特集 **経営リスクとしてのサイバー脅威**

2030年のサイバーセキュリティ
セキュリティランドスケープを捉える



木村　匠



南朴木里咲

CONTENTS

Ⅰ　2030年のサイバーセキュリティを見通すために
Ⅱ　変化１：セキュリティインシデントは経営において災害と同等の備えが必要になる
Ⅲ　変化２：エマージングテクノロジーの実装と伴走できる「ちょうどいい」セキュリティガバナンスが求められる
Ⅳ　変化３：サイバーセキュリティは社会技術的な事象として捉えられるようになる
Ⅴ　おわりに：心置きなく挑戦するためのサイバーセキュリティ

要　約

1　サイバーセキュリティに関する中長期的な対策を組織が実装するには、経営層が中長期的なサイバーセキュリティの総体的な景観を可能な限り具体的にイメージすることが重要である。本稿では、2030年にかけて想定されるサイバーセキュリティに関する変化を示す３つのセキュリティランドスケープを提示する。

2　１つ目は、「セキュリティインシデントは経営において災害と同等の備えが必要になる」である。サイバーセキュリティ上の脅威は単に一企業の事業にとどまることなく、社会全体を巻き込む「災害」としての側面を持つようになる。インシデント対応を単にIT-BCPの観点から捉えるのではなく、企業全体の事業継続性を確保するための計画から捉え直す必要がある。

3　２つ目は、「エマージングテクノロジーの実装と伴走できる『ちょうどいい』セキュリティガバナンスが求められる」である。社会を変革させ得る新興技術がもたらす旨みを享受しつつ、避けるべき悪影響を管理するという「ちょうどいい」ガバナンスの構築が重要となる。

4　３つ目は、「サイバーセキュリティは社会技術的な事象として捉えられるようになる」である。ソリューションの導入をはじめとする技術的な要素は引き続き重要であるが、サイバーセキュリティは「技術だけの問題」ではない。人間の認知の脆弱性を突く脅威も確認されており、技術と社会の相互作用に着目した対策を実装することが重要となる。

Ⅰ 2030年のサイバーセキュリティを見通すために

1 「セキュリティランドスケープ」とは

サイバーセキュリティを取り巻く環境は予測が難しい。AIをはじめとする周辺技術の急速な進化、地政学的緊張の変動、規制環境の変化などが複合的に作用するためである。実際、過去10年を振り返っても、ランサムウエアの企業活動への深刻な影響、サプライチェーンを経由した攻撃被害など、そのときどきの脅威が事前に正確に想定されていたわけではない。また、2026年４月以降のフロンティアAIに関する目まぐるしい趨勢に鑑みると、もはや数週間後の見通しを確定的に語ることすら難しい。

それでもなお、中長期的な見通しを持つことは企業経営にとって重要である。サイバーセキュリティにかかわる経営判断、すなわち各企業の中長期的な経営計画におけるセキュリティ投資、新規事業の検討、組織体制やガバナンスの設計などは、いずれも数年単位の時間軸で意思決定される事項であり、その時点での目先の脅威にのみ反応していては変化に追随できない。

本稿では、こうした経営判断に活用できる、サイバーセキュリティに関連する変化の見通しを俯瞰的に整理したものを「セキュリティランドスケープ」と呼ぶ。個別の脅威動向や技術トレンドを点として捉えるのではなく、それらを取り巻く環境変化の総体を「景観（landscape）」として把握することが、経営判断の質を高めるうえで重要となる。

企業経営においてセキュリティランドスケープを把握することには大きく２つの意義がある。第１に、サイバーセキュリティを単なるコストや技術的課題としてではなく、事業継続・競争優位・社会的責任に関連する経営課題として位置づけ直すための共通認識を、経営層・経営企画部門・事業部門・セキュリティ部門などの間で形成できる点である。第２に、業界団体や行政といった外部ステークホルダーとの連携の必要性を経営層自らが認識し、これらのガバナンスを主導する示唆を得られる点である。

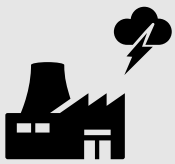
2 2030年にかけて現れる３つの変化

予測が困難な領域において中長期の経営判断を行う際には、目先の事象の延長線上で未来を考えるだけでは不十分である。サイバーセキュリティを取り巻く環境は、政治・経済・社会・技術の多様な要因が複雑に絡み合いながら変化していくため、個別の出来事の正確な予測よりも、中長期的にどのような構造変化が起こり得るかを見通す視点が重要になる。

本稿では、2030年を一つの節目として設定する。長期過ぎて抽象論に陥ることなく、短期過ぎて足元の課題整理にとどまることもない、経営の意思決定と接続しやすい時間軸であると考えるからである。2030年を見据えたとき、経営層が直接関与すべきサイバーセキュリティ上の重要な変化として、次の３つが浮かび上がる（図１）。

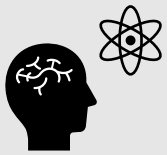
１つ目の変化は、セキュリティインシデントが経営において災害と同等の備えを必要とする事象になるという点である。サイバー攻撃による被害が金銭的損失にとどまらず、エ

図1　2030年までにかけて現れると考えられるサイバーセキュリティに関する３つの変化



変化１：セキュリティインシデントは経営において災害と同等の備えが必要になる

- サイバーセキュリティ上の脅威は単に一企業の事業にとどまることなく、社会全体を巻き込む「災害」としての側面を持つようになる
- IT-BCPにとどまらない、全社レベルでの事業継続を意識した「サイバーレジリエントBCP」が重要となる



変化２：エマージングテクノロジーの実装と伴走できる「ちょうどいい」セキュリティガバナンスが求められる

- ムーンショット型研究開発などによってエマージングテクノロジーの実装が進む
- エマージングテクノロジーの利点を享受しつつ、そのリスクを適切に管理できる「ちょうどいい」セキュリティガバナンスが求められる



変化３：サイバーセキュリティは社会技術的な事象として捉えられるようになる

- サイバーセキュリティの対象は、人間の認知や意思決定へと拡大していく
- 技術と社会をそれぞれ単独のものではなく、これらの相互作用に着目しながら統合的に捉える「社会技術的アプローチ」がサイバーセキュリティにおいてより重要視される

ネルギーや医療といった社会インフラの機能停止にまで波及する事態が現実に発生しており、自社のIT部門に閉じない、同業他社を含めた業界全体やサプライチェーン全体でのレジリエンスの構築が求められる。

２つ目の変化は、エマージングテクノロジーの社会実装に伴う「ちょうどいい」セキュリティガバナンスが求められるという点である。AI、量子、ロボティクスなどの新たな技術が産業構造を変容させていく中で、セキュリティに関するネガティブなリスク[注1]を抑え込むだけでなく、これらの技術の便益を享受することまで包含したガバナンスが求められる。

３つ目の変化は、サイバーセキュリティが社会技術的（socio-technical）な事象として捉えられるようになるという点である。守るべき対象が情報システムから人間の認知や意思決定にまで拡大し、攻撃者もまた技術と社会の双方の脆弱性を突いてくる中で、技術的対策と組織内外のガバナンスを一体的に設計する社会技術的アプローチが不可欠となる。

以降では、これら３つの変化について順に論じる。

Ⅱ　変化１：セキュリティインシデントは経営において災害と同等の備えが必要になる

１「災害」としてのサイバー脅威

企業経営において、サイバーセキュリティは長らく「ITの問題」として位置づけられてきた。しかし、近年のセキュリティインシデントの中には、その被害規模や影響範囲の広さについて、単に「ITの問題」と済ませるべきでないものが多くある。詳細は後述す

るが、たとえば、エネルギー供給や医療提供体制の停止など、個々の組織の範囲にとどまらない、社会への広範な影響が及ぶセキュリティインシデントが発生している。

実際、社会的に影響が大きかった情報セキュリティの事故や攻撃の状況などを考慮して情報処理推進機構（IPA）が毎年発表している「情報セキュリティ10大脅威」では、2022年以降、「サプライチェーンの弱点を悪用した攻撃」あるいは「サプライチェーンや委託先を狙った攻撃」が「『組織』向け脅威」の順位３位以内に毎年ランクインしている[注2]。このように、サイバー攻撃はもはや自社以外にも影響を及ぼすレベルの課題となっており、企業経営にとって災害と同等水準の備えをもって対応すべきものといえる。さらに、セキュリティインシデントの発生を完全に防ぐことは難しい。発生することを常に念頭に置いた対策が必要となる点も、災害への対応と類似する。

このようなセキュリティインシデント発生の状況は、2030年に向けてさらにエスカレートしていく可能性が高い。その主要な要因は２つ考えられる。まず、AI技術によるサイバー攻撃の高度化である。世界経済フォーラムの「Global Cybersecurity Outlook 2025」によれば、72％の組織がAIの進化と連動したサイバーリスクの増大を報告している[注3]。このようなリスクは、今後ますます増加していくことが予想される。次に、地政学的緊張の長期化による、国家関与型攻撃増加の可能性である。本特集の第三論考でも見たように、安全保障環境の変化は今後もサイバー脅威のあり方に影響する可能性がある。

日本では2025年５月にサイバー対処能力強化法および同整備法が成立した。2027年の全面施行に向け、サイバー安全保障という枠組みでの官民連携環境の整備が進みつつある。この法律の施行に向けての方針が定められた「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針」の冒頭には、「サイバー脅威は国民生活・経済活動を脅かすまさに災害のような存在となっている」という一文がある[注4]。さらに、2025年７月には内閣官房が「社会的影響が特に深刻な大規模インフラ障害への対応について（ガイダンス）」を公表し、サイバー攻撃やシステム障害により電力・通信などの重要インフラに広範な機能停止が生じた場合について、災害対策基本法などの関係法令の適用関係を明確化した[注5]。これにより、サイバー攻撃に起因するインフラ障害についても、自然災害と同様に災害対策本部の設置や災害救助法の適用が可能となる整理が示されたことになる。

加えて、2025年12月に政府が公表した新たな「サイバーセキュリティ戦略」では、「レジリエンス（インシデントが発生した際に、その影響を最小化し、早急に元の状態に戻す仕組みや能力、耐性）」の重要性が強調されており、全41ページの文書内で23回も言及されている[注6]。2021年に公表された一世代前のサイバーセキュリティ戦略においてもレジリエンスへの言及はあったが、文書全体での言及は３回にとどまっていた[注7]。

レジリエンスはもともと、心理学・精神医学における精神的な弾力性を意味する用語であるが、特に東日本大震災以降は「災害レジリエンス」という文脈で学術界や公共政策においても広く用いられるようになった概念である。サイバーセキュリティ戦略においてレ

ジリエンスへの言及が急増していることは、セキュリティインシデントがもはや災害級の脅威として認識されるようになっていることの証左である。

2　サイバー脅威による経済的被害

サイバー脅威がどのような観点で災害と同程度といえるかについて、具体的な被害規模から見ていく。Cybersecurity Ventures社の推計によると、2024年のサイバー犯罪による世界全体の被害額は約9.5兆米ドルとされる[注8]。一方、ドイツの再保険企業であるミュンヘン再保険（Munich Re）による自然災害統計では、2023年の自然災害による世界全体の経済損失は約2500億米ドルである[注9]。異なる調査であるため厳密な比較をすることはできないが、経済的被害という点に着目する場合、サイバー犯罪による被害は桁違いに大きい。

セキュリティインシデント一件当たりの被害規模も深刻である。IBMとPonemon Instituteが共同発表する「Cost of a Data Breach Report 2025」によれば、一件当たりの平均コストは世界全体で444万米ドルであった[注10]。また、同レポートによれば調査対象組織の86％がインシデント発生後に業務中断・サービス停止・生産停止といった事業上の支障を経験している。

3　サイバー攻撃による社会機能への重大な影響

さらに、被害の深刻さは金銭的な損失額だけにとどまらない。セキュリティインシデントが引き起こす最も重大な問題は、エネルギー・医療といった、人々の生活に直結する社会インフラが機能を失うという点にある。

2021年５月に発生したコロニアル・パイプラインへのランサムウエア攻撃はその典型例である[注11]。同社は米国東海岸に供給される燃料の約半分を担う最大の石油精製品パイプラインであり、攻撃を受けて事業継続上の判断としてパイプラインの操業を停止した結果、米国東海岸全域で燃料不足が発生し、バイデン大統領（当時）が非常事態宣言を発令するという事態に至った。

また、2024年２月に発生したChange Healthcare社へのサイバー攻撃では、医療支払い処理システムへの攻撃により、薬局が保険を介した請求処理を行えなくなったことで、患者が処方薬を入手できない、あるいは高額な実費負担を強いられる事態が広範に発生し、当初推計で米国民最大約１億9000万人が影響を受けることとなった。

一組織が被ったサイバー攻撃による被害が、単に被害組織の金銭的損失にとどまらず、社会のインフラとしての役割を担う機能の停止まで引き起こす事態は、まさにセキュリティインシデントが災害級の備えを必要としていることを意味する。

4　IT-BCPから「サイバーレジリエントBCP」へのシフト

ITシステムが企業の事業活動にとって重要な位置づけを占めて久しくなり、自社が運用するITシステムやそこで取り扱われるデータの継続性を確保するための事業継続計画である「IT-BCP」を策定している企業も多い。IT-BCPでは、重要システム・データの特定を行ったうえで、RTO（目標復旧時間）やRPO（目標復旧時点）の定義を行う。ま

た、IT-BCPの実効性を担保するためのセキュリティ対策検討や訓練が実施されることも多い。

一方で、もはや災害級となる被害規模や影響範囲を及ぼし得るセキュリティインシデントに備えるには、単にITシステムだけをスコープとしたBCPではなく、企業全体の事業継続性を確保するための計画（全社BCP）において、セキュリティインシデント発生時の多方面にわたる事業影響を盛り込むことが重要となる。

つまり、IT-BCP単体でセキュリティインシデントへの備えをするのではなく、セキュリティインシデントによる事業影響を全社BCPの想定事象として正面から位置づけ直すというシフトが求められる。このような、従来のIT-BCPのスコープを超えて全社レベルでの事業継続を意識し、かつセキュリティインシデントによる影響を考慮したBCPを、ここでは「サイバーレジリエントBCP」と呼ぶことにする。IT-BCPとサイバーレジリエントBCPの主要な違いは次の３点である（表１）。

まず、「意思決定の主体」が異なる。IT-BCPにおける意思決定はIT部門長レベルにとどまることが多い。しかし前述したコロニアル・パイプラインへのサイバー攻撃において、CEOが数時間以内に440万ドルの身代金支払いという判断を迫られたように、大規模なセキュリティインシデントは発生直後から経営トップレベルの判断を必要とする事象である。「誰が・何を・どの情報を基に・いつまでに決めるか」を、経営層が主体となって事前に設計しておくことが不可欠である。

次に、「想定する影響範囲」の相違である。IT-BCPが主に自社システムの復旧を射程に置くのに対し、サイバーレジリエントBCPはサプライチェーン全体への連鎖的影響を想定する必要がある。前述のChange Healthcare社へのサイバー攻撃が示すように、１社のシステム停止が取引先の業務を広範に停止させ、社会インフラへの影響に至るリスクがある。自社のシステムが直接の攻撃対象でない場合でも、取引先を経由した影響が自社の事業継続を脅かす事態は現実に生じている。こうしたシナリオを自社の被害想定に織り込ん

表1　IT-BCPとサイバーレジリエントBCPの相違

	IT-BCP	サイバーレジリエントBCP
意思決定の主体	主にIT部門長レベル	経営層
想定する影響範囲	主に自社システムの 復旧を範囲として捉える	サプライチェーン全体への 連鎖的影響を想定
復旧に関する考え方	システムの技術的な復旧 （例：RTOやRPOの達成） が主眼	システムが復旧せず 利用できない状態においても 事業を継続することを優先

でおくことが求められる。なお、このようなサプライチェーン全体に及ぶセキュリティ脅威への具体的な対策については、本特集の第一論考および第二論考で解説している。

そして最後に、「復旧に関する考え方」の相違である。IT-BCPはRTOやRPOの達成、すなわちシステムの技術的な復旧を主眼とする。しかし、先に言及した「Cost of a Data Breach Report 2025」によれば、サイバー攻撃において侵害の発生から検知・封じ込めに至るまでの平均日数は241日に達する。完全復旧を前提とした計画では、長期にわたる機能停止の局面での事業継続が成り立たない。サイバーレジリエントBCPでは、システムが利用できない状態においても事業を継続するための手順と優先順位を事前に設計しておくことが求められる。さらに、こうした計画を経営層が参加する定期的な演習を通じて実行可能な状態に保つことが、その実効性を担保する上で不可欠である。

5 「サイバー災害」に備える

2030年に向けて災害級の脅威となりつつあるセキュリティインシデントについて、もはやIT部門の所管だけにとどめておくべきではない。従来のIT-BCPの射程を、経営の意思決定やサプライチェーン・システムの停止下での事業継続にまで広げたサイバーレジリエントBCPとして検討することで、セキュリティインシデントを全社的な備えの対象として位置づけ直すことが求められる。このような備えを定期的な演習を通じて実行可能な状態に保ち続けることが、2030年に向けた企業経営に不可欠となる。

Ⅲ 変化2：エマージングテクノロジーの実装と伴走できる「ちょうどいい」セキュリティガバナンスが求められる

1 パラダイムシフトに求められる社会受容

革新的な技術はわれわれの生活を一変させる。2010年代のスマートフォンの普及は、コミュニケーションと情報享受のあり方を根本から変えた。そして2020年代、AIの急速な普及は、知的生産の概念そのものを再定義しつつある。これら過去のパラダイムシフトは、昨日の空想が今日には不可欠なインフラとなり、明日には競争力の源泉になることを示している。

このようなパラダイムシフトを偶発的にではなく、国家戦略として必然的に生み出そうとする試みが、内閣府の推進するムーンショット型研究開発制度である[注12]。これは超高齢化社会や温暖化など、従来の技術では解決困難な社会課題に対し、破壊的なイノベーションを創出することを目的とする。本制度では、未来から逆算し、現在なすべき研究を特定するバックキャスティングの手法を採っており、将来像として10のムーンショット目標が掲げられている。

そのうちの一つが「2050年までに、人が身体、脳、空間、時間の制約から解放された社会」の実現である。一見するとSFのようだが、具体的には、人のあらゆる能力を機能拡張したアバターやロボットを複数同時に操作することで、人手不足の解決や生産性の向上に寄与するという現実的なものである。

こうした各目標に共通して、新興技術によ

るプロトタイプの作成や実証実験の実施、安全性・信頼性の確保などが2030年までのマイルストーンとされている。これを踏まえると本制度では、研究開発促進だけではなく、社会受容の基盤構築にも主眼が置かれていることが読み取れる。

2 エマージングテクノロジーの実装による経済成長への期待

前述のような新興技術として位置づけられているのがエマージングテクノロジー（以下、ET）である。ETとは、単に出現したばかりの新しい技術を指すのではなく、表2に示す5つの特性を持つ技術のことである。

2026年上半期において、「Claude Mythos」をはじめとするフロンティアAIの出現はETの特性が顕著に表れた例といえるだろう。同モデルは、AI分野とサイバーセキュリティ分野が高度に融合しており、未知の脆弱性を自律的に発見するという新規性を備えている。また、技術の成長力と社会への影響力により、脆弱性管理のあり方を急速に変えつつある。このように、ETの劇的な進歩の速さと技術的な複雑さは、従来のリスク管理の限界を露呈させている。

ただし、こうしたETのリスクには、社会に利便性をもたらすというポジティブな側面もある。たとえば、自律的な脆弱性解析技術は、サイバー攻撃に悪用される可能性（ネガティブリスク）がある一方で、適切に活用すれば、自社システムの未知の脆弱性を瞬時に検知する利便性（ポジティブリスク）をもたらす。未知の事象を過度に恐れてETの活用自体を忌避することは、組織にとって大きな機会損失を招く。ETの便益を享受するには、考えられる脅威を分析し、組織としてどのような方針でネガティブリスクを制御し、ポジティブリスクを最大化していくかという能動的なセキュリティガバナンスの構築が必要である。

また、ETはその影響力から他国に先駆けて社会実装できた際には、経済成長への影響も大きい。産業競争力懇談会（COCN）によると、日本の産業競争力における重要なETの一例として、大規模言語モデル（LLM）のメモリ使用量と消費電力を劇的に削減可能

表2　エマージングテクノロジー（ET）の5つの特性

①根本的な新規性（Radical Novelty）	従来とは根本的に異なる考え方や仕組みにより目的を達成する
②急速な成長（Fast Growth）	技術にかかわる主体、資金、研究、プロトタイプにおいて同領域の技術よりも急速に成長する
③凝集性（Coherence）	初期段階では単一的な技術に見えるが、成熟するにつれ多分野を融合した相乗効果を発揮
④顕著な影響力（Prominent Impact）	社会全体に対して、制度、知識生産プロセスを大幅に変革する潜在能力を持つ
⑤不確かさと曖昧さ（Uncertainty and Ambiguity）	技術の用途が流動的かつ幅広いため、社会への影響の予測が困難

出所）Daniele Rotolo, Diana Hicks & Ben R. Martin "What is an emerging technology?"より作成（日本語訳はNRIセキュアテクノロジーズ作成）

な１ビットAI推論が選定されている[注13]。激化するAI開発において、コストと消費電力の削減は世界共通の課題であり、早期に実装できれば経済的恩恵を得られるだろう。

こうしたETの実装をめぐっては、政府が設置した日本成長戦略会議による取り組みが重要な契機になると考えられる。同会議は、危機管理投資と経済成長投資を不可分なものと捉え、AI・半導体、航空・宇宙、デジタル・サイバーセキュリティ、防衛産業などの戦略17分野への官民による投資を通じて、自国の供給力強化を図る、と公表している[注14]。また2026年６月24日には戦略17分野における「主要な製品・技術等」の官民投資ロードマップ（案）が公開された[注15]。

同案によると、デジタル・サイバーセキュリティ分野では2030年までにガバメントクラウドの利用システム数を現在の２倍に、情報通信分野では2030年までにオール光ネットワーク（APN）のグローバルシェアを現在の約５％から10％に拡大するといった、具体的な数値目標が示されている。

その他、2030年およびその前後を最初のマイルストーンとした目標が数多く挙げられていることから、今後、ETの実装に向けた投資および事業活動が本格化するものと考えられる。

3　ポジティブリスクの出現によるセキュリティガバナンスの変化

こうした政策動向を踏まえると、民間企業も追随してETの便益を享受すべく、正負両面のリスクをコントロールするガバナンスの構築が目下の課題となる。

その中でも、これからのセキュリティガバナンスを考えるうえで重要な指針となるのが、欧州を中心に提唱されているELSI（Ethical, Legal and Social Issues：倫理的・法的・社会的課題）やRRI（Responsible Research and Innovation：責任ある研究・イノベーション）の概念である[注16]。ELSIは、科学技術がもたらす倫理的、法的、社会的側面からの課題自体や、それらの課題に適切に対処する枠組みを指す。一方、RRIとは、そうした課題への配慮も含め、科学技術やその研究をよりよい形で社会の中に位置づけようとするアプローチである。

セキュリティガバナンスを構築するに当たり、ELSI／RRIの観点をかけ合わせることには大きな意義がある。セキュリティは、万が一インシデントが発生すれば、サプライチェーンの停止や法的責任、ステークホルダーへの経済的不利益といった深刻な社会的影響を与えるELSI／RRI上のリスクへと変化しつつあるからである。実際、昨今の国内外のガイドラインでは、セキュリティは経営層が直接関与すべき経営課題と定義されている。

セキュリティガバナンスを構築する際に着目すべきなのは、このリスクに対する認識の変化である。これまでセキュリティ投資は、インシデントによる損失や賠償といったネガティブリスクを抑え込むためのコストと捉えられてきた。しかし、セキュリティが多角的な経営課題へと昇華した今、ETがもたらす影響は単なる脅威にとどまらず、ポジティブリスクとしても再定義できる。リスクの両面性を適切に管理することで、ETの利便性を享受し、他社に先んじた市場参入や社会からの信頼性を武器とした組織価値の向上を狙う戦略的機会となる。

このようにポジティブリスクとネガティブ

リスクをバランスよく管理するセキュリティガバナンスを、ETの実装と伴走する「ちょうどいい」ガバナンスと呼ぶこととする。

従来のセキュリティガバナンスは、ネガティブリスクを減らすことを目指すあまり、ユーザーにとっての利便性をはじめとするポジティブリスクには焦点が当てられないことが多かった。しかし、ETがもたらすポジティブリスクを活かすことが求められる「ちょうどいい」ガバナンスでは、変化する状況に応じて組織が最適なセキュリティ施策を自律的に意思決定することが不可欠となる。つまり、今後求められる「ちょうどいい」ガバナンスにおいてセキュリティとは、自動車（ETがもたらす事業成長や利便性）が加速して心地よく走行するためのガードレールに例えることができる。

4 生成AIの普及過程にみる「ちょうどいい」ガバナンス

「ちょうどいい」ガバナンスのあり方を具体化するうえで、近年の生成AIの急速な普及過程は重要な先行事例である。ここで、普及過程において顕在化した事象を整理してみる。

生成AIは、従来の定型業務の効率化や高度なデータ分析による意思決定、クリエイティブ領域における生産性向上といった利便性をもたらした。これらはポジティブリスクとしての生成AIが組織に利益をもたらした結果である。

一方で、入力データがモデルの学習に再利用されることによる機密性の低下や、学習データおよび生成物の法的妥当性をめぐる著作権などの権利の侵害、ハルシネーションに起因する誤情報の拡散といったネガティブな事象も発生した。また、組織の統制外で安易にツールが導入されるシャドーAIは、ガバナンスの形骸化を浮き彫りにした。これらはネガティブリスクとしての生成AIが組織に損失をもたらした結果である。

リスクの両面性が混在する事象に対し、総務省および経済産業省が策定した「AI事業者ガイドライン（第1.2版）」は、リスクベースのアプローチによるAIの開発者、提供者、利用者といった主体別の対応を記載している[注17]。具体的には、人間中心、安全性、公平性、プライバシー保護、セキュリティ確保、透明性という共通の指針を土台とし、各主体が果たすべき具体的な責務を定義している。

たとえば、開発者やサービス提供者の立場であれば、開発段階からのセキュリティ対策のための仕組みの導入や常に変化する脆弱性への対応が要請される。一方で、AI利用者の立場においては、プロンプトへの個人情報の目的外の入力防止やプライバシー侵害への対策、開発者および提供者によって想定されたセキュリティ対策の実施といった運用面に即した対応が求められる。

ガイドラインが提示する主体別のフレームワークを踏まえると、ETに対するセキュリティガバナンスを実効的なものにするには、主体別の役割と責任からリスクの所在を精緻に特定することが不可欠である。リスクの解像度を上げることで初めて、ポジティブリスクによる便益の享受とネガティブリスクによる損害の回避を両立させるためのセキュリティ対策優先度が明確化される。したがって、「ちょうどいい」ガバナンスの目的は、どのリスクを経営戦略として受容し、どのリスクを技術的・組織的対策によって低減すべきかを

区分し、自律的な管理体制を敷くことにある。

5 「ちょうどいい」ガバナンスの全体構想

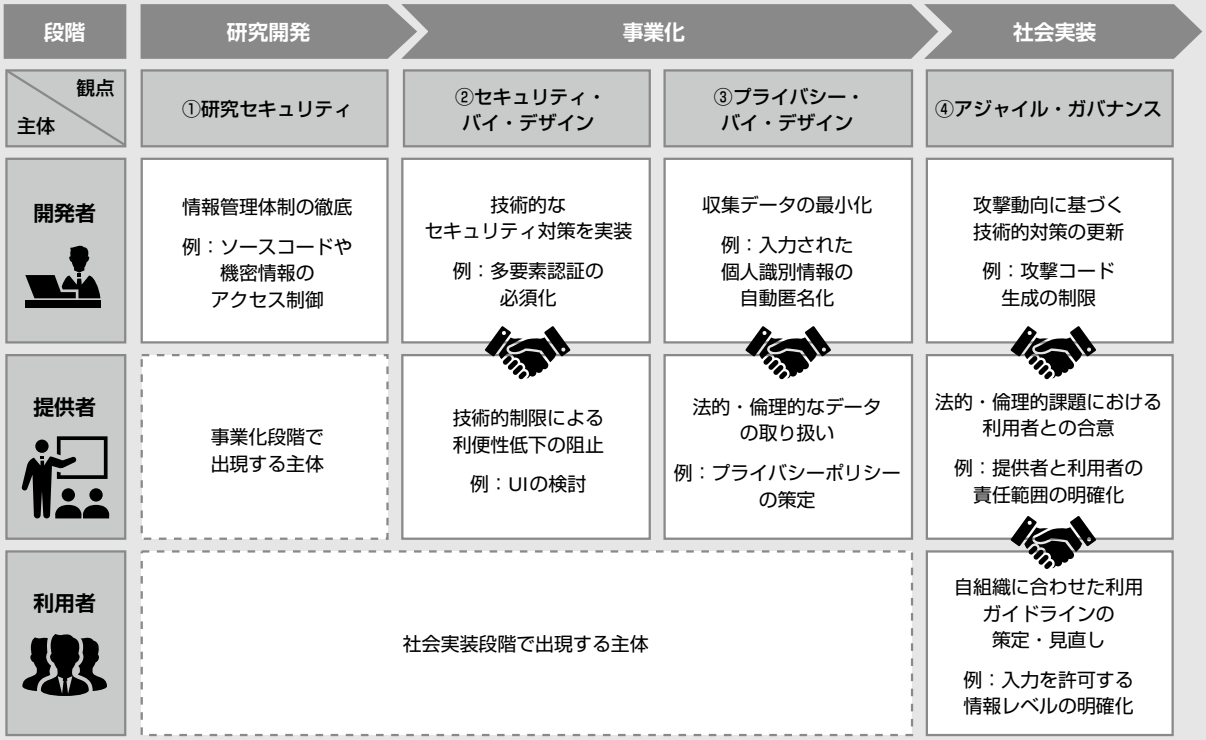
2030年に向けたETの社会実装には、技術に関係する各主体による「ちょうどいい」ガバナンスの構築が必要である。その全体構想は、図2に示す4つの観点および3つの主体から構成される。

まず、ETが実社会で使用されるようになるまでには、「研究開発」「事業化」「社会実装」の3段階がある。そして、ETの実装にかかわる主体は「開発者」「提供者」「利用者」の3つに分類される。

開発者はETを研究開発する立場であり、企業の研究開発（R&D）部門や研究機関、大学などが該当する。提供者は、ETの事業化段階において実際にサービスとして社会に提供し利益を得る立場であり、企業の経営層やマーケティング部門、法務部門、営業部門などが挙げられる。なお、経営層が開発者の立場を兼ねるスタートアップ企業などのように、開発者と提供者が同一組織である場合もある。利用者は提供されたサービスを利用する立場であり、ここでは特に企業としての利用を指す。社会実装に向けた各段階では、これら3つの主体によって取り組むべき対応が変化するため、各観点の達成には主体間の対話と連携が不可欠となる。

なお、ここで利用者に該当する企業の経営層が留意すべきは、開発者・提供者に求められることを他人事として捉えるのではなく、自社が安全にETを調達・活用するためのエコシステム全体の評価基準として認識することである。ETの実装にかかわる主体は「開発者」「提供者」「利用者」の3つに分類され

図2 「ちょうどいい」ガバナンスの全体構想



※例は生成AIにおける各主体の対応を具体化したもの

るが、利用企業はサプライチェーンを通じて自社に持ち込まれるリスクをコントロールするために、開発者や提供者に対して以下の観点を要請・評価することが重要である。

第1に、研究セキュリティとして、開発者はETの持つ凝集性や影響力に鑑み、意図しない技術流出や悪用を防止するための情報管理体制を確立する。研究セキュリティとは、軍事転用技術など国家安全保障上の技術流出を防ぐ枠組みを指す。研究環境における信頼性を担保することは、安全保障上のリスクへの対応だけでなく、技術の健全な普及を後押しすることにつながる。

第2に、セキュリティ・バイ・デザインとして、開発者はETの構想・サービス開発段階からセキュリティ要件をアーキテクチャの根幹に組み込む。設計段階からセキュリティを検討することにより、結果としてセキュリティに関する実装コストを抑えることができる。また、「ちょうどよい」ガバナンスの観点からは、セキュリティ要件の程度によってユーザーにとっての利便性が著しく低下していないかを確認することも肝要である。

第3に、プライバシー・バイ・デザインとして、個人情報やデータの保護機能・ポリシー策定をサービス開発段階から要件とする。これはセキュリティ・バイ・デザインを土台としつつ、提供者が収集データの透明性やユーザーへの同意取得といった、前述のELSIの観点からデータの取り扱いに対処するアプローチである。また、開発者はデータの取り扱いに当たり、技術的な仕組みを実装する。これにより、運用のフェーズにおけるデータの不適切利用やプライバシー侵害に起因するネガティブリスクを低減することができる。

第4に、アジャイル・ガバナンスとして、技術の成長速度や社会情勢の変化に即応できるよう、開発者、提供者、利用者の各主体が対話を通じて管理策を継続的に見直し、最適化を図る。この実践に当たっては、利用者の中でも現場のみに判断を委ねるのではなく、経営層が自組織の置かれた状況を深く理解し、現場や他主体との連携の下でETの活用方針を決定しなければならない。さらに、その方針を定期的に見直し、柔軟にアップデートしていく運用の定着が求められる。

ここでは、コストとしてのセキュリティ投資ではなく、正負両面のリスクを戦略的機会へと転換する「ちょうどいい」ガバナンスについて解説した。セキュリティガバナンスに求められる変化が、2030年に向けたETの社会実装を成功に導き、持続的な経済成長と市場における信頼を両立させるための要諦となるだろう。各主体が「ちょうどいい」ガバナンスの構築に取り組むことで、組織だけでなく、社会全体として責任あるETの実装を実現できるはずである。

Ⅳ 変化3：サイバーセキュリティは社会技術的な事象として捉えられるようになる

1 「技術だけの問題」ではないサイバーセキュリティ

サイバーセキュリティは紛れもなく技術に関する問題である。しかし同時に、「技術だけの問題」ではない。

たとえば、近年普及が進んでいるセキュリティ対策である多要素認証は、複数の認証要素を用いることで不正アクセスのリスクを低

減させることのできる技術的手段である。しかし昨今では、多要素認証を実装しているにもかかわらず不正アクセスを許してしまう、多要素認証疲労攻撃（MFA Fatigue Attack）が存在する。攻撃者が何らかの方法でユーザーの認証情報を取得しログイン試行を繰り返すことで、正規ユーザーにプッシュ認証通知を誤ってクリックさせてしまう。大量のプッシュ通知が届くことでユーザーは心理的に耐え切れなくなり、承認ボタンを押してしまうのである。

さらに、SNS上での偽情報の拡散や生成AIを活用した偽動画の作成など、人間の弱点を直接突く攻撃も存在する。これらの攻撃への対処は近年、コグニティブセキュリティという枠組みで議論がされている。科学技術振興機構（JST）の研究開発戦略センター（CRDS）では、コグニティブセキュリティの研究課題に関するワークショップも開催されている[注18]。

これらの例から分かるように、サイバーセキュリティは技術にとどまる問題ではなく、人間を含む社会に関する問題でもある。単に技術の側面にだけ着目するのではなく、技術と社会を一体的な仕組みとして捉えられる系は「社会技術システム（socio-technical systems）」と呼ばれ、技術哲学や科学技術政策においてこれまで検討されてきているトピックである。ここでは、技術と社会をそれぞれ単独のものではなく、これらの相互作用に着目しながら統合的に捉える見方を「社会技術的アプローチ」とする。さまざまなテクノロジーがわれわれの日常に浸透していく昨今、社会技術的アプローチは今後のサイバーセキュリティを検討するうえでますます重要になる。

2 AI分野で進む社会技術的アプローチ

国内外の政府機関も、セキュリティを含むAIの安全性の領域において社会技術的アプローチを重視している。英国政府が公表する「国際AIセーフティ報告書2025」では、AIシステムについて、「安全性とパフォーマンスを維持するには、システムを社会技術システムの中に組み込み、継続的にリスクを特定・分析し、防御する仕組みを構築することが重要」としており、社会技術的アプローチの必要性に触れている[注19]。さらに、AIの安全性に関する評価手法や基準の検討・推進を行うための日本の政府機関であるAIセーフティ・インスティテュート（AISI）もまた、AIの社会技術的な側面に着目した調査報告書を2025年10月に公開している[注20]。

当該報告書ではたとえば、生成AIサービスの普及により、フィッシング攻撃の件数が増加していることに加え、より自然な日本語を用いた攻撃が増えていることに言及し、ソリューション導入をはじめとする技術的対策と業界内での脅威情報共有などの社会的対策の双方が重要であることを強調している。

AI分野でこれほどまでに社会技術的アプローチが重視されているのは、AIシステム自体が人間の価値判断を含む学習データによって日々変化をし続ける社会技術システムであるという点に加え、社会の多様な領域でAIの利活用が進展しているからであろう。

このような状況下において、単に技術的対策を実装するだけでは攻撃を防ぐことはできない。また、個人のリテラシーに依存した対策や、社内ルール整備などのマネジメント的な対策だけでも当然不十分である。つまり、

技術的要素と社会的要素を統合した仕組みを組織ガバナンスの中に位置づけることによる防御が必要になる。また、これらの組織ガバナンスを実際に構築する際には、経営層によるイニシアチブの発揮が必須となる。

以降ではより具体的に、2030年に向けたサイバーセキュリティにおいて、どのような場面で社会技術的アプローチを用いることが必要となるかについて、2つの例に沿って示す。

3 例1：エージェント型AIの導入に伴うセキュリティリスク

人間の問いかけに対して回答するチャット型の生成AIに加え、Claude Codeをはじめとするエージェント型AIの普及が進んでいる。このような傾向は2030年に向けても継続していくだろう。

エージェント型AIの最も大きな特徴は、ユーザーに代わって判断を行い、ほかのシステムとの連携やタスクの実行を担う自律性にある。エージェント型AIの導入は、従来の生成AI活用とは異なるセキュリティ上の課題をもたらす。外部システムへのアクセス権限を与えられることで、外部からの攻撃による情報漏洩や不正な業務実行などのリスクが存在するからである。

たとえば、社内の開発環境やSaaS、顧客情報を扱う業務システムと連携したエージェント型AIが導入された場合、プロンプトインジェクションにより、情報窃取や不適切なシステム操作が行われる可能性がある。さらに、AIに過剰な権限が付与されていた場合、その影響は単一の端末やユーザーにとどまらず、組織全体の情報資産や業務プロセスに波及し得る。

このようなリスクに対する技術的対策の一つとして、エージェント型AIが参照あるいは操作できる範囲を制限するよう、権限管理やアクセス権限の設定を行うことが考えられる。しかしながら、そもそもこのような対策を実施するには、どの組織の要員がどこまでの情報にアクセス可能であるべきなのか、また、組織として何をどこまでAIに任せるべきかというマネジメント上の判断が必要となる。

たとえば、経理部門のエージェント型AIには会計データや請求処理に必要な情報へのアクセスのみを認める一方で、人事情報や営業部門の顧客情報にはアクセスさせないなど、各部門の業務遂行に必要な範囲に応じてAIが参照・操作できる情報を切り分けるといった判断である。

このように、エージェント型AIのセキュリティは、単なるアクセス制御などの技術的対策の問題ではない。エージェント型AIを活用することは、AIという「部下」に一定の裁量を与えて業務を実施してもらうことを意味するため、「誰に何を任せるのか」という組織設計そのものの問題でもある。技術的対策と、責任分界や業務プロセスの設計を一体として検討する社会技術的なアプローチが重要となる。

4 例2：データボイドの脆弱性

2030年に向けて、サイバーセキュリティにおいて守るべき対象は、情報システムやデータそのものだけではなく、人間の認知や意思決定へと拡大していくと考えられる。生成AIの普及により、自然な文章や画像、動画を低コストかつ大量に生成することが容易になり、偽・誤情報を用いた攻撃の規模と精度が飛躍的に高まるためである。本章冒頭で述べたとおり、人間の認知や判断に働きかける

ことで組織や社会に影響を与える脅威は、コグニティブセキュリティとして近年研究が進んでいる。

たとえば、Microsoft Researchの研究者であるDanah Boyd氏らが2018年に提唱した「データボイド（Data Voids）[注21]」という概念がある[注22]。データボイドは、信頼できるデータがほとんど存在しないキーワードやトピックに対して、検索エンジンや生成AIが低品質な、あるいは悪意ある情報を参照しやすくなってしまう脆弱性を指す。

たとえば、ある金融機関が新たな資産運用サービスを発表した場合、公開直後には公式Webサイト以外に十分な解説や第三者による評価が存在しないことが多い。このような状況下で、悪意のある者が当該サービスに関する誤解を招く情報や偽サイトを先回りして公開した場合、検索エンジンや生成AIがそれらを参照し、顧客に誤った情報を提示してしまう可能性がある。結果として、誤認に基づく問い合わせの発生、顧客の詐欺被害、さらにはブランド毀損にまで発展する恐れがある。

データボイドには表3のような5つの種類があるとされる。提唱者であるBoyd氏の言葉を借りると、データボイドとは「人間、業務慣行、技術、企業活動の相互作用から生じる社会技術的な悪用」である[注23]。

このような脆弱性への対策として、たとえば、自社や自社製品・サービスに関する情報がオンライン上でどのように流通しているかを継続的に監視することが考えられる。具体的には、自社名や関連キーワードに対する検索結果、SNS・ニュースサイト・レビューサイトなどにおける言及、ダークウェブ上での情報流通、さらには自社ロゴや製品画像の不正利用までを横断的にモニタリングし、ブランドへの脅威を早期に検知する監視ソリューションの導入が一つの手段となり得る。

もっとも、データボイドの脆弱性が顕在化する場である検索エンジンや生成AIは、個々の企業の管理下にあるものではなく、一企業が実施できる技術的対策には限界がある。こ

表3　データボイドの種類

①速報 （Breaking News）	大事件の発生直後、検索急上昇ワードを狙う。正確なニュースが出るには時間がかかるため、わずかな時間差を突き、偽情報などを蔓延させる
②戦略的な新語 （Strategic New Terms）	独自の新しい言葉をつくり出す。新しい言葉を使った有害な情報をインターネットに仕込み、気になって検索した人を誘導する
③時代遅れの言葉 （Outdated Terms）	使われなくなった古い用語の隙を突く。検索エンジンの「最新情報を優遇する」仕組みを悪用し、検索上位を奪って有害なコンテンツに誘導する
④断片化された概念 （Fragmented Concepts）	本来は関連している情報同士のつながりを断ち切り、特定のスタンスに偏ったエコーチェンバーをつくり出す
⑤問題のあるクエリ （Problematic Queries）	陰謀論など、大手メディアが使用しない「特殊なワード」の検索結果。正確な情報による上書きがされず、問題のある情報が残り続ける

出所）Michael Golebiewski, Danah Boyd "Data Voids: Where Missing Data Can Easily Be Exploited"より作成（日本語訳はNRIセキュアテクノロジーズ作成）

のため、データボイドへの対応は、個社レベルでの技術的対策のみならず、社会技術的アプローチにのっとり、より広い視野での取り組みと組み合わせて検討される必要がある。たとえば、業界団体を通じた組織間の連携が考えられる。サイバーセキュリティに関する取り組みにおいては、業界ごとに脅威情報を共有するISAC（Information Sharing and Analysis Center）がすでに設立されており、加盟企業間で攻撃の兆候や対応事例を共有する枠組みが運用されている。データボイドをはじめとするコグニティブセキュリティに関する脅威情報（自社業界を標的とした偽情報キャンペーンの兆候や、悪用されやすいキーワード、効果的な対応事例など）についても、こうした既存のISACの枠組みを活用することが有効となる可能性がある。

Boyd氏はデータボイドを「解決する（solve）」ものではなく、「体系的、意図的に、思慮深く管理（manage）されなければならないセキュリティ脆弱性」と位置づけている[注24]。このように、データボイドへの対応は、単なる個社の技術的対策の問題ではなく、業界や社会全体での情報空間のあり方をいかに設計し、管理していくのかという問題でもある。自社で実施できる迅速な一次情報の発信や自社情報に関するモニタリングのような対策と、業界ごとの脅威情報共有を実施しているISACなどでの組織横断的な情報共有や連携の仕組みの設計を、総合的に検討する社会技術的アプローチが重要となる。

5 社会技術的アプローチの実装に向けて

2030年に向け、テクノロジーが社会と複雑な織り目をつくり上げる状況はより加速していくだろう。当然、サイバーセキュリティは「技術の問題でもある」ため、技術的対策の検討は必須である。

しかし、前述した例からも分かるとおり、これらは「技術だけの問題」ではない。そのため、技術的対策の積み上げのみではもはや不十分である。技術と社会の相互作用に着目し、組織内のガバナンス、業務プロセス、組織間の連携などを技術的対策と一体のものとして社会技術的アプローチを設計し、経営層のイニシアチブの下で実践されることが、2030年に向けたサイバーセキュリティにおいて不可欠となる。

V おわりに：心置きなく挑戦するためのサイバーセキュリティ

ドイツの社会学者ニクラス・ルーマンは、「危険（danger）」と「リスク（risk）」を区別した[注25]。ルーマンによれば、危険とは、自らの意思決定とは関係なく外部から降りかかる脅威であり、リスクとは自らの意思決定によって引き受けるものである。2030年に向けたサイバーセキュリティを考えるうえで、この区別は示唆に富む。

本稿でこれまで見た3つの変化を踏まえると、サイバーセキュリティは、経営として何をどのように引き受けるのかというリスクの問題である。

本稿で示した変化1から3のいずれも、企業に問うているのは、未来は完全には見通せないということを前提にどのような意思決定を行うかという経営判断である。セキュリティインシデントが災害級の影響を及ぼし得る

時代においては、インシデントの発生を完全に防ぐことはできないという考えの下、どの程度の事業継続リスクを見越し、どのようなレジリエンスを構築するのかが問われる。エマージングテクノロジーの社会実装が進む中では、新たな価値創出と引き換えにどのようにポジティブリスクとネガティブリスクのバランスを取るかという判断が必要となる。さらに、守るべき対象が情報システムやデータそのものにとどまらず、人間の認知や意思決定へと拡大する中では、自社の技術的対策だけではコントロールし切れないリスクに対し、どのような組織設計やガバナンス、組織間連携を構築するのかが問われる。

ルーマンの含意を踏まえると、サイバーセキュリティは脅威への防御という側面を持ちながらも、それだけにとどまらず、どのような未来を選び取るのかという経営の意思決定の問題として捉え直すことができる。社内外の知見を動員し、本稿も参照したうえで、それぞれの企業におけるセキュリティランドスケープを描いてほしい。そうすることで、サイバーセキュリティは、不確かな状況下で企業が心置きなく挑戦するための条件となる。私たちが今立っているのは、まさにそんな未来への入り口である。

注

1 「リスク」は分野や文脈によってさまざまに定義され、使用される用語である。本稿では、セキュリティ分野において参照されることが多いISO 31000:2018にならい、「リスク」を基本的に「目的に対する不確かさの影響」として捉える

2 情報処理推進機構「情報セキュリティ10大脅威」https://www.ipa.go.jp/security/10threats/index.html

3 世界経済フォーラム“Global Cybersecurity Outlook 2025”（2025/1/13）https://jp.weforum.org/publications/global-cybersecurity-outlook-2025/

4 内閣府「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針」（2025/12/23）https://www.cao.go.jp/cybersecurity/pdf/kihonhoushin.pdf

5 内閣官房「社会的影響が特に深刻な大規模インフラ障害への対応について（ガイダンス）」（2025/7）https://www.cas.go.jp/jp/seisaku/Infura_syougai/pdf/guidance.pdf

6 国家サイバー統括室「サイバーセキュリティ戦略」（2025/12/23）https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025.pdf

7 内閣サイバーセキュリティセンター（現 国家サイバー統括室）「サイバーセキュリティ戦略」（2021/9/28）https://www.cyber.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf

8 Cybersecurity Ventures “Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024”（2023/10/25）https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

9 Munich Re “Record thunderstorm losses and deadly earthquakes: the natural disasters of 2023”（2024/1/9）https://www.munichre.com/en/company/media-relations/media-information-and-corporate-news/media-information/2024/natural-disaster-figures-2023.html

10 IBM “Cost of a Data Breach Report 2025” https://www.ibm.com/reports/data-breach

11 National Security Archive “FACT SHEET: The Biden-Harris Administration has Launched an All-of-Government Effort to Address Colonial Pipeline Incident”（2021/5/11）

https://nsarchive.gwu.edu/sites/default/files/documents/20706743/03-20210511-fact-sheet_-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident-_-the-white-house.pdf
12 内閣府「ムーンショット型研究開発制度」
https://www8.cao.go.jp/cstp/moonshot/index.html
13 一般社団法人産業競争力懇談会「COCN 10 Emerging Technologies 2026」(2026/3)
https://www.cocn.jp/material/74dadbf7ea0f3331ae75d3a7374de434e3902d19.pdf
14 内閣官房 日本成長戦略会議(第1回)資料8-2「総合経済対策に盛り込むべき重点施策(案)」(2025/11/10)
https://www.cas.go.jp/jp/seisaku/nipponseichosenryaku/kaigi/dai1/shiryou8-2.pdf
15 内閣官房 経済財政諮問会議(令和8年第8回)・日本成長戦略会議(第5回)資料3「戦略17分野における『主要な製品・技術等』の官民投資ロードマップ(案)」(2026/6/24)
https://www.cas.go.jp/jp/seisaku/nipponseichosenryaku/kaigi/dai5/shiryou3.pdf
16 標葉隆馬『責任ある科学技術ガバナンス概論』ナカニシヤ出版、2020年
17 総務省・経済産業省「AI事業者ガイドライン(第1.2版)」(2026/3/31)
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20260331_1.pdf
18 国立研究開発法人科学技術振興機構 研究開発戦略センター「コグニティブセキュリティー」(2025/9)
https://www.jst.go.jp/crds/report/CRDS-FY2025-WR-04.html
19 Yoshua Bengio他 "International AI Safety Report (UK Department for Science, Innovation and Technology〈DSIT〉)" (2025/1/29)
https://internationalaisafetyreport.org/publication/international-ai-safety-report-2025
20 AIセーフティ・インスティテュート「『AIセーフティに関する具体的な影響の調査報告書』の公開」(2025/10/31)
https://aisi.go.jp/output/output_information/251031/
21 直訳すると「データの欠落」を意味する
22 Michael Golebiewski & Danah Boyd "Data Voids: Where Missing Data Can Easily Be Exploited" Data & Society (2018/5)
https://datasociety.net/research-library/data-voids-where-missing-data-can-easily-be-exploited/
23 Danah Boyd "Making Sense of Data Voids" Data & Society (2024/8/7)
https://datasociety.net/points/making-sense-of-data-voids/
24 Michael Golebiewski & Danah Boyd "Data Voids: Where Missing Data Can Easily Be Exploited" ResearchGate (2019/10)
https://www.researchgate.net/publication/356909935_Data_Voids_Where_Missing_Data_Can_Easily_Be_Exploited
25 ニクラス・ルーマン／著、小松丈晃／訳『リスクの社会学』新泉社、2014年

著者

木村 匠(きむらたくみ)
NRIセキュアテクノロジーズ マネジメントコンサルティング事業本部 グローバル・リサーチコンサルティング部 グループマネージャー
専門は国内外のサイバーセキュリティ政策に関する調査研究、重要インフラ領域を中心としたセキュリティ戦略策定や実行支援

南朴木里咲(みなみほうのきりさ)
NRIセキュアテクノロジーズ マネジメントコンサルティング事業本部 グローバル・リサーチコンサルティング部 セキュリティコンサルタント
専門は国内外のセキュリティ動向に関する調査研究、グローバルに展開する企業を対象としたセキュリティ対策評価支援