレーターのコアネットワークを使用せずに互いに直接通信することがあり、通信データを法執行機関が検索することを難しくする。

・エンドツーエンド (E2E) 暗号化プロトコル

5Gの次の標準化プロセス中に、必須標準としてエンドツーエンド (E2E) 暗号化プロトコルが含まれることになる予想される。端末メーカーが自発的にこの機能を組み込む可能性もある。どちらの場合でも、E2Eによって捜査目的で通信を傍受したとしても、その中身を解読できないようになる。このため、法執行機関が合法的な傍受の枠組みの中で通信の内容分析を行うことが不可能になる。

・ネットワーク機能仮想化 (NFV)

5Gのネットワークの物理的部分の仮想化の結果、既存のセキュリティ対策の多くは無効となる。犯罪者のネットワーク利用も仮想化されることになるので、その捜査は極めて困難となる。

5Gを巡るアメリカと中国の主導権争いが熾烈なものとなっている今日、5Gによるサイバー犯罪の増加の恐れに対する方策の策定を国際機関に求めることは、かなり難しい。トランプ政権による HUAWEI 製品の排除要求にどのように対応するかをはじめとして、セキュリティも含めた5Gに関連する政策決定について、EU加盟国やシンガポール、日本のような国々は難しい位置に立たされている。アメリカにとっては5Gに関する方針に同調するかどうか安全保障上の同盟国であるかどうかの踏み絵になっている面があるが、各

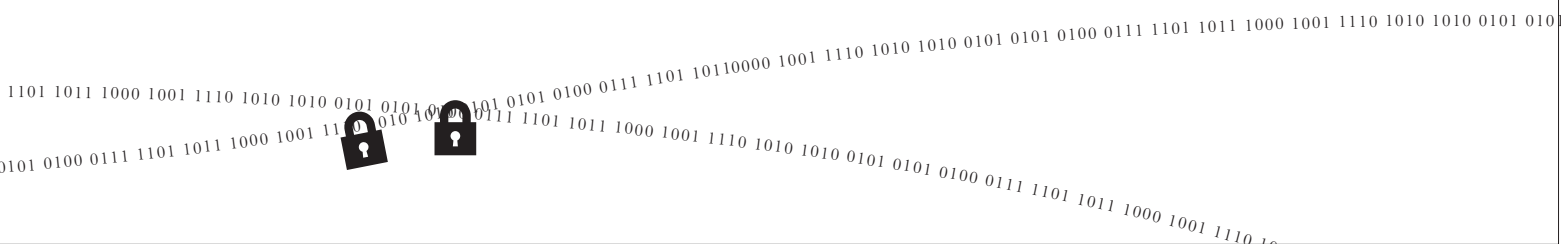
国から見れば、それは独自性や中立性を喪失し、これからの社会の基盤となる5G通信ネットワークのアメリカへの依存度を高め、結果的に社会全体がアメリカに従属する状況をつくり出しかねないという懸念がある。

このような状況の中で注目されるのは、2019年にユンケル委員長の後任として就任したフォン・デア・ライエン委員長の下で、2020年2月に欧州委員会が提示した新たなデジタル戦略⁸⁾である。

新たなデジタル戦略では、これまでの「デジタイゼーション (digitization)」という言葉に代えて、「デジタルライゼーション (digitalization)」という言葉が使われている。デジタイゼーションは、アナログで処理されていたデータのデジタルへの変換を指すものであったが、デジタルライゼーションは、社会の相互作用と社会構造への影響を重視するものであるという。

フォン・デア・ライエン委員長は、新たなデジタル戦略に関連して、三つの目標を提示した。データの取り扱いを「need to know」から「need to share」に変革すること、5G ネットワークに関する基準を整備すること、AI の人間的・倫理的影響について EU 全体が足並みをそろえて対応すること、の三つである。

2020年2月、このデジタル戦略にどのようにユーロポールが対応すべきかについての政策ペーパーが公開されている⁹⁾。その中では、5G についての対応が提案されているが、特に強調されているのは、前述のエンドツーエンド (E2E) 暗号化プロトコルに関する問題を解消するために、暗号化されているデータの復号能力を強化することである。



ユーロポールはIoT機器を含めたインターネットに接続される機器類の解析能力を強化する方針を掲げているが¹⁰⁾、2018年からユーロポールは欧州サイバー犯罪対策センター（EC3）の中に刑事捜査において復号を行うプラットフォームを運営しており、復号のためのツールを提供している。政策ペーパーでは、このような動きを強化すべきであるとし、加盟国間の連携や情報共有も促すべきであるとしている。

ただし、暗号化されているデータへのアクセスは、後述するような法的問題を抱えていることも事実であり、慎重な検討が必要となろう。

3. 法的課題と捜査上の課題

3.1. インターネットに接続される機器類のセキュリティの法的規制

最後に、5Gの本格的な普及を前に、法制度の整備が必要な点は存在するか、捜査上の課題はないかという点について検討してみたい。

法的な論点の第1は、急増していくと予想されるIoT機器のセキュリティについて、法的な規制を行うべきかどうかという点である。

インターネットに接続する機器類のセキュリティ対策を、技術標準やガイドライン等ではなく、法的な規制の下に置くべきかどうかについては、製造物責任法の適用の是非も関連して、これまでも議論が行われてきた。セキュリティ対策の法的義務化については、必ずしも積極的な意見が多かったというわけではないと思われるが、アメリカのカリフォルニア州で「接続

される機器（コネクテッド・デバイス）のセキュリティに関する法律」（カリフォルニア州IoTセキュリティ法）が制定され、2020年1月から施行されたことの影響は大きいであろう。

この法律は、インターネットに接続される機器（コネクテッド・デバイス）のセキュリティを規制するものとしては全米初の州法であり、次のように規定している。

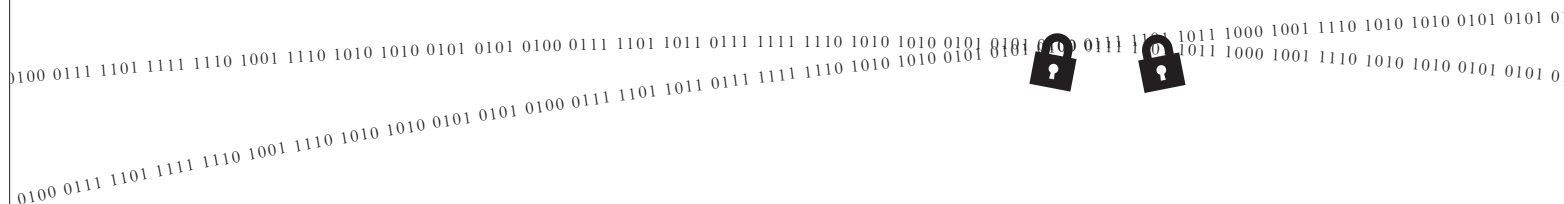
・1798.91.04条

(a)接続される機器の製造者は、当該機器に次の全ての基準を満たす一の合理的なセキュリティ機能または諸機能を装備しなければならない。

- (1)機器の性質および機能に適するもの
- (2)収集し、包有し、または発信することができる情報に適するもの
- (3)機器および機器に含まれる情報を、不正アクセス、破壊、使用、改変または開示から保護するように設計したもの

(b)接続される機器がローカルエリアネットワークの外部に認証手段を備えている場合、(a)項の要件を全て満たすことを条件として、以下のいずれかの要件が満たされている場合は(a)項に基づく合理的なセキュリティ機能と見なされるものとする。

- (1)あらかじめプログラムされたパスワードは、製造された機器ごとに固有のものであること
- (2)当該機器は、初回アクセスが許可される前にユーザーが新しい認証手段を生成しなければならないセキュリティ機能を備えていること



カリフォルニア州IoTセキュリティ法は、インターネットに接続される機器の製造者に対して、合理的な(reasonable)セキュリティ機能を装備することを義務付けるものである。「合理的なセキュリティ機能」とは何かについては条文の中に明記されていないが、機器がローカルエリアネットワークの外部に認証手段を備えている場合、一台一台の機器にあらかじめ固有のパスワードを割り当てるか、デフォルトのパスワードのままでは接続して使用することができないようにすればよいこととされている¹¹⁾。

日本においても、電気通信事業法に基づく技術基準適合証明等(技適)の在り方などについて議論が行われた結果、端末設備等規則及び電気通信主任技術者規則の一部を改正する省令(平成31年総務省令第12号)が公布され、IoT機器にセキュリティ対策機能を実装することが求められるようになった。

また、5Gによって転送される大量のデータの保護については、2018年に不正競争防止法が改正され、限定提供データ制度が設けられた。これまで不正競争防止法では営業秘密を保護対象としてきたが、新たに限定提供データも保護されることとなった。これは、ID・パスワードなどの技術的な管理を施して提供されるデータを不正に取得・使用等する行為を、新たに「不正競争行為」として位置付け、不正に取得・使用した者に対して差し止め請求等ができるようにするものである。

5Gによって大量のデータが送受信されることになると、それを窃取しようとする者も増加することが予想され、個人情報、プライバシーに関わる情報、営業秘

密などの企業情報、各種のセンサー情報などの窃取と不正な利用も増加する恐れがある。現時点では限定提供データに関しては刑事罰の規定が設けられていないが、今後、さらに法改正が行われて不正行為に対する罰則が設けられる可能性もある。

3.2. ログ保存と通信の秘密

法的な論点の第2は、ログ保存の義務化と通信の秘密である。各種のサイバー犯罪の捜査に欠かせないのは、通信情報ログである。5Gの実用化によって同時に多数の機器類がネットワークに接続されるようになる結果、通信ログも、従来と比べて極めて膨大な量になるものと予想される。

通信の秘密の保護の観点から、総務省はログ保存について、記録目的に必要な範囲で保存期間を設定することを原則とし、保存期間が経過したときは速やかに通信履歴を消去(個人情報の本人が識別できなくすることを含む。)する必要があるとしている。保存期間は6カ月とされ、より長期に保存する業務上の必要性がある場合に限り1年程度保存することも許容される、とされている。なお「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律」により、刑事訴訟法197条3項及び4項の規定が新設され、通信履歴の電磁的記録の保全要請等の制度が設けられた。

5Gによって増加すると予想されるサイバー犯罪に対応するため、今後はIoT機器類も含めた通信ログ保存の義務化や保存期間の長期化の議論が起きることも考えられる。しかし、わが国の場合は通信の秘密が憲法

上の規定であるので、その厳格な保護を図る必要があることに加え、大量のログの長期間の保存にはコストを要するため、誰がそれを負担するかという問題点がある（この点に関しては、AIの判断の事後的検証についても、同様の問題が発生する）。

また、通信の秘密の意義については、いわゆる漫画村事件の際にも大きな議論となったが、5Gによって接続される大量の機器類からのデータ送受信についても従来と同じような通信の秘密の解釈が適用されるべきであるかどうかについても、議論が必要であろう。

3.3. 捜査上の課題

IoT機器に関係するサイバー犯罪について、捜査機関はインターネットに接続される大量の機器類について、捜査対象となる機器類とその通信情報ログが保存されているISPの特定を速やかに行い、必要に応じて適切に保全要請等を行っていく必要がある。しかしその際、数万台、数十万台という機器類の中から捜査対象を特定し、数千台、数万台のログを分析するという作業が要求されていくことになると予想される。捜査機関の人員だけでは対応しきれない事態が発生すること考えられるので、ツール類の開発・利用による省力化や、新たなISPとの連携・協力体制の構築も急務となろう。

また、5Gによって接続される機器類のデジタル・フォレンジックについても検討する必要がある。デジタル・フォレンジックについて、デジタル・フォレンジック研究会では「インシデントレスポンス（コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等を言う。）や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術」と定義している¹²⁾。

捜査における5G時代のデジタル・フォレンジック

の課題は、大容量化と大量接続への対応であろう。大容量化については、現在でも大容量のディスク類のコピーや解析にかなりの時間を要しているが、5Gの実現によって分析対象のデータの量は飛躍的に増加する。分析対象となるデータの量、機器類の数が、現在の数千倍、数万倍になるということも予想されるが、新たなツール類の開発・利用によって、解析作業の自動化を進め、限られた人的な資源を高度な解析等に集中することも必要となつてこよう。

5Gによる大容量化の実現は、データの保全という問題も生じさせる。現行の刑事訴訟法の規定では、解析対象となる機器類のデータを保全し、その複写を行って、複写したデータを解析して証拠とすることが認められている。このため、捜査機関は、通常ハードディスク等のデータはそのデータを別のハードディスク等にコピーして、コピーしたデータに対して解析を実施する。しかしログの場合と同様に、5G時代には数万台、数十万台という機器類の中から捜査対象を特定し、機器類の中のデータを保全するという作業が必要となるので、数千台、数万台という機器類のデータを1台ずつコピーするという作業をどのように実施すればよいかが、大きな課題となる。

3.4. 暗号化

データが暗号化されている場合の捜査や捜査機関による解析については、Apple対FBI事件以来、世界的な議論を呼んでいる¹³⁾。暗号化されたデータの捜査機関による復号について、スマートフォンやタブレット、パソコンなどに保存されている人的な作為性や創作性があるものと、5Gによってインターネットに接続される機器類が自動的に収集生成し送受信するものとを同列に扱うべきであるかどうか、捜査機関が暗号化の解除を第三者であるISPやその他の事業者を求めることを許容するかどうかについての議論も必要になると思われる。

第三者である事業者への復号の協力要請や協力義務

化については、2018年末にオーストラリアが事業者による支援 (industry assistance) を新たに規定する通信法その他の法律の改正法 (支援およびアクセス法) を制定したことが注目される¹⁴⁾。

支援およびアクセス法は、通信環境の進展に伴う法執行機関および情報機関の課題を解決するための法律であり、暗号化された通信の拡大を含め、通信環境の進展に伴う法執行機関および情報機関の課題を解決するため、通信サービスを提供する事業者と、インターネットを利用するサービスを提供する事業者の義務を強化するものである。

詳細は、附則 (schedule) 1 から附則4までの部分で定められているが、附則1は民間事業者による産業支援 (Industrial Assistance)、附則2はコンピューターアクセス令状、附則3および附則4は捜索および押収権限の強化、附則5は捜査機関等に自発的に支援する者の免責規定について規定している。本法の下で、オーストラリア国内において通信サービスまたは通信デバイスを提供する全ての事業者は、法執行機関および情報機関の支援の要請に従う義務を有する。この規定は、オーストラリア国外企業、オーストラリア国外に製造工場やサーバーを保有する企業に対しても適用されるので、国外企業に対しても適用されることになる。

附則2に定められている民間事業者による産業支援 (Industrial Assistance) は、政府および通信産業 (民間事業者) が協力して法執行および国家安全保障の調査を行うための枠組みを定めるものであり、次の3種類の事項を可能とする¹⁵⁾。

・技術支援要請

Technical Assistance Request (TAR)

通信傍受機関 (連邦、州および準州の法執行機関、オーストラリア刑事情報委員会)、オーストラリア安全保障情報機関 (ASIO)、オーストラリア秘密情報機関 (ASIS) またはオーストラリア信号局 (ASD) により、

後述する指定通信プロバイダーがTARに基づいて自発的に支援を提供するように求められた場合、そのプロバイダーとその役員、従業員、および代理人は、支援した行為に関する民事法上の免責と、限定的な免責を付与される。

・技術支援通知

Technical Assistance Notice (TAN)

通信傍受機関またはオーストラリア安全保障情報機関の長は、強制命令を発行することができる。通信プロバイダーがTANの下で支援を提供するように要求された場合、通信プロバイダーが現在の能力で支援を行うことができるときは、支援を提供する義務を有する (ただしTANは、プロバイダーがまだ有していない機能を構築することまでを求めるものではない)。

・技術的能力に関する通知

Technical Capability Notice (TCN)

通信プロバイダーがTCNに基づいて支援を提供するように命じられた場合、その支援を提供する機能を新たに構築して、支援を提供する義務を有する。

TCNは最も強い要請であるため、TCNを発出する際には、原則として最低28日間の協議期間を置かなければならない。ただし司法長官が緊急性を認める場合は、協議期間に関する規定は適用されない (317条W)。

法執行機関および情報機関に対する支援内容は、支援およびアクセス法317条Eに次のように定められている。

- ・プロバイダーが電子的保護を解除できる場合には、一つまたは複数の形式の電子保護を解除すること。ただし、プロバイダーは、電子保護の形式を削除する機能を実装することは要求されない。
- ・技術情報を提供すること。
- ・ソフトウェアまたは機器のインストール、保守、

テスト、使用、またはそれらの活動の支援を行うこと。

- ・デバイスまたはサービスへのアクセスを支援すること。ただし、私的なコミュニケーションとデータには、既存の令状の枠組みに準拠した合法的な権限でのみアクセスできる。
- ・サービスの変更を法執行機関および情報機関に通知すること。
- ・本法に基づいて行われた行為を秘匿すること。
- ・令状または許可の発効を促進するか、情報の効果的な受信を可能にする行為を実施すること。

第三者の安全な情報のセキュリティを危険にさらすことは本法の支援内容からは除外されており、第三者のセキュリティを危険にさらす復号化機能の構築、認証または暗号化の体系的な方法の効果を低下させるためのあらゆることは許容されない。

支援対象の要請となるのは「指定通信プロバイダー」(DCP)であり、広範囲のエンティティをカバーするために意図的に広く定義されている¹⁶⁾。支援およびアクセス法317条Cでは、指定通信プロバイダーの一覧を明示しており、その中には通信キャリア等、オーストラリアに少なくとも1人のエンドユーザーがいる電子サービスプロバイダーおよびその関連事業者(Facebook、Google、Amazon Web など)、電子機器の製造業者および関連事業者が含まれている。

4. おわりに

本稿執筆時点で、日本も含めた世界中の国々が新型コロナウイルス感染症とその拡大防止対策による深刻な社会や経済への影響に苦しんでいる。5Gにより実現されると予想されているサービスの中には、新型コロナウイルス感染症をはじめとする未知の疾病の蔓延と共存していかなければならないことが予想される「アフター・コロナ」の社会において、大きな役割を果た

すと期待されるものが多い。

例えば、各国において外出を規制・抑制する施策が取られたことから公共交通機関の乗客が大幅に減少し、特にタクシーは乗客の激減¹⁷⁾により各国で事業者の倒産や運転手の生活困窮という事例が相次いでいるほか、地方のバス事業者等の交通事業者の経営も深刻な打撃を受けている。もともと少子高齢化の進行によって交通事業者の経営が苦しかった地方においては、これを機会に減便や廃止が加速する恐れが強い。他方で、感染者の通院や移動の際には公共交通機関の利用は制限され、感染者以外にも定期的な通院などが欠かせない高齢者などの移動の足をどのように確保するかという問題がある。5Gの普及による自動運転の自動車や無人タクシーの実用化は、このような問題への解決策の一つとなるであろう。

他方で、安心・安全な5G社会を実現するためには、5Gによる犯罪を防止し、適切に捜査ができるような環境を整備することが不可欠である。5Gの負の側面にも目を向けつつ、5Gの利点を私たちが日常生活において享受できるような日が早く到来することを願って執筆することにした。



Harumichi Yuasa

湯浅 壱道

情報セキュリティ大学院大学 副学長

1970年生まれ。青山学院大学法学部卒業。九州国際大学法学部教授を経て2008年九州国際大学副学長。2011年情報セキュリティ大学院大学教授。2020年より現職。一般財団法人日本サイバー犯罪対策センター理事、総務省情報通信政策研究所特別研究員、法制審議会臨時委員などを務める。

注

- 1) 総務省「平成30年度5G総合実証試験の開始」
https://www.soumu.go.jp/menu_news/s-news/01kiban14_02000347.html
- 2) 谷脇康彦『サイバーセキュリティ』(岩波新書、148頁)。
- 3) Klaus Schwab, *What is the fourth industrial revolution?*,
<https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/>
- 4) Schwab, 前注3。
- 5) Joanna Swiatkowska, *Tackling Cybercrime to Unleash Developing Countries' Digital Potential*, Pathway for Prosperity Commission Background Paper No. 33 (2020).
- 6) Tolu Akerele, *Cyber threats on African subjects*,
https://www.ict.org.il/Article/2275/Cyber_threats_on_African_subjects#gsc.tab=0
- 7) https://www.europol.europa.eu/sites/default/files/documents/report_do_criminals_dream_of_electric_sheep.pdf
- 8) European Commission, *Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence*, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273
- 9) Franca König, *Big Data, 5G and AI*,
https://www.hertie-school.org/fileadmin/20200219_Europol_Franca_Koenig.pdf
- 10) Council of the European Union. "Position paper on 5G by Europol" (Council doc. 8268/19). Brussels, April 11, 2019.
- 11) 湯浅壘道「カリフォルニア州 IoT セキュリティ法に関する若干の考察」情報法制研究第5号(2019年) 32頁以下。
- 12) デジタル・フォレンジック研究会「デジタル・フォレンジックとは」<https://digitalforensic.jp/home/what-df/>、安富潔・上原哲太郎編『基礎から学ぶデジタル・フォレンジック』(日科技連、2019年) 2-3頁。
- 13) 指宿信「Apple対FBI問題を考える」法学セミナー 2016年7月号(2016年) 6頁以下、湯浅壘道「暗号化とアメリカ憲法」情報ネットワーク・ローレビュー 15巻(2017年) 83頁以下、湯浅壘道「サイバー攻撃に対するセキュリティ」大沢秀介監修『入門・安全と情報』(成文堂、2015年) 107頁以下を参照。
- 14) 条文についてはオーストラリア議会のウェブサイトを参照。https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/bills/r6195_aspassed/0000%22 また法案内容については、議会の委員会による報告書も参照。Parliamentary Joint Committee on Intelligence and Security, *Parliament of Australia, Advisory Report into the provisions of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, (2018), available at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1.
- 15) Department of Home affairs, Australian Government, *Lawful access to telecommunications*, available at <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-industry-assistance-framework>.
- 16) Arthur Kopsias, *Going Dark: The Unprecedented Government Measures to Access Encrypted Data*, 52LSJ74(2019).
- 17) 2020年5月前半のタクシーの営業収入は、対前年比で33.8%まで落ち込んだという。『東京交通新聞』2020年6月9日。

5G時代の 情報セキュリティ 2

サイバーセキュリティの未来 ——米中対立の先に待ち構える三項対立——

慶應義塾大学 グローバルリサーチインスティテュート 客員所員

小宮山 功一朗 Koichiro Komiyama

技術者による協調で維持されてきたインターネットとサイバー空間において、分断と、ユーザーのデータを囲い込む動きが進行している。この新たなサイバー空間を支配するのは誰なのか。米国の覇権と、それに挑戦する中国という米中対立の図式が通説である。しかしサイバー空間を支配するとは、ある者がより多くのデータにアクセスして、他者の行動に影響を与える能力を持つことである。この競争において、グローバルなテックカンパニーは国家に比肩し得る。米中両国とグローバルテックカンパニーとの間の緊張と協調に着目し、サイバー空間の支配を巡る米国と中国とグローバルテックカンパニーの三項対立という視座を提供したい。

キーワード

サイバーセキュリティ 米中対立 GAFA インターネットガバナンス

第1章 はじめに

サイバー空間はいずれの国家による干渉も受けないグローバルな空間であるべきという主張は、インターネットが発明されたサイバー空間の黎明期から、政治家・官僚・学者・技術者によって繰り返されてきた。多くの国は宇宙、公海、サイバー空間をグローバル・コモンズと見なしており、一国だけの境界設定を主張していたわけではなかった(塩原 2019)。しかし、今

日のサイバー空間は国家単位で分断されつつある。国家によって、インターネットの断片化が進められ、自国民のデータを自国内に囲い込む動きが進行している。

サイバー空間に多くを頼る現代社会において、その支配者は、国家安全保障において有利な立場を約束される。それ故、国際政治学や地政学の研究者はサイバーセキュリティに着目している。

本論文は、繰り返し論じられてきた¹⁾「誰がサイバー空間を支配するのか」という問いに改めて向き合

う。サイバー覇権の行く末を占うことは容易でないが、そのための下準備として、サイバー空間を巡る対立の構図を描き出す。サイバー空間の覇権を米国と中国が争っているという米中対立論 (Triolo et al. 2020; 佐橋 2020) が広く信じられている。現在の米国と中国の間の摩擦を見れば米中対立論の妥当性には疑いの余地は少ない。一方で、その論はグローバルテックカンパニーという第三のグループの影響力を過小評価している。グローバルテックカンパニーとは世界の多数の国において経済活動を行い、加えて情報通信技術分野で競争力を持つ企業群である。サイバーセキュリティの未来は、米中対立でなく、米国と中国とグローバルテックカンパニーの三項対立という構造の上に成り立つのではない。

本論文の構成は次のとおりである。まず第2章ではサイバー空間における米中対立論の背景にある、インターネットとサイバー空間の発展の経緯をひもとく。2010年から2013年の間に、国際社会が米国への信頼を失い、中国が台頭した。第3章では、グローバルテックカンパニーの影響力の拡大を説明する。そして、既存の研究で十分に検討されてこなかった、米国のグローバルテックカンパニーと米国政府の衝突、中国のグローバルテックカンパニーと中国政府の緊張という事象に着目し、三項対立の構図が成立することを論じる。第4章ではこれらの議論をまとめ、日本のとり得る選択肢についても考察する。

第2章 米中の対立

第1節 損なわれた米国への信頼

インターネットは米国で産声を上げた。米国は、今でも技術的に、制度的にさまざまなアドバンテージを持つ。それを米国のサイバー覇権と呼ぶものもある。この米国の優位は、技術開発力と「民主的で自由でグローバルなサイバー空間」というビジョンの両輪によって支えられていた。米国のサイバー空間における

優位は、ブラジルや中国やロシアやサウジアラビアによって批判されてきた。しかし、日本や欧州諸国を含む多くの民主主義国家はこれを支持した。西側諸国と東側諸国の見解の相違があったものの、東西のバランスが取られていたため、大きく政治問題化することはなかった。

転機は2010年から2013年までの間に起こった。まず2010年に、米国においてサイバー軍 (CYBERCOM) が公式に発足した。そして米国がイランの核処理施設をサイバー兵器によって攻撃した、いわゆるスタックスネット事件が公に知られることとなった。次に2013年6月に、元契約職員であるエドワード・スノーデン (Edward Snowden) が持ち出した文書により、米国家安全保障局 (NSA) を中心とするインテリジェンス機関がドイツやフランスや日本などの友好国に対しても、情報収集活動を行っていることが明らかになった。

一連の出来事で、米国が自らの影響力をサイバー空間において躊躇なく行使することが明らかになった²⁾。米国の製品とサービスへの不信が生まれ、350億ドルとも1,800億ドルともいわれる売上の減少が起きたと見積もられている (Staten 2013)。それ以上に米国政府への信頼が損なわれ、米国政府がリーダーシップを失ったことのインパクトは大きかった。これ以降、世界は、米国に代わる新たなリーダーと「民主的で自由でグローバル」に代わる新たなビジョンを模索している。そして、その答えは、国連が主導する、国家主権に立脚した多国間共存であると主張しているのが中国である。

第2節 中国の台頭

中国の国内総生産 (GDP) は毎年7%近い成長をしている。経済成長を支えているのはデジタル技術を活用したビジネスである。デジタル経済の GDP への貢献はおおよそ26.6% (2015年) から32.3% (2017年) まで急増した (Sui & Guan 2018:252)。サイバー空間での影

響力拡大は、中国経済の発展と強固に結び付いており、経済の発展は中国共産党による統治を安定させる。近年の中国は半導体部品などの国産化を強力に推進し、技術的な自給率を高めている。また移動通信の新規格5G関連技術、AI、量子コンピューティングなどの新技術分野への助成も活発に行われている。

中国のサイバー空間におけるリーダーシップへの野心が明確になったのは、2013年に習近平が国家主席となったのとほぼ同時期である。習近平はサイバー空間を通じて全人類が「未来を共有する運命共同体」であると繰り返す(Xi 2015)。そして途上国への技術供与などの国際協力を積極的に打ち出している。

デジタルシルクロードと呼ばれる情報通信技術を用いた中国の影響圏拡大政策は、一帯一路政策の重要なコンポーネントでもある。これはIT企業(アリババ社、テンセント社、バイドゥ社、ファーウェイ社)と通信事業者(チャイナ・モバイル社、チャイナ・テレコム社、チャイナ・ユニコム社)が一帯一路の対象国の市場で成功することを国が支援する取り組みである(Triolo et al. 2020: 1)。中国の支援で、多くの国に海底ケーブル、地上ケーブル、5G通信インフラ、データセンターなどがもたらされている。

一般に中国の製品は安価で、調達までの時間が早い。西側の企業が利用者のプライバシーへの配慮から採用しない技術も用いるため、情報のコントロールという観点で優れている部分もある。中国製品の泣き所は、製品に中国政府と情報を共有するスパイプログ

ラムが埋め込まれているなどのセキュリティ上の懸念である。しかし、今後も中国製品の採用は止まらないだろう。中国製品を使うことによる情報漏えいの確たる証拠が公の場に示されることはなく、中国の情報活動の危険性について問われたマレーシアの首相マハティール・ビン・モハマド(Mahathir bin Mohamad)が「マレーシアにスパイの対象となるような情報があるだろうか?」と強がったように、セキュリティ確保の優先度は国によって異なるからである。

技術開発で、米国に迫ろうとする努力と並行して、中国政府はサイバー空間における「国連が主導する、国家主権に立脚した多国間共存」というビジョンを繰り返している。中国は、サイバー空間において米国の実効的な支配が成立していると考えている。その解決策として、全ての国家が対等に議論できる場で、つまり国連で、サイバー空間の将来を決することを提案している。実現すれば、安保理常任理事国である中国の影響力がさらに強まることは間違いなく、欧米諸国や日本はこれに反対している。

第3節 米中対立の構図の問題点

ここまで、サイバー空間における、米国の影響力の弱まりと中国の台頭を描いてきた。米中対立論の課題も見えてきた。

まず、米国と中国の間の対立がどこまでエスカレーションするかという点は予測が困難である。米中の経済相互依存度は高い。特に中国は、日本の約3倍の3



兆ドルを超える外貨準備を抱える。ドル基軸通貨体制の安定は中国の経済の安定とほぼ同義である。国際政治学者が描く米中戦争という最悪のシナリオ³⁾は双方にデメリットが大きい。米中対立論は、米国と中国が二国に有利な合意をする可能性をあまり考慮していないようである。

もう一つの課題は本論文の主題に直結する。2013年ごろに、サイバー空間の管理の政治性が改めて認識され、インターネット冷戦・デジタル冷戦・インターネットのヤルタ体制など、大国間の競争を連想させるキーワードを使って安全保障学の文脈でサイバー空間が語られるようになった。サイバー空間は陸・海・空・宇宙に続く「第5の戦場」であるといわれることも多い。既存の空間を支配してきた論理を振り返り、応用するのは自然な流れである。研究者たちは第5の戦場を巡る国家間の争いを「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 2018:2)と捉えている。より多くの軍隊がサイバー攻撃能力を備え、より多くのインテリジェンス機関や法執行機関がサイバー監視能力を高めている。国家の役割、軍隊の能力、政府の方針などが分析の対象となってきた。

一方で、サイバー空間は物理的・地理的制約が少なく、行動の単位としての国家や政府の有効性は減少している。米国のインターネット統治の研究者ミルトン・ミュラー (Milton Mueller)は国家間の競争のみを分析する姿勢を、次のように鋭く批判した。

サイバー空間においては独自の利害に基づいた、独自の統治の機構があり、それらは特定の政府の利害と一致しない。もし、我々がインターネット統治を巡る軋轢^{あつれき}を、いずれの国家がライバル国家より力を持つかという視点で捉えるならば、我々の精神は17世紀の産業主義から大きく前進したと言えない (Mueller 2017:19)。

もし、サイバー空間に起こっているのが単純な米中間の競争ではないなら何が起きているのか。次章では、影響力を増しているグローバルテックカンパニーに着目する。

第3章 サイバーセキュリティのトリレンマ

第1節 グローバルテックカンパニー

2015年9月、マイクロソフト社の創業者ビル・ゲイツと最高経営責任者のサティア・ナデラは、ワシントン州レッドモンドにある本社で習近平率いる中国からの訪問者一行と向き合った。当時の米国の大統領バラク・オバマ (Barack Obama) との米中首脳会談のために訪米した習近平は、レッドモンドで8社のハイテク企業の幹部と面会した (Smith & Browne 2019:252)。習近平はなぜわざわざレッドモンドを訪れたのだろうか。中国が、マイクロソフト社や米国のハイテク企業と直接に接触を図るのはなぜなのだろうか。グローバルテックカンパニーの重要性に迫りたい。



サイバー空間を語る上で、それがおおむね民間企業が所有・管理する空間であることは強調しておかないといけない。海底ケーブル、データセンターなどがあって初めて我々は「インターネットを使う」ことができる。それらの民間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し、対価に応じて平等にサービスを提供する存在と捉えるのは単純化が過ぎる。実際のところサイバー空間における民間企業はさまざまな調整の役割を果たして、その行動を支える指針は単に経済的な合理性と決めつけることはできない。

民間企業の中でも、とりわけグローバルテックカンパニーの担う役割は大きい。グローバルテックカンパニーとは、世界の多数の国において経済活動を行い、なおかつ情報通信技術分野で競争力を持つ企業のことである。具体的にはFAAAMと通称される、フェイスブック社、アマゾン社、アルファベット(グーグル)社、アップル社、マイクロソフト社や、BATHと通称されるバイドゥ社、アリババ社、テンセント社、ファーウェイ社などを指す。

グローバルテックカンパニーの市場における、経済的な力は圧倒的である。まずGAFA⁴⁾の合計売上は70兆円以上といわれる。これは世界3位の経済大国である日本の税収60兆円をしのぐ(菊地 2019)。BATHの一つ中国のアリババ社のビジョンは「米国、中国、欧州、日本に次ぐ世界第5位のアリババ経済圏を構築すること」である。2016年における流通総額の実績は60

兆円、これを2020年に110兆円までに成長させることを目標としている(田中 2017: 22)。

グローバルテックカンパニーは鉄鋼、自動車、半導体などの従来の製造産業と異なる。一番先に動いて市場を得たプレーヤーが極めて有利な立場を得る。生産コストがないため、逆転劇が起こりにくい。そしてグローバルテックカンパニーはこれまでの産業との比較において、国に富をもたらさない。企業が雇用を生み、中間層が豊かになり、国の経済が成長するという図式はグローバルテックカンパニーにはことごとく当てはまらない。グローバルテックカンパニーの収益の多くは株価の上昇、配当金の支払いという形で株主に還元される。膨大な売上からの税収についても、さまざまな節税の手法が用いられていることに、税務当局の不満は募っている。国連大学の推計によるとグローバル企業全体の法人税の徴収逃れ額は年5000億ドル(約56兆円)に上るという。労働者への課税ではなく、プラットフォームの活動の拠点、つまりユーザーが存在する位置に基づいて課税するなどの、新たな徴税の仕組みが検討されつつある(クラウド・シュワブ 2019: 14)。

加えて、インターネットやサイバー空間は分散ではなく集約に向かっている。何事も集約して管理するほうが効率が良い。良いサービスが、多くのユーザーを引き付ける⁵⁾。多くのユーザーは多くのデータをもたらす。多くのデータはさらに良いサービスを生み出す。このサイクルが繰り返された結果、少数のグロー



バルテックカンパニーによって多くの人のデータが握られている状態が生まれている⁶⁾。米中両国を股にかけ活躍する台湾生まれのベンチャーキャピタリストであるリー・カイフー (Lee, Kai-Fu) が予測する、「今後もデータの寡占が進み、米国と中国の少数の企業によって独占され、残りの多くはスクラップを拾う」(Lee 2018:169) という未来は絵空事ではない。

第2節 衝突する国家とグローバルテックカンパニー

米国に本拠を置くグローバルテックカンパニーと、米国政府の利害は常に一致するわけではない。グローバルテックカンパニーは自らの成長が、米国以外の市場に大きく依存していることを理解している。2017年時点で、米国のテックカンパニーの収益の6割は米国外からもたらされている (Segal 2017: 68)。米国政府と米国に本社を置くグローバルテックカンパニーとのより直接的なせめぎ合いもある。例えば、NSAはヤフー社に対してサーベイランスプログラムに協力しなければ1日当たり25万ドルの罰金を科すと通知した。暗号ソフトの開発販売をしているRSAセキュリティ社に対しては、必要に応じて当局が復号できるような弱い乱数生成アルゴリズムを暗号ライブラリの標準に設定するよう求め、その対価を支払った。

グローバルテックカンパニーは対抗措置として、より高度な暗号を用いるようになっており、連邦捜査局 (FBI) ですら押収した電子デバイスに含まれる暗号化された情報を復号するのに苦心している⁷⁾。米国政府

はグローバルテックカンパニーの協力を得るために、なだめたり、脅したり、金を払ったりしている。少なくとも、「国家安全保障上の理由で」という但し書きが付けば、企業が政府に無条件に協力するという環境ではない。

米国に本拠を置くグローバルテックカンパニーと中国政府の関係はどう変化していくだろうか。中国市場で最も成功している米企業アップル社の近年の決断は興味深い。中国で2016年に成立した网络安全法は、データを中国の領土内に保存することを義務付けた。欧米の研究者はこれにより、グローバルテックカンパニーが中国市場から離れると予想した。米国に本拠を置くグローバルテックカンパニーは、自国政府が中国の経済政策、政府と民間企業の関係の構造改革を求めていることを理解しているはずであり、自国政府との関係維持を望むグローバルテックカンパニーが中国政府と接近するはずがないという言説が見られた。

この予想は外れ、グローバルテックカンパニーは中国市場にさらに投資を行った。アップル社は2018年に同社のクラウドサービスの中国人ユーザー専用のサーバーを貴州省に設け、グーグル社の中国向け検索エンジン開発もこの時期に行われた。「アップルはアメリカ国内では5万人しか雇っていないけれども、中国で50万人分もの仕事を増やしている」(佐々木 2013:288) ということもあり、米国のグローバルテックカンパニーは中国政府の望む規制をクリアした上で、中国でのビジネスの維持と拡大する道を選んだ。

前節で習近平がマイクロソフト社を訪れたことも、中国政府と米国のグローバルテックカンパニーとの間のギャップを埋めるための努力の一環だったのかもしれない。

では、中国に本社を置くグローバルテックカンパニーはどうだろう。つまりファーウェイ社、アリババ社、テンセント社を我々はどこまで信じることができるのだろうか。西側の政府も、研究者も「共産党が民間部門への影響力を持っている以上、中国企業は国から離れた独立した存在ではあり得ないという懸念に突き動かされている」（ロバート・ウィリアムズ 2019: 71）ようである。確かに米国政府と米国のグローバルテックカンパニーの間の緊張と比べると、中国政府と中国のグローバルテックカンパニーの対立は顕在化していない。実態を外部からうかがい知することは困難である。ここでは、中国は巨大な市場であるが、それでも有限であることを指摘するにとどめたい。中国のグローバルテックカンパニーは近い将来、国内でのユーザー数拡大を望めなくなり、国外市場開拓に取り組むことになる。中国のグローバルテックカンパニーの収益に占める海外の割合が増えるにつれて、中国政府の声の重要性は失われていくだろう。

第3節 三つのグループによるデータを集めるための競争

ここまで本論文では、サイバー空間を巡る米中対立の構図をひもとき、特にグローバルテックカンパニーの力を確認した。これらの議論を受けて、本節では米国と中国とグローバルテックカンパニーの三項対立が成立することを論ずる。

まず対立の争点を明らかにしておきたい。現代のサイバー空間における三項対立は、より多くのデータにアクセスするための競争と捉えることができる。サイバー空間におけるパワー、つまりサイバーパワーとは、より多くのデータにアクセスして、他者の行動に影響を与える能力のことである。データは現代におけ

る戦略資源であり、フェイスブック社がアフリカ諸国でユーザーを獲得しようとするのも、中国政府が個人の購買履歴のデータを得ようとするのも、欧州連合加盟国が欧州域外へのデータの保存を禁ずるのも、より多くのデータにアクセスするための戦術である。そしてサイバー空間を支配する者とは、より多くのデータにアクセスできる者である。

現在のところ、その競争者として有利な位置にあるのは米国と中国とグローバルテックカンパニーであることは既に述べた。三者の関係は右下の図表に示される。

「誰がサイバー空間を支配するのか」というリサーチクエスチョンに答える上で、新型コロナウイルスへの対応は重要な試金石であることを書き添えたい。パンデミックは世界を変えてきた。ペストの流行は、教会の権威を損ない、近代国家による支配の嚆矢となった（船橋 & 細谷 2020）。歴史は、危機に際して有効な対策を打ち出すものがその後の世界で影響力を得ることを示唆している。

それ故に、ウイルス感染者に接触した可能性のある人物を特定する仕組み（コンタクトトレーシング）の技術開発競争の行く末は興味深い。複数の政府は、GPSから得た位置情報を国が所有するデータベースに登録するという方式を採用する。他方で、グーグル社とアップル社は共同でBluetooth通信を使用した、個人情報収集しない、よりプライバシーに配慮した方式を提案している。いち早く効果的なコンタクトトレーシングの仕組みを提供できるのは誰か、より多くの人を受け入れるのはどの方式か、経過を見守りたい。

第4章 まとめ

ここまで「誰がサイバー空間を支配するか」という問いに答えるため、サイバー空間を巡る対立の構図を読者に提供すべく論を進めてきた。第2章ではサイバー空間における米中対立論の背景にある、インター

ネットとサイバー空間の発展の経緯をひもといた。米中の国家間対立とパワーバランスの変化を認めることができた。続く第3章では、グローバルテックカンパニーの影響力が拡大していることを主張した。そして米国のグローバルテックカンパニーと米国政府の衝突、中国のグローバルテックカンパニーと中国政府の衝突という事象に着目し、米国と中国とグローバルテックカンパニーの三項対立の構図が成立すると主張した。

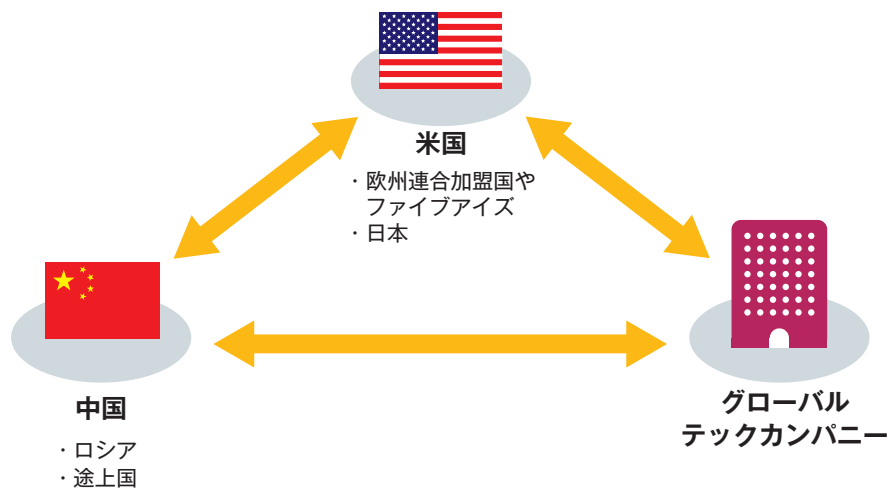
日本は、民主主義などの基本的な価値観を同盟国である米国と共有している。サイバー空間の対立についても米国に同調するのが基本的な行動パターンである。米国との同調は、サイバー空間が国家安全保障と密接に関わるようになって一層強くなった。

もしサイバーセキュリティの問題を米中対立と捉えたと、その議論の出口は、米国と中国の二者のどちらの派閥に所属するかという択一問題となる。言うまでもなく、日本は安全保障で米国を必要とし、同時に経済で中国を必要としている。本論文が三項対立という

構図を提案するのは、それによって、どのようなサイバー空間が好ましいかの議論が始まることを願うからである。現在のところ、三項対立は同時に「米国が掲げる民主主義の普及」「中国が掲げる国家主権の強化」「グローバルテックカンパニーが維持しようとするグローバリゼーション」という三つの価値のコンペティションという側面を持つようである⁸⁾。

日本政府は一貫して情報の自由な流通を訴えている。現在の国際社会において最もリベラルなポジションを取っている。多くの国がインターネットの分断を甘受し、サイバー空間において国家主権を確保し、データを囲い込んで流出を防ごうとしている。日本政府が唱える「信頼に基づく自由なデータ流通(データ・フリー・フロー・ウィズ・トラスト)」という理念を実現するのは、勢いを失っているリベラルな国際秩序をよみがえらせるのと同じくらい困難な作業である。部分的にでも成功を収めるには、米中のグローバルテックカンパニーとのグローバリゼーションを目指す共闘が不可欠ではないか。

図表 サイバー空間の三項対立





Koichiro Komiyama

小宮山 功一郎

慶應義塾大学 グローバルリサーチ
インスティテュート 客員所員
2019年慶應義塾大学大学院政策・
メディア研究科(博士後期課程)単
位取得退学。博士(政策・メディ
ア)。専門分野はサイバーセキュリ
ティと安全保障、サイバー空間の規
範、インシデント対応組織CSIRT
など。JPCERTコーディネーショ
ンセンターの国際部マネージャとし
て、セキュリティインシデント対応
に従事する傍ら、研究を行う。サイ
バー空間の安定性に関するグ
ローバル委員会(GCSC)やFIRST.
Orgの活動に参画。

注

- 1) 例えば持永、村野、土屋(2018)、横澤(2019)。
- 2) 米国中央情報局および国家安全保障局の元長官マイケル・ヘイデン(Michael Hayden)は、サイバー空間での衝突をホームコートアドバンテージと呼んだ。
- 3) 例えばAllison(2017)。
- 4) グーグル社、アマゾン社、フェイスブック社、アップル社の呼称。
- 5) ネットワーク効果による独占や寡占が働きやすい点については、本誌で大木(2018:17)が既に論じている。
- 6) 例えば、米国の3社(グーグル社、フェイスブック社、マイクロソフト社)と中国の1社(テンセント社)が10億人以上のユーザーを獲得している。
- 7) 2017年3月、当時のジェームズ・コーミー (James Comey) FBI長官の発言によれば「FBIは2016年の第4四半期におよそ2,000台の電子デバイスを受け取り、1,200台についてはデータにアクセスできなかった」。
- 8) 紙幅の都合で触れることができないが、トルコ出身の国際経済学者であるダニ・ロドリック(Dani Rodrik)が提唱した「我々は民主主義と、国家の自立と、経済のグローバリゼーションの三つを同時に達成することはできない」というパラドックスはサイバー空間に起こる競争の説明として有効と見込まれる(Rodrik 2012: 181; 林 2020)。

参考文献

- Allison, Graham. 2017. *Destined for War: Can America and China Escape Thucydides's Trap?* Kindle Edi. Houghton Mifflin Harcourt.
- Lee, Kai-Fu. 2018. *AI Superpowers: China, Silicon Valley, and the New World Order*. Kindle Edi. Houghton Mifflin Harcourt.
- Lewis, James Andrew. 2018. "State Practice and Precedent in Cybersecurity Negotiations." *Center for Strategic and International Studies* 9. Retrieved January 9, 2019 (<https://www.csis.org/analysis/state-practice-and-precedent-cybersecurity-negotiations>).
- Mueller, Milton. 2017. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Cambridge, UK: Polity.
- Rodrik, Dani. 2012. *The Globalization Paradox: Why Global Markets, States, and Democracy Can't Coexist*. Kindle Edi. OUP Oxford.

参考文献

- Segal, Adam. 2017. "Chinese Cyber Diplomacy in a New Era of Uncertainty." *Hoover Institution Aegis Paper Series* 1703: 1–23.
- Smith, Brad and Carol Ann Browne. 2019. *Tools and Weapons: The Promise and the Evil of the Digital Age*. Kindle Edi. Hodder & Stoughton.
- Staten, James. 2013. "The Cost of PRISM Will Be Larger Than ITIF Projects." *Forbes.Com*. Retrieved May 29, 2019 (<https://www.forbes.com/sites/forrester/2013/08/15/the-cost-of-prism-will-be-larger-than-itif-projects/#2e699df5795f>).
- Sui, Dang-chen and Yihan Guan. 2018. "Research on 'Combination of Medical Treatment and Endowment' from the Perspective of Digital Economy." pp. 251–54 in *2nd International Conference on Education Innovation and Social Science (ICEISS 2018)*. Vol. 275. ATLANTIS PRESS.
- Triolo, Paul, Kevin Allison, Clarise Brown, and Kelsey Broderick. 2020. *The Digital Silk Road : Expanding China's Digital Footprint*.
- Xi, Jinping. 2015. "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference." Retrieved August 15, 2019 (https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml).
- ロバート・ウィリアムズ. 2019. "米中貿易戦争とファーウェイ — テクノロジー競争の政治学." *フォーリン・アフェアーズ・レポート* 3月号 70–76.
- 大木良子. 2018. "オンラインプラットフォームと競争." *Nextcom* 33:12–21.
- 菊地毅. 2019. "膨張 GAFA 国家が逆襲 (分断の先に) — 富の流出歯止めへ 課税や規制の動き —." *日本経済新聞 電子版*, March 10.
- 佐々木俊尚. 2013. *レイヤー化する世界*. Kindle Edi.
- 佐橋亮. 2020. "米中対立と日本: 関与から戦略的競争に移行する米を中心に." *国際問題* 688: 5–17.
- 塩原俊彦. 2019. *サイバー空間における覇権争奪 — 個人・国家・産業・法規制のゆくえ*. 社会評論社.
- クラウド・シュワブ. 2019. "デジタル世界に即した統治システムを — 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.
- 田中道昭. 2017. *アマゾンが描く 2022年の世界 すべての業界を震撼させる「ベゾスの大戦略」*. PHP ビジネス新書. PHP 研究所.
- 林紘一郎. 2020. "サイバーセキュリティと国際法・国際政治." *ITUジャーナル* 50 (1): 28–32.
- 船橋洋一., 細谷雄一. 2020. "<ポストコロナのメガ地経学 — パワー・バランス / 世界秩序 / 文明> ポストコロナ「日本特殊論」との決別が必要な訳." *東洋経済オンライン*. Retrieved May 19, 2020 (<https://toyokeizai.net/articles/-/347405>).
- 持永大., 村野正泰., 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.
- 横澤誠. 2019. "デジタル・エコノミーの地政学." *外交* 55 (May/Jun): 32–37.

5G時代の 情報セキュリティ 3

5G/IoT時代の 情報セキュリティ

株式会社 KDDI 総合研究所 セキュリティ部門 部門長

杉山 敬三 Keizo Sugiyama

2020年に商用サービスが開始された5Gは、4Gに比べて通信速度の高速化や遅延時間の低減、同時接続数の増加により、センサーや機械、自動車など“あらゆるモノ”がサービスの対象となり、新たな利用形態が創出されることが期待されている。一方、5Gネットワークは従来とは構造等の点で異なる特徴を有しており、新たなセキュリティ脅威も想定される。5Gのもたらすメリットを十分に享受するには、5GネットワークやIoT機器等のセキュリティを確保すること、ハードウェア・ソフトウェアの両面からサプライチェーンの信頼性を確保することが重要となる。

キーワード

5G IoT サプライチェーン セキュリティ

1. はじめに

スマートフォンが急速に普及し、私たちの生活に欠かせない情報通信機器となっている。総務省の令和元年版情報通信白書によると、移動系通信の契約数は2018年度末で1億8,045万となっている¹⁾ことから、1人1台を上回る機器を保有している計算となる。これに伴って移動通信を利用して授受されるデータ量も急増しており、今後も増加が見込まれている。図表1に示すように、移動通信システムの技術規格はおおよそ10年に一度、世代交代しており、最大通信速度は30

年間で約10万倍にもなっている。

2020年は次世代の移動通信システムである第5世代移動通信システム(5G)の商用サービスが開始された年である。当初の5Gは「超高速・大容量」という、これまでの4Gの延長線上の特徴を有するが、段階的に「超低遅延」「多数同時接続」といった新たな技術的な特徴を拡充していく。「超高速・大容量」により、高精細なコンテンツの瞬時のダウンロードや、写真や動画を多用したビジュアルコミュニケーションなど、超高速なモバイルブロードバンドサービスが享受でき、スマートフォンでの通信が今まで以上に快適になる。これに加えて、「超低遅延」「多数同時接続」により“あらゆる

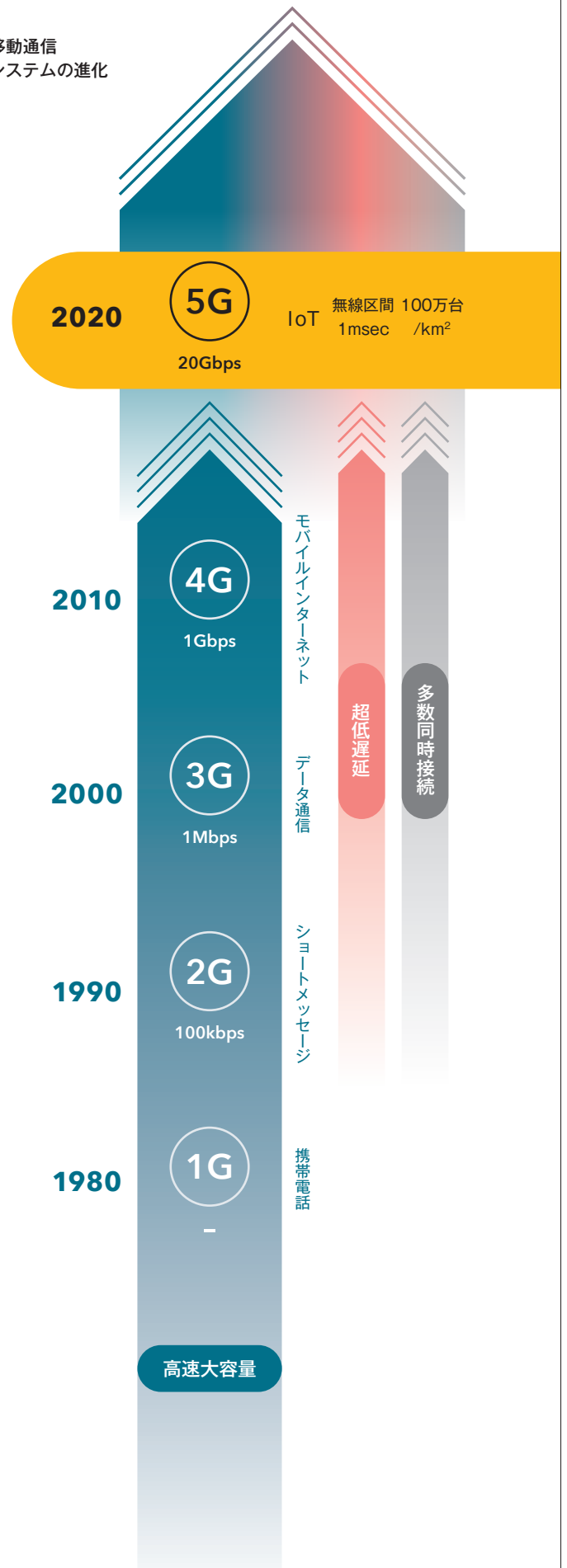
図表1 移動通信
システムの進化

モノ”がサービスの対象となり、新たな利用形態が創出されるものと思われる。

具体的には、今までインターネットに接続されていなかったセンサーや機械、自動車など、モノも含めた通信、いわゆる Internet of Things (IoT) の活用がさまざまな業界において活性化するものと予想される。2019年から2025年の間に世界のIoT接続は2倍の250億台になると推定されており²⁾、ウェアラブル端末やIoT家電といったコンシューマー向けから、農業のような第一次産業での環境センサーの活用、建設機械の遠隔操作など工場や作業現場での活用、スマートシティーなど、あらゆる産業分野でIoT化による経済効果が期待されている。5GによりIoT化が促進され、IoTが生み出すデータと人工知能(AI)がサイバー空間で連動して現実空間にフィードバックすることで、サイバー空間と現実空間が高度に融合するSociety5.0³⁾に進化していくことになる。

また、新型コロナウイルス感染症(COVID-19)の拡大により、社会生活が一変している。外出の自粛に伴い、テレワーク、遠隔授業、オンライン診療、電子契約など、これまでも検討されたり仕組みは提供されたりしたもの、利活用が進まなかった分野において、情報通信技術(ICT)の利活用が急速に進んでいる。今後、5Gの超高速・大容量、超低遅延、多数同時接続といった特徴を活用することで、ICTの利活用が進んでいなかった分野だけでなく、従来は適用できなかったミッションクリティカルな分野においても利活用され、ICTがコミュニケーション手段から真の生活インフラになることが想定される。

このように、5Gは4Gから格段に通信速度が向上するだけではなく、私たちの生活を変える、新たな体験価値を提供できる可能性を秘めているといえる。その一方、5Gは悪意を持つ攻撃者に対しても、新たな機会を提供することになり、その結果、日常生活や経済活動に重大な影響を及ぼしかねない。まず、5Gネットワークにおける新たな機能や構造の変化により、新た



なセキュリティ上の脅威が発生する。また、昨今ではサイバー攻撃の対象がIoTに広がっており、IoT機器の普及に伴い攻撃対象が拡大する可能性がある。さらに、製品の流過程がサイバー攻撃を受けたり、通信機器に不正に侵入するための裏口（バックドア）が組み込まれたりするようなサプライチェーンリスクも高まっている。

本稿では、5Gの概要について述べた後、5Gネットワークにおけるセキュリティ上の脅威を説明し、関連する脅威としてIoTのセキュリティ脅威、および、サプライチェーンリスクについて述べる。

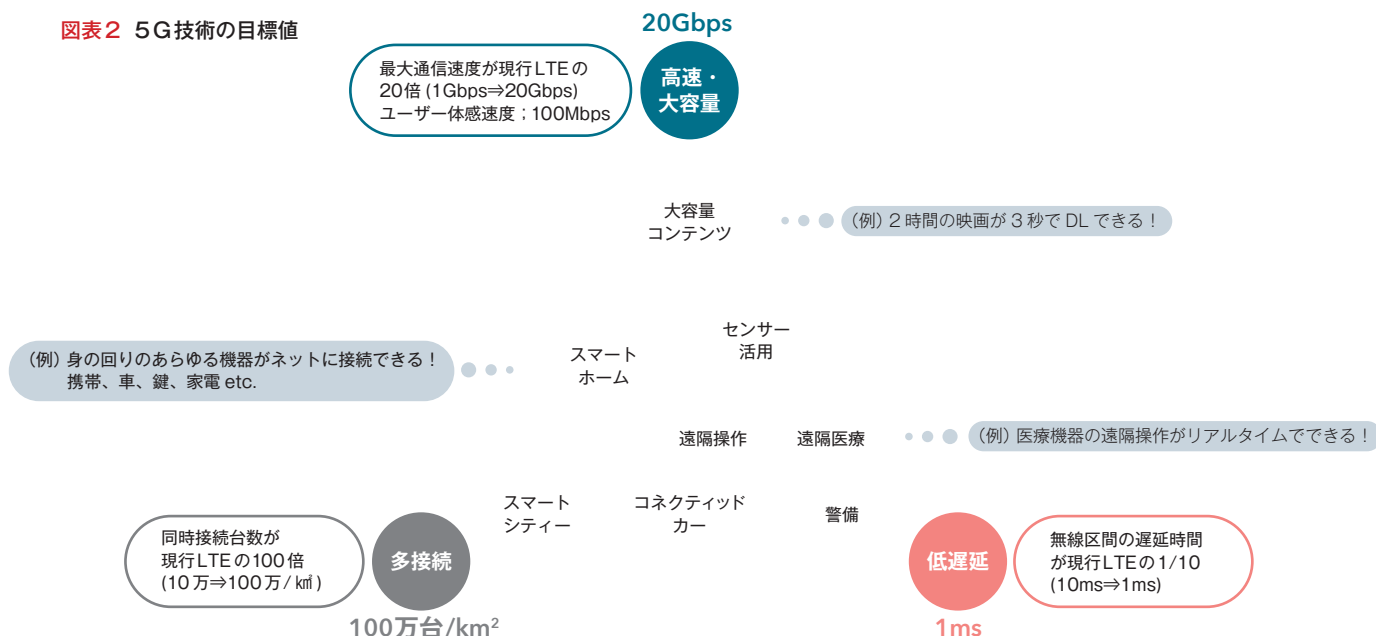
2. 5Gの概要

前述したように、5Gは超高速・大容量、超低遅延、多数同時接続といった技術的特徴を有する。標準化機関である国際電気通信連合（ITU）では、図表2に示すように5Gの技術要件を、4Gの通信規格であるLTEの最大通信速度の20倍に、無線区間の遅延時間が

1/10に、同時接続台数が100倍になるものとして規定している⁴⁾。5Gの超高速・大容量を実現するにはデータ伝送に使われる周波数の幅である帯域幅を広げる必要があるが、4Gが使用する従来の周波数帯だけでは十分な帯域幅の確保が難しく、ミリ波と呼ばれる、より高い周波数も用いることとなった。高い周波数の電波は遠くまで届きにくく、無線基地局の数を増やしたり電波のビームを絞ったりするなどの工夫が必要である。

4Gは、スマートフォンのような人が介在する機器による通信が主であり、通信事業者はユーザーに対して情報配信を効率的に行うことに主眼があった。そのため、通信事業者による移動通信サービスの利用可能なエリアの広さを示す指標としては、サービスエリアがカバーする居住地域の割合である「人口カバー率」が用いられてきた。一方、5G導入に際し、総務省による通信事業者への周波数割り当て審査では、新たに「基盤展開率」という指標が導入された。基盤展開率は、全国を10km四方のメッシュ（約4,500個）に区切

図表2 5G技術の目標値



り、都市部・地方部など人口の多寡にかかわらず事業可能性のあるエリア数を全対象メッシュ数で除した値となる。また、通信事業者が提供する5G ネットワークとは別に、自らの建物や敷地内に自営の5G ネットワークを運営できる「ローカル5G」が2019年12月に制度化された。これにより、地域の企業や自治体が独自のニーズに基づいて柔軟に5G ネットワークの構築が可能となる。

換言すると、5Gは超スマート社会への変革を実現可能にする社会基盤であり、地方部も含めた早期の通信インフラ整備により、IoTやAI技術を通じた課題解決や地方創生へつなげることが求められている。

3. 5G ネットワークのセキュリティ脅威

5Gのネットワークを大別すると、無線基地局などの無線通信を提供する「無線アクセスネットワーク」と、5Gネットワーク機能の中心的な役割を果たす「コアネットワーク」から構成される。コアネットワークは、移動通信の加入者同士を接続する交換機能や加入者情報を管理する各種機能群から構成され、移動端末は無線アクセスネットワークを経由してコアネットワークとの通信を行う。

5Gネットワークのセキュリティ脅威のうち、5G無線アクセスネットワークは4Gを踏襲しつつ機能向上を図っており、本稿では言及しない。5Gコアネットワークはその構造が4Gから大きく変化しており、セキュリティ脅威の例を図表3（次頁）に示した。

これら脅威への対策については、国際的な標準化プロジェクトである3rd Generation Partnership Project (3GPP)等で検討されている。また、諸外国や地域では、それぞれが目指す5G環境の展開において必要とされるセキュリティ対策を策定する動きを見せ始めている。

2019年5月にチェコ共和国のプラハで開催された5G国際会議では、米国や欧州連合(EU)、日本など

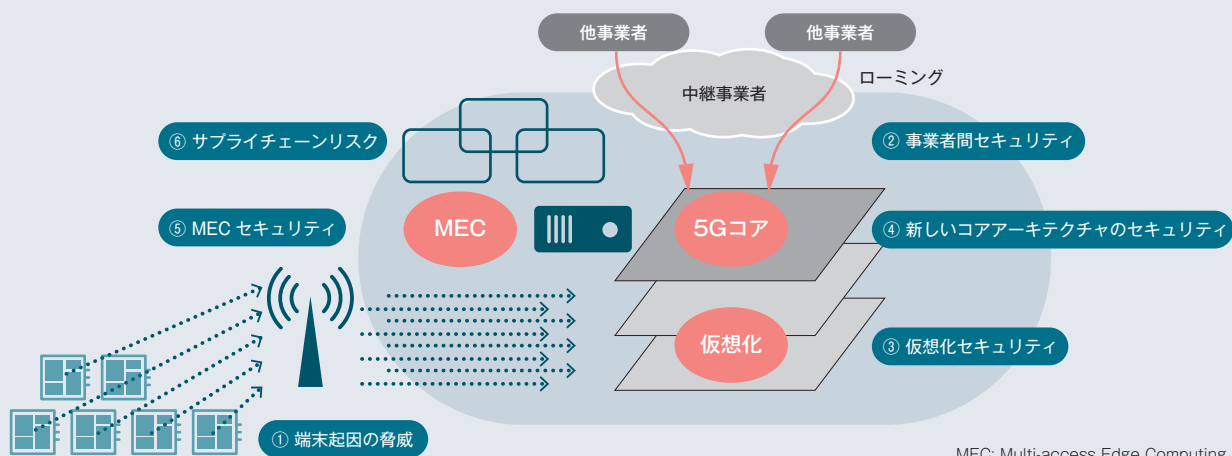
が参加し、5Gネットワークの安全指針を定めた議長声明「プラハ提案」が採択された。欧州委員会(EC)では、2020年1月に、5Gの展開に関連したセキュリティリスクに対応するための5Gセキュリティ基準ツールボックス⁵⁾を策定し、各加盟国に5Gネットワークのサイバーセキュリティ・リスクについて評価するよう要求した。同ツールボックスでは、通信機器の設定ミスや特定サプライヤーへの依存など、九つのリスクに対する具体的なリスク緩和策が挙げられている。米国の国立標準技術研究所(NIST)では2020年5月に、5Gネットワークの構成要素におけるセキュリティ機能の相互運用性確保を支援するプロジェクトを開始した。日本では、総務省が2019年度より「5Gネットワークにおけるセキュリティ確保に向けた調査・検討等の請負」を実施し、5Gネットワーク構築のためのセキュリティガイドラインの作成を進めている。

4. IoTのセキュリティ脅威

IoT機器を狙うマルウェア(悪意のあるソフトウェア)に感染した数十万台のホームルーターやネットワークカメラによる大規模な分散型DoS攻撃が2016年9月に海外で発生し、攻撃を受けた各種のサービスが一時利用不能になった。また、国立研究開発法人情報通信研究機構(NICT)の観測レポート⁶⁾によると、2019年に観測されたサイバー攻撃の通信で最も多いのがIoT機器を狙ったものである。

IoTのセキュリティ対策に関する課題として、セキュリティ上の問題箇所である脆弱性の管理の難しさが挙げられる。PCやスマートフォンで用いられる基本ソフト(OS)であるWindowsやiOS、Android等の場合、利用者が多いため影響も大きい。経済産業省では「ソフトウェア等脆弱性関連情報取扱基準」を定めるなど、対策のフレームワークは存在している。脆弱性が発見され、受付・分析機関に報告されると、公表日の決定や海外の調整機関との連携など適切に管

図表3 5Gコアネットワークに関するセキュリティ脅威の例



① 端末起因の脅威：4G 以前でも存在するが、5G ではIoT 機器のような端末が大量に接続されたり通信量が増大したりすることで、サービスを不能にする攻撃 (DoS：Denial of Service) がより深刻化・大規模化する可能性がある。IoT のセキュリティ脅威については本文で解説する。

② 事業者間セキュリティ：海外の通信事業者など他事業者からの接続 (ローミング) に関するセキュリティであり、5G ではセキュリティを向上させるための仕組みが導入されている。

③ 仮想化セキュリティ：サーバーやネットワーク機器などの物理的な構成に縛られずに、システムやネットワークが論理的な構成で柔軟に構築可能となるのが仮想化である。1 台のサーバーが複数のサーバーのように振る舞うといったように、仮想化技術はクラウドにおいて導入されているが、コアネットワークの設定が複雑化する等により、新たな攻撃対象となる可能性がある。

④ 新しいコアアーキテクチャのセキュリティ：5G コアネットワークは機能追加を容易にする構造となっており、各機能の独立性を高め、機能間では統一的な手順で情報のやりとりを行う。統一的な手順としてインターネットの世界で広く使われている仕組みを採用しており、新たな攻撃対象となる可能性がある。

⑤ MEC セキュリティ：超低遅延を実現するために、クラウドでなく、できるだけ端末に近い部分 (エッジ) に計算機資源を配置する仕組みが Multi-access Edge Computing (MEC) である。通信事業者だけでなく第三者のアプリケーションを動作させることも想定され、外部からの攻撃の対象や攻撃元になる恐れがある。

⑥ サプライチェーンリスク：通信機器は従来、専用のハードウェアで構築されてきたが、汎用ハードウェア上にネットワーク機能をソフトウェアで実現するソフトウェア化 (Network Softwarization) が進展しており、サプライチェーンで不正な機能を混入される恐れがある。サプライチェーンのセキュリティ脅威については本文で解説する。

理され、速やかに対策を施した上で最終的には OS のアップデートなどが行われる。

一方、IoT 機器は、①PCのような高い処理能力を持たず、セキュリティをあまり考慮していない状態で製品開発・出荷されることがある、②いったん、設置されると長期間運用される場合があり、脆弱性が発見されても管理されない未対策のIoT機器が蔓延する可能性がある、③PCのようにセキュリティアップデートを頻繁に行うことも少ないのに加え、ユーザーもIoT機器の脆弱性にあまり関心がなく、ユーザーレベルでの対応も困難である。従って、これまで検討されてきた ICT 分野におけるセキュリティ対策に加え、IoT システム・サービスの動向および特徴を踏まえた、IoT 独自のセキュリティ対策が求められる。

総務省のサイバーセキュリティタスクフォースでは、2017年10月に「IoTセキュリティ総合対策」を公表した。この中で具体的施策として挙げられた主なものを図表4に示す。総務省は2019年2月より、サイバー攻撃に悪用される恐れのあるIoT機器の調査、および、当該機器の利用者への注意喚起を行う取り組み NOTICE (National Operation Towards IoT Clean

Environment)を進めるとともに、2020年4月には、電気通信事業法に基づく端末機器に対し、アクセス制御機能、初期設定のパスワードの変更を促す等の機能、ソフトウェアの更新機能を具備するよう、技術基準を定める省令を改正した。

その他にも、2018年9月に制定された米国カリフォルニア州のIoTセキュリティ法⁷⁾や各種団体のガイドライン等⁸⁾が発行されているが、運用時の対策だけでは不十分であり、IoT システムの企画・設計段階からセキュリティを考慮するセキュリティ・バイ・デザイン (Security by Design)が重要である。

5. サプライチェーンのセキュリティ脅威

サプライチェーンに影響を及ぼすリスクの例として、地震などの自然災害や貿易規制などの政治リスク、パンデミックによるサプライチェーン寸断などが思い浮かぶが、昨今、情報漏えいやサイバー攻撃など、セキュリティに関するリスクへの関心が高まっている。サプライチェーンへの攻撃には、サプライチェーン上の組織に対してサイバー攻撃を仕掛けるも

図表4 IoTセキュリティ総合対策の具体的施策

具体的施策	主な取り組み項目
脆弱性対策に関わる体制の整備	IoT 機器に対するセキュリティ認証マークの付与 セキュリティ検査の仕組み作り 重要 IoT 機器の脆弱性調査 被害拡大防止のための取り組み
研究開発の推進	広域ネットワークスキャンの軽量化 ハードウェア脆弱性への対応 AI を利用したサイバー攻撃検知・解析
民間企業等におけるセキュリティ対策の推進	民間企業のセキュリティ投資の促進 事業者間での情報共有を促進するための仕組みの構築 情報共有時の匿名化処理に関する検討
人材育成の強化	実践的サイバー防御演習の充実 2020 年東京大会に向けたサイバー演習の実施 IoT セキュリティ人材の育成
国際連携の推進	ASEAN 各国との連携 国際的な ISAC (Information Sharing and Analysis Center) 間連携 国際標準化の推進

のと、開発・製造過程等において悪意のあるソフトウェアやハードウェアを製品に組み込むものがある。前者として、2018年に台湾のハードウェアメーカーのアップデートサーバーが攻撃を受け、正規アップデートに見せかけて数十万ユーザーの機器にマルウェアがインストールされた事例があった⁹⁾。後者として、同年に米大手通信会社のネットワーク機器で、海外製のハードウェアに悪意のあるチップが組み込まれていたとの報道があった¹⁰⁾。

特に5Gにおいては、ネットワーク構築に必要な機器の種類が増大するとともに、ネットワークのソフトウェア化に伴い、通信機器の開発や製造、事後の運用保守において悪意のある機能が組み込まれやすくなる懸念がある。通信機器においてもオープンソースソフトウェア (OSS) の活用が増えているが、スマートフォンのアプリケーション開発に利用した OSS にバックドアが仕込まれていた事例もあり、注意が必要である。前述した「IoT セキュリティ総合対策」は2019年には「IoT・5Gセキュリティ総合対策」として公表され、その中でサプライチェーンリスクの管理の重要性を上げている。

米国では、2019年5月に ICT やサービスに関するサプライチェーンを保護するための大統領令が公布され、国家安全保障または安全保障に容認できないリスクをもたらす取引を禁止する権限を商務長官に委譲している。商務省の規則案は、取引禁止の対象企業を名指しはせず、ケースバイケースで取引の禁止を判断する内容となっている。また、米国 NIST では、サプライチェーンのリスク管理に関する主要プラクティス集へのパブリックコメントを2020年2月に開始し、近々最終版をリリースする予定である。

日本では、2018年12月に「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」が行われた。2019年4月には、サプライチェーン全体のサイバーセキュリティ確保を目的として「サイバー・フィジカル・セキュリティ対策フレームワーク」

が公表され、これに基づいてビル分野など各産業におけるセキュリティ対策のガイドラインを策定している。また、セキュアな Society5.0 の実現に向け、戦略的イノベーション創造プログラム (SIP) 第2期「IoT 社会に対応したサイバー・フィジカル・セキュリティ」において、サプライチェーンにおける信頼の創出と確認を行う仕組みを構築するための研究開発を2018年度から進めている。さらに、2019年度には、官民研究開発投資拡大プログラム (PRISM) 「設計・製造におけるチップの脆弱性検知手法の研究開発」において、ハードウェアチップに組み込まれた不正回路を検知するための取り組みも実施された。

以上のように、サプライチェーンリスクの観点から、5G ネットワークのハードウェア・ソフトウェアそれぞれの信頼性を確保するための取り組みの強化が必要である。

6. おわりに

通信は、社会生活や企業活動のあらゆる場面で利用されるライフラインである。移動通信が5Gになることでビジネスチャンスの創出やデジタルトランスフォーメーションの加速が見込まれるが、新たなセキュリティ脅威も顕在化している。5G 技術の標準化においては、4G のセキュリティを踏襲しつつ、脅威事例を踏まえたセキュリティ対策の強化が図られているものの、AI の進展等に伴って攻撃手法も複雑化・巧妙化していること、IoT 機器へのサイバー攻撃はサイバー空間だけでなく現実空間にも影響を及ぼすことから、従来とは異なるセキュリティ対策を講じる必要がある。5G の導入がもたらすメリットを安心して享受できるように、5G ネットワークや IoT 機器等のセキュリティを確保すること、ハードウェア・ソフトウェアの両面からサプライチェーンの信頼性を確保することが重要となる。

本稿では言及しなかったが、コネクティッドカーの

ような5Gを活用したユースケースやサービスに依存したセキュリティ要件、IoTが生み出すモノやヒトに関するデータを保護するための仕組みの検討も必要である。日本では、第5世代モバイル推進フォーラム(5GMF)のセキュリティ調査研究委員会が、5Gを活用した安心安全なサービスに必要なセキュリティに関する調査研究を行っている。

現在、2030年ごろの実用化を見据えて、5Gの次の世代である Beyond 5G/6G に関する研究開発の動きが国内外で表面化している。日本は移動通信の分野で世界をリードしてきたものの、5Gの展開ではグローバル企業との競争で苦戦を強いられている。6Gについてはまだ具体的なコンセプトは固まってはいないが、COVID-19を契機に訪れる社会構造の変化、5Gの利活用で得られたサービスやビジネスに関するアイデア、ならびに、技術の進展なども踏まえ、日本が強みを持つ技術分野としてセキュリティに関する研究開発を強化すべきであろう。



Keizo Sugiyama

杉山 敬三

株式会社KDDI総合研究所 セキュリティ部門 部門長

1987年4月国際電信電話株式会社入社。2001年4月株式会社KDDI研究所出向。2016年8月株式会社国際電気通信基礎技術研究所適応コミュニケーション研究所所長、2018年7月株式会社KDDI総合研究所執行役員、現在に至る。入社以来、OSI(開放型システム間相互接続)プロトコル、EDI(電子データ交換)、ネットワーク管理、ITS(高度道路交通システム)、無線LAN、シームレス通信、ビッグデータ、M2Mの研究に従事。博士(情報学)。

参考文献

- 1) 総務省、情報通信白書令和元年版 PDF 版
<https://www.soumu.go.jp/johotsusintokei/whitepaper/r01.html>
- 2) GSMA, "IoT Connections Forecast: The Rise of Enterprise"
<https://www.gsma.com/iot/resources/iot-connections-forecast-the-rise-of-enterprise/>
- 3) 内閣府、Society 5.0とは
https://www8.cao.go.jp/cstp/society5_0/
- 4) ITU-R M.2083-0, IMT Vision - "Framework and overall objectives of the future development of IMT for 2020 and beyond"
- 5) Secure 5G networks: Questions and Answers on the EU toolbox
https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127
- 6) 情報通信研究機構、NICTER観測レポート
<https://www.nict.go.jp/cyber/report.html>
- 7) 湯淺壘道、「カリフォルニア州IoTセキュリティ法に関する若干の考察」、情報法制研究第5号、2019年5月
- 8) 情報処理推進機構、IoTのセキュリティ
<https://www.ipa.go.jp/security/iot/>
- 9) Kaspersky Corporate News、2019年3月26日
https://www.kaspersky.com/about/press-releases/2019_operation-shadowhammer-new-supply-chain-attack
- 10) Bloomberg Businessweek、2018年10月4日
<https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>

サプライチェーン・レジリエンスの再考

—ブロックチェーン・メカニズムの導入による取り組み—

追手門学院大学 経営学部／同大学院 経営・経済研究科 准教授

崔 宇
Yu CUI

世界情勢の激変や自然災害の頻発が続く中、サプライチェーン・レジリエンス (SCR) の重要性が一層高まっている。一方、既存のサプライチェーン・システムにおいて、SCRの強化を図るには限界があり、SCRの向上とそれに必要な資源投入の均衡点 (適度なレジリエンス) を求めることも難題である。本研究では、サプライチェーンの寸断に至る要因分析から始まり、SCRの研究軌跡に沿って、文献レビューを通じて、SCRの発展・形成のメカニズムを図式化した。また、SCRの向上とブロックチェーン・プラットフォームの構築とのマッチングの根拠を明らかにし、ブロックチェーン・メカニズムを反映させた新しいサプライチェーン・システムの概念図を示した。

キーワード

サプライチェーン・レジリエンス (SCR) システム・アーキテクチャ ブロックチェーン・メカニズム

サプライチェーンの寸断による影響

2020年から全世界に蔓延^{まんえん}してきた新型コロナウイルス感染症 (COVID-19) の影響により、多くの産業や分野が深刻なダメージを受け、COVID-19のパンデミックの拡大により、グローバル・サプライチェーンの寸断が相次いで発生している。同年4月末の時点で、世界の新車販売台数は2019年比14～20%減となっており (Nikkei, 2020)、一方、5月上旬の時点で英調査会社

LMC オートモーティブの調査では、2020年の世界の自動車工場の年間稼働率は49%まで落ち込む見通しとなった (日経、2020)。

COVID-19の拡大によるサプライチェーンへの打撃という視点から、サプライチェーンのレンジごとにカテゴリー化した場合、三つのレンジともに、最も深刻な状態をもたらしている (図表1を参照)。とりわけ、2008年のリーマンショックと2011年の東日本大震災と比べて、規模の度合い・時間的長さ・深刻度は全て最上級なものといえる (崔、2013)。サプライチェーン

の寸断に至るコンテキストとはリーマンショック、3.11 東日本大震災や今回の COVID-19 といった自然災害や 人的災害による外部的・内部的な混乱作用からサプライチェーンの物流・情報流・商流などの運営が予期せぬ方向に乖離させられ、サプライチェーンのメンバーに想像を絶する危機をもたらす一連の負の作用連鎖である。

混乱作用には、サプライチェーンの川上において、原料不足による調達や部品供給の混乱の状況から生産停止が余儀なくされることが挙げられる。サプライチェーンの川下において、商品流通の停滞や市場価格の高騰などによる混乱事態に伴って、企業のキャッシュフローなどの断裂が発生することが考えられる。また、交通手段の封鎖や人流の停滞などにより、サプライチェーンのシステム全体の混乱状態がもたらされ、物流、情報流や商流の全てが機能不全の状況に陥る結末もあり得る。

さらに、突発的事件によるサプライチェーンのダメージ度合いに対して、規模的・時間的・破壊的なインパクトを測ることによって、どのような対処法が適切であるかについて判断することが可能である。例えば、Chan ら (2015) はファジー時系列分析法を用いて、サプライチェーンの混乱作用を予測し、離散事象シミュレーションの手法を使い、突発的事件による

打撃のレベルによって可能な範囲で被害を免れるように事前防止のアラート機能のメカニズムを実証した。Nader ら (2017) はサプライチェーンのシステム再設計によって、危機メカニズムを導入し、新たな配送ルートを構築するシステムの最適化を図るサプライチェーン寸断の対処法を提案した。Zhu ら (2018) はシステム工学の観点からサプライチェーンの寸断による混乱作用をシミュレーションモデルで再現し、サプライチェーン・メンバー間の契約と調整メカニズムの活用がサプライチェーンの寸断による混乱作用の最小化に有効であると例証した。

サプライチェーンへの打撃度合いに対する対処法を下記のクライテリア比較表に加え、サプライチェーンの寸断による混乱作用の解決フレームワークを構想し、サプライチェーン・レジリエンス (SCR) の必要性を強調した。つまり、上述のサプライチェーン上における混乱作用の対処法には限界があり、規模が限定的で、時間が一時的で破壊インパクトが衝撃的なサプライチェーンへの打撃度合いには有効だが、今回の COVID-19 のように、規模が全面的で、時間が継続的で、破壊インパクトが致命的なダメージを受けた場合、サプライチェーンの正常状態への回復には、新たな解決策が必要であり、SCRの実現が必要である。

次節では、SCRに関する近年の研究成果と新たな発

図表 1 サプライチェーンへの打撃に対するクライテリア比較

サプライチェーンのレンジ	リーマンショック	3.11 東日本大震災	COVID-19
上流の調達と供給セグメント	限定的 一時的 衝撃的	全面的 一時的 衝撃的	全面的 継続的 致命的
下流の流通と市場セグメント	限定的 継続的 衝撃的	限定的 一時的 衝撃的	全面的 継続的 致命的
サプライチェーン・システム全体	限定的 継続的 衝撃的	限定的 一時的 衝撃的	全面的 継続的 致命的

● 規模の度合い ● 時間的長さ ● 深刻度

筆者により作成

見について述べる。

サプライチェーン・レジリエンスの研究

1980年代初期のサプライチェーン・マネジメント(SCM)の概念が確立して以来、上述の突発的事件[ブラックスワン(Black Swan)・イベント¹⁾や灰色のサイ(The Gray Rhino)理論²⁾といった不確実性の高い事件を含む]が起こる度に、サプライチェーンのリスクマネジメントやBCP(事業継続計画)などの重要性が挙げられ、レジリエンスの概念も2000年以降、SCM分野の文献から言及されるようになった(Cui, 2012)。レジリエンス(Resilience)とは(システムが)逆境や攪乱^{かくらん}の状態から回復する能力のことである。元々機械学の分野から誕生した言葉として、17世紀に、「材料が弾力的に変形した際にエネルギーを蓄積し(absorb)、解放される時にエネルギーを放出する能力」と定義された(Garcia, 2017)。つまり、最初は物質の弾力や靱性(耐力)を表すために使われていた。19世紀に入ってから、心理学、生物学や社会学などさまざまな分野の研究者によって、レジリエンスの概念とその応用領域が拡大され、充実されるようになった。

一方、SCRの研究は上述のさまざまな分野からの研究成果を吸収しながら、とりわけ、システム工学、コンピューター・サイエンスや経営学領域からの影響を受け、突発的事件への対処やセキュリティ・マネジメントへの展開に焦点を当てた。

Hohenstein ら(2015)の4段階モデルに基づき、さらに、サプライチェーンの寸断による業績の変化パターンを加え、右図のように、SCRの発展・形成のメカニズムを説明できる(図表3を参照)。

図表3で示しているように、まず、予防段階(Readiness)と対処段階(Response)の境線において、突発的事件(ブラックスワン・イベント)が起こり、サプライチェーンの寸断(Disruption)により、業績が継続的に下落していく。サプライチェーンはそれを探知し、素

早く対処しながら、業績の下落スピードを緩和させる。業績の下落に歯止めをかけてから、正常状態に回復しつつ、自己学習のプロセスがスタートする。最終的に、回復段階(Recovery)から成長段階(Growth)にわたって、自己学習のプロセスの完成に伴い、業績がサプライチェーン寸断前より向上し、自己再形成の目標達成になる。言い換えれば、SCRの発展・形成のプロセスはいつも正常状態から均衡が破れ、変形され、また、秩序の整ったレベルに回復しながら、新たな均衡状態に進化していくダイナミックなプロセスである。

SCRの定義はまちまちであるが、大きく三つの視点から代表的なものをまとめることにした(図表4を参照)。つまり、SCRとは複雑で深刻な状況に対して、組織が備えるべきケーパビリティ、あるいは一種の固有能力(回復力)であるが、組織の存在する環境(業態)や組織自身のビジネスモデルによって、定義の着眼点が異なる。

SCRの性能を向上させるために、さらに次のいくつかの視点が大きい参考となる。

(1) SCM 手法の戦略的活用

Peter ら(2015)は、リーン生産方式やシックス・シグマといったSCMの手法を活用し、リスクマネジメントの組織文化と組織間の柔軟な協力を強化することによって、SCRの柔軟性や創造性の向上につながると立証した。また、Wang ら(2015)は、組織の柔軟な体制の構築や戦略的連携をベースとしたセキュリティ整備の実施がSCRの柔軟性と協調性の向上に有効であると論証した。

(2) 事前防御策と事後緊急対応策の実施

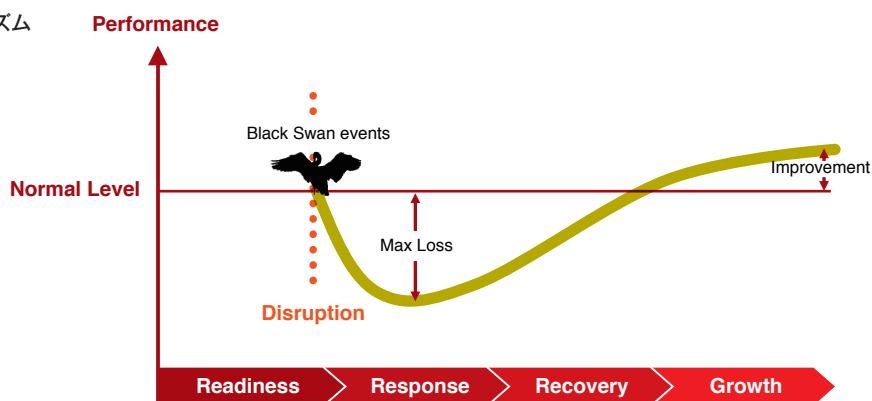
Hohenstein ら(2015)は事前防御³⁾に対して、情報共有、安全在庫(バッファー)の設定、協力関係と緊急計画の事前策定、スタッフのトレーニング、マルチ・サプライヤーによる調達分散化や混乱を監視するため

図表2 サプライチェーンへの打撃度合いによる解決策の選択



筆者により作成

図表3 SCRの発展・形成メカニズム



図表4 SCRの代表的な定義分類

定義の着眼点	SCR の定義	主に向上すべき性能
機敏性と反応力	サプライチェーン寸断に直面する際、あらゆる事態の深刻化に備え、寸断の危機をいち早く探知し、瞬時に反応できる (Chowdhury et al., 2017)。	透明性、冗長性、(上流と下流の) 分散性などの向上
柔軟性と革新力	SCR は一種のダイナミック・ケーパビリティであり、危機が発生後、各種の状況に柔軟に対処でき、万全な調整と改善を行い、新たな理想の状態に進化できる (Elluru S. et al., 2017)。	協調性、創造性、(リーンマネジメントによる) 効率性などの向上
適応性と対応力	突発的イベントが発生する際に、一貫性の維持やシステムの構造と機能の制御を通じて、いかに一定の許容期間内で混乱の状況に適応させながら、正常状態に回復できるように対応する (Ribeiro J. et al., 2018)。	情報共有の水準、システムの知能性 (自己学習力)、安定性などの向上

筆者により作成

の早期警告インジケータの導入を提言した。また、事後緊急対応⁴⁾には、サプライチェーンの機敏性の向上、メンバー間の協力の強化、生産および流通チャネルの柔軟性の確保、混乱に対処するための冗長性の補強などが含まれる。

(3) サプライチェーンの脆弱性^{ぜいじょく}および費用対効果の評価

Berle ら (2015) は、サプライチェーンの脆弱性の評価、混乱軽減策の策定、費用対効果の測定基準に基づくレジリエントな意思決定のメカニズム、シミュレーションによる最適化設計の効果に対する定量分析により、エネルギー産業におけるサプライチェーンの柔軟性を最適化する方法が効果的であることを確認した。つまり、無制限の冗長性向上はかえってサプライチェーンの複雑さと管理コストを増加させる結果をもたらす。生産サービスの継続性を確保するために、サプライチェーンの脆弱性および費用対効果の測定基準に沿って、必要な資源を余分に保持することによって、貴重な冗長性を確保することができ、SCR の性能向上に真の効果が期待できる。

(4) サプライチェーンのエンティティ間のトポロジー関係の強化

サプライチェーンはエンティティ (メンバー) 間のトポロジー関係で構成されており、突発的事件に対して、エンティティ自身の混乱に対処する機能を備えるべきであり、参加エンティティの多様性、およびエンティティの自己適応性の維持が SCR の性能向上に有効である (Jamison, 2015)。言い換えれば、エンティ

ティ間のトポロジー関係を通じて、エンティティ間のクラスタリングと接続性、短いエンティティ間の距離や高いエンティティ間の冗長性といった特徴を生かし、サプライチェーン・ノードの柔軟性を高めることが可能である。

(5) 双面性 (Ambidexterity) の効果

双面性とは既存資源の適応性と新しい機会に挑戦する素質を兼備するダイナミック・ケーパビリティと定義付けられている (Lee et al., 2016)。Lee ら (2016) の実証研究から、構造方程式モデリング手法を用いて、ダイナミック・ケーパビリティを通じたサプライチェーンの双面性によって、突発的事件後の混乱の悪影響が軽減され、SCR の性能向上に効果的であることが確認された。また、Hohenstein ら (2015) により企業の創造性、イノベーションの度合い、サプライチェーンの寸断による混乱の深刻度、SCR という四者間の関係について、データ検証が行われた結果、企業の創造性とイノベーションの度合いは SCR と正の相関関係になっており、企業のイノベーションは SCR を推進する重要な駆動力であることが確認された。

以上の叙述から、SCR の性能が高いほど、混乱作用に対処する際のパフォーマンスが高く期待できるが、実際に SCR を最適化するには、高額のコストがかかる。制約なしにレジリエンスを高めると、企業の利益が浸食され、本来の SCM の理念に反することになる。次の節では、SCR の性能を向上させる際、注意すべき点について明らかにし、現時点における、SCR 実現の問題点と課題を述べる。

SCR 管理の必要性と SCR 実現の課題

リスクはSCRに対する挑戦であり、資源の投入はSCRを強化する要素である。両者間のマッチング度合いは、SCRの性能発揮とサプライチェーン・ノードのパフォーマンスに直接影響を及ぼす。リスクが高く、資源投入率が低い場合、SCRの性能が低過ぎて混乱に効果的に対処できず、サプライチェーンがリスクにさらされ、サプライチェーンの寸断および寸断による損失をもたらす可能性が増す。逆に、リスクが低く、資源投入率が高い場合、過度のレジリエンスは過度に高いSCR強化コストをもたらす、サプライチェーンの全体的な利益を損なう。リスクのレベルが資源投入率と一致する場合にのみ、適切なSCRの発揮により、競争優位を獲得できる。従って、SCRを適切に管理し、適度なレジリエンスを維持することによって、サプライチェーンの存続と発展を促進することが可能になる。

サプライチェーンの協調と最適な設計を達成することは、適度なレジリエンスを形成する効果的な手段である。サプライチェーン協調とは、サプライチェーンのメンバー間の物流、情報流、商流に基づいて、適切な協調インセンティブ・メカニズムを設計することである。また、システムのシーケンスパラメーターを制御することにより、システム全体が無秩序から秩序まで効果的に制御され、協同の状態を達成し、システムの全体の利益を最大化にするものである。

Shukla (2011)はリスク許容度を考慮し、インフラストラクチャーコスト、マテリアルハンドリングコス

ト、輸送コストの観点からサプライチェーンの堅牢性と整備コストを定義した。また、サプライチェーン寸断のシナリオの発生数と発生確率に基づいて予想される寸断によるコストを定義し、効率と堅牢性の重み付けを検討し、混合整数線形計画法モデルを定式化した。さらに、緊急対応の観点からサプライチェーン構造の最適化を行うことにより、適度なレジリエンスの下でいかにサプライチェーンを最適化するかについてより明確な方法論を提示してくれた。

一方、上述のように、2000年以降、SCRの研究が盛んになり、多くの研究成果が収穫されていると同時に、問題点と課題も多く顕在化してきた。

(1) SCRの研究が近年注目されるようになったが、それまでに、リスクマネジメントという領域でカバーされてきたため、サプライチェーンへの打撃の深刻度などについて、あまり区別せず、研究対象や必要性の有無なども問わず、一律にSCRの研究範疇にくく^{はんちゆう}る傾向がある。図表2で示しているように、まず、サプライチェーンの寸断がどのレンジで発生しているのか、時間的に短期的なものかどうか、深刻度がどのレベルのものなのかなどについて、基準を設け、測る必要がある。今回のCOVID-19による大規模なサプライチェーンの寸断が発生しているが、川上、あるいは川下のみならず、システム全体のダメージが致命的であるため、今までのSCRの手法では根本的な解決策を提示することが難しいと考えられる。

(2) SCRの性能を評価する手法は多く提案されているが、ほとんどSCRの結果に基づく評価基準に従って

測定と分析を行っており、ダイナミックな評価方法を導入する必要がある。確かに、現在のサプライチェーンのシステムにおいては、サーバー／クライアント式のアーキテクチャが主流であり、中央集権から分散処理への仕組みとなっている。それ故、ローカルのネットワークにおいて、リアルタイムのデータ収集や検証などの作業を行うことは困難といえる。

(3) SCRの性能を最適化する研究において、モデリングを行い、最適化要素、最適化シーケンス、および最適化方策を提示するなどさまざまな点があるが、その多くは準備段階と回復段階の緊急対応の部分に焦点が当てられており、対処段階の適応の部分と成長段階においてSCRの最適化を図る研究はまれである。

以上の問題点を基に、新たにサプライチェーンの寸断の要因から最も深刻な課題を取り上げ、システム・アーキテクチャの視点からSCRの性能を最適化する方法論を考案し、サプライチェーン・システムの再構成を考えていきたい。つまり、今回のCOVID-19のように、システム全体にわたって寸断による混乱作用が及んでおり、長期的かつ致命的なダメージを根本的に取り除くには新しいシステム・アーキテクチャへのトランジションが必要である。次節では、この新しいシステム・アーキテクチャ、すなわち、ブロックチェーンの特徴を紹介し、今後のSCRの性能の充実にいかに効果的な役割を果たすかについて明らかにしたい。

ブロックチェーンの特徴

2008年に世に登場したビットコイン (BTC, Bitcoin) の基本技術として知られるようになったブロックチェーン (Blockchain) は、全ての取引記録を登録するために使用される、一種の分散型台帳技術 (DLT, Decentralized Ledger Technology) である (Swan, et al., 2015)。誰でもブロックチェーンのネットワークに参加でき、各デバイスをノードにすることができる。各ノードはデータベースの完全なコピーを取得できる。ノードはコンセンサス・メカニズムに基づいており、ブロックチェーン全体は競争力のある計算によって維持される。いずれかのノードに障害が発生しても、残りのノードは正常に機能し、従来の中央集権型システム・アーキテクチャが攻撃や改ざんに対して脆弱であるという問題を解決している。次に、いくつかのブロックチェーンのメカニズムを通じて、その特徴を詳しく説明していく。

(1) 自律分散型メカニズム

自律分散型 (Decentralized) メカニズムは、ブロックチェーン技術の最大の特徴である (Maria-Lluïsa Marsal-Llacuna, 2018)。一般的に、組織 (間) にはリーダーがおり、他の参加者はそのリーダーの指示に従って行動しているが、いざシステムが大規模な麻痺状態に陥り、あるいは、深刻なダメージを受けた場合、自律分散型システムはその固有のレジリエントな素質が発揮できる。ブロックチェーンのシステム・アーキテクチャでは、分散型会計と記録を行うことで、どの



ノードの権利と義務も等しくなっている。言い換えれば、システムの全ての参加者が情報提供者と意思決定者になることができる。これにより、情報がより多様になるだけでなく、エラーの確率が大幅に減少する。サプライチェーンの寸断による緊急対応の場合、システムに関わる情報の適時性の欠如が大幅に解決される。自律分散型のアーキテクチャは、収集された情報の多様性と適時性を促進し、関連するさまざまな組織間の情報交換の円滑性と情報の対称性を保証できる。

(2) セキュリティ・メカニズム

ブロックチェーン技術は強力なセキュリティを提供でき、すなわち、分散型台帳技術(DLT)である(Kshetri, 2017)。つまり、ブロックチェーン内の分散型台帳は改ざん不可能である。言い換えると、いったんデータが検証され、ブロックチェーンに追加された後、それは永続的に保存され、保存されたデータを変更することは非常に困難である。このメカニズムにより、データの安定性、セキュリティ、信頼性が大幅に保証され、外部からの攻撃を防ぐ効果も大いに期待できる。このような特徴は、SCRの補強において、非常に重要な役割が發揮できる。今までサプライチェーンの寸断による深刻度の予測と分析のほとんどの方法は、過去の履歴データに基づいている。分散型台帳技術がSCRの研究・分析に使用されると、データの信頼性と即時性が保証され、ダイナミック・ケーパビリティの開発と検証に大いに有効である。

(3) コントラクト・メカニズム

ブロックチェーンのスマート・コントラクト(Smart

Contract)は、より公正で公平なコントラクト・メカニズムである。コントラクト・メカニズムの特徴は、トランザクションの当事者双方がプログラミングを通じてさまざまなトランザクション条件に同意できるため、当事者双方の権利と義務、およびコントラクトの実行が保証されることだ(Kshetri, 2018)。スマート・コントラクトは、さまざまなプログラムルールが適用するシナリオと領域で効果的である。突発的事件の発生時に、サプライチェーン・システムにおいて各ノードが互いに通信し、自動的に役割分担を合意して、緊急対応のプロセスを効率良く成し遂げることができる。また、スマート・コントラクトは、ノード間の関係を効果的に協調し、双方に満足のいく契約関係を確立し、サプライチェーンの寸断時に、システム全体の安定性を保ち、SCRの資源投入の公平性と効率性を向上させる。

(4) 共有メカニズム

ブロックチェーンの共有メカニズムによって、ブロックチェーン内の情報が、一部の個人・機密情報を除いて、全ての参加者に公開される。サプライチェーン寸断時の交通の閉鎖や担当者の不在による供給の停滞や顧客対応の不足などの問題の多くは、物が地域ごとに止められ、各地域の実際の状況はその地域に精通している人にしか分からないため、情報の非対称性が発生し、多くの時間やエネルギーのロスが余儀なくされることである。ブロックチェーンの情報共有(透明性)の徹底化により、各地の担当者の情報が常に平等に保たれており、自律分散型システムの効果が最大に發揮され、SCRによる混乱対処への資源投入も最小限



に抑えられる。それによって、サプライチェーンの寸断時でも物流・情報流・商流のスムーズな運営が確保され、担当者（経営者）の意思決定基準がより正確になり、意思決定コストが削減され、意思決定の精度と役割分担の合理性が高められる。

（5）パフォーマンス・メカニズム

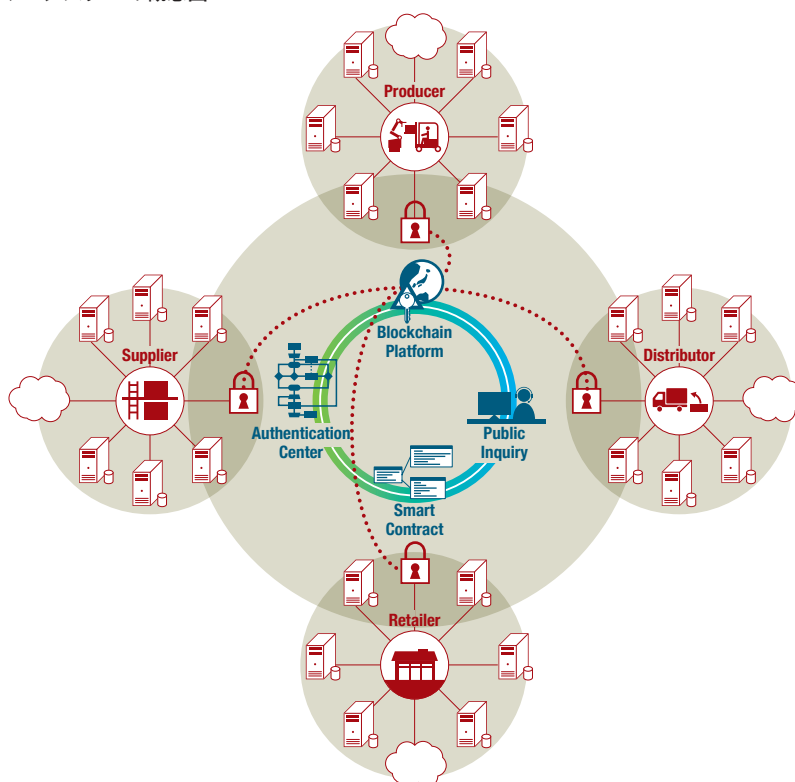
ブロックチェーンのP2P（Peer to Peer）伝送技術は、サプライチェーン全体の運営パフォーマンスを向上させる。P2P伝送⁵⁾は、もともとビットコインの経済取引に使用されていたが、ブロックチェーン技術の発展により、徐々に多くの分野に適用されるようになった。サプライチェーンの寸断時に、システムのノード間の接続でP2P伝送技術を使用できる場合、物理的に

遮断されたローカル・ネットワークから、最低限の情報通信が可能となり、SCRの補強に関わるデータ伝送やコミュニケーションのコストと時間が大幅に削減できる。

SCR性能の向上を導くブロックチェーン・プラットフォームの構築

上述のように、SCR性能の向上とブロックチェーン技術のメカニズムが非常にマッチングしており、今後の突発的事件の頻発やダメージの深刻化などを見据えて、いち早くサプライチェーンのシステム・アーキテクチャのトランジションを行うことが肝要である。また、図表1の部分でも述べているように、サプライ

図表5 ブロックチェーン・プラットフォームを位置付けたサプライチェーン・システムの概念図



チェーンへの打撃度合いがひどいほど、物流・情報流・商流の正常の運営ができなくなり、とりわけ、人間の動きが最も制限され、既存のサプライチェーン・システムの下では、自ら、即時に効果的な対応を講じることが困難であり、SCRの有効な役割発揮を期待することも限界がある。

そこで、サプライチェーンが最も深刻なダメージを受けた場合を想定し、人間の活動を最小限に抑え、ブロックチェーン・メカニズムを最大限に発揮できるように、新たなサプライチェーン・システムの概念図を考案した(図表5を参照)。

図表5では、四つの典型的なサプライチェーンのメンバーであるサプライヤー (Supplier)、製造メーカー (Producer)、流通業者 (Distributor)、および小売業者 (Retailer)によって構成され、さらに、それぞれのメンバーには自社が関わっているネットワークも存在する。四つのネットワークがブロックチェーン・プラットフォームによって接続され、ネットワーク上の他のプレイヤーは全員このブロックチェーン・プラットフォームに参加している。

このブロックチェーン・プラットフォームにおいては、参加者の協力によって前述のブロックチェーン・メカニズムが発揮され、自律分散型の情報収集・伝達、データの安定性・セキュリティ・信頼性の保証、スマート・コントラクトによるシステムの公平性の確保、情報共有の徹底化による情報の非対称性の排除、およびP2P伝送技術によるパフォーマンスの向上といった特徴が徐々に反映される。また、ブロックチェーン・プラットフォームの構築によるサプライチェーン・システムのトランジションを実行することで、SCRの性能の向上と資源投入率の低下をもたらし、SCRの最も効果的な実現に貢献できる。

結論と展望

世界情勢の激変や自然災害の頻発が続く中、サプラ

イチェーン・レジリエンスの重要性が一層高まっている。一方、既存のサプライチェーン・システムにおいて、SCRの強化を追求するには限界があり、SCRの向上と資源投入の均衡点(適度なレジリエンス)を求めるのも難題である。

本研究では、サプライチェーンの寸断に至る要因分析から始まり、サプライチェーンへの打撃の程度を規模の度合い、時間的長さ、および深刻度という三つの角度から検討し、今回のCOVID-19のような最も深刻な状況に対して、伝統的なリスクマネジメントの手法で解決する難しさを示した。次に、SCRの研究軌跡に沿って、文献レビューを通じて、多くの研究成果をオリジナルに分類し、SCRの発展・形成のメカニズムについて図式化した。以上の研究から、現段階のSCR研究の限界と問題を分析し、サプライチェーンのシステム・アーキテクチャのトランジションを行う必要性について論証した。つまり、サプライチェーン・システムを再設計し、ブロックチェーン・プラットフォームを構築する解決案を提示した。また、SCRの向上とブロックチェーン・プラットフォームの構築とのマッチングの根拠を明らかにし、ブロックチェーン・メカニズムを反映させた新しいサプライチェーン・システムの概念図を示した。

現在、既に多くの企業がサプライチェーン・システムにブロックチェーンのメカニズムを導入しようと試みているが、既存のシステム・アーキテクチャとの互換性の問題やブロックチェーン技術自体の未解決の問題などさまざまな課題に直面していることは事実である。しかし、現時点では、SCRの向上に最も適したソリューションはブロックチェーン・メカニズムの導入と考えており、今後、ブロックチェーン技術の充実化とサプライチェーン・システムのトランジションの早期実行を期待し、継続的にブロックチェーンとSCRの融合の実現に向けて努めたい。



Yu CUI

崔 宇

追手門学院大学 経営学部／同大学院 経営・経済研究科 准教授
 博士（経営学）2009年 オーストラリアMacquarie University, Master of Commerce in Information Systems and Technology and Master of Information Technology取得。
 2010年大阪市立大学都市研究プラザG-COE特別研究員。その後、大阪市立大学商学部、岐阜経済大学経営学部を経て、2018年より現職。専門は経営情報学、オペレーションズマネジメント。現在、同大学オーストラリア・アジア研究所副所長を兼任。オペレーションズ・マネジメント&ストラテジー学会理事（2018年～）。

注

- 1) ブラックスワン・イベント (Black Swan events) とは、通常、市場での連鎖反応をもたらし、さらには人間の常識の転覆さえ引き起こす非常に予測できない異常な事象を指す。17世紀末、白い白鳥しか見たことのないヨーロッパの人がオーストラリアで初めて黒い白鳥を発見したことが由来といわれ、特に、事前に予測不可能で起きた後のインパクトや影響などがあまりにも大きい事件のことである。
- 2) 灰色のサイ (The Gray Rhino) 理論とは、長い間、問題の兆候が見られるが、十分な注意が払われず、無視され、重大な結果を伴う事件が発生することを指す。灰色のサイはMichele Wucker (2016) が最初に提起したもので、一種の高確率の危機であり、さまざまな分野で繰り返し起きている。
- 3) 事前防御とは、混乱が発生する前に事前設定することで、一部の混乱作用を吸収し、サプライチェーンの寸断の可能性を最小限に抑えることである。
- 4) 事後緊急対応とは、サプライチェーンの寸断後に、迅速に回復するように対応し、継続的な寸断や崩壊を回避することである。
- 5) P2P伝送とは、中間ノードによる監視を必要とせず、多層の監査も通さずに、両ノード間で直接に信頼を確立することである。

参考文献

- 日本経済新聞社 (2020) 世界のメーカー工場稼働率49%、日本経済新聞朝刊、2020年5月13日、p3。
 Nikkei Monozukuri (2020) 世界の自動車販売は19年比14～20%減 感染再拡大なら最悪2021年まで影響残る、日経BP社、May 2020、p56。
 崔 宇 (2013) サプライチェーン・レジリエンス実現に向けての意思決定モデル、＜特集＞リスクマネジメント、日本情報経営学会誌、34巻 (2013) 1号。
 Azad, N., Davoudpour, H., Saharidis, G.K.D. et al. (2014) A new model to mitigating random disruption risks of facility and transportation in supply chain network design. *The International Journal of Advanced Manufacturing Technology*, Vol. 70, pp.1757-1774.

参考文献

- Berle, Ø., Norstad, I. and Asbjørnslett, B.E. (2013), Optimization, risk assessment and resilience in LNG transportation systems, *Supply Chain Management*, Vol. 18 No. 3, pp. 253-264.
- Chan, Felix T.S.; Samvedi, Avinash; Chung, S.H. (2015) Fuzzy time series forecasting for supply chain disruptions, *Industrial Management & Data Systems*, Volume 115 (3): pp. 419-435.
- Chowdhury, Md Maruf H. & Quaddus, Mohammed (2017) Supply chain resilience: Conceptualization and scale development using dynamic capability theory, *International Journal of Production Economics*, Elsevier, vol. 188 (C), pp.185-204.
- Cui, Yu (2011) A theoretical analysis of sustainable supply chain realization, *Journal of Information and Management in Japan*, Japan Society for Information and Management, 31(4), pp.100-111.
- Cui, Yu (2012) Literature review in SCM studies and future outlook, *The Business Review*, The Society of Business Research Osaka City University, 63 (2), pp.43-70.
- Elluru, S., Gupta, H., Kaur, H. et al. (2019) Proactive and reactive models for disaster resilient supply chain. *Ann Oper Res* 283, pp.199–224.
- Garcia, Emilio (2017). *Unravelling sustainability and resilience in the built environment*. Vale, Brenda. London. ISBN 978-1-138-64402-1. OCLC 956434144.
- Golgeci, Ismail; Pomomarov, Serhiy Y. (2013) Does firm innovativeness enable effective responses to supply chain disruptions? : an empirical study, *Supply Chain*, Vol. 18.2013, 6, pp. 604-617.
- Hohenstein, N.-O., Feisel, E., Hartmann, E. and Giunipero, L. (2015), "Research on the phenomenon of supply chain resilience: A systematic review and paths for further investigation", *International Journal of Physical Distribution & Logistics Management*, Vol. 45 No. 1/2, pp. 90-117.
- Jamison M. Day (2014) Fostering emergent resilience: the complex adaptive supply network of disaster relief, *International Journal of Production Research*, 52:7, pp.1970-1988.
- João Pires Ribeiro, Ana Paula Barbosa-Povoa. (2018) Supply Chain Resilience: Definitions and Quantitative Modelling Approaches – a literature review, *Computers & Industrial Engineering*, Vol.115, January 2018, pp.109-122.
- Junwei Wang ; Raja R. Muddada ; Hongfeng Wang et al. (2016) Toward a Resilient Holistic Supply Chain Network System: Concept, Review and Future Direction, *IEEE Systems Journal*, Volume: 10 , Issue: 2 , pp. 410 – 421.
- Kshetri, Nir. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy, *Telecommunications Policy*, Volume 41, Issue 10, November 2017, pp.1027-1038.
- Kshetri, Nir. (2018). 1 Blockchain's roles in meeting key supply chain management objectives, *Int. J. of Information Management*, Volume 39, April 2018, pp. 80-89.
- Lee, S.M. and Rha, J.S. (2016), Ambidextrous supply chain as a dynamic capability: building a resilient supply chain, *Management Decision*, Vol. 54 No. 1, pp. 2-23.
- Maria-Lluïsa Marsal-Llacuna. (2018). Future living framework: Is blockchain the next enabling network, *Technological Forecasting and Social Change*, Volume 128, March 2018, pp.226-234.
- Peter Mensa, Yuri Merkuryev. (2014) Developing a Resilient Supply Chain, *Procedia - Social and Behavioral Sciences*, Volume 110, 24 January 2014, pp.309-319.
- Shukla, A., Agarwal Lalit, V. and Venkatasubramanian, V. (2011), Optimizing efficiency-robustness trade-offs in supply chain design under uncertainty due to disruptions, *International Journal of Physical Distribution & Logistics Management*, Vol. 41 No. 6, pp. 623-647.
- Swan, Melanie. (2015). *Blockchain: blueprint for a new economy*, O' Reilly Media.
- Wucker, Michele (2016) *The Gray Rhino: How to Recognize and Act on the Obvious Dangers We Ignore*, St Martins Press.
- Zhu, Q., Krikke, H. and Caniels, M. (2016), Collaborate or not? A system dynamics study on disruption recovery, *Industrial Management & Data Systems*, Vol. 116 No. 2, pp. 271-290.

「Nextcom」 論文公募のお知らせ

本誌では、情報通信に関する社会科学分野の研究活動の活性化を図るため、新鮮な視点を持つ研究者の方々から論文を公募します。

【公募要領】

申請対象者：大学院生を含む研究者

＊常勤の公務員（研究休職などを含む）の方は応募できません。

論文要件：情報通信に関する社会科学分野の未発表論文（日本語に限ります）

＊情報通信以外の公益事業に関する論文も含まれます。

＊技術的内容をテーマとするものは対象外です。

およそ1万字（刷り上がり10頁以内）

選考基準：論文内容の情報通信分野への貢献度を基準に、Nextcom 監修委員会が選考します。
（査読付き論文とは位置付けません）

公募論文数：毎年若干数

公募期間：2020年4月1日～9月10日（書類必着）

＊応募された論文が一定数に達した場合、受け付けを停止することがあります。

選考結果：2020年12月ごろ、申請者に通知します。

著作権等：著作権は執筆者に属しますが、「著作物の利用許諾に関する契約」を締結していただきます。

掲載時期：2021年3月、もしくは2021年6月発行号を予定しています。

執筆料：掲載論文の執筆者には、5万円を支払います。

応募：応募方法ならびに詳細は、以下「Nextcom」ホームページをご覧ください。

その他：1. 掲載論文の執筆者は、公益財団法人KDDI財団が実施する著書出版助成に応募することができます。
2. 要件を満たせば、Nextcom 論文賞の選考対象となります。
3. ご応募いただいた原稿はお返しいたしません。

「Nextcom」ホームページ

<https://rp.kddi-research.jp/nextcom/support/>

問い合わせ先：〒102-8460 東京都千代田区飯田橋3-10-10 ガーデンエアタワー
株式会社 KDDI 総合研究所 Nextcom 編集部

2020年度 著書出版・海外学会等参加助成に関するお知らせ

本誌では、2020年度も公益財団法人KDDI財団が実施する著書出版・海外学会等参加助成に、候補者の推薦を予定しています。

【著書出版助成】

助成内容：情報通信に関する社会科学分野への研究に関する著書

助成対象者：過去5年間にNextcom誌へ論文を執筆された方

助成金額：最大3件、各200万円

受付期間：2020年4月1日～9月10日（書類必着）

【海外学会等参加助成】

助成内容：海外で開催される学会や国際会議への参加に関わる費用への助成

助成対象者：情報通信に関する社会科学分野の研究者（大学院生を含む）*

助成金額：北米東部 欧州 最大40万円 北米西部 最大35万円 ハワイ 最大30万円
その他地域 別途相談（総額100万円）**

受付期間：随時受け付け

*常勤の公務員（研究休職などを含む）の方は応募できません。

Nextcom誌に2頁程度のレポートを執筆いただきます。

**助成金額が上限に達し次第、受け付けを停止することがあります。

推薦・応募：いずれの助成もNextcom監修委員会において審査・選考し、公益財団法人KDDI財団へ推薦の上、決定されます。応募方法ならびに詳細は、以下「Nextcom」ホームページをご覧ください。

「Nextcom」ホームページ

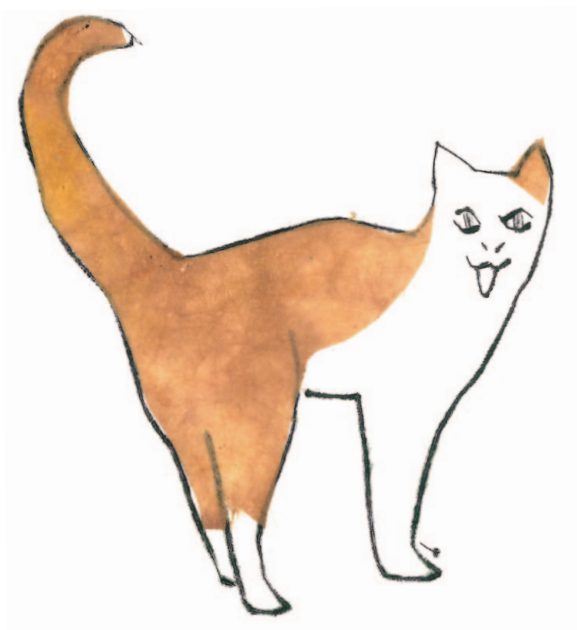
<https://rp.kddi-research.jp/nextcom/support/>

問い合わせ先：〒102-8460 東京都千代田区飯田橋3-10-10 ガーデンエアタワー
株式会社 KDDI 総合研究所 Nextcom 編集部

彼らの流儀はどうなっている？ 執筆：齋藤 慈子 絵：大坪 紀久子

呼べども、飼い主を無視するネコ。はて、自分の名前が分からないのか、それともあえての冷たい態度？ 気になる研究結果は……。

ネコは 自分の名前を 知っている



ネコは コトバが分かる？

「吾輩は『タマ』である」と認識している可能性は低いが、タマと呼ばれているネコは、「タマ」が「椅子」や「首都」といったその他の名詞とは違って、自分にとって重要なコトバ（人間の発する音）である、ということはどうやら分かっているらしい。つまり自分の名前を「自分のことを指す」と分かっているかは不明であるが（ネコに自己意識があることは証明されていない）、名前を他の単語から区別している、ということである。

そんなこととっくに知っているよ、とネコを飼っている人にとっては当然のことかもしれないが、動物がどのくらいわれわれのコトバを分かっているのか、厳密に、客観的にその能力を示すのは容易ではない。例えば、日常の状況では、動物はにおいや時間、声以外、音、身振り等、音声以外の手掛かりに反応している可能性もあ



る。その他の要因を取り去って、しっかりとコトバにだけ反応しているかを調べるには、音声だけ再生して実験をする必要がある。

100匹に 名前を 聞かせてみると

さらにネコ独特の難しさもある。多くの場合、ネコはエサで釣れない、ヒトの言うことを聞いてくれない、研究室に連れてきたらまともに行動してくれない。そのため、ネコを飼っている家庭を回り、時には訪問しただけで逃げられて無駄足に終わるという経験も積み重ねながら、延べ100匹を超えるネコを対象に実験を行った。(ちなみに、イヌの場合、特別に訓練された個体ではあるが、「○○を取ってこい」というコマンドを用いる方法で、1,000語以上のコトバを区別することが示されている。)

私たちが行った研究では、ネコが人の発するネコの名前を、他の

同じ長さの単語や、同居する他のネコの名前と区別しているかどうかを調べた。用いた方法は馴化^{じゅんか}脱馴化法という赤ちゃんなどにも使われるものである。

動物は同じ(あるいは同じカテゴリーの)刺激を繰り返し提示されると、最初強く見せていた反応(音源の方を素早く向くなど)をだんだん見せなくなる。これを馴化という。馴化が見られた後、別の(カテゴリーの)刺激が提示されると、また強く反応する。これを脱馴化という。このような現象が見られれば、馴化した刺激と脱馴化した刺激を、動物が区別しているといえる。この方法であれば、訓練が難しいネコでもその認知能力を調べることができる。

実験では、名前と同じ長さの異なる単語四つ、あるいは同居ネコの異なる名前四つを繰り返し提示した後、対象とするネコの名前を提示した。その結果、馴化した個体では脱馴化が見られたことから、冒頭の結論に至ったのである。

歴史が異なる イヌとネコ

先述のように、ネコを飼っている人には驚きのない研究結果かもしれない。しかし、ネコはヒトと系統的に遠く離れた種であること、また、イヌとならび伴侶動物としての地位を確立しているが、イヌとは全く異なる家畜化の歴史をたどってきたことを考えると、ネコでこのような認知能力が示されることは非常に興味深い。イヌは最古の家畜であり、ヒトとの長い共生の歴史の中でヒトと共同作業を行い、また、ヒトも積極的に人為的な選択交配を行ってきたのに対し、ネコとヒトの共存の歴史の長さは他の家畜と変わらず、かつ、人為的な選択交配はほとんどかけられてこなかったにもかかわらず、ネコも複雑な音を生成し、操るヒトという異種のコトバ(言語音)を聞き分けているのである。ネコの歴史と能力を詳しく知ること、より一層愛猫への思いも強くなるのではないだろうか。



安全な時にこそ防御を固めよ。
真に危険を逃れるのはそのような人である。
……プブリウス・シルス

謝って、逃げて、打ち勝つ

高橋秀実

攻撃と防御——。学生時代から柔道やボクシングに精進してきた私はそう聞いただけで、つい身構えてしまう。長年の癖というか、いまだに体が反応してしまうのである。

振り返れば、高校生の頃は「攻撃は最大の防御」と教えられた。とにかく攻め続ければよいのかと思ったのだが、無闇な攻撃は隙をつくるばかりで足をすくわれる。かといって防御に専念すると、「消極的」と判定されて負けたりする。攻撃しつつ防御する。防御しつつ攻撃する。つまり「攻防一如」こそ闘いの極意だと悟ったこともあるのだが、下手に悟ると勝負も一如となって、勝ち負けを忘れてしまう。

古代ローマの格言に「安全な時にこそ防御を固めよ。真に危険を逃れるのはそのような人である」*¹という言葉があるようだが、私の実戦経験からすると、これは間違っている。闘いの最中に「安全な時」などない。安全な時と思うこと自体が油断の証

拠であり、固めている隙に防御を崩される。もしやこれは敵を欺く罫ではないかと調べてみると、この格言にはもうひとつの解釈があった。「危険からは常に距離を置く。そういう人は安全でいられる」*²。原文はラテン語なので、どちらが正しいのか私には判断できないのだが、後者は「君子危うきに近寄らず」に似ており、今でいうなら「ソーシャル・ディスタンス」の維持である。古今東西に通用する防御法といえるのだが、危険を避けるだけでは問題の解決にならない。やはりどこかに攻撃の要素を入れるべきではないか、と考えてふと思い出したのは、先日会った空手道の師範である。

彼によると、闘いの基本はまず謝ることだという。たとえ自分が悪くなくても「すみません」と頭を下げる。それでも攻撃してきたら、今度は逃げる。ひたすら逃げて、逃げ切れなくなった時に相手の攻撃を受ける。正確にいうと「受け」の技で立ち

article: **Hidemine Takahashi**

ノンフィクション作家。1961年横浜市生まれ。東京外国語大学モンゴル語学科卒業。

『ご先祖様はどちら様』で第10回小林秀雄賞、『弱くても勝てます』開成高校野球部のセオリー』で第23回ミズノスポーツライター賞優秀賞受賞。

他の著書に『からくり民主主義』『損したくないニッポン人』『不明解日本語辞典』『定年入門』『悩む人』『パワースポットはどこです』など。最新刊は『一生勝負』（文藝春秋）。

向かう。繰り出された腕をへし折るつもりで力強く払い落とすのだ。逃げることで相手を疲弊させ、防御でダメージを与える。相手を倒すというより、自ら倒れるように仕向ける。勇ましさに欠けるようだが、闘いに見栄や体裁は禁物。防御こそ最大の攻撃なのである。古代ローマの格言も「危険から逃げ続ける人は安全」という単純な話だったのかもしれない。これこそ闘いの極意ではないかと思ったのだが、師範曰く、

「闘いに極意はありません」

なんでも闘いは相手の調子次第とのこと。同じ極意を持つ相手には勝てそうもないわけで、あくまでひとつの戦術として心にとどめておこう。

*1 『The Routledge Dictionary of Latin Quotations』
(Jon R.Stone著 Routledge 2004年)

*2 『The Moral Sayings of Publius Syrus』(Darius Lyman訳 Enhanced Media 2016年)

【背景】プブリウス・シルス(BC85～43年)の劇作品は散逸し、格言だけが伝えられている。1856年に発表されたDarius Lymanの英文訳が有名で、今回の引用書籍もLyman版を定本にしている。

編集後記

「ガラスの家に住む者は石を投げてはならない」という諺^{ことわざ}があります。他人を批判すれば自分の身に跳ね返ってくるから慎みなさい、と戒めたものです。人には誰も後ろめたい部分があり、そんな脆さ^{もろさ}をガラスの家に例えたのでしょう。また、ガラスの家の中の様子は外から丸見えなので、秘密にしておきたいことも簡単に暴かれてしまうよ、という意味も込められているのかもしれません。

個人情報^{個人情報}が詰まったスマホやIoT機器なしでは生活できない私たちも、実は既にガラスの家の住人なのかもしれません。

サイバー犯罪の格好の標的にならないためにも、これまで以上に高いモラルとセキュリティ意識を持ちたいものです。(編集部 神山 遥)

Nextcom (ネクストコム) Vol.43 2020 Autumn
2020年9月1日発行

監修委員会

委員長 菅谷 実 (慶應義塾大学 名誉教授)
副委員長 辻 正次 (神戸国際大学 学長/大阪大学名誉教授)
委員 依田 高典 (京都大学 大学院 経済学研究科 (五十音順) 教授)
川濱 昇 (京都大学 大学院 法学研究科 教授)
田村 善之 (東京大学 大学院 法学政治学研究科 教授)
舟田 正之 (立教大学 名誉教授)
山下 東子 (大東文化大学 経済学部 教授)

発行 株式会社KDDI総合研究所
〒102-8460 東京都千代田区飯田橋3-10-10 ガーデンエタワー
URL: www.kddi-research.jp

編集長 花原克年 (株式会社KDDI総合研究所)
編集協力 株式会社ダイヤモンド社
株式会社メルプランニング
有限会社エクサビーコ (デザイン)
印刷 瞬報社写真印刷株式会社

本誌は、わが国の情報通信制度・政策に対する理解を深めるとともに、時代や環境の変化に即したこれからの情報通信制度・政策についての議論を高めることを意図しています。ご寄稿いただいた論文や発言などは、当社の見解を示すものではありません。

- 本誌は当社ホームページでもご覧いただけます。
<https://rp.kddi-research.jp/nextcom/>
- 宛先変更などは、株式会社KDDI総合研究所Nextcom (ネクストコム) 編集部にご連絡をお願いします。(Eメール: nextcom@kddi-research.jp)
- 無断転載を禁じます。



