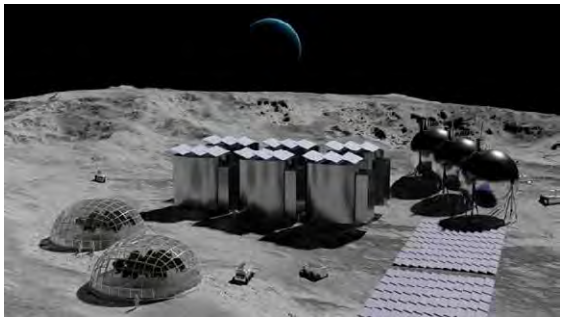
また、日本では「みちびき」が発信する補強信号と呼ばれる特殊な信号を受信することで、位置情報の誤差を6センチ以内にとどめることができるようになり、自動車の自動運転、農作業の無人化、小型無人機ドローンによる配達サービスなど、精緻な位置情報のビジネス利用が期待されている[733]。

７．極低温流体管理技術（CFM：Cryogenic Fluid Management）

(1) 技術の概要

近年、月・惑星への軌道間輸送機の必要性が高まるなか、極低温液体推進剤を利用した高比推力のロケットエンジンを、いかに長期間利用可能とするかが課題となっている。日本の基幹ロケット H2A（－235℃の液体水素と、－183℃の液体窒素を推進剤として採用）のように、極低温液体推進剤を利用したロケットは、タンク内の推進剤が太陽熱などによって容易に蒸発して失われてしまい、長期間の使用に適していないからだ[734]。例えば、現在では使用前数時間なら保管が可能だが、今後のミッションでは数年間の保管が必要となる場合も想定される。そのため、より長期間にわたり極低温流体推進剤を管理する方法が求められている。

宇宙空間での極低温流体管理技術に関しては、1980 年代から NASA を中心に研究が進められてきた[735]。軌道間輸送機の推進方法として極低温流体推進剤が採用されようが、あるいは前述の核熱推進が採用されようが、極低温流体管理技術（CFM）は必用不可欠な技術とされていることに違いはない。CFM は、核熱推進を支える技術でもあるからだ。また、極低温流体推進剤は月・惑星の表面においても製造可能であるため、軌道間輸送機などが実現すれば、月周辺のゲートウェイを経由し、他の惑星へ至る道を整備することが可能となる[736]。



[733] 内閣府　「みちびきを利用した実証事業」　https://qzss.go.jp/ex-demo/

[734] 名古屋大学大学院　衝撃波・宇宙推進研究グループ　「Cryogenic Liquid Propulsion （極低温液体推進）」 http://akagi.nuae.nagoya-u.ac.jp/research/cryo/

[735] 河南（2001）

[736] 名古屋大学大学院　衝撃波・宇宙推進研究グループ

(図 18-11　月面の水の電気分解プラントと液体水素・液体酸素貯蔵設備[737])

NASA は CFM のうち温度管理（受動的/能動的）、圧力管理などの大きな分野を、さらに細かい 25 の技術に分別し、それぞれのロードマップを作成している[738]。下記の図は 25 の技術分野を示している。

Technology	No	Technology	No
Advanced External Insulation	1	Propellant Densification	14
Autogenous Pressurization	2	Propellant Tank Chilldown	15
Automated Cryo-Couplers	3	Pump Based Mixing	16
Cryogenic Thermal Coating	4	Soft Vacuum Insulation	17
Helium Pressurization	5	Structural Heat Load Reduction (Active)	18
High Capacity, High Efficiency Cryocoolers 20K	6	Thermodynamic Vent System	19
High Capacity, High Efficiency Cryocoolers 90K	7	Transfer Operations	20
High Vacuum Multilayer Insulation	8	Tube-On-Shield Broad Area Cooling	21
Liquefaction Operations	9	Tube-On-Tank Broad Area Cooling	22
Liquid Acquisition Devices	10	Unsettled Liquid Mass Gauging	23
Low Conductivity Structures (Materials)	11	Valves, Actuators & Components	24
Line Chilldown	12	Vapor Cooling	25
Para to Ortho Cooling	13		

(図 18-12　25 の技術分野[739])

８．大気突入、降下、着陸

(1) 技術の概要

月や火星への探査が本格的に進む中、探査機の大気突入、降下、着陸（EDL：Entry, Descent, Landing）はミッションの成否を決定づける段階の一つである。NASA が行った 2020 年の火星探査ミッションにおいても、探査機の EDL に要する 7 分間は「ミッションの中でも最も短く最も緊迫した時間」

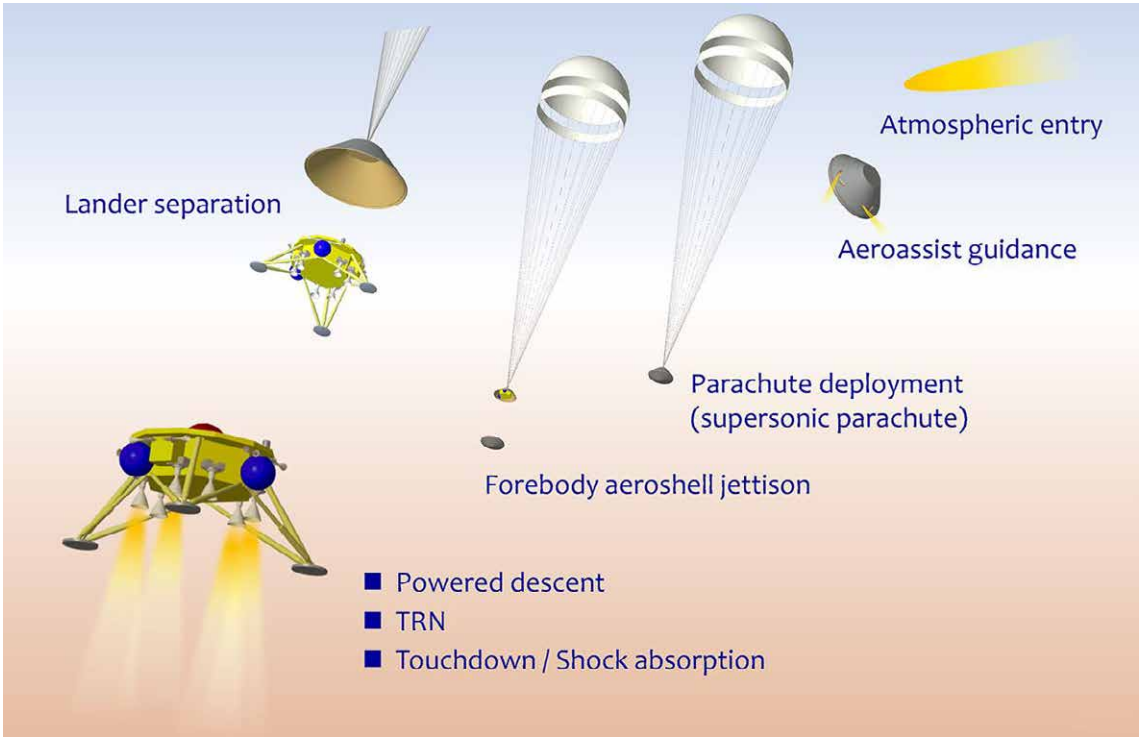
[737] ibid.

[738] NASA “NASA’s Cryogenic Fluid Management Technology Development Roadmaps” https://ntrs.nasa.gov/api/citations/20190000305/downloads/20190000305.pdf

[739] ibid.

と表現されている[740]。NASA の火星探査機の場合、時速 2 万キロメートルで大気圏に突入し、地表到達までに速度を低減しなければならない。この EDL の難度もあり、これまで火星に送られた火星探査機のうち約 40%しかミッションに成功していない[741]。

日本では JAXA を始めとして EDL の開発が行われているが、大気突入ミッションの数が多いとは言えず、着実な技術の継承と発展が難しいのが現状だ[742]。JAXA では現在、高頻度で継続的なフライト実証機を利用した EDL＆R（大気突入・降下・着陸および回収）の研究や、将来の火星探査アーキテクチャの検討が進められている。



（図 18-13　火星探査機着陸の一例[743]）

2020 年に打ち上げられた NASA の火星探査機「パーシビアランス」は、EDL のために Range Trigger（レインジ・トリガー）、Terrain-Relative Navigation System（地形追従航法装置）、Advanced aeroshell sensor package などの新機能を搭載していた。

---

[740] NASA “Entry, Descent, and Landing” https://mars.nasa.gov/mars2020/timeline/landing/entry-descent-landing/

[741] ibid.

[742] JAXA 『大気突入・降下・着陸および回収（EDL&R）技術の研究』
https://www.kenkai.jaxa.jp/research/edlr/edlr.html

[743] 同上

火星探査機を火星の地表に向けて放出する際、その着地地点をなるべく調査対象のアリアに近づける必要がある。その際鍵となるのが、機体からパラシュートを広げる「トリガー」のタイミングだ。レインジ・トリガーは機体の現在地と目的地を照らし合わせることで、パラシュートを広げるタイミングを調整し、着地地点の精度を従来よりも 50%以上高めている[744]。

探査機が着陸する際、急斜面や大きな岩は阻害要因となる。これらを避けて着陸するために導入されたのが地形追従航法装置だ。この装置は降下中に地形画像をモニターし、安全な着陸を阻害するような要因があれば、避けてより安全な地点に向かわせる[745]。この技術は、月や火星への有人飛行でも活用されることが期待されている。

Advanced aeroshell sensor package は新型の防護カプセル用センサで、大気突入の際に機体が受ける熱や圧力を測定する。熱シールドとバックシェルに装備される MEDLI2（MSL Entry, Descent, and Landing Instrumentation 2）というセンサによって、火星の大気成分への理解が深まるとともに、今後の EDL 研究に応用できるデータが取得される[746]。

まとめ

これまで、宇宙技術における各技術分野の研究開発動向と、公的・民生利用の両側面からの展望を概観してきた。最後に、これまでの日本の宇宙政策を整理し、今後注力すべき方策を考える一助としたい。

日本では 2008 年に「宇宙基本法[747]」、そして 2016 年に「人工衛星等の打上げ及び人工衛星の管理に関する法律[748]」および「衛星リモートセンシング記録の適正な取扱いの確保に関する法律[749]」が公布された。2009 年には「宇宙基本法」に基づき「宇宙基本計画」が閣議決定され、現在に至るまで改定を経て宇宙政策の方針を示している[750]。最新の「宇宙基本計画」では、「宇宙を推進力とする経済成長

---

[744] NASA “Entry, Descent, and Landing”

[745] Ibid.

[746] Ibid.

[747] 2008 年 5 月 28 日公布、法律 43 号。2008 年 8 月 27 日施行。

[748] 2016 年 11 月 16 日公布、法律 76 号。2018 年 11 月 15 日施行。

[749] 2016 年 11 月 16 日公布、法律 77 号。2018 年 11 月 15 日施行。

[750] 内閣府.「宇宙基本計画」

https://www8.cao.go.jp/space/plan/keikaku.html

とイノベーションの実現」のために、衛星データの利用拡大や国のプロジェクトにおけるベンチャー企業等からの民間調達の拡大を掲げている[751]。一方で、宇宙技術の民的利用には様々な課題が残る。

近年、日本でもスタートアップを中心に宇宙ビジネスの事業領域は拡大しているとはいえ、依然として国内需要の大半が官需であり、米国などと比較して民間市場の拡大はまだまだ十分といえない。政府主導による官民共同事業や、公共サービスへの積極的な利用はもちろん、そこから宇宙技術によっていかなる民生サービスを創出し、需要を生み出していくかが、将来的なデュアルユースの成否にもつながっていく。その際、政府は新技術の中でも分野を絞った、選択的な援助・補助を行い、国際的な競争力確保の後ろ盾をする必要があるだろう。本稿では、センシング衛星による新サービスの展開や、OSAM 技術における B2B の新ビジネス創出など、分野を横断して活用され始めた宇宙技術の実態を確認してきた。日本はロケットの打ち上げ回数は各国に比べて少ないものの、従来からロボットや小型衛星の製造については国際競争力を有してきた。近年宇宙分野で開発力を伸ばしている中国に公的・民的いずれの面でも対抗するためには、友好国とも連携しながら、国内における宇宙ビジネスの拡充を促し、好循環を生み出す必要があるだろう。

[751] ibid.

第 19 節 サイバーセキュリティ

1. 技術の概要

国家の重要インフラや企業・個人の機密情報を含む社会のあらゆる領域がコンピュータやインターネットとつながり利便性が飛躍的に向上した一方、サイバーセキュリティの重要性は安全保障の根幹に関わるようになった。

2. 民生上のインプリケーション

民生上最も被害の多いサイバーセキュリティ上の脅威はデータ漏洩であろう。IBM/Ponemon Institute によると、データ漏洩の世界平均コストは 2020 年の平均 386 万ドルから 424 万ドルに増加したことが確認された[752]。また、11 年連続で平均被害額が最も高いアメリカでは、データ侵害の平均総額は 864 万ドルから 905 万ドルに増加した（世界全体の平均総額は 424 万米ドル）。以下、近年の代表的なデータ漏洩事件を例示する。

(1) SocialArks のデータ流出

2021 年 1 月 11 日、SafetyDetectives のレポートによると、中国のソーシャルメディア管理会社である SocialArks は、400GB を超えるデータが流出する被害に見舞われた。これは、世界中の２億人以上のソーシャルメディアユーザーの個人を特定できる情報(PII)に影響を与え、また Facebook や Instagram、LinkedIn のアカウントも含まれていた。

(2) Bykea の設定ミスサーバー

2021 年 1 月 28 日、セキュリティ研究者が、パキスタンに拠点を置く輸送・物流・代金引換決済会社 Bykea のデータセキュリティ事故を公表した。4 億件を超える 200GB のデータを含む同社の完全な本番サーバーが、パスワードや暗号化なしで公開され、2020 年 11 月 14 日に研究チームによって発見された。Elasticsearch サーバーには、同社の Web サイトやモバイルサイトの API ログや PII が保存されていた。保護されていないデータベースに含まれる情報は、フルネーム、電話番号、メールアドレスなどの顧客データや、住所、CNICI(コンピューター化された国民 ID カード)、運転免許証情報、体温などのパートナー（ドライバー)情報、内部 API ログ、集配場所情報、クッキーの詳細とセッションログを含むユーザートークン ID、特定の GPS 座標、車両情報、ユーザデバイス情報、暗号化された IMEI ナンバーなどが含まれていたという。

[752] IBM, Cost of a data breach report 2021. https://www.ibm.com/security/data-breach

(3) Facebook のデータ流出

2021 年 4 月 3 日、Bleeping Computer のレポートによると、未知の脅威者が Raid Forums で 5 億人以上のユーザーデータを流出させるデータ侵害を共有した。盗まれたデータには、ユーザーのフルネーム、電話番号、所在地、電子メールアドレス、Facebook ID、および経歴が含まれていた。

このように、これらの侵害で見つかった情報は、多くの場合、個人情報を含む顧客や従業員のデータで構成されている。攻撃者はこれらの情報を利用して、フィッシングやスピアフィッシング攻撃、総当たり式のパスワードクラッキング攻撃を行うことができる。

2021 年、ランサムウェア事業者は大規模な攻撃を行い、アメリカの食品加工会社 JBS や IT マネジメント会社 Kaseya などの著名な被害者に影響を与えた。しかし、この年の最も注目すべき攻撃は、米国のガス会社コロニアル・パイプラインを標的としたもので、同社の業務の混乱は、米国東海岸のガス流通と価格設定に大きな影響を及ぼした[753]。この攻撃は、ランサムウェアによって甚大な被害が発生することを示し、米国政府や国際的な法執行機関によるランサムウェアの取り締まりの転機となった[754]。

サイバー犯罪者は、価値の高い標的に対する作戦から得られる大きな利益を観察しているため、新しいランサムウェアグループが出現し続けている。新しい脅威は、ほぼ例外なく、二重の脅迫を行うデータ漏洩モデルを採用しており、被害者に身代金の支払いを求める圧力をさらに強めている。また、脅威者は Linux システムを標的とするように戦術を変化させており、Linux システムでは仮想マシンやコンテナをホストしていることが多いため、組織にとってのリスクが高まっている。さらに、ProxyShell や Log4Shell のような脆弱性や[755]、Kaseya に対するランサムウェア攻撃 REvil のようなゼロデイ脆弱性を悪用するグループも現れている[756]。また、企業ネットワークに侵入するために内部関係者を勧誘したり、被害者の顧客に連絡して身代金の支払いを要求したり、ランサムウェアの被害者

[753] Turton, William and Mehrotra, Kartikay, “Hackers Breached Colonial Pipeline Using Compromised Password” Bloomberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[754] Romo, Vanessa, “Panic drives gas shortages after colonial pipeline ransomware attack.” NPR. https://www.npr.org/2021/05/11/996044288/panic-drives-gas-shortages-after-colonial-pipeline-ransomware-attack

[755] Cimpanu, Catalin, “First Log4Shell attacks spreading ransomware have been spotted.” The Record, December 14, 2021 https://therecord.media/first-log4shell-attacks-spreading-ransomware-have-been-spotted/

[756] Cimpanu, Catalin, “Kaseya zero-day involved in ransomware attack, patches coming.” The Record, July 4, 2021 https://therecord.media/kaseya-zero-day-involved-in-ransomware-attack-patches-coming/

を DDoS 攻撃で脅したり[757]、サプライチェーンやマネージドサービスプロバイダーを標的にして攻撃の影響を増幅させるといった新しい手口も出てきている[758]。

3. 国防上のインプリケーション

近年、サイバー戦、サイバー防衛は、国防上最も重要な領域になりつつある。国家当局や情報機関への攻撃（情報システムへの攻撃や不正操作、情報の窃取など）や、重要インフラ、金融システム、電力・通信ネットワーク、知的財産、軍事施設や兵器へのサイバー攻撃ならびにサイバースパイのリスクが高まっている。

サイバー戦には以下のような種類がある。①マルウェアによる攻撃。マルウェアは、コンピュータ・システムを混乱させたり、損害を与えるように設計されたソフトウェアの一種で、マルウェア攻撃は、機密情報の窃取、重要インフラの破壊、軍事作戦への損害などに利用される。②サービス妨害（DoS）攻撃。DoS 攻撃は、ネットワークやウェブサイトのトラフィックを急増させ、ユーザーのアクセスを遮断する攻撃である。DoS 攻撃は、重要なインフラや軍事作戦を妨害するために使用されることがある。③ランサムウェア攻撃。ランサムウェアは、マルウェアの一種で、被害者のデータを暗号化し、身代金等を支払うまでアクセス不能にするというものである。ランサムウェア攻撃は、金銭の強要や重要インフラの破壊に利用される可能性がある。④サイバースパイ活動。他国の機密情報へのアクセスを得るために、サイバースパイ活動が行われている。サイバースパイ活動は、軍事作戦、政治戦略、または経済活動に関する情報を収集するために使用されることがある。⑤サイバー妨害行為。サイバー妨害行為とは、コンピュータ・システムを意図的に破壊したり、損害を与えたりすることである。サイバー妨害工作は、電力網、交通システム、通信ネットワークなどの重要なインフラストラクチャーを破壊するために使用されることがある。

(1) ウクライナ情勢に見るサイバーセキュリティ

2022 年 2 月初旬、政府系ウェブサイトや銀行を標的とした DDoS 攻撃[759]、ウクライナとロシアの国境での軍事的プレゼンスの強化[760]など、ロシア政府によるウクライナに対する攻撃的なサイバー行動と

---

[757] Palmer, Danny, “This new ransomware encrypts your data and makes some nasty threats, too.” ZDNet. (October 14, 2021) https://www.zdnet.com/article/this-new-ransomware-encrypts-your-data-and-makes-some-nasty-threats-too/

[758] Cybersecurity & Infrastructure Security Agency, Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers. https://www.cisa.gov/uscert/kaseya-ransomware-attack

[759] https://www.bleepingcomputer.com/news/security/ukrainian-military-agencies-state-owned-banks-hit-by-ddos-attacks/

[760] https://www.nytimes.com/interactive/2022/world/europe/ukraine-maps.html

して始まったことは、2022 年 2 月 24 日のロシアによるウクライナへの軍事侵攻で頂点に達する[761]。それ以来、ハクティビスト、サイバー犯罪者、国家が支援するグループが、戦争においてロシアとウクライナのいずれかを支援するためにサイバー攻勢を開始した。ロシアは、ハクティビストと国家支援グループからなる十分なリソースを持つサイバー組織であるにもかかわらず、侵攻の過程を通じての影響力行使は、一部のサイバーセキュリティ専門家が予測したほどには大きなものではなかった。

ハクティビスト集団は、ウクライナ戦争に積極的に参加し、国家が支援する脅威行為者が、自国や各国政府の目的のためにサイバー作戦を展開している[762]。特に、親ロシア派のハクティビスト集団である Killnet は、ウクライナと同盟関係にある西側諸国の組織を標的とし、欧州議会、ブルガリア政府、イタリア政府、米国の各州を含む複数の国家ウェブサイトに対して DDoS 攻撃を仕掛けている[763]。ハクティビストグループ以外では、ロシア対外情報庁（SVR）が 2022 年を通じて、ロシアのウクライナ侵略における戦略的目的と政策目標を推進するために、豊富な資金を持つ脅威グループの資源を採用した。例えば、ロシアの APT グループ UAC-0113（Sandworm Team と中程度の信頼性でリンク）は、2022 年 8 月から電気通信プロバイダーになりすまし、ウクライナの組織などを標的にした。

(2) 中国の動向に見るサイバーセキュリティ

中国の APT とサイバー犯罪の活動は、2022 年を通じて安定した高いレベルを維持し、近年中国の脅威主体から見られる積極的なサイバー偵察プログラムと同レベルであった。中国の国家支援グループは伝統的に、南シナ海やインド、台湾など、中国のライバルである領土主張者をターゲットに非常に積極的で、活動のテンポはしばしば地政学的緊張を反映することになった[764]。中国は国際関係を管理するアプローチにおいて自己主張が強く、自国の国防、政治的安全、国際的地位、領土保全の追求のために、中国共産党（CCP）は定期的に幅広い強制的な行動に出ている。中国は、台湾、インド、アフガニスタンといった地域の標的に対しても、米国という海外の大きな戦略的敵対者に対しても、サイバー能力を使用している[765]。

---

[761] https://www.csis.org/analysis/cyber-war-and-ukraine

[762] https://www.mandiant.com/resources/blog/gru-rise-telegram-minions

[763] https://www.lawfareblog.com/what-impact-if-any-does-killnet-have?s=09

[764] https://www.recordedfuture.com/chinese-state-sponsored-cyber-espionage-expansion-power-influence-southeast-asia

[765] https://www.recordedfuture.com/from-coercion-to-invasion-the-theory-and-execution-of-china-cyber-activity

現在活動中の中国の国家支援グループは多数存在するにもかかわらず、グループ間のインフラや能力には顕著な重複が見られる。インフラストラクチャーでは、運用インフラにモノのインターネット（IoT）デバイスを採用する傾向が強まったほか[766]、中国の国家支援組織が使用する仮想プライベートサーバー（VPS）プロバイダーの利用傾向も継続的である。能力面では、中国の国家支援組織は、インターネットに接続された企業向け機器のゼロデイ脆弱性や一般に公開された脆弱性を一貫して利用して初期アクセスを行い、グループ間でエクスプロイトやマルウェア機能を共有している[767][768]。具体的な活動形態にかかわらず、中国のサイバー活動は通常、政府の敵対者に対する非対称的な優位性を獲得するための情報取得、中国内外の少数民族の標的、中国政府が国内の潜在的脅威に関する情報収集に協力することを目的としている。

地域の競争相手だけでなく、中国のサイバー活動は地政学的な動向や競争にも左右される。ロシアがウクライナに侵攻した後、欧米やロシアのエンティティを標的とした中国の APT 活動が見られたが、これは戦争が敵味方問わず、中国の情報収集イニシアチブの強化を優先させたことを意味する。例えば、2022 年 6 月には、ロシアの政府機関や国家機関を標的とした中国の国家支援型脅威活動グループ Tonto Team に起因する活動を確認された[769]。また、中国のグループ RedDelta、Twisted Panda、Curious Gorge もロシアを標的としたサイバースパイ活動を行っていた[770][771][772]。

4．アトリビューション

能動的なサイバー防衛活動に関する議論から明らかなように、これらの手法の多くを効果的に利用するためには、誰がネットワークを攻撃しているのかについてある程度理解し、能動的サイバー防御 (ACD) 手法を無実の傍観者ではなく、実際の悪意ある行為者に対して適用することが必要だ。

アトリビューションとは、特定の悪意ある行為に関与した脅威者を正確に特定する行為だ。サイバー脅威の行為者の帰属を成功させることは、ネットワーク防御、法執行、抑止力、および外交関係の

---

[766] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-158a

[767] https://www.mandiant.com/resources/blog/apt41-us-state-governments

[768] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

[769] https://www.sentinelone.com/labs/targets-of-interest-russian-organizations-increasingly-under-attack-by-chinese-apts/

[770] https://research.checkpoint.com/2022/twisted-panda-chinese-apt-espionage-operation-against-russians-state-owned-defense-institutes/

[771] https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe/

[772] https://www.secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx

改善を含むいくつかの理由で重要である。アトリビューションがもたらす潜在的なメリットを例示すると以下となる。

- 悪意あるサイバー行為者は、その行為に対して責任を負わされる。
- その行為に責任を負わされることになり、特定され責任を問われることへの恐怖、あるいは単に風評被害を受けることで、攻撃に対する抑止力となる可能性がある。
- アトリビューションが公開されることで、悪意あるサイバー行為者は、今後の追跡を避けるためにデバイスやインフラの使用を中止し、その動きを鈍化させることができる。
- アトリビューションは、攻撃者、ターゲット、TTP について知ることで、組織のネットワーク防御を強化するのに役立つ。
- アトリビューションは、サイバー防御と運用に向けたリソースの優先順位付けを支援することができる。
- 被害組織に関連する政府は、攻撃者に関連する政府に対して、制裁措置や規制の強化などの措置を講じることができる。
- アトリビューションは、組織が攻撃の責任を誰に負わせるべきかというニーズを満たす。
- 攻撃をある国に帰属させた後、非難している政府は、その国に対する支援のために同盟国を結集させることができる。
- 攻撃を帰属させることで、政府は攻撃者を追跡する能力があることを国民に示すことができる。
- 攻撃を帰属させることで、政府は悪意のあるサイバーアクターに対して、彼らを追跡する能力があることを示すことができる。
- 政府が攻撃を特定の行為者に帰属させると、民間企業は、情報セキュリティの取り組みにおいて政府と接触し、協力する動機付けを得ることができる。
- 帰属は、民間企業がどの法執行機関に連絡すればよいか、また法的な選択肢を決定するのに役立つ。

アトリビューションプロセスでは、技術的、分析的、法的、および政治的な証拠を融合して、悪意のある活動の背後に誰がいるのか、またそれに対して何をすべきかを判断するための全体像を可能な限り明らかにする。技術的な原因究明の努力は必要だが、責任の所在の問題に答えるには不十分である。悪意のある行為者による誤誘導や、攻撃開始時にキーボードを操作していたのが誰であったかを特定できないなどの理由で、技術的証拠の限界を超えるには、法執行機関と情報ソースに基づく従来の分析技術がしばしば必要とされる。法的証拠は、活動が法律に違反しているかどうかを調べ、プライバシーの権利など個人の権利を侵害することなく使用できる技術を決定したり、国際法の違反があったかどうかを評価したりすることができるものだ。最後に、政治的証拠は、特定の活動が特定の国家または民間団体と結びついているという判断を可能にする最後の断片を提供することができる。

アトリビューション能力は、プラスとマイナスの両方の意味を持つ可能性がある。オンライン活動の帰属は、システムにアクセスする人がその人であると主張することを確認するための ID 管理機能に

とって望ましい場合がある。たとえば、オンラインで自分の銀行口座にアクセスする個人は、承認されたユーザだけが口座にアクセスできるようにするシステムを望んでいる。したがって、活動を認可されたユーザに帰属させることができる ID 管理ツールは、積極的な使用の一例である。一方、抑圧的な政府は、政府に反対するコンテンツへのアクセスを求めたり作成したりする個人を特定し、そのような活動を停止したりその個人を罰したりするために、属性付与技術を使用することができる。

本章では、他者のネットワークや情報システムに損害を与えようとする悪意ある行為者に対する抑止効果を高めるとともに、悪意ある行為者からの攻撃に対するシステムの防御と応答を改善することを目的としたアトリビューション技術に焦点を当てる。ここでいうアトリビューションとは、ネットワーク上の攻撃者、または攻撃者の仲介者の身元および/または位置、あるいはネットワークに含まれるデバイスを特定することと定義される。

正確なアトリビューションは、防御を強化したり攻撃者に苦痛を与えたりする上で高い価値があるものの、高度に洗練されたアトリビューションは、一般に政府機関や高い能力を持つサイバーセキュリティ企業のみが可能な、時間とコストのかかる活動であることを認識する必要がある。さらに、政府機関以外の団体が責任者に対して意味のある行動を取る能力が限られているため、帰属の価値が損なわれる可能性がある。したがって、包括的な帰属の取り組みを行うかどうかに関するあらゆる決定は、特定の活動を特定の行為者に帰属させることができることから得られる可能性のあるプラスの成果のレベルが、希少なリソースの使用に見合うものかどうかを判断する必要がある。

まとめ――当該技術の喪失・窃取・劣位が発生することで生じる問題／リスク

サイバー領域は現代の政治・経済・社会・テクノロジー（PEST）の全方面で基幹となっている。したがって、サイバーセキュリティは民生上も軍事上も最も重要なエリアに位置づけられる。この分野でアメリカの圧倒的な優位性がゆらぎ、米同盟国のイスラエルの他にも、敵対している中国やロシア、北朝鮮が高い能力を持っていることは、日本の国家安全保障・経済安全保障上の大きなリスクとなっている。日本はすでに当該技術領域において、中国や北朝鮮に劣後しており、これが大きなリスクとなっている。

研究者の数でみても、大半の科学技術領域で日本は世界シェア 3 位圏内にランクインしているのに対して、サイバーセキュリティに関しては 4 位圏外との結果がアスタミューゼ社の調査で明らかになった[773]。研究者数ではインド人の研究者比率が高い傾向にある。研究者でもても日本がサイバー領域でまだ課題が多いことがわかるだろう。

[773] アスタミューゼ社への再委託報告書。

防衛の側面では、日本は自衛隊統合幕僚部にサイバー防衛の部隊を有しているが、たとえばイスラエルのようにレッドチームとパープルチーム（すなわち防衛と攻撃）の双方を保有しているわけではない。ただし、「攻撃」の訓練や実践から防衛へのフィードバックやインプリケーションを得ることは多い。実際にイスラエルでは軍出身のホワイトハッカーが経済界で活躍し、エコシステムを形成している。各国で人材育成・獲得競争が激しさを増すなか、日本は人材育成や活用（報酬を含む）面で国際的に大きく遅れを取っており、今後劣位の差が開くほど、追いつくのが困難となっていくものと考えられる。

第 20 節　医療・公衆衛生

1.経済安全保障上の課題としての医療・保健（公衆衛生）分野

我が国における特定科学技術での経済安全保障、特に医療・保健（公衆衛生）分野での社会、経済、軍事をも含む影響が考えられ、社会経済上の課題として重要視されている。2020 年に発生した新型コロナウイルス感染症（以下、COVID-19）の流行をきっかけに、一国だけでなくグローバルに感染が広がるその影響から、人々の生活や経済までも脅かすものとなった。このコロナウイルスを含む新興・再興感染症に、世界中の人々が脅威にさらされている。そのため世界各国でも早期に感染症対策を行う必要性が増し、ワクチンを含む治療薬や医療品の研究開発（R&D）を促進させることに加え、医療体制やシステムの迅速な対応も求められた。このように感染症は今後もコロナにとどまらず国策として開発支援や整備が必要となってくるであろう。我が国の医療・保健分野での安全保障の位置づけは「人間の安全保障（Human Security）」を基に、人々の安全を確保し国際的な保健に投資することで経済成長へも寄与すると提言されている。日本が率先して質の高い医療・保健制度である国民皆保険（Universal Health Coverage）を提供している恩恵には、世界でもトップクラスの医療保健水準を達成していることから平均寿命も上位を誇っている。このように、日本はあらゆる人々に基本的な保健医療サービスが提供でき健康改善により経済成長を促すような取り組みに自国のみならず世界へ貢献している。2022 年に公表された疾病負荷(Global Burden of Disease：GBD)の論文によると、高所得国である日本の GBD は呼吸器感染疾患で低所得国と同じ 4 位であるが、アルツハイマーや脳卒中は高位であった。このように新型コロナウイルスの世界的感染拡大の教訓により、呼吸器感染症は低所得国と同様の疾病負荷が課されており、医療・保健には社会・経済・安全保障に通ずる国際的な重要課題であると再認識することができた。

さらには、保健・医療分野の重要技術に関して、（グローバル）疾病負荷、いわゆる病気のトレンドに基づいた国の保健政策に関連する。画期的な新興技術であっても、保健・医療分野においては、この疾病負荷の要素を深く取り入れるだけでなく、安全・信頼性を確保した上でのイノベイティブな医療技術に素早くアクセスできるようにするための多角的な R&D プロセスが必要となってくる。それによって、それぞれの国における政策（医療・健康、科学技術、経済、環境、国防含む）への影響も鑑み、技術開発へのアクション・選択・優先順位・資源の観点からの政策決定が求められる。そのため資源の確保から先端技術の使用優先を選択し、医療システムや規制・法整備を整えた上で技術開発をさらに推進させることが重要となってくる。各国の進むべき保健政策の方向性による特定科学技術は、それぞれ違う技術を特定していることもある。

アメリカの National Strategy for Critical and Emerging Technologies 2020 においては、医療・公衆衛生分野での（Medical and Public Health Technologies）が新興科学技術リストとして公表され

ている。優先的なアクションとしてアメリカにおける規制や法律に沿って研究や開発を行うことを根底に、あらゆるパートナーと協力しながら新興技術を守ることを目的としている。しかし、医療・公衆衛生分野においては具体的な新興特定技術がどう経済安全保障において守る必要性があるのか明確ではなく、この経験が基となった概念形成を作り出せるのかは今後の課題である。日本においても経済安全保障の重要性が増す中、新興技術開発を推進する中でどのような重要科学技術が研究開発しているのか認識し、技術喪失のリスクを防ぐための検討を行うことが第一優先に必要と考えられる。よって、今後の我が国の経済安全保障戦略へ医療・保健分野の注目すべき重要科学技術を多角的に調査することが必要である。今回調査において医療・保健分野技術での主要なターゲット項目は「Pandemic preparedness/ Public（Global）Health Emergency」と「Medical technology」であり、１）研究開発状況、２）産業・民生経済もしくは軍事・国防目的の技術リスト特定とその用途、３）実用化に伴う研究・開発戦略や国民社会レベルへの影響、４）技術喪失が考えられる際での生じるリスク、これらの点を包括的に考慮した上で調査を行うことを目的とした。

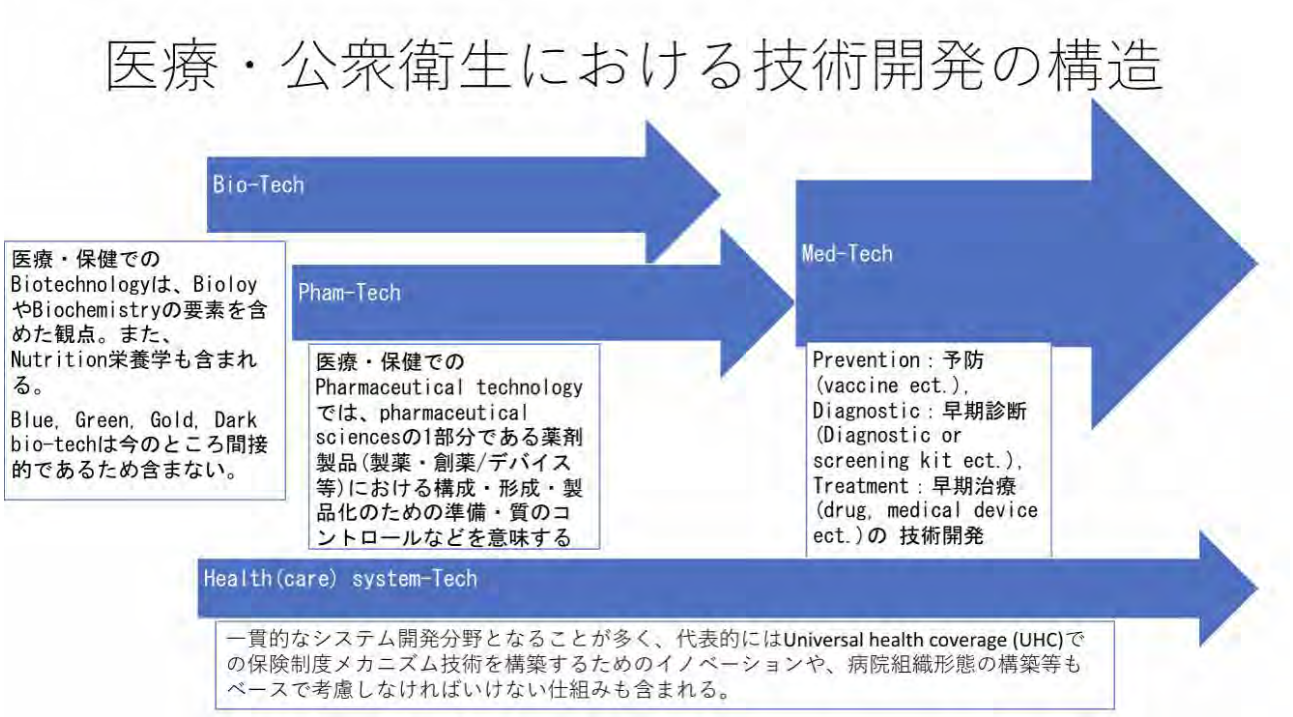
2.医療・保健（公衆衛生）分野での重要科学技術

経済安全保障における医療・保健（公衆衛生）分野での重要科学技術の主要ターゲット項目「Pandemic preparedness（世界流行の備え）/ Public（Global）Health Emergency（公衆衛生上の有事）」と「Medical technology（医療技術）」より、個別項目を絞ることを最優先とした。前述で述べた通り、各国の疾病トレンドや政策に左右されるが、感染症等の世界流行の備えや公衆衛生上の有事、今後必要とされる医療技術の新興技術を個別項目として調査した。

第一主要項目である「Pandemic preparedness（世界流行の備え）/ Public（Global）Health Emergency（公衆衛生上の有事）」とは、確固としたヘルスシステムの基盤がある中での疾病の感染対策を流行の備えとして全ての人々へ医療を提供できる体制である。また、WHO では、この疾病流行の備えや公衆衛生上の有事において、医療保健上の必要とされる医薬品・医療機器研究開発や公衆衛生の介入等を含む特異的な疾病への医療体制の能力強化のために尽力することの必要性を提言している。要するに、緊急事態時に対応できるイノベイティブな医療技術の能力強化に伴うソフト面の開発促進と、各々の医療システムの基盤が機能しやすくなるような整備を上手く仕組みたてるということと理解する。

第二主要項目「Medical technology（医療技術）」とは、医療システムの基、疾病予防や治療・リハビリテーションといった医療介入を通した技術が含まれている。特に、ワクチン開発や診断に関わる検査機器・治療薬が医療・臨床介入により研究開発が必要とされ、さらには医療機器や健康増進に関

わる分野も含まれる。このように、幅広い医療健康に関わる技術が取り入れられており、技術開発での基礎・応用・介入研究を経て医療技術開発の構造が仕組みだっている（図 20-1）。



(図 20-1 医療・公衆衛生における技術開発の構造)

このようにヘルスケアシステムが基本となり、バイオテクノロジーやファーマテクノロジーの創薬やデバイス等の構成・形成・製品化への開発を経てメディカルテクノロジーでの予防や治療の観点から早期診断・治療へと技術開発を進めていくと理解する。革新的な医療技術であってもヘルスシステムに基づく医療制度のインフラ整備やシステム構築も考慮し、開発を進めていくような戦略モデルを構造化することは重要である。よってサブカテゴリーを選定するにあたり、二層の技術分類（Technological classification）に分け、それぞれ主要項目での重要な医療技術を特定した。

第一主要項目「Pandemic preparedness（世界流行の備え）/ Public（Global）Health Emergency（公衆衛生上の有事）」での、Pharmaceutical technology (Pharma technology and Biotechnology) シーズ開発を含めた 薬剤・製薬・創薬的観点からは「Vaccine, Precision medicine, Cell and Gene Therapies, Monoclonal Antibodies」を選定し、Health technology ヘルスシステム的観点からは、「Contact tracing, E-health Telemedicine, Smart healthcare, Virtual meeting medical consultation, Medical drone, Essential robot worker, Medical robot」とした（図 20-1）。第二主要項目「Medical technology（医療技術）」での、Pharmaceutical technology (Pharma technology and Biotechnology) シーズ開発を含めた。薬剤・製薬・創薬的観点からは「Nutrigenomics, 3D food printing, food bioactive ingredients, Food allergies and intolerances, Omics techniques, Next

Generation Sequencing, Digitalized clinical trial, Monoclonal Antibodies and Biosimilars, Cell and Gene Therapies, Vaccine, Personalized Treatment, Precision medicine, Cytogenetics, Biobank, Biomechatronic, Biotherapeutic, Biomedicine, Bioinformatics, Diagnostic kit, Bioprinting, “In silico” testing, Microscopic robots, Medical robots, 3D pathology imaging, 3D radiology imaging, Physiotherapy, Smart Neural Interfaces, Neuromodulation, Brain-Computer Interfaces」を選定し、Health technology ヘルスシステム的観点からは、「eHealth, Telehealth, Wearable health(care), Medical Regulatory technology (“MedRegTech”), Virtual Reality in health(care), Augmented Reality in Health(care), cyber security mesh (Architecture) in health(care), Cloud computing in health(care), Blockchain in Health(care), Artificial intelligence in Health(care), Next-Generation Computing in Health(care), 3D printing in health(care), Machine learning algorithm in Health(care)」とした（図 20-2）。

Main term	Technological classification	Sub term (based on emerging or new technological trend)
Pandemic preparedness / Public (Global) Health Emergency	Pharmaceutical technology (Pharma technology and Biotechnology) シーズ開発を含めた 薬剤・製薬・創薬的観点 (Medical device含む)	Vaccine, Precision medicine Cell and Gene Therapies, Monoclonal Antibodies
		Smart Thermometer, Quarantine e-tracking (social distance detector), Detection or diagnosis kit (test), Next Generation Sequencing
	Health technology (more broad aspects) ヘルスシステム的観点	Contact tracing, eHealth Telemedicine, Smart healthcare Virtual meeting medical consultation Medical drone, Essential robot worker, Medical robot

(図 20-1 Public (Global) health emergency のサブカテゴリー)

Main term	Technological classification	Sub term (based on emerging or new technological trend)
Medical technology	Pharmaceutical technology (Pharma technology and Biotechnology) シーズ開発を含めた 薬剤・製薬・創薬的観点 (Medical device含む)	Nutrigenomics, 3D food printing, food bioactive ingredients, Food allergies and intolerances, Omics techniques, Next Generation Sequencing, Digitalized clinical trial, Monoclonal Antibodies and Biosimilars, Cell and Gene Therapies, Vaccine, Personalized Treatment, Precision medicine, Cytogenetics, Biobank, Biomechatronic, Biotherapeutic, Biomedicine, Bioinformatics, Diagnostic kit, Bioprinting, “In silico” testing, Microscopic robots, Medical robots, 3D pathology imaging, 3D radiology imaging, Physiotherapy, Smart Neural Interfaces, Neuromodulation, Brain-Computer Interfaces
	Health technology (more broad aspects) ヘルスシステム的観点	eHealth, Telehealth, Wearable health(care), Medical Regulatory technology (“MedRegTech”), Virtual Reality in health(care), Augmented Reality in Health(care), cyber security mesh (Architecture) in health(care), Cloud computing in health(care), Blockchain in Health(care), Artificial intelligence in Health(care), Next-Generation Computing in Health(care), 3D printing in health(care), Machine learning algorithm in Health(care)

(図 20-2 Medical technology のサブカテゴリー)