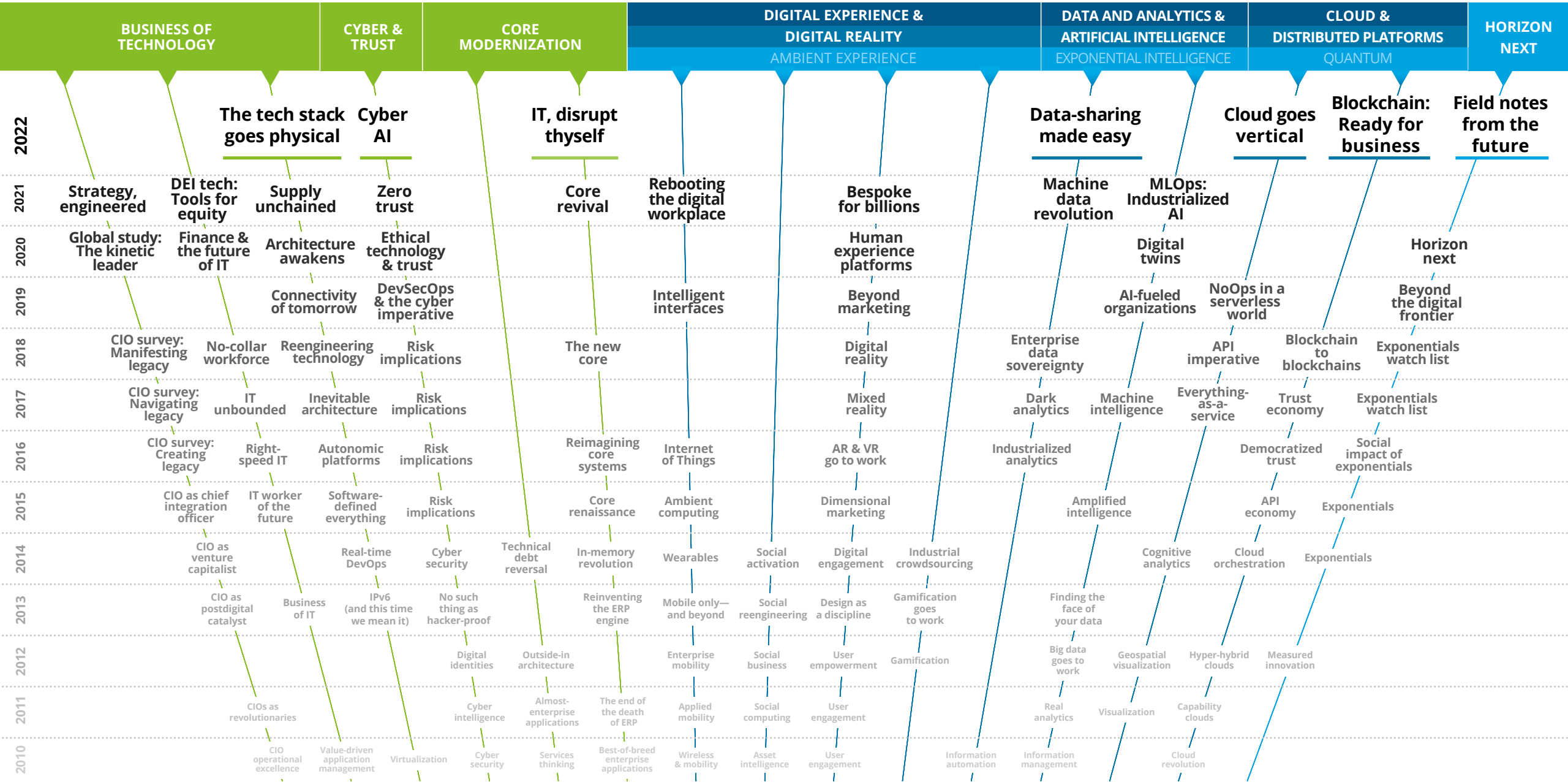
Deloitte.
Insights

Tech Trends 2022

日本版

Trending the trends: Thirteen years of research



日本版発行に寄せて

「Tech Trends」では、毎年、今後1年半から2年の間に、ビジネスに大きな影響を与えるであろうテクノロジーのトレンドを考察しており、今回でグローバル版は13回目、日本版は8回目の発行となる。2022年版では、最初の3章で“Advancing the enterprise”つまり企業がテクノロジーをいかに戦略的に活用し、新たな価値を創出していくかにフォーカスしている。その中では、データやブロックチェーンを活用した、企業の枠を超えた新たなビジネスモデルの可能性や、クラウドを活用した競争優位獲得について考察する。次の3章では、“Optimizing IT”つまり企業が高度な自動化によって事業運営を最適化することや、デジタル化によって企業が新たに考慮すべきガバナンスについて考察する。前者が「攻め」であるとすれば、後者は「守り」であるともいえるが、それはただの効率化や、現状の延長線上にあるものではなく、新たな視点であり、人と機械が協働する世界で人をより付加価値の高い業務にシフトしていくことを狙いとしたものである。そして、最後の1章では視点を少し先に延ばし、今後数年の間に普及期を迎えるであろうテクノロジーの方向性を考察する。

2022年版で取り上げたトレンドの特徴としては、過去のものと比してよりテクノロジーそのものに着目したトレンドの割合が多い印象である。この数年はMLOps（機械学習をスケールするためのDevOps）やエシカルテクノロジーなど、テクノロジーそのものよりも、テクノロジーに対する組織としての構え方・考え方を考察した章の割合が多かった。その背景を考えると、3点が想像できる。

1つ目として、テクノロジーの成熟度が増し、新興と呼ばれていたテクノロジーの多くが実用に耐えられる段階（PoC（概念実証）の次のステージ）まで進化している。例えば、第3章で取り上げたブロックチェーンはもはや新しい技術ではないが、これまで金融業界を中心に活用が模索されていたものが、幅広い業界においても活用事例が見られるようになり、普及期に入りつつある。非金融分野でのブロックチェーン活用は海外企業が先行するが、国内でもデジタルIDや、NFT（Nonfungible Token、非代替性トークン）を活用したエンターテインメント事業など、徐々に事例が増えてきている。

2つ目として、パンデミックの影響でテクノロジー利用が加速し、利用する側の組織も成熟度が増してきた。コロナ禍で新たな経営スタイルやワークスタイルへの急速なシフトを進めた、あるいは強いられた企業は多く、結果としてシステム環境や体制の変革が一定程度進んだ企業も多い。日本企業も例外ではなく、手続きの電子化、業務の遠隔化・自動化や、営業・販売活動のオンライン化といった新たなチャレンジを進め、それに合わせてITガバナンスの見直しやテクノロジー人材のリスキルなど、テクノロジー機能の強化を図った例が多く見られた。コロナ禍という想定外かつ不確実な状況の中で、システム老朽化や人材不足だけではなく、意思決定の遅さなど、コロナ前から認識されつつも先送りされていた課題に対しての危機感が増し、投資計画の具体化が進ん

だ企業も多いのではなかろうか。

3つ目として、企業戦略とテクノロジーがより密接となり、むしろテクノロジーの活用が戦略そのものになってきていることが挙げられる。「Tech Trends 2021」の第1章「新たな戦略への舵取り」においても考察された通り、テクノロジーは市場開拓や新製品開発など、戦略として掲げた事項の重要な実現手段である以外にも、戦略を策定するための環境理解や、戦略の実行状況の把握に至るまで、必要不可欠なものになっている。それは、1〜2年前から急速に注目度が高まっているESGといった取り組みも例外ではない。「2030年までのカーボンゼロ」など、ESGを戦略上の優先事項として経営計画に組み込んでいる企業が増えているが、環境や社会にやさしい新製品の開発（製品そのもの、あるいはR&Dプロセスでのテクノロジー利用）、バリューチェーン・サプライチェーンにおけるGHG排出のモニタリングや最適化、ESG情報開示に至るまで、実現手段としてテクノロジーは欠かせず、逆にテクノロジーの選択において戦略的意図は不可欠になっている。

日本のテクノロジー活用は出遅れているといわれているが、実際はどうなのであろうか。さまざまな調査や、日本企業の方と接している中では、日本企業のDXもキャッチアップが進み始めているように感じている。社内のデータ基盤を刷新し、データドリブン経営にシフトする取り組みや、AIを活用した新規サービスを開発する取り組み、サブスクリプションによる新たなビジネスモデルの開発など、我々がクライアントを支援する機会も増えている。一方で、IPAが発表しているDX推進指標の自己診断結果からは、成熟度に偏りが見られる点は気になる。2019年と2020年のDX推進指標の平均値を比較すると若干の上昇が見られるが、DXに未着手あるいはほぼ実施できていない（成熟度1未満）とする企業の割合は約3割と変化がないことから、キャッチアップしている企業とそうではない企業の二極化が進んでいる可能性はありそうだ[1]。

海外に目を向けてみると、昨年IPAから発行された「DX白書」からは、日米におけるDXの取り組み状況の差が依然として大きいことが分かる。全社戦略、あるいは個別部署でDXに取り組んでいる企業は米で79.4%に対し、日本では55.8%にとどまっているが、差はどこにあるのか。特に大きい差が出ている取り組みとしては、全社的なアジャイル型アプローチ・協調体制の有無、顧客体験といった関連指標の評価への反映、IT基盤の整備状況などが挙げられていたが、興味深かったのは、リーダーにあるべきと考えるマインド・スキルが日米で大きく異なっていた点である。米国企業ではリーダーの「顧客志向」（49.3%）、「業績思考」（40.9%）、「変化思考」（32.0%）に次いで「テクノロジーリテラシー」（31.7%）が重視されているのに対し、日本企業では「リーダーシップ」（50.6%）、「実行力」（48.9%）、「コミュニケーション能力」（43.8%）が重視されており、「テクノロジーリテラシー」を挙げたのは9.7%に過ぎない[2]。海外企業の経営層が日本企業と比べてテクノロジーに明るく、テクノロジーへの関与が高い傾向は、デロイトの「2020 Global Tech Leadership Study」からも読み取れ、我々はそれを、DXの推進力に影響している重要なポイントの1つと捉えていた[3]。これは、日米企業の間だけではな

く、前述の二極化においても差として存在すると推察される。DX自体は目的ではないが、経営戦略を実現する重要な手段である。したがって、経営層がそれを理解し、コミットし、全社的な取り組みとすることが、本来は重要である。また、経営上の意思決定にもテクノロジーが活用される中では、意思決定者がその考え方を理解することも重要であろう。日本的な企業文化に鑑みると、リーダーシップや実行力などが上位に来ることは想像に難くないが、今後のDX推進を加速するにはリーダーが一定程度のテクノロジー知見を持つことも必要である。それは、テクノロジーそのものの仕組みを理解し、作り上げるための専門性ではなく、テクノロジーを客観的・俯瞰的に理解し、ビジネスへの影響を把握し、適用領域を想像することである。そして、本レポートはその手助けができると考える。

デロイトが「Tech Trends」をまとめることにあたっては、2つのこだわりがある。

他社が発行するトレンドの中には2030年の世界観を描いているものもあるが、「Tech Trends」は5〜10年後も見据えながら、1年半から2年先に敢えて注目している。5〜10年後だと先過ぎてアクションにつながらず、1年半から2年後というスパンであれば、今から着手すべき課題として現実感を持って捉えられる上、1〜2年前のトレンドを振り返っても陳腐化しない。

また、技術論ではなく、事業・組織への潜在的なメリットやリスクなど含め、ビジネスの視点でテクノロジートレンドを考察している。そのために、毎年、デロイトのリサーチャーやフューチャリストだけではなく、現場にいる各国のコンサルタントが幾度となく議論を重ね、先進的なクライアント事例も参照しながら数ヶ月をかけて、できるだけリアリティのあるものを作成している。トレンドとしては普遍的なものとなるよう考慮しているが、当然、国・業界によって状況は異なるため、各国で必要に応じて考察を加えており、日本版には日本特有の状況を踏まえた「日本のコンサルタントの見解」を加えて編集している。テクノロジーへの造詣の深さに関わらず、自社においてテクノロジーをどう活用すべきかを考えるきっかけにしやすい内容ではないかと考える。

「Tech Trends」を手に取っていただいた日本の読者は、その事業環境やDXの成熟度など幅広く、すべての企業にすべてのトレンドが今すぐ必要であるということはない。一方で、それぞれのトレンドの背景にある「変化」は多くの企業にとって、今目の前で起きていることであり、どこかのタイミングで何らかの対応は必要になるであろうと考えられる。その「変化」を読み解き、自社の状況と照らし合わせ、今どうすべきか、ビジネス戦略を実現する上でのヒントとして捉えていただきたい。「Tech Trends」では毎年さまざまな視点からトレンドを選定しているため、状況によっては、過去のトレンドを振り返ってもいいであろう。本レポートが貴社のDX推進の一助になれば幸いである。

参考文献

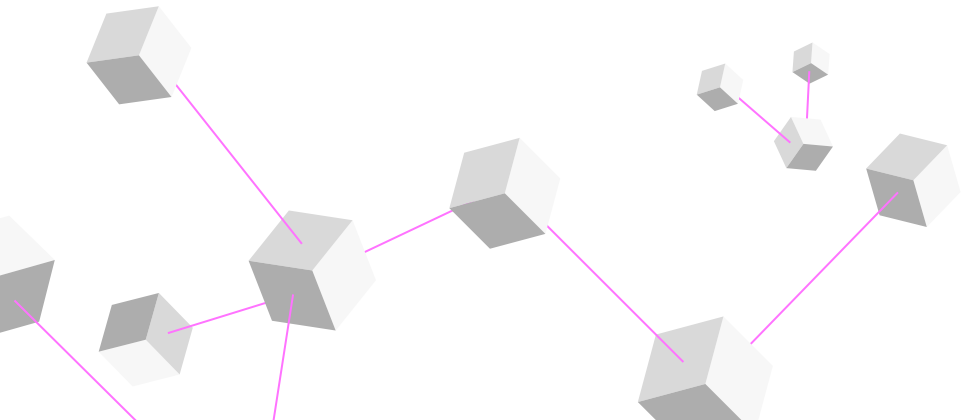
1. IPA, “DX 推進指標 自己診断結果 分析レポート（2020年版）,” “DX 推進指標 自己診断結果 分析レポート（2019年版）,” accessed Feb 22, 2022
2. IPA, “DX白書 2021,” accessed Feb 22, 2022
3. Deloitte, “2020 Global Technology Leadership Study,” Nov 27, 2020

川嶋 三香子

デロイト トーマツ コンサルティング
シニアマネジャー
リサーチ＆インサイトリーダー

Technology Strategy and Transformation

目次



はじめに

過去2年間にわたり、世界はパンデミックの衝撃に揺さぶられてきた。そして我々は今、皆で力を合わせて「新しい日常（ネクストノーマル）」を方向づけようとしている。我々「*Tech Trends*」チームは、この動きがより良い未来を作る機会、つまり単に従来のITを表面的に見直すだけではなく、どうすれば皆が一緒に前進できるかを、根本から考え直すことにつながると信じている。

明言しておくが、前進は排除を意味するものではない。最高のアートは人間の在りように語りかけ、最高のジャーナリズムは人々の懸念を表出させるように、最高のITは我々の生活・活動を革新する。一部の報道が示すように、「スティールワールド」（原題「Robot Overloads」、2014年イギリスで公開）のようなロボットに支配された世界のはじまりを懸念する人々も多い。実際には、AIが支援する未来は暗澹たるものでもなければ、口先だけの万能薬でもない。地に足をつけて見ると、現実は次の通りだ。組織は、AIを用いた自動化によって耐え難いほど退屈な反復作業から人々を解放し、より興味深くより価値の高い課題に集中できるようにしている。それどころか、人々は企業にとってより重要になった。特にテクノロジー領域において、人材の争奪戦はかつてないほど熾烈になってきている。

2022年の「*Tech Trends*」レポートでは、ますます性能が高まるテクノロジーツールを用いて、さまざまな方法によりビジネスプロセスの自動化、省力化、および外部化を進める先駆的な企業を分析する。これらの企業は、このような取り組みを通じて、競争上の差別化をもたらす革新的なプロジェクトにチャレンジするための武器を従業員に持たせている。例えば、ブロックチェーンは、第三者間で発生するプロセスを組織が自動化できるようにするとともに、手動によるデータ交換、データ入力や報告を不要にし、記録すること自体が報告となる環境を作っている。また、主要インフラの大部分の自動化により、IT部門は貴重なエンジニアが本来の業務に集中できるようにしている。そして、サイバーセキュリティーの力を増幅させるAIは、自動的に脅威を検知し対応することで、サイバーセキュリティーを担う従業員の負担を軽減している。

パンデミックが2022年のトレンドを加速させたことは明白だ。しかし、これらのトレンドをCOVID-19による混乱への直接的な対応ととらえるのは間違いであろう。パンデミックは、ビジネスのゴールを再設定するよりもむしろ、シンプルに既存の優先事項の重要性をさらに高めたのである。これまで5〜10年後の取り組みとして受け止められていた、我々が提示するトレンドは、現実には今すぐに取り組むべきものとなっている。顧客は、デジタルとリアルの両方において、極めて優れたエクスペリエンスを求めている。従業員は、どこでも仕事ができることを求めている。競合企業はどうか。昔からの競合企業はこれまで以上に経営を効率化し、新規に参入してきた競合企業

は、進んであなたの会社を蹴落としにかかるであろう。デジタル時代の創造的破壊者は、企業規模の小ささゆえに勝利するわけではない。その無駄のなさによって、決断力、機敏性、レジリエンスに優れた状態となるために勝利するのだ。今日の環境で繁栄するために、老舗企業は、大きく考える（Think big）ためには小さく動く（Act small）ことが必要だと認識し始めている。そのため、これらの企業は自動化、省力化、および外部化に期待を寄せており、同様にしてクラウド、セキュリティーやデータといった、これらのコンセプトをサポートするテクノロジーに関心を向けている。

パンデミックは、自分たちが成し遂げられることの限界にチャレンジするよう人々を仕向けた。生産性の妨げとなるものが取り除かれ、従業員が集中するための環境と力を与えられた場合、我々がどれだけ多くのことを成し遂げられるか、パンデミックは図らずも示したのである。ITの領域においては、リモートワークのインフラ構築と顧客の心を動かす新たな手法の整備を行うために、従業員は山をも動かすような努力で対応した。このことは、IT部門への信頼を高めた。今、企業は次のイノベーションの牽引役となることをIT部門に期待している。つまり、さらに先の山を見つけ、それをも動かすことを期待しているのだ。

同時に、IT部門は自分たちが不安定な立場に置かれていることに気づいている。必要人材が充足していると考えるITマネジャーは少ないだろう。野心に限りはないが資源には限りのある世界において、企業はどのようにして、より少ない資源でより多くの実りを得るかについて頭を悩ませている。

2022年の「*Tech Trends*」では、基本的なオペレーションを維持・高度化するための重要な鍵として自動化を位置づけ、それがどのように従業員の労力をバリューチェーンの上流にある高付加価値の課題解決にシフトさせることにつながるのか、その歩みをたどっていく。

人間こそが未来である。さぁ、仕事に取り掛かろう。

Scott Buchholz
Emerging technology research director and Government & Public Services chief technology officer
Deloitte Consulting LLP
sbuchholz@deloitte.com
@scott_buchholz

Mike Bechtel
Chief futurist
Deloitte Consulting LLP
mibechtel@deloitte.com
@mikebechtel

Bill Briggs
Global chief technology officer
Deloitte Consulting LLP
wbriggs@deloitte.com
@wdbthree

エグゼクティブサマリー

ケーススタディ、洞察、トレンド

データシェアリング時代のはじまり

- CVS Health
- Catena-X
- DARPA
- Kyle Rourke, Snowflake

インダストリークラウドの潮流

- Marijan Nedic, SAP

ブロックチェーン：ビジネス利用への期待

- Caisse des Dépôts
- Chow Tai Fook
- US Department of Treasury
- Andre Luckow, PhD, BMW Group

IT部門の再構築：加速する自動化

- Capital One
- UiPath
- Anthem
- Bill McDermott and C.J. Desai, ServiceNow

サイバーAI：真の防御

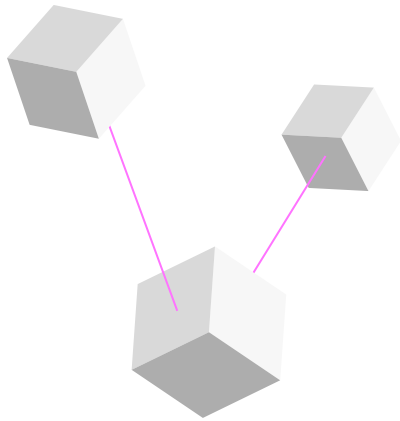
- Sapper Labs Cyber Solutions
- Mike Chapple, University of Notre Dame
- Adam Nucci, US Army

技術スタックは物理化する

- Southwest Airlines
- Southern California Edison
- Sheba Medical Center
- Brad Chedister, DEFENSEWERX

未来のフィールドノート

- Mike Bechtel, Deloitte



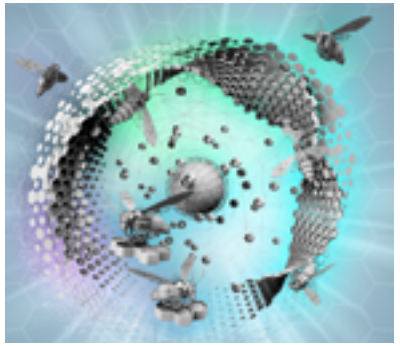
データシェアリング時代のはじまり

いま、多くの新技術によって、企業はプライバシーというベールを纏ったまま社外へデータを共有することが容易になりつつある。それにより、企業はますます、従来制限されていた社外のソースから大量のデータを取り込み、保有する機密データと組み合わせることで、データからより多くの価値を引き出しつつある。これは、事業やオペレーションに対してデータドリブンな進化の機会を新たに提供するだろう。その証左として、エコシステムやバリューチェーン内でも、セキュアなデータを他者と共有することによって新たなビジネスモデルや製品が生み出されつつある。例えば、COVID-19のパンデミック初期においては、臨床データを共有プラットフォーム上で共有することで、研究者、医療当局、製薬会社は治療法やワクチンの開発を加速することができた。さらに、共通のデータ共有プロトコルは広範なワクチン接種プログラムの調整・実施に貢献し、製薬会社、政府機関、病院、薬局が、自身の知的財産を守りながら効率性と安全性に目を向けるという、旧来の二律背反を打開するために大いに役立ったのである。

インダストリークラウドの潮流

デジタルトランスフォーメーションの重心は、従来の業界に依存しない業務のITニーズを満たすことから、各業界・業種固有の戦略や事業運営のニーズを満たすことへ変わりつつある。ハイパースケーラーとSaaSベンダーは、グローバルのシステムインテグレーターやクライアントと協力し、モジュール化された特定分野向けのビジネスサービスを提供している。このサービスは、顧客のビジネス拡大に寄与するアクセラレーターとなることで、顧客に採用され、ビジネス差別化の構築を容易としている。このトレンドが勢いを増すにつれて、アプリケーションのデプロイは「作り込み」から「組み合わせる」プロセスになり、価値創造の考え方そのものを再編しうる変革となるであろう。そして、ビジネスプロセスは購入可能な戦略的な商品と化し、組織は戦略的かつ競争力のある差別化領域へリソースを集中できるようになる。

ブロックチェーン：ビジネス利用への期待

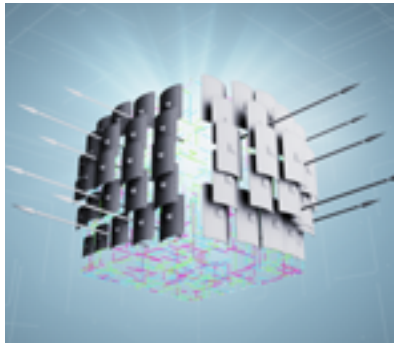


昨今の暗号資産とNFTの流行はメディアを賑わせ、それを目にする人々の想像力を掻き立てているが、こうしたブロックチェーンやDLT（Distributed Ledger Technology、分散型台帳テクノロジー）はエンタープライズ領域でも関心が高まっている。実際のところ、ブロックチェーンとDLTによるプラットフォームはハイプサイクルにおける幻滅の谷を越えて、真に生産性の向上を実現する段階に差し掛かっている。組織間の境界を越えて行うビジネスの本質を変え、企業がアイデンティティ、データ、ブランド、原産地情報、認証、著作権、そのほか有形無形を問わない資産をどのように創出し、管理するかを再考する機会を提供している。特にプライベートなネットワークやプラットフォームにおける技術的な進歩と規制基準の策定が、金融サービスを超えた組織での普及を促進している。企業がブロックチェーンとDLTを使い慣れるにつれ、多くの業界で創造的なユースケースが生まれ、業界を牽引する伝統的な企業は新たな収益源を創造してポートフォリオを拡大し、スタートアップ企業は刺激的で新たなビジネスモデルを考え出していくであろう。

IT部門の再構築：加速する自動化

テクノロジーの複雑さが増し、安定性と可用性に対する期待が高まる中、一部の先駆的なCIOはIT部門の抜本的な変革に取り組んでいる。では、どのように変革を進めているのか。クラウドプロバイダーが持つベストプラクティスを参考にしながら取り組んでいるのだ。クラウドベンダーは、繰り返し人手を介して行われる業務を特定し、自動化やセルフサービスを組み合わせてその効率化を実現している。その結果として、サービス提供までの業務の標準化や価値提供の迅速化、そしてIT基盤全体の効率化と安定化に寄与している。このように自動化は、IT部門を大きく変える可能性を秘めている。過去の「Tech Trends」でも取り上げたNoOpsやZero Trust、DevSecOpsといった技術トレンドには、「組織の枠を超えた自動化の重要性」という共通のテーマがある。従来のような手動管理（モノを人手で管理すること）から、自動化（モノを管理するプログラムを管理すること）へ変革することで、組織は複雑なシステムをより効率的に管理できるようになり、可用性とレジリエンスを高めることでより良い顧客体験を提供できるであろう。

サイバーAI：真の防御

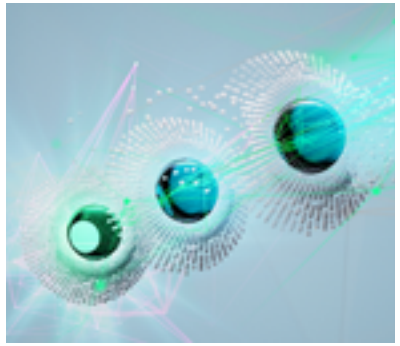


近い将来、セキュリティーチームはサイバー攻撃の膨大な量とその巧妙さ、検出の困難さに圧倒されるであろう。企業における攻撃対象となる領域は急激に拡大している。ネットワークに接続されたデバイス数とともに5Gの利用は拡大、リモートワークも定着し、第三者からの攻撃もますます悪質になっている。すでにAIの助けを借りる時が来ている。サイバーAIはアタッカーの動きよりも高速に対応できるだけでなく、彼らの動きを予測し事前に行動できるため、戦力を何倍にも増強できる可能性を秘めている。データ分析の高速化や異常の特定、脅威の検知など、既存の用途以外にも活用の幅を広げることができる。これら新たなAI技術は、人がサイバー攻撃に対する予防と復旧に集中することを可能とし、より積極的で弾力的なセキュリティー体制の構築を手助けしてくれる。また、AIがビジネス全体に活用されることになれば、それにより、AIリソースの保護やAIによる攻撃への対策も可能となる。

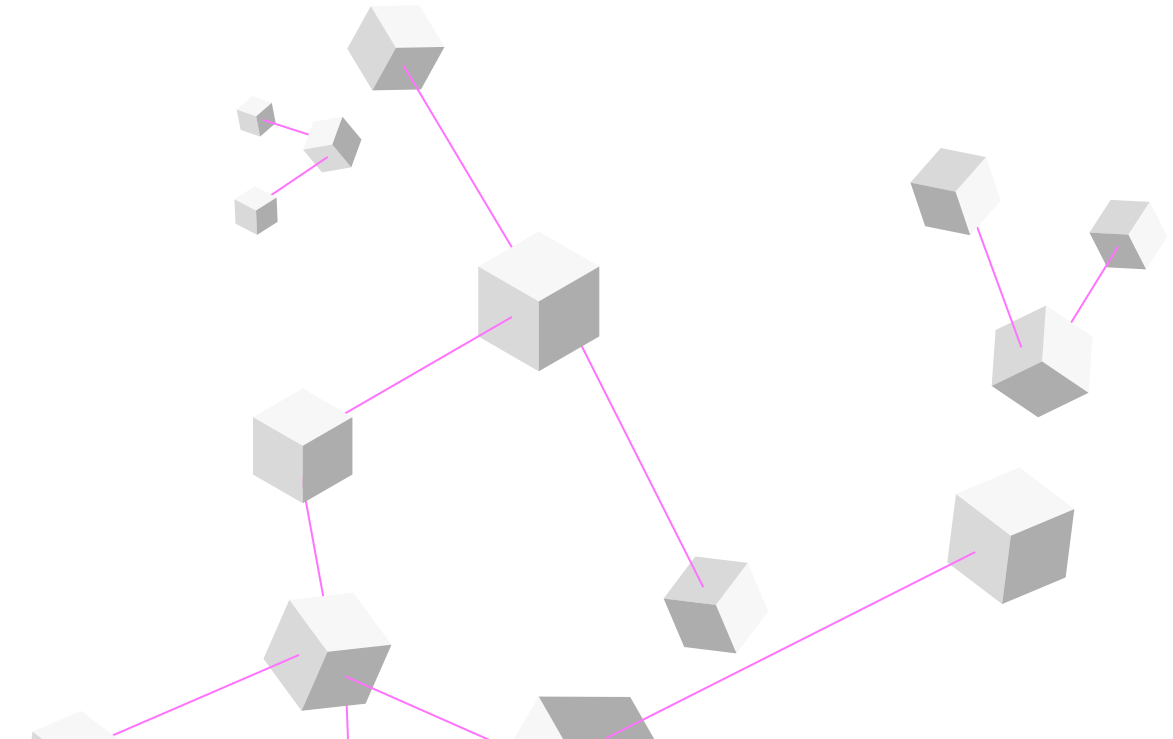
技術スタックは物理化する

「スマートデバイス」の爆発的な普及と、物理的資産の管理作業の自動化が進展することに伴い、ITが担うべき範囲が、ノートパソコンや携帯電話の枠を超えて拡大している。CIOは今後、スマートファクトリーの設備、自動調理ロボット、検査用ドローン、健康モニター機器など、ビジネスに不可欠な数えきれないほどの物理的な資産をどのようにして導入・保守・管理し、安全に保っていくかを検討しなければならない。システム停止はビジネスや人命をも脅かす可能性があるため、進化を続けている物理的な技術スタックに含まれるデバイスには、最高レベルの稼働時間と耐障害性が求められている。また、IT部門には馴染みの薄い基準や規制機関、責任と倫理の問題の管理を支援するため、デバイスのガバナンスと監視に対する新しいアプローチが必要になる場合もある。加えて、CIOは必要なIT人材を確保するとともに、現在の従業員をリスキル（再教育）する方法を検討する必要があるであろう。

未来のフィールドノート



テクノロジーにより洗練された力強い未来が待ち構えている。しかし現在の我々の視界からでは、この力強い未来がどのようなもので、そこで我々がどのように発展しうるかを正確に見極めることはできない。果たして、起こりえそうではあるものの、漠然とした事象に対して我々はどのように対処すべきだろうか。「*Tech Trends 2022*」の最終章である「*未来のフィールドノート*」では、量子技術、エクスポネンシャルインテリジェンス、そしてアンビエントエクスペリエンスという、今後十数年かけてデジタル世界において主流となるであろう、3つのテクノロジーについて検証を行う。まだ黎明期ではあるものの、それぞれのテクノロジーは研究者の想像力を掻き立て、ベンチャーキャピタリスト、スタートアップ、そして企業の投資資金を獲得している。これらのテクノロジーを通じて何か画期的なことが起こる前に、しっかりと計画を立てておくことで、その未来が訪れた際に速やかに行動を起こす準備ができるのである。



データシェアリング時代のはじまり

共有と繁栄

他者とのデータ共有によって新たな機会を創出する

データ資産のマネタイズ

データプラットフォームがデータ売買の安全な仕組みを提供する

データの保護

多岐にわたるプライバシー保護技術が共有データの安全性を担保する

トレンド1

データシェアリング時代のはじまり

データ共有技術・プライバシー保護技術の発展がデータマネタイゼーションに新たな局面をもたらす

データ共有技術の進歩によって、潜在的な価値のある情報資産をクラウド上で誰もが売買できるようになってきた。このデータを、完全準同型暗号化（FHE：Fully Homomorphic Encryption）技術や差分プライバシーなどの新しいプライバシー保護テクノロジーと組み合わせることで、暗号化されたデータを復号化することなく共有し処理できるようになる。セキュリティーとプライバシーを維持しながらデータを共有するという、世界中の可能性を組み合わせて最大の価値を生むためのプラットフォームができつつある。

今日、これらの技術が新たなトレンドに拍車をかけている。プライバシーや規制上の懸念のため世界中のサーバー内に格納されていた機密データは、新しいビジネスモデルの形で、企業の壁を越えて価値をもたらし始めている。今後1年半から2年の間に、より多くの企業が、シームレスで安全なデータ共有方式を模索するであろう。企業は自社の情報資産をマネタイズするとともに、他者のデータを活用しながら自らの事業目標を達成しようと取り組むのだ。

現在はまだ初期段階だが、このデータシェアリングのトレンドは勢いを増している。Forrester Researchの最近の調査によると、世界中のデータドリブンな意思決定者のうち70%以上が外部データの利用を拡大中であり、17%が今後12ヶ月以内にその予定であるという[1]。

さらに、世界のFHE技術市場は単独でも年率7.5%で成長し、2028年には4億3,700万米ドルに達すると見込まれている。現時点では、ヘルスケアおよび金融セクターが多くのFHE技術の活用事例をリードしている[2]。

世界中のデータドリブンな意思決定者のうち70%以上が外部データの利用を拡大中である。

この急速な拡大の要因は何だろうか。簡単にいえば、データは共有されることで価値を増す。ガートナーは、データシェアリングを推進する企業は、2023年までに多くのビジネス指標で競合他社に対して優位になると予測している[3]。

次のようなデータシェアリングの活用例を考えてみよう。

- **データを集約して共通の目標をセキュアに達成する。**提携関係であっても競合関係であっても市場内の各企業と連携して、顧客に対する洞察を深めること、マーケット共通の不正パターンを検出することや、共通の目標を達成することができる。

- **効率性を向上しコストを削減する。**データ提供者はもはやハードウエアのプロビジョニング、データベースのメンテナンス、アプリケーションプログラミングインターフェース（API）の構築を行う必要がなくなった。顧客はボタンを押すだけで、匿名化され、キュレーションされたデータフィードにアクセスできる。企業内においても、暗号化されたデータによってAI（Artificial Intelligence）や機械学習（ML：Machine Learning）の処理がよりセキュアとなり、コンプライアンスの監査も容易になるであろう。

- **コラボレーションによる研究を拡大する。**重要な研究イニシアティブを他者と協力して加速させるために、基礎的または初期段階の調査結果であれば、競争優位性を損なうことを恐れずに共有することができるであろう。

- **知的財産のセキュリティーを高める。**AIトレーニングデータなどの非常に機密性の高いデータは、パブリッククラウドに蓄積されている場合も含め、より適切に保護することが可能となる。

- **高速通信中のデータを暗号化する。**高頻度取引、ロボット手術、スマート工場などの分野では、機密データの通信が組織を跨って高速に行われる。FHE技術によって、重要なデータも暗号化キー無しで素早くアクセス可能となる。

共有とプーリングによってデータをマネタイズする機会は先行者利益を生むと考えられるため、今日の各市場のリーダーたちは大いに関心を寄せている。近い将来、データシェアリングのエコシステムへ新たに参画する者は、同じプラットフォーム上にすでにいる競合他社がデータ資産を活かしてはるかに多くのことを実現してきたことを知り、神の慈悲にすがる思いを持つであろう。このとき、企業は、AIとデータを最大限駆使する組織に変革しなければならないと、改めて意志を固めることになるのだ。

データ共有の新しい在り方

デジタルトランスフォーメーションの生命線であるデータは、「*Tech Trends*」で幾度となく取り上げている。例えば「*Tech Trends 2021*」では、企業がMLOpsを実現するためには、データをこれまでとは全く異なる方法で管理する必要があることを述べた[4]。今日、データシェアリング革命により、企業は

社内外の境界を越えて、より安全に、より多くのデータにアクセスすることが可能となりつつある。しかし、改めていおう。データが共有されることの価値を享受するためには、データの管理方法を大きく変える必要があるのだ。ここにきて、情報資産を従来のプライバシーやセキュリティーの制限から解放する革新的なテクノロジーと手法が登場してきた。

今年は、**機会**、**使いやすさ**、**プライバシー**の３つの観点からデータに関するトレンドを見ていこう。

共有と成功：新しいビジネスモデルと機会の創出

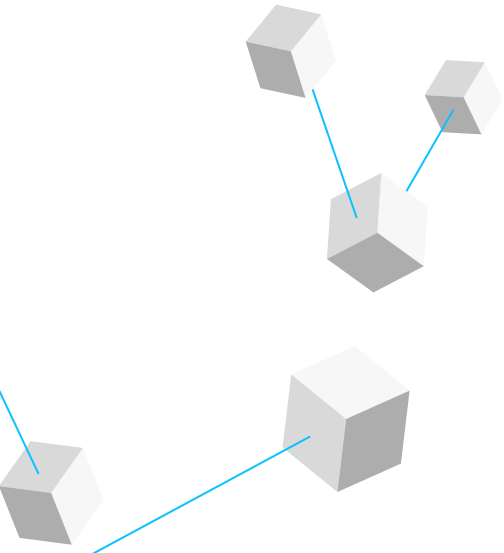
共有されたデータは、新しいビジネスモデルを生み出すことができる。データ共有のトレンドが進むにつれ、共通課題の解決、相互に有益な新たなビジネスや研究の機会として「データコラボレーション」に取り組む企業が増えることが予想される。さらに外部のデータ管理サービスプロバイダーと安全にデータを共有することで、企業はデータ管理プロセスを合理化し、関連コストを削減することができる。ここではデータ共有によってもたらされる新たな機会について考えてみたい。

- **業界別の市場。**手強い競合他社との間でさえ、「データコラボレーション」により解決できる共通課題は多々ある。例えば食品業界のサプライヤー全社が機密性の高い販売・配送データを匿名化し、分析・蓄積を可能にしたとしたら、おそらく業界内での需要と供給の全貌を明らかにすることができるであろう。あるいは発展途上国の銀行においては、匿名化された信用データを蓄積して、銀行間の信用リスクスコアリングシステムを構築することも可能である。また、最も大きな可能性の１つとして、製薬業界においてデータを蓄積して共有することにより、研究者や医師が患者の命を救うための新たなイノベーションを、より早く市場にもたらすことにつながるかもしれない。

データ共有のトレンドが進むにつれ、共通課題の解決、相互に有益な新たなビジネスや研究の機会として「データコラボレーション」に取り組む企業が増えることが予想される。

- **バリューチェーン内でのデータ共有。**多くのメーカーや小売業者は、第三者であるデータブローカーから消費者データを購入しているが、企業活動に影響を与えるほどのデータは十分に入手できていない。サプライヤーからメーカー、マーケティング担当者まで、バリューチェーン内のパートナーのシステムが顧客データを蓄積して、需要に関するより精細なイメージを作成するのはどうであろうか。

- **AIモデルトレーニングの外注化。**AIモデルは、よく機密性の高い知的財産とみなされる。しかし、AIモデルは一般的なUSBメモリーに収まってしまう程度のサイズしかなく、高いセキュリティーリスクを伴っていることから、これまで多くの企業は社内で独自のモデリングを行ってきた。しかし、暗号化技術の進歩でその状況は変わりつつある。モデリングデータが保護されていれば、データ管理の責任者は安全にAIモデリングとトレーニングを第三者に委託することができるようになるのだ。



- **データ購入の効率化。**データ共有プラットフォームでは、ボタンをクリックするだけでリアルタイムの市場データやロジスティクスデータへのアクセスを購入することができる。データプロバイダーはAPIやデータファイルを提供する必要がなくなるのだ。

外部データの取得はボタンひとつに

クラウド型のデータシェアリングプラットフォームは、組織がデータをシームレスに共有、購入、販売することに役立っている。これらの仮想化された高性能のデータマーケットプレイスは、通常、サービス加入者が有料でデータを管理、キュレーション、およびカスタマイズできる「データシェアリング・アズ・ア・サービス」モデルとして構成されている。また、サービス加入者は、プラットフォームが提供するデータ分析のための安全な「クリーンルーム」を使用して、ある程度データを保護することもできる。最後に、サービス加入者は、自分のデータを集約してほかのサービス加入者にデータへのアクセス権を販売することもできる。データ購入者は、市場、製品、調査においてこれまでと異なる側面を見ることが可能となる。

この「シェアリング・アズ・ア・サービス」モデルを支える基本的なビジネス戦略は、音楽ファイル共有やソーシャルメディアなど、ほかの注目を集める情報やコンテンツ共有の分野ですでにその有効性を実証している。これらの例では、ベンダーが使いやすいデータシェアリングプラットフォームを提供し、顧客がコンテンツ（データ）を提供している[5]。

データマーケットプレイスの分野は、現在、ゴールドラッシュの初期フェーズにあり、Databricks、Datarade、Dawex、Snowflakeなどのスタートアップと、AWS、Microsoft Azure、Google Cloud、Salesforceなどのハイパースケールクラウドプロバイダーが、この有望な市場のシェアを求め競い合っている。デジタルトランスフォーメーションの加速とともに、データの成長とデータの民主化が結びつく

ことで、外部データの需要が急増するという未曽有の変化を創り出している[6]。もはや、データは経営陣の意思決定のためのツールではなく、販売、購入、取引、共有されるビジネス上で重要な資産である。そして、データの共有を最も簡単かつ効果的に促進するプラットフォームが、最終的には特定業界向けまたは市場全体でのデータ共有の標準になる可能性がある。

多くの組織がデータ資産の収益化と拡張の機会を追求し始めたことにより、データ共有のユースケース（一部は成功事例）が急増している。例えば：

- COVID-19のパンデミックがはじまった当初、激しい競争を繰り広げていたグローバル製薬企業は、データ共有プラットフォームを介して前臨床研究データを共有する方法を模索するようになった[7]。
- COVID-19のワクチン管理者は、国が運営する一元化されたプラットフォームを使用して、毎日、詳細なワクチン接種と検査データを公的医療機関と共有した[8]。
- グローバル金融サービス会社の投資マネジャーは、バックオフィス、ミドルオフィス、フロントオフィスからリアルタイムにデータを収集して分析している。その結果、投資データをクライアントに共有するために必要な時間が、「数ヶ月から数分」に短縮された[9]。

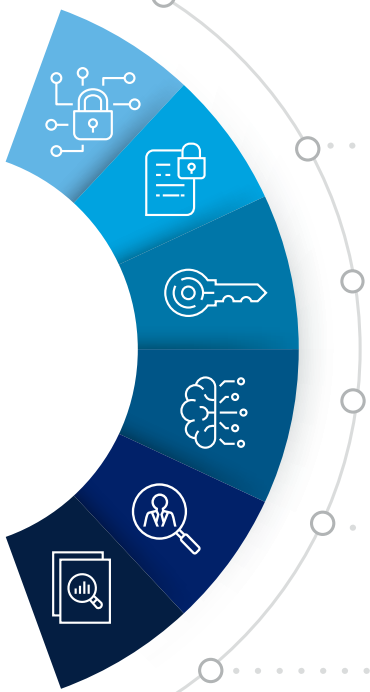
今後、データシェアリングプラットフォーム市場がどのように進化するかはまだ見えていない。最終的には、ある程度の統合と標準化が行われ、複数のプラットフォーム市場が根付く可能性がある。例えば、プライベートデータマーケットプレイスには、独自のニーズをターゲットにしたシステムやパートナーが出現する可能性がある。データ市場が最終的にどのような形になるにせよ、ベンダーが強固なセキュリティーを開発して、より多くの組織がこれらのプラットフォームに参加するようになり、消費可能な外部データの量が増加していくにつれて、ゴールドラッシュは続き、勢いは増していくであろう。

プライバシーを犠牲にすることなくデータを共有する

データは、共有することでその価値を発揮する。しかし、データに関するプライバシーポリシーや競争上必要とされる秘密保持は、この価値を実現する際の妨げとなってきた。今日、*プライバシー保護コンピューティング*（または、機密コンピューティング）と呼ばれる新しい技術が、プライバシーの足枷からデータと組織を解放しようとしている。FHE、差分プライバシー、機能的暗号化などの技術によって、組織はプライバシーを犠牲にすることなくデータを共有し、その利益を得ることが可能になる（図1）。

図1

データ共有における6つのプライバシー保護技術



完全準同型暗号：データは共有される前に暗号化される。
分析は可能だが、元の情報を解読することはできない

差分プライバシー：データセットにノイズを追加することで
元データのリバースエンジニアリングを防ぐ

関数型暗号：特定のユーザーに鍵を与え、
暗号化されたテキストのうち鍵の該当部分のみを復元可能とする

統合分析：データ自体を共有することなく、
分析から得た洞察を共有できる

ゼロ知識証明：ある値に関する知識を持っていることを、
その知識に関する情報を明らかにすることなく証明することができる

マルチパーティ計算：データをいくつかの断片情報に分割し、
計算を行うことで、元のデータを見ることなく処理が実行される

出典：Deloitte research and analysis

データの共有を可能にするためのプライバシー保護に関する技術は、同じ業界の競合他社間の協業すら可能にする。複数の領域で競合する金融機関の例を考えてみよう。彼らは互いに競争関係にあるが、一方で過度な与信集中リスク、高度な詐欺パターン、金融犯罪を見つけるという、共通の目標を達成するために競合を超えた連携を望む場合がある。

ほかの例として、競合はしていないものの、旅行業界のように複数の企業と連携する例を考えてみる。航空、ホテル、レンタカーなどの旅行関連企業がデータを共有し、共同マーケティングや割引キャンペーンを行うなどのユースケースが考えられる。そのデータ共有の仕組みに参加している企業は、ほかの企業の顧客動向や活動について知ることにより、それぞれの顧客に対して、より高い価値や良いカスタマーエクスペリエンスを提供できると考えている。しかし、それぞれの企業は、顧客の情報を守る義務がある。プライバシーを保護する技術は、企業がより深く協業する画期的な触媒になるであろう。

現在、データの共有を進める鍵となるプライバシー保護技術の進展を遅らせている課題が４つある。

1. プライバシー保護技術の多くは、データを利用するための新しいツールの導入とシステムの変更を必要とする。これらのツールの導入やシステム変更を行うためには、すでに多忙なチームがさらに多くの労力を割かなければならない。

2. プライバシー保護技術の導入により、処理速度やパフォーマンスに影響がでる場合があり、それは、データインモーションやリアルタイムのデータ分析や共有を行う場合に問題となる可能性がある。

3. 現時点では、他者の手に渡ったデータに対して、ガバナンスを維持する簡単な方法はなく、潜在的なプライバシーやコンプライアンスに関するリスクが残る。

4. プライバシー保護技術による利益を享受する前に、プライバシーとデータ所有に関する規制という壁に対処する必要がある。

しかし、これら４つの課題への対応は進展を見せているため、今後１年半から２年のうちに、プライバシー保護技術によってさまざまなデータシェアリングのユースケースが登場するのは合理的な予測の範囲内といえよう。

進むべき道

プライバシー保護技術と高度なデータ共有技術は、データの共有により新たなビジネス展開を目論む組織にとって、データからより多くの価値を引き出す手助けとなっているが、これらの技術はすべてのデータ管理要件と課題に対する万能薬ではない。引き続き、強力なデータガバナンスが必要であり、タグ付けやメタデータも今まで通り必要とされるであろう。

さらに、新しいツールとアプローチは、長年にわたって培われた企業のデータに関する文化を一夜にして変えるものではない。例えば、既存の企業はデータを管理し、利用するためのプロセスや標準を確立していることが多いが、スタートアップやデジタルネイティブはもっと緩やかなアプローチをとる可能性がある。また、家族経営の企業では、意思決定や戦略に個人が強く関わっているため、一般的には、企業の壁を越えてデータを共有することに（たとえデータが匿名化されていても）消極的である。

現時点では、データ共有の推進を阻む課題は確かに存在する。ただし、それは、今までとは全く異なる、データシェアリング時代に至る道に現れた、ちょっとした凹凸に過ぎないのではないか。サーバーには多くの未開発の資産が眠っているというのに、これ以上ぐずぐずしてはいられない。

最前線からの学び

ワクチン配布のためのデータ基盤を構築したCVS

全米で約10,000店舗を展開し、インフルエンザなどのワクチンを年間通じて提供してきた実績を持つCVS Healthは、歴史的なCOVID-19ワクチンの導入に大きく貢献してきた。それでも、ワクチンが2021年春に広く普及してきた際、薬局や大手小売店は予防接種が最も必要とされる時期と場所を把握するためにアナリティクスが必要となった。小売データエンジニアリングのシニアディレクターであるKarthik Kirubakaranは、「効果的なデータ戦略を導入していたため、数ヶ月ではなくわずか数週間で機能を拡張し、新しいシステムを展開することができた」と語り、組織のデータマネジメントプロセスおよびテクノロジーにより課題に対応できたと述べる[10]。

Kirubakaranとチームは、ワクチンサプライヤーやアメリカ疾病予防管理センター（CDC）から外部データを収集し、需給を予測した。そして、この情報を社内システムに取り込み、患者の予約やパートナーのクリニック開業、さらにはアナリストによる活動の効果測定などに活用した。さらに、研究機関や大学ともデータを共有し、ワクチン接種率測定の支援も行った。彼らはパンデミックの中、これらすべてをかつてないスピードで実施したのである。幸いにもCVS Healthが採用するデータ構成により、データ共有ツールで安全かつほぼリアルタイムのデータ交換を実現しながら、受け取ったデータを素早く理解することができた。「ただひとつのテクノロジーに集約するのではなく、複数のプラットフォーム上でデータメッシュアーキテクチャーを構築していたことが、我々の迅速な行動につながった」とKirubakaranは語る。

チームは直ちにガバナンスを確立し、データ保護およびプライバシーやデータセキュリティーに関する法令への対応に注力した。さらに、データの所有者と管理責任者を明確に定義し、転送中のデータおよび保管データに対してそれぞれ異なるレイヤーでセキュリティーをかけた。ひとつの例として、外部のデータクリーンルーム技術を活用しデータを匿名化することで、アナリストが個々人の識別情報ではなく人口統計学に基づいたセグメンテーションを利用してプログラムを評価したことが挙げられる。

ワクチンの導入を続ける中で、CVSは新たな課題にも直面した。小売店にワクチンの提供を続ける際、Kirubakaranのチームはバーチャル上で集い、人口動態と需要データを入念に調べ、ワク

チンが行き届いていない地域を特定することに注力した。「より正確な予測を立て、必要とされるところにワクチンを届けることが重要だった」とKirubakaranは語る。また、チームは各店舗からの供給情報をもとに予測を更新し、さらには、COVID-19のワクチンの在庫状況をインターネットで検索することで、需要が高い地域を把握した。

CVSはワクチンの導入が落ち着くにつれ、このデータシェアリングのノウハウをほかのユースケースにも活用していくつもりだ。例えば、リアルタイムデータを使い、小売店での顧客の買い物かごの中身を把握し、それらと過去の購買行動を照合することで、会計時にその顧客に最適なクーポンを発行する取り組みなどにチャレンジしている。これは、顧客は物を売る相手ではなくサービスを提供する相手として接する、というCVS上層部の方針に沿ったものである。「重要なのは、社会に貢献し、かつそれらを顧客とシームレスな方法で行うこと、さらにアクセスできるデータのみを活用することだ」とKirubakaranは述べる。

自動車業界のバリューチェーンにおけるコラボレーションモデルに変革をもたらしたCatena-X

ヨーロッパにおいて、自動車業界はすでに成熟した産業である。この業界の慣習は洗練されており、綿密な計画のもと、「必要なものを、必要なときに、必要な分だけ」供給するジャストインタイム生産方式を採用しており、予測不能な事態に影響されることはほとんどなかった。しかし、COVID-19による供給遅延および半導体不足という2つの危機に直面する中、ヨーロッパの自動車業界は迅速な対応が求められる一方で、サプライヤーから顧客、そしてリサイクル業者までを含む自動車業界のバリューチェーン全体において得られる情報はわずかであった。そこで、BMWグループ、Siemensといった複数の大手メーカー、サプライヤーそしてテクノロジー企業は力を合わせ、新たな働き方を考案した。

その結果、28社のパートナーによる、「Catena-X」と呼ばれる情報交換のエコシステムが設立され、企業が好きな時に、プライバシーおよびセキュリティーが担保された状態で情報を共有することが可能となった。「我々はバリューチェーンにおけるパートナーと協業し、新たな道を切り開くコラボレーションプラットフォームが必要であった」とCatena-Xの代表であるOliver Ganserは述べる[11]。

Catena-Xはラテン語で「チェーン」を意味するが、GAIA-Xとして知られる欧州連合（EU）のデータシェアリングに関する認証基準に基づいた最初の主要事例の1つとして2021年8月に発足した[12]。GAIA-Xが採用する分散型アプローチは、EU共通基準に準拠した複数のプラットフォームから構成され、GAIA-Xを利用することで、企業はデータ主権を保護しつつ、業界を越えたデータの共有および活用ができるようになる。「企業が各々でデータの信頼性を担保せずとも、GAIA-Xのフレームワークを介してすべてのデータの信頼性が担保される」とGanserは述べる。

GAIA-Xは一定の基準を設けていたが、中小企業や大企業はCatena-Xに参画し、彼らが抱えるサプライチェーンの問題に対処することを決断した。ひとつの例として、ある自動車メーカーの事例が挙げられる。メーカーが数万台に影響を及ぼす可能性がある品質問題を発見した際、通常は大規模なリコールを行い、サプライヤーに数億円にのぼる賠償金を請求するが、その自動車メーカーは、Catena-Xによりサプライヤーとデータを共有することで品質の問題点をピンポイントで特定し、リコールが必要な車の台数を80%以上削減することができたのである[13]。

近い将来、Catena-Xは企業資源計画（ERP）と連携してデータを転送できる、より使いやすい環境を提供する予定だ。また、小規模サプライヤーが直接データをアップロードできるSaaS（software-as-a-service）のようなポータルサイトの準備も進めている。Catena-Xは、新たな企業が参画し、バリューチェーンにおけるさまざまな分野のパートナー同士がつながることで、新たなビジネスモデルが生み出されることを期待している。例えば、パートナーは特定のパラメータを含んだデータ共有に対して成功報酬を支払うかもしれない。サステナビリティやサーキュラーエコノミーの実現もまた主要な取り組みである。Ganserは、「企業がこのアライアンスに参画する一番の理由は、彼らが抱える複雑なビジネス問題を、共有されたデータを用いて解決することである。データでマネタイズすることは我々の優先事項ではない」と語る。

一方、Catena-Xのボードメンバーは、ドイツの製造業のような長い歴史を持つ産業を変革することの難しさを認識している。Cantena-Xのボードメンバーの1人であり、Siemensの取締役でもあるClaus Cremersは、「これはテクノロジーに限ったことではない。自動車業界そのものの変革である」と述べる[14]。ボードメンバーはバリューチェーンの見直し、そしてメンバーへのベンチャー精神の植え付けに注力しており、いずれはヨーロッパにとどまらずグローバルで受け入れられ、コラボレーションができることを目指している。「我々は今後も車を製造し続けること自体は変わらないが、従来のやり方にこだわらず、新たな手法でビジネスを続けていくことができる」とGanserは述べる。

データ暗号化技術を強化したDARPA

アメリカ国防高等研究計画局（DARPA）は、新技術を生み出してきた歴史がある。アメリカ国防総省の機関であるDARPAは、インターネットやパソコンから、ドローン、GPSなどに至るまで、あらゆる技術の開発に資する研究を支援してきた。最近では、DARPAは拡大するクラウドコンピューティングや仮想ネットワークに対応するため、プライバシーとセキュリティー上のリスクを抑えつつデータを共有するための新しい手法の研究を進めている。DARPAのプログラムマネジャーであるTom Rondeau博士は、プライバシー保護技術を通して信頼を築くことがデータ民主主義の価値観にとって重要だと考えている。「プライバシーとセキュリティーが保たれる方法で情報を共有できることは、データ民主主義にとって欠かせない」と、Rondeauは語る[15]。

Rondeauは、「Data Protection in Virtual Environments」（DPRIVE）プログラムを主導し、高度な暗号化技術の実現を支えるハードウエアを開発するスタートアップや既存企業に出資している。標準的な暗号化技術では、転送中または保管データの安全性を保つことができるが、計算時はデータを復号する必要があるため、データがサイバー攻撃の脅威にさらされていた。一方、DPRIVEは、計算中でもデータ安全性を保つことができる技術である完全準同型暗号化（FHE）の実現に注力している。これまで、機密データストアにFHE技術を適用する際、数ヶ月もの計算時間を要することもあったが、DARPAは特殊なチップやコプロセッサーを開発することで、この時間を大幅に短縮することを目指している。このプライバシー保護技術が普及し、スマートフォンやタブレットに組み込まれると、全ユーザーのデバイス上でデータが安全に取得かつ保管できるようになり、また、暗号化されたデータのみが分析のために別の場所に送信される。「FHEの実行時間を短縮することができれば、ほぼすべてのアプリケーションにおいて、この技術はデータ処理アプローチの基本的な部分となるであろう」とRondeauは述べる。

DPRIVEチームはFHE技術を利用し、その厳密さ、つまり計算難度をもってセキュリティー規格を作成しており、データの安全性は明白である。Rondeauによると、セキュリティーのレベルを把握することは、金庫の選び方に似ているはずだという。金庫は熟練した強盗が破るのにかかる時間で評価される。このセキュリティー評価は、購入者が貴重品の保管手段に関する意思決定を行う際に役立つ。同様に、データ管理チームが、さまざまな種類の暗号化をハッキングするのにかかる時間を把握していれば、セキュリティーが最も必要な情報や、ハッキングを防ぐために暗号化コードを変更すべき頻度を見極めることができる。Rondeauは、「我々は、ユーザーがデバイスを使用する際に守られている、と感じてもらうだけでなく、自国の安全性をより正確に測定するためにも、何がどれだけ安全であるかを正確に示す必要がある」と語る。

また、DPRIVEは、国家安全保障上の脅威に関するデータをほかの政府と安全に共有するための重要なユースケースを実現している。「FHEは、情報源や機密情報の収集技術を保護しつつ現場からの機密情報を共有する手段になりうる」とRondeauは述べる。同様に、金融犯罪の分析の場合、銀行は顧客データの保護が義務付けられている一方で、法執行機関は犯罪を分析するためのデータを必要とする。Rondeauは、高度な暗号化技術により、プライバシーを侵害することなくマネーロンダリングの特定に必要なデータを双方が共有し、分析できるようになると考えている。

今日において、FHE処理は非常に計算負荷が高く、多くの用途において時間がかかりすぎてしまう。DARPAはパートナーと協力し、高性能なハードウエアを用いてこの技術的な問題を解決しようとしているが、最終的には、この問題に対する解決策の選択肢を増やすことを目指している。Rondeauとチームによると、プライバシー保護の技術者、技術、そして規格が当たり前のものとなれば、時間とともにすべての人のプライバシーを向上させることができるという。Rondeauはこの技術について、「これは、情報のセキュリティーとプライバシーに関する民主主義の原則を支え、実現する技術であり、今後大いに貢献していくだろう」と語る。

私の見解

Kyle Rourke
Vice president of global platform strategy, Snowflake

大多数の企業のIT環境がハイパースケイラーと呼ばれる主要クラウド企業のものに移行していくにつれ、世界中のデータがクラウドプロバイダーを介し、ほんの一握りの物理データセンターに集約されてきている。

しかし、この現象だけで、データへのアクセス性の向上や、自社の範囲を超えたデータを活用したマネタイズが可能になるわけではない。Snowflakeは、企業が効果的にデータを共有し活用するためにはデータのサイロ化（孤立化）を解消する技術に支えられ、かつ信頼性とガバナンスに優れたネットワークが必要だといち早く気づいた。

Snowflakeのサービスは、企業がクラウド上にデータを保管し、分析することを実現してきた。顧客は我々のテクノロジーの高いパフォーマンスや同時処理

能力を実感するにつれ、より多くのデータを活用することへの意欲が高まっていった。そして、そのデータにはほかの企業が所有するデータも含まれていた。そこで昨年、我々はすべての顧客が接続可能な単一のネットワークを構築する基盤技術を発表したのである。これは、1つの大規模なリレーショナルデータベース、もしくはデータのための一種のソーシャルネットワークに似ている。この技術により、企業はプラットフォーム上でアクセスを許可するだけで、ほかの企業とリアルタイムにデータを共有できるようになった。我々は、企業間のやりとりが急激に増えていることを実感している。

さらに、企業はほかの企業とのデータ共有やデータを結合することで、さまざまな革新的な製品やサービスを生み出している。例えば、位置情報を収集している企業は、ドライバーが最も必要とされている場所に関するデータを、ボタンをクリックするだけでライドシェア企業に配信できる。出版社などのメディア企業は、顧客データと小売店からのデータを組み合わせて新しいデータセットを作成することで、自社の広告や製品のターゲット選定に活用することが可能だ。将来的には、データのネットワークはソーシャルネットワークのように成長する可能性すら秘めている。この技術が飛躍的に広まっていくことで、新しい、かつ、誰も予期しない方法で価値を創造していくに違いない。

いまや、データの共有方法は業界の垣根を越えて進化している。これまで企業は、データの収集や収集したデータの自社サーバーへのアップロードを安全な方法で行うこと、かつそれらがポリシーに準拠していることを担保することなどが求められてきた。しかし、我々の技術を通して「生きた」データの市場が拡大し続けることで、企業はデータの取り込み、メンテナンスやコンプライアンス維持にコストをかけずに、データをサービスとして購入または販売することができるようになるのだ。データ共有に対する障壁が低くなることで、企業はさらに創造力を発揮できる可能性を秘めている。かつて企業内でサイロ化されていたデータは解き放たれ、多くの企業に利益をもたらしつつあるが、今後どのような斬新かつ利益を生み出す使い道が見つかるのか、その可能性は未知数である。

もちろんデータ共有においては、プライバシー保護のための対策を講じる必要がある。我々が提供するようなデータネットワークは、ガバナンスを強化することで、企業からの信頼を得て、データ共有への意欲を促進することが重要だ。例えば、「クリーンルーム」と呼ばれる環境により、データの安全性を維持するためのガイドラインを遵守した上で複数企業のデータを収集し、分析することができる。制限されたクエリにより、アナリストが個人を特定できる情報（PII：Personally Identifiable Information）などの機密データへドリルダウンすることなく、匿名化されたレコードを収集し、作成したモデルに取り込むことができるのだ。

外部データを利用した解析やモデル作成を可能にするこの技術はそのうち珍しくないものとなるであろう。顧客がデータのさまざまな活用方法を模索するとともに、我々が目指すべき方向性をも教えてくれているのだ。我々が今目にしている変化は、インターネットが情報へのアクセスの自由化・民主化をもたらしてきた一連の流れに似ている。データを安全かつ信頼できる方法で活用できるこの技術は、ビジネスに全く新しい可能性をもたらしてくれるだろう。

今後の展望

ストラテジー

CEOは、データシェアリングから生まれる新たなビジネスモデルに目を光らせておくべきだ。もし今日のデータ交換プラットフォームが次世代のバーコードのような存在にまで成長すると、データのマネタイズ、もしくは新たなパートナーシップ展開などさまざまなチャンスが生まれてくるであろう。その際、この新たなデータのパラダイムシフトの波にいち早く先駆者として乗るか、それとも、後れをとらずに追従者として乗るかの決断が重要になってくる。各社のビジネスの性質によっては、早期にこのトレンドに乗ることが、今後のデータシェアリングの取引条件形成において主導権をもたらす可能性がある。

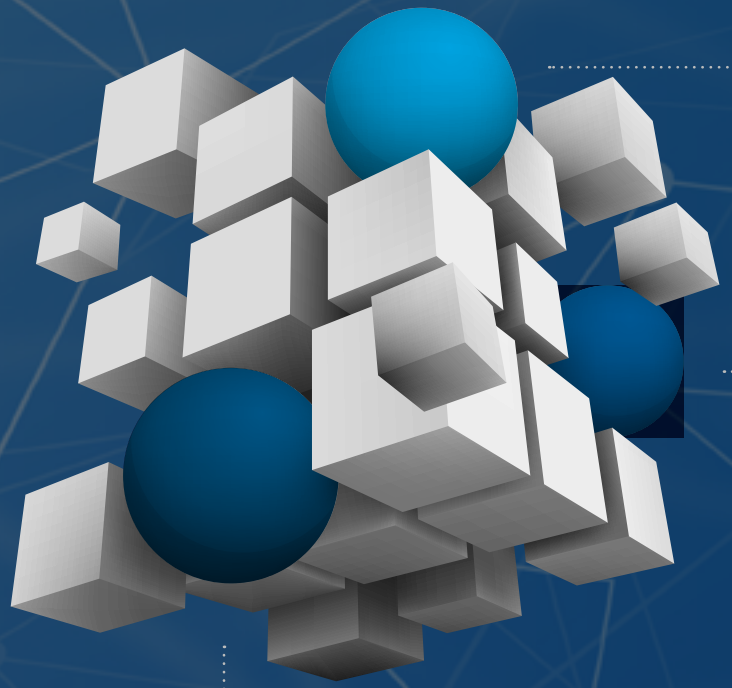
ファイナンス

このデータシェアリングのトレンドに対して不安を覚え、市場競争力の低下や規制への対応、さらには会社の評判への影響を危惧しているCFOもいるかもしれない。しかし、新たなデータシェアリングのビジネスモデルが急増するにつれ、きっと彼らは自社のテクノロジー担当やリスク担当と連携し、生み出されるビジネスチャンスを特定し始めるであろう。このトレンドが広まると、CFOは長期的な利益とデータを共有することのリスクとを天秤にかけることが必要になる。そしてその判断は、企業の成長そして存続にすら多大な影響を及ぼすであろう。

リスク

この1年間に、大規模なサイバー攻撃によってサプライチェーン全体の遮断まで発生した。サプライネットワークやアタックサーフェス（攻撃対象領域）が拡大している中で、第三者リスク管理はますます重要になるだろう。最高リスク管理責任者（CRO）はIT部門と連携し、ベンダーネットワークまで巻き込んでデータ、セキュリティー上の脆弱性、および規格の共有を推進していくべきである。また、最新のプライバシー保護技術やセキュリティー技術を適用するともに、IT環境の可視性やセキュリティーアウェアネスを向上させることで、CROは、将来のサプライチェーンのリスクに対応する心構えを強化することができる。

さあ、はじめよう



要点

1 共通課題の解決や相互の利益、さらに経営上や研究におけるチャンスの追求のため、どのデータ資産をパートナーと共有できるか。

2 これまでデータ市場のプラットフォームを介して外部データを活用し、自社のデータ資産を強化したことはあるか。より多くの情報にアクセスできるようになった結果、どのように意思決定プロセスが向上したか。

3 どのプライバシー保護技術を利用しているか。匿名化されたデータを分析することで、どのように新たなユースケースや画期的な試みが生まれたか、または生まれる可能性があるか。

執筆者

Frank Farrall
AI ecosystems leader
Deloitte Consulting LLP
frfarrall@deloitte.com

Nitin Mittal
US AI strategic growth offering leader
Deloitte Consulting LLP
nmittal@deloitte.com

Chandra Narra
Managing director
Deloitte Consulting LLP
cnarra@deloitte.com

Juan Tello
Chief data officer
Deloitte Consulting LLP
jtello@deloitte.com

Eli Dow
Analytics and cognitive technology fellow
Deloitte Consulting LLP
elimdow@deloitte.com

SENIOR CONTRIBUTORS

Tiago Durão
Partner,
Deloitte & Associados, SROC S.A.

Marcin Knieć
Director,
Deloitte Poland

Rajeev Pai
Director,
Deloitte MCS Limited

Markus Schmidthuysen
Director,
Deloitte Consulting GmbH

Vivek Shrivastava
Partner,
Deloitte India

Rajeev Singhal
Partner,
Deloitte & Touche LLP

Yves Toninato
Senior director,
Deloitte Belgium CVBA

Jeroen Vergauwe
Partner,
Deloitte Belgium CVBA

Dinesh Dhoot
Specialist leader,
Deloitte Consulting LLP

Lakshmi Subramanian
Senior manager,
Deloitte Consulting LLP

Karl-Eduard Berger
Manager,
Deloitte France

参考文献

1. Jennifer Belissent, *Chief Data Officers: Invest in your data sharing programs now*, Forrester, March 11, 2021.
2. Data Bridge Market Research, *Global fully homomorphic encryption market – Industry trends and forecast to 2028*, March 2021.
3. Laurence Goasduff, "Data sharing is a business necessity to accelerate digital business," Gartner, May 20, 2021. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
4. Christina Brodzik, Kristi Lamar, and Anjali Shaikh, *Tech Trends 2021: Disrupting AI data management*, Deloitte Insights, December 2021.
5. Michael Gorman, "Data marketplaces will open new horizons for your company," *VentureBeat*, December 23, 2020.
6. Tomas Montvilas, "Understanding the external data revolution," *Forbes*, June 25, 2021.
7. Dr. Nicola Davies, "Covid-19: The importance of data sharing within the pharma industry," Data Saves Lives, June 26, 2020.
8. California Immunization Registry, "Covid-19 vaccine reporting information and resources," California Department of Public Health, accessed November 5, 2021.
9. Snowflake, "State street accelerates investment insights by building alpha data platform," accessed November 5, 2021.
10. Karthik Kirubakaran (senior director of retail data engineering at CVS Health), phone interview, September 22, 2021.
11. Oliver Ganser (head of the consortium, Catena-X) and Claus Cremers (board member of Catena-X) interview, September 15, 2021.
12. Gaia-X, "What is Gaia-X?" accessed November 18, 2021.
13. Ganser and Cremers interview.
14. Ibid.
15. Dr. Tom Rondeau (program manager at DARPA), phone interview, October 26, 2021.

日本のコンサルタントの見解

データは共有されることで価値を増す

「Data gains value when we share it.」── 組織や個人が知識や情報を共有し煮詰めあうことによってイノベーションは生まれ、それを目指し企業や研究機関はさまざまなコラボレーションを探索してきたのが我々現代社会だが、今日そのイノベーションのドライバーにデータとAIが加わった。そのプラットフォームとしてさらなる技術革新が「データシェアリング」を実現し、時には人の解釈を介さずともAIが新たな示唆を生む可能性が現実のものとなってきている。本年の「Tech Trends」が言及した技術領域はセキュリティー・プライバシーであるものの、世界中のデータが組み合わさって真にデータドリブンな最善解が生まれる未来像を示唆している点が興味深い。

「ビッグデータ」「データアナリティクス」という概念が日本で普及してから7、8年の間、DX実現に向けた障壁としてデータを挙げる企業は非常に多い。デロイト トーマツ グループではInsight Driven Organization（インサイトドリブン組織）と呼ぶグローバル共通のフレームワークに沿ったアセスメントを国内各業界の多数の企業で実施してきたが、やはりその傾向は顕著であり、データがつながらない、データを処理しきれない、データを読み解けない、といった問題意識が必ず聞こえてきた[1]。また日本ではさらに、縦割り組織や保守的な発想に囚われ、そもそもデータを取り出せない、共有して活用することがなかなか進まない、といった悩みが多く、グローバル競争の足枷になりかねないと思われる。こうした課題を1つずつ解消してデジタルやデータの活用を各ビジネス・各オペレーションへ適用し収穫していく、地道な改善の積み重ねがこれまでのDXの王道であった。

データは喩えるなら石油のような存在であり、無限といってよいほど示唆や価値を生むゆえ、粗々な分析であっても、実施すること、進めることが善とされてきた[2]。個別業務において、コスト削減、オペレーションの改善や顧客・提案分析など、教科書通りで誰もが一定の成果を上げられた。ゆえに分析で解くべき「問い」の具体性や目的変数が何であるかが肝であった。

しかしながら我々は、このDXへのアプローチが近く変わると考えている。いまや個別業務ごとにコスト削減を行うという意味での日本企業でも広く見られる取り組みとなり、それ自体が競争優位性を生むということは無い。データが何を生むかが分かってきた今日、業務を横断して、あるいは既存の業界の枠を超えて、AIとともにさらなる変革を目指すには何をすべきかが、いよいよ論点となってきている。自社の中で長期にわたり大きく価値を生むのはどのようなデータか、GAFAのようなプラットフォーマーによる業界構造の変化には何を準備しておくべきか、こうした問いが近年各業界のクライアントとの議論の中で真実味を伴いつつ増えてきている。こうした新たな段階に、我々日本はどのように立ち向かっていくのであろうか。

データ流通革命をにらむ政府の動き出し

昨年の「Tech Trends 2021」の中の「マシンデータ革命」では、「官民の協業で生まれる新たなデータバリューチェーン」と題し、複数の巨大なデータソースの活用が進むことで、行政のデジタル化を刺激し、行政のルールや仕組みを変え、それが民間にオープンデータという形で還元されるという新たなサイクルが誕生する未来について書いた[3]。それから1年、日本ではどのような動きがあったか。

2021年9月1日のデジタル庁発足に先駆けて、日本初の「包括的データ戦略」を含む「デジタル社会の実現に向けた重点計画」が6月に閣議決定された[4, 5]。その中では、官民の双方に共通する基本的行動指針として、以下の3点が挙げられている。

1. データがつながり、いつでも使える
   - つながる（相互運用性・重複排除・効率性向上）
   - いつでもどこでもすぐに使える（可用性・迅速性・広域性）
2. データを勝手に使われない、安心して使える
   - 自分で決められる、勝手に使われない（コントローラビリティー・プライバシーの確保）
   - 安心して使える（セキュリティー・真正性・信頼）
3. 新たな価値の創出のため皆で協力する
   - 皆で創る（共創・新たな価値の創出・プラットフォームの原則）

これらの指針は、まさに「新たなデータバリューチェーンの誕生」につながるものといえ、特に2と3の指針は、本編「データシェアリング時代のはじまり」と深く関連している。また、データシェアリングという観点では、2019年1月のダボス会議で「信頼性のある自由なデータ流通（DFFT：データ・フリー・フロー・ウィズ・トラスト）」が日本により提唱され、2019年6月のG20大阪サミットではDFFTに基づき、デジタル経済、特にデータ流通や電子商取引に関するルール作りを進めるための「大阪トラック」が立ち上げられた。2021年12月時点で「大阪トラック」の交渉参加国は86ヶ国まで増加しており世界的な潮流となっている[6]。

来るデータシェアリング時代においては、データプラットフォームを通じて容易に外部データを購入することができ、自社内の固有データと組み合わせることで、新たな洞察を生み出すことができるようになる。また、プライバシーや機密を保護しながらデータを共有することが容易になるため、自社内の固有データをプラットフォームに提供してマネタイズすることも可能になるであろう。さらに、最大のデータ保有者である行政機関がデータの提供元となることによって、国内での利活用だけでなく、海外へのデータ輸出などを通じて日本経済に貢献する可能性もある。本編では、プライバシー保護技術などの登場によってデータ共有とそれによる新たなビジネス機会の創出が加速することが示唆されているが、新しくて便利そうな技術だからといって盲目的に活用するのは当然リスクがあり、そもそも現行法制下では行政情報の目的外利用や個人情報などを含むデータの共有には限界がある。そこで、政府には、ルール（法制度）の整備のみならず、例えばデータ共有に関する規制を緩和するデータシェアリング特区などを作った上でフィージビリティースタディを実施するな

ど、政府にしかできない取り組みが求められていくであろう。その結果が制度に反映された時、真のデータシェアリング時代が始まる。

長らく我が国はデジタル敗戦国といわれてきたが、データエコノミーに関しては、二の轍を踏まないように政府は動きを速めている。来るべき時に向けて、企業が今やるべきことは何か。

デロイトは2015年、機械時代の到来に際しての次世代オペレーションモデルをInformation Value Loop（情報のバリュー・ループ）として提唱した[7]。そこでは、設備に取り付けられたセンサーやウエアラブル、またWebを行き交う様々な顧客トランザクションがさまざまなレイヤーで洞察（示唆）を生み、それが人やロボを介していち早くアクションと価値をもたらし、さらにはその経験が次なるデータを生む、いわば人・知識とAI・データの協働モデルを予言していたように思う。データアナリティクスの結果がさらに上のレイヤー・視座で示唆を生むことが当たり前になる。また、AIの実用化、例えばData Robotといった自動で機械学習モデルを導出する仕組みによって、従来のアナリティクス作業も人力が取って代わられ高速化されるものが出てきている。前述のループやサイクルはますます加速する一方だ。人が考えるべき仮説、また指し示すべき方向性も、さらに一段上のものへと変容を求められることであろう。データやAIの仕組みが企業の隅々まで行きわたるとき、ひとりひとりが身に着けなおすべき知識やスキルという観点でも、対象となる人の幅広さという観点でも、求められる変化はあまりに大きい。すでに多くの企業ではDXに備えデジタル技術についての研修を導入している今日だが、こうした文脈に照らして使えるスキル、また強みを磨く知恵を身につけさせられるようなプログラムとなっているか、検証すべきだ。20年後の自社のビジネスを担う人材がいまの教育の選択肢1つで大きく方向づけられることに鑑み、活発な議論が行われることを期待したい。

執筆者

三木 聡一郎　シニアマネジャー
Analytics & Cognitive

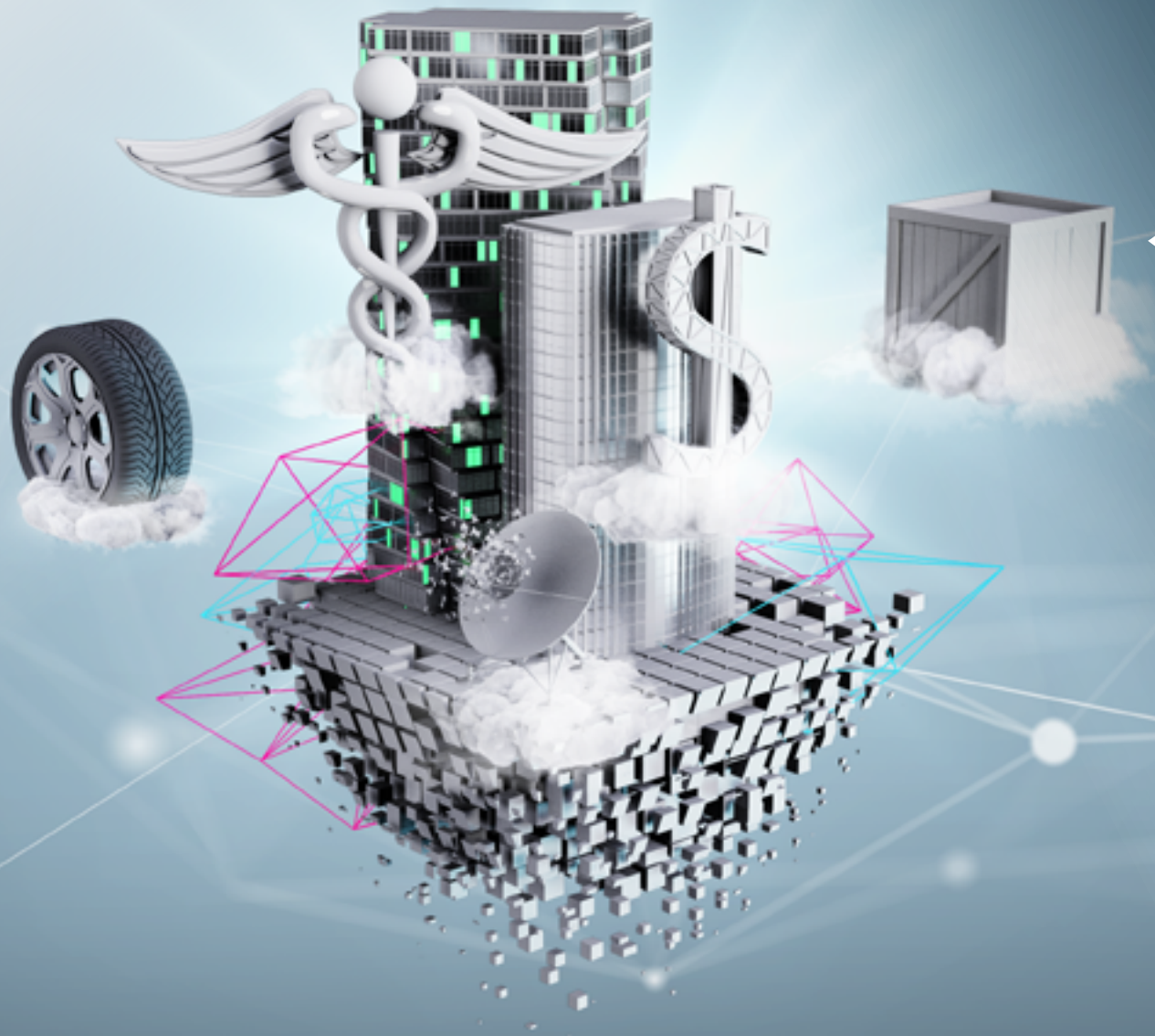
外資系ソフトウエアメーカー、日系コンサルティング会社を経て現職。金融・製造・サービス業を中心に、システム構想策定や業務立ち上げ、クロスボーダー・大規模トランスフォーメーションプロジェクトに従事。近年は営業・マーケティングを中心にAI・データの利活用戦略やDXに求められる組織・体制づくりの支援を手掛けている。

小倉 康司　マネジャー
Analytics & Cognitive

中央省庁、独立行政法人、外資系生命保険会社、大手電力会社などで大規模ITプロジェクトの経験を有する。特に、中央省庁などを中心とした公共領域におけるデータを利活用したデジタルトランスフォーメーションの支援に強みを持ち、対応領域は戦略、組織、人材、ガバナンスなど多岐に渡る。

参考文献

1. デジタルトランスフォーメーションやデータ・AIの利活用に求められる要素を戦略・人・プロセス・ロジック・データ・テクノロジーの6カテゴリーにまとめたデロイト独自のフレームワーク
2. 総務省, “第1部 特集 人口減少時代のICTによる持続的成長,” July 2018.
3. デロイト, “Tech Trends 2021 - マシンデータ革命：データが機械を巡る,” May 20, 2021.
4. 内閣官房 情報通信技術（IT）総合戦略室, “包括的データ戦略,” June 18, 2021.
5. 高度情報通信ネットワーク社会推進戦略本部, “デジタル社会の実現に向けた重点計画,” June 18, 2021.
6. IT総合戦略本部, “DFFT：Data Free Flow with Trustとは,” June 7, 2019.
7. デロイト, “Tech Trends 2016 - Internet of Thingsが価値を生むまで,” April 6, 2017.



インダストリークラウドの潮流

テクノロジースタックの拡張

差別化への注力

変化に対応するためのキャパシティの確保

クラウドベンダーは、各業界向けに最適化されたプラットフォームを構築するために、これまでになく高度なビジネスプロセスを自動化および抽象化している

コモディティー化した各業界のプロセスをクラウドソーシングすることで、CIOは競争優位性を生み出すシステムに人材と予算を再集中させることができる

クラウドベースのケイパビリティーを備えることで、組織は、より小さな動きでこれまで以上に大きく考える力を生み出すことができる。作り込みを少なくすることで、さらなる俊敏性を生むことができる

トレンド2

インダストリークラウドの潮流

業界特化型のクラウドソリューションにより、組織はビジネスプロセスを自動化し、競争力のある差別化領域へ重点を移すことができる

世界経済がパンデミックの流行からエンデミック（日常的な感染症）へと移っていく未来を見始めるのにつれて、多くの組織はビジネスプロセスをクラウドに移行することにより、迅速化・効率化の機会を模索している[1]。

こうした動きに応えるため、クラウド大手のハイパースケーラー、ソフトウエアベンダー、システムインテグレーターらは、業界横断で共通のユースケースをサポートするよう事前構成された一連のクラウドベースのソリューション、アクセラレーター、およびAPIを開発している[2]。これらのソリューションは容易に導入できるように設計されており、デジタルによる差別化を支援している。

これらのソリューション群からユーザーがどのようなアプリケーション、ツール、またはサービスの組み合わせを採用したとしても、クラウドは、それらをつなぎ合わせて強力なビジネスプロセスソリューションを構築するファブリック（繊維の格子状のように組み合わされた構造）となる。例えば、ある世界的な自動車メーカーは、クラウドベンダーと提携して、運輸業界向けのクラウドベースのコネクテッドカーアプリケーション開発サービスを開発している。このプラットフォームには、IoT、機械学習、アナリティクス、コンピュートサービスとともに業界固有のソリューションが搭載されており、メーカーはこれらのサービスを活用して、コネクテッドカーアプリケーションを開発することができる[3]。

ヘルスケア業界は当初、バックオフィスのデータを管理するためにクラウドプロセスを導入してきた。そして、1996年に制定されたHIPAA法（アメリカのHealth Insurance Portability and Accountability Act）の遵守が、ヘルスケア業界におけるクラウドジャーニーを一段階推し進め、医療機関は患者データをクラウドで管理するようになった。今日、先駆的なヘルスケアプロバイダーは、クラウドベースのHIPAAモデルを利用し、ヘルスケア事業プロセスを改善する方法を模索している[4]。

今後1年半から2年の間に、市場セクター全体でますます多くの組織が、業界独自のニーズを満たすためにインダストリークラウドを活用する方法を模索し

始めると予想される。実際、デロイトの分析によると、インダストリークラウド市場の価値は今後5年以内に6,400億米ドルに達する可能性があると予測されている[5]。

*インダストリークラウドの潮流*は明らかに勢いを増しており、組織にとっての可能性を探求し始める時期にきている。まずは、組織のビジネスプロセスのエコシステムの評価を実行し、クラウド化を検討するプロセスと、そのメリット・デメリットの見極めから着手するのがいいだろう。

その際、現在のプロセスが短期と長期のビジネス戦略をどの程度サポートできているか、また、どこに改善の余地があるかを評価することが重要である。さらに、クラウドで提供される機能は急速に増えており、これらの機能を用いて、新しいビジネスモデルを簡単に実現できる可能性についても考えておきたい。

最後に、インダストリークラウドの潮流は、ITを再構築するという長い間待ち望まれていた機会を提示している。組織は、競争優位性をもたらさないIT機能やビジネスプロセスをアウトソーシングすることで、その労力や投資を、競争優位性をもたらすシステムやサービスに振り向けるとともに、変化へ継続的に対応できる能力を創出することができる。

この評価は、2年がかりの巨大なプロジェクトである必要はない。実際、細かなプロジェクトの積み重ねで、ほとんどのプロセスに効率性と有効性をもたらすことができる。同時に、組織の人材とリソースを、競争優位性をもたらす差別化に再集中させることができるようになる。

インフラから業界へ

現在、*インダストリークラウドの潮流*を推進しているビジネスとテクノロジーのニーズは新しいものではない。2000年代以降、コンプライアンス、ビジネスプロセス、またはデータ管理といった、似たようなニーズを持つ組織がクラウドベースのソフトウエアを採用し始めた。また、ほぼ同時期に、CIOはコストを削減して効率性を高めるため、一部のオンプレミスシステムをパブリッククラウドに「リフト&シフト」し始めた。

今日において、共通のニーズを満たすソフトウエアを共有して利用すること（クラウドベースのソフトウエアの採用）、ITインフラの運用を他者に委託すること（システムのリフト&シフト）という2つのアプローチは、*インダストリークラウドの潮流*においても続いている。新しくなったのは、クラウド利用の目的が一般的な機能や共通的なアプリケーションライブラリーの利用から、業界固有のビジネスプロセスのデジタル化や、その可用性の実現へと変化したことである。さらに、組織はクラウドベンダーに対して、業界やエコシステム全体で共有されるニーズに対応する、「共通のコア」ソリューションの構築をますます期待している。その結果、クラウドおよびソフトウエアベンダーは、APIを介して利用できる業界固有のモジュール化したビジネスプロセスの広範な機能を提供し、ユーザーはボタンを押すだけでそうした機能にアクセスできるようになった。例えば、APIを使用するこ

とで、エンジニアやシステムアーキテクトは、利用したいスマートファクトリーシステムを共有クラウドネットワークに接続することができる。このような開発力は、ほんの数年前のFedRAMP（Federal Risk and Authorization Management Program、アメリカ政府のクラウドサービスに関するセキュリティー評価・認証の統一ガイドライン）のようなコンプライアンスに基づく対応から、飛躍的に進歩した。

こういった背景から、*インダストリークラウドの潮流*は次のような段階で展開されていくだろう。

ハイパースケーラーはテクノロジースタックを登る

ハイパースケーラーと呼ばれる「3大」クラウドサービスプロバイダーであるAmazon Web Services（AWS）、Google Cloud、Microsoft Azureは、ヘルスケア、製造、自動車、小売、メディアなどの分野に業界固有のビジネスプロセスを自動化するクラウドベースのソリューションを提供している。

ハイパースケーラーは、最初はサービスとしてのインフラ機能（IaaS：Infrastructure-as-a-Service）を開発し、徐々にサービスとしてのプラットフォーム機能（PaaS：Platform-as-a-Service）へと進化させた。しかし、彼らはそこで止まってはいない。彼らはテクノロジースタックをインフラからプラットフォーム、そしてビジネスアプリケーションへ登り続けており、これまで以上に高度なプロセスを体系的に自動化し、各業界に最適化されたプラットフォームを構築している。このプラットフォームは、場合によっては、オンプレミスに存在するシステムが現在提供しているものよりも機能的に堅牢で効率的である。例えば、接客業の一部では、クラウドベースの予約や顧客管理システムを利用している。同様に、製造部門はクラウドの予測メンテナンスソリューションを活用している。

組織は、ハイパースケーラーが開発した製品やサービスよりもはるかに多くのものを、インダストリークラウドに見出すことになるだろう。実際、MuleSoft、Oracle、Salesforce、SAP、ServiceNowといった既存ベンダーや、スタートアップやオープンソースプロジェクトが提供する、業界固有のビジネス機能のエコシステムは拡大している[6]。

差別化に注力する

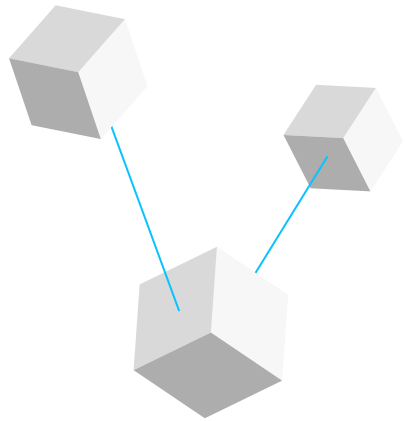
おそらく、組織にはゆずれないスクラッチ開発のプログラム資産があるだろう。これは時間と予算を費やして開発され、優れた計画と実行により競争優位性をもたらし、市場で組織を差別化するための鍵になる。あなたが小売業者で、時間と予算を費やして店舗の在庫管理システムを開発した場合、CxO（と市場）は、その在庫管理システムのロジックこそが、競争優位性をもたらす最高クラスの能力を保持していると認識する。クラウドベンダーが在庫管理APIを提供しているからといって、それを妄信的に採用する必要はない。自社で開発したプログラム資産が競争上の差別化に大きく貢献している場合、是非利用し続けるべきである。当然クラウドでも実行できるが、重要なのは、それが組織にとってのIP（知的財産）であり、既製品ではできない方法で独自のニーズを満たすということである。

行動を起こす前に選択肢を評価することが重要である。現在利用可能なインダストリークラウドのソリューションの範囲は、数年前よりもさらに洗練され、きめ細かくなっている。プロセスを実行するための組織の能力について考えた時に、現在の機能が既成のものより優れている場合は、独自のロジックを維持するべきである。しかし、もしデジタルネイティブと競合していて、組織のプロセスとそれをサポートする機能がもはや特別でない場合は、業界API（インダストリークラウドのソリューション）の利用を検討すべきである。

多くのテクノロジーおよびビジネスのリーダーにとって、*インダストリークラウドの潮流*に乗るためには、ある程度の計算と見通しが必要になる。リーダーは協力して、企業が市場のどこで勝利し、どの技術がその勝利を可能にするかを判断しなければならない。例えば、従来とは異なる手法によるカスタマーサービスを通じて成功を収めた場合は、社内の分析機能に多額の投資を行うべきである。これらの機能により競争上の差別化と、新しい革新と収益創出の機会がもたらされたのであり、それは執拗に守らなければならないものである。対照的に、市場で差別化につながらないものはすべてコモディティー化しており、クラウドおよびソフトウエアベンダーからビジネスサービスとして利用できる。

*インダストリークラウドの潮流*がもたらす機会を探るには、次に示す手順を検討すべきである。これらの手順が進んでいないと手遅れになる可能性がある。

1. ビジネス部門リーダーとIT部門リーダーは協力し、企業が現在と将来にわたって、どこで勝利するかを決定する必要がある。この取り組みを成功させるには、テクノロジーの理解をIT部門に丸投げせず、ビジネス部門がテクノロジーをより深く理解する必要がある。同様に、IT部門はビジネス戦略と、それを推進する上でテクノロジーが果たす重要な役割を理解する必要がある。そうして初めて、双方のチームは勝利を達成するための重要なテクノロジーを特定することができる。
2. ビジネスプロセスと、それをサポートするクラウドベースのサービス機能のインベントリーを作成する。
3. 社内に維持すべき、差別化につながるプロセスと、それを支えるテクノロジーを特定する。同様に、クラウドによって実現される新しいテクノロジー製品からメリットを得られる可能性があるビジネス分野を特定する。
4. クラウドサービスプロバイダー、ソフトウエアベンダー、システムインテグレーターと協力して、クラウドジャーニーにおける次のフェーズを計画する。



モダンエンジニアリング

システムの調達方法が既製品の組み合わせ型に進化しても、また別の形のシステム構築が必要となる。ここでは巨大なカスタムシステムを構築するために年単位のプロジェクトに取り組んでいる大規模な開発チームではなく、クラウドサービス、プラットフォーム、ツールを迅速に統合して展開するために、小規模なチームで作業するモダンなソフトウエアエンジニアリングを想定している。

この新しいスタイルの重要な部分は、目標に向かって緊密に連携するフルスタックチームである。主要な組織は「ポッド」または「ツーピザ・チーム（無駄がなく生産性が高いチーム人数の条件は、ピザ2枚を配りきれる8～10名程度であるという、Amazon CEOの提唱したルール）」を採用しており、クラウドエンジニア、UXデザイナー、データサイエンティスト、品質保証、製品マネジャーが協力して作業するにつれ、専門分野の垣根が取り払われて一体化していく。チームのメンバーは、スプリントの目的に向けて活動する中でチームに必要なものを学習し、成長していく。重要なことは、チームが一丸となってビジネス上の問題を解決し、自発的にロードマップを作成することである。これは、「why」や「so what」を何も考えずにただ与えられた要件を実装することから脱却した、歓迎すべき変化を示すものである。

もう1つの鍵はエンパワーメントである。現代のエンジニアは、その職務遂行にあたって幅広い裁量を組織に求めている。彼らは、目的の観点（自分が信じていることに取り組む選択肢があるかどうか）、ツールの観点（開発に使うツール、ライブラリー、サービスを選べるかどうか）、パーソナルな観点（服装、勤務時間、勤務場所など個人的な好みや事情が受け入れられるかどうか）を大事にしている。

伝統的な組織のテクノロジーリーダーはハイテクのスタートアップ組織をしばしば誤解している。デジタルネイティブ組織のエンジニアリングチームが成功している理由は、職場のテーブルサッカーや無料の食事や飲み物、さまざまな報酬や手当などではない。これらの若い組織の成功の理由は、エンジニアリングを中核的な創造的分野として高く評価していることにある。さらに、彼らはエンジニアを尊重し、彼らが成功するために必要な権限を与えている。もちろん、セキュリティー、コンプライアンス、知的財産の保護の分野では、専門家の支援が必要である。しかし、それらは、組織戦略と組織文化の中核としてのモダンエンジニアリングを推し進めるという、より大きな文脈の中で展開されるべきものである。

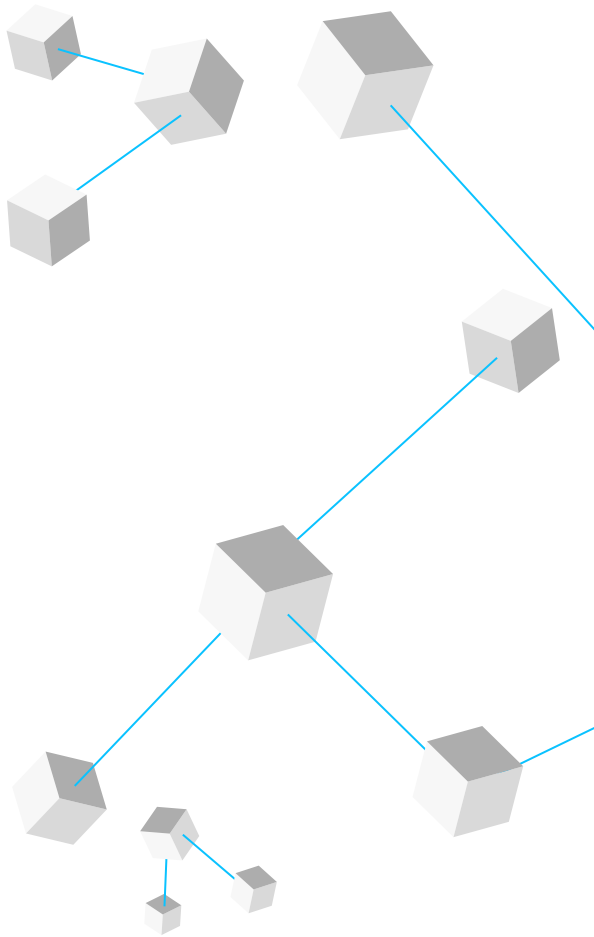
変化に対応するための キャパシティを確保する

ディスラプションと急速なイノベーションの時代には、最高クラスのソリューションや時には実験的なツールを活用することで、組織は多面的なデジタルトランスフォーメーション戦略のすべての点をつなぐことができる。しかし、これらを実際に活用できるかどうかは、変化への対応能力にかかっている。

考えてみてほしい。特定の業界のニーズに合わせてカスタマイズされたクラウドは、革新的なソリューションやサービスが登場するにつれて継続的に進化していくだろう。競争上の差別化を維持するためには、組織は破壊的な変革を受け入れ、最新のインダストリークラウド製品を活用する必要がある。急速に変化する環境の中で、未来は常に急速に近づいている。クラウド技術は、組織変化への対応能力だけでなく、継続的に変化するためのアジリティを生み出すことに役立つ。現在社内にある独自のシステムやプロセスが少なければ少ないほど、将来の管理、アップグレード、更新の手間も少なくなり、変化に対応しやすくなる。ほとんどの企業はすでにある程度クラウドを利用している。もしすでにクラウドの基本的なコストメリットとスケーラビリティーを活用できているのであれば、インダストリークラウドの潮流をクラウドジャーニーの次の段階として考えてほしい。

進むべき道

*インダストリークラウドの潮流*の導入にビッグバン的アプローチは必要ないということは、組織にとって良いニュースだろう。実際に、複雑なレガシーアプリケーションの更新や破壊的な基幹システムのモダナイゼーションの取り組みを避けながら、注意深く小さなステップの繰り返しによって実現できる。そしてそれらを経るごとに、システムをより効果的で効率的に変化させることができるのである。



私の見解

Marijan Nedic

Vice president, head of IT business solutions, SAP

組織の業務の大部分は差別化をもたらさず、その5〜10%が市場で組織を競合他社から引き離し、優位性を生む。

インダストリークラウド（特定の業界で使用される一般的なアプリケーションとコンフィギュレーションからなるパッケージソリューション）の登場により、事業プロセス運営に必要な最低限の機能のセットアップに費やす時間を短縮し、ビジネス差別化に影響力のある領域により多くの時間を費やすことができるようになった。SAPの目標は、クライアントが利用開始してすぐにほとんどのニーズを満たし、パートナーソリューションに簡単に接続でき、統合プラットフォームで独自の差別化要因を管理できる、インダストリークラウドを構築することである。

病院であれ、工場であれ、レンタカー会社であれ、そのほかの企業であれ、多くのプロセスと業務は競合他社とほぼ同じである。そのため、業務プロセス上の問題のほとんどは、業界によってある程度特定される。そして、この問題のほとんどはすでに解決されている。

したがって、十分な価値があるインダストリークラウドにはいくつかの共通機能がある。第１に、インダストリークラウドは、業界に必要な機能のほとんどを、特にコモディティー機能をすぐに利用できる状態で提供する必要がある。第２に、顧客やパートナーが革新的なソリューションを開発できるオープンなプラットフォームでなければならない。プラットフォームは、これらのソリューションの接続と管理を容易にする必要がある。第３に、需要に応じてキャパシティとプロセスを拡大または縮小できるようにする必要がある。最後に、ほかのビジネスおよびテクノロジーサービスに容易にアクセスできるようにする必要がある。例えば、今日の主要なクラウドサービスにはすべて、すぐに使える共通のツールが含まれている。自然言語処理（NLP：Natural Language Processing）は今や一般的なツールだが、問題はNLPをビジネスに統合する方法である。これらすべての機能にわたって、インダストリークラウドはより広範なエコシステムをサポートする必要がある。

最近、アジャイルな生産手法を利用して大口顧客と小口顧客の両方の注文に対応している製造業のクライアントを訪問する機会があった。クライアントのビジネスは非常に収益性の高いビジネスだが、生産ラインを頻繁に再構成する必要があった。機器のパフォーマンスを最適化するために、機械学習モデルで注文データを解析し、必要な機器の構成と注文を満たすための最適な処理順序を決定している。このプロセスは非常にうまくいっているが、すべてを自組織で作るには、クライアントのデジタルチームの多大な労力を要するものだった。

その代わりに、これらの機能が利用可能な１つのインダストリークラウドを採用することが考えられる。これらのプロセスの構築とメンテナンスによる負担の大部分をインダストリークラウドへシフトすることで、データサイエンティストは、注文への迅速な対応を実現するMLモデルの開発により多くの時間を費やすことができる。マシンビジョンと機械学習モデルを組み合わせることで、品質管理チームは生産ラインから出荷される製品の多くを検査できるようになる。本質的に重要な作業に対してより多くの時間を割くことで、クライアントは自組織で機能を構築するよりも迅速に業務を拡張できる。こういった取り組みがメーカーを際立った存在にするのだ。

この機能の組み合わせにより、ビジネスは俊敏性を増す。主要なオペレーションプラットフォームが業界の典型的なビジネスニーズに合わせて構成されている場合、事業の中でほかと一線を画す領域へエネルギーを集中させることができ、ビジネス、パートナーネットワーク、サプライヤーネットワーク、システムのデジタル情報に直接アクセスできる。最終的には、真に組織を差別化できるイノベーションを開発するためのアジリティを持つことになる。

今後の展望

ストラテジー

クラウドおよびソフトウエアベンダーは、ますます洗練された性能が高いビジネス機能をサービスとして開発している。それらの新たなサービスを活用する上で、CEOは組織独自のバリュープロポジション（顧客への提供価値）を明確にする必要がある。まさにERPがほとんどのバックオフィス業務を標準化するように、リーダーはビジネス機能のどの部分が競争上の差別化要因となるかを特定する必要がある。今やサービスによって置き換えられる対象は財務・会計部門に留まらず、企業戦略に関わる事業の中核部門にまで及ぶ可能性がある。

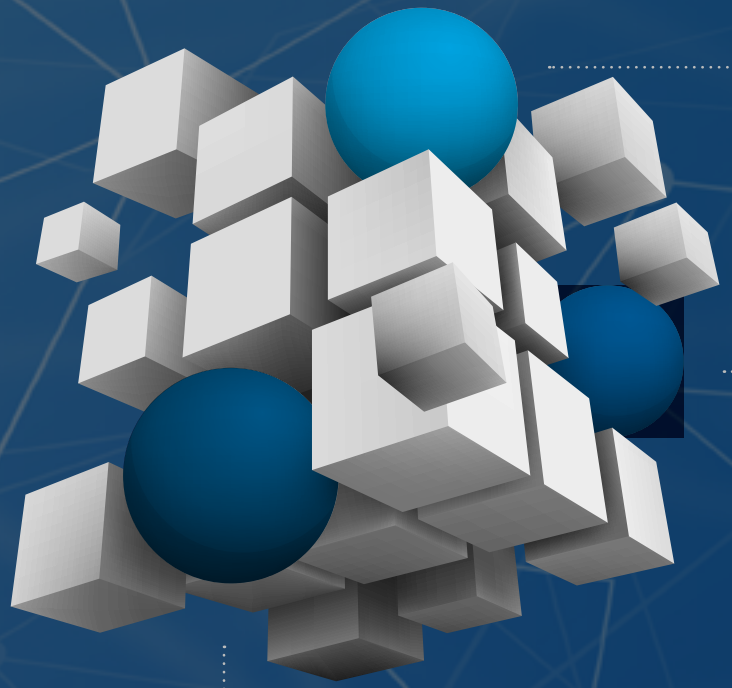
ファイナンス

予算とコンプライアンス要件に関心のあるCFOは、業界固有のニーズに合わせて開発されたクラウドベースのアプリケーション（インダストリークラウド）に対して、2つのメリットを見出すことができる。具体的には、インダストリークラウドを活用することで、少ない労力でテクノロジーや規制の変化に対応でき、さらに、より付加価値の高いプロジェクトに人材を配置することができるようになる。CFOは、すべての関係者が新しいクラウドサービスの潜在的メリットを最大化する方法を理解できるよう、財務、IT、コンプライアンス、リスク、法務部門間の緊密な連携を確保する必要がある。

リスク

CROは、新しいインダストリークラウドの導入初期に、サイバーリスク管理を統合する機会がある。ベンダーの標準的なサイバーセキュリティーコンポーネントでは組織のアプリケーション要件を満たせない可能性がある。インダストリークラウドが担うビジネス機能が増えるにつれて、自社に合ったクラウドセキュリティーの組み合わせがより重要となる。CROとIT部門は、サイバーセキュリティーを後付けのものではなく、自社のクラウド技術スタックを差別化する要素としてとらえるべきである。特に消費者向けのサービスを提供する企業では、最初からサイバーセキュリティー対策を組み込むことで、長期的なコスト低減につながる可能性もある。

さあ、はじめよう



要点

1 現在、同業他社にも存在する、テクノロジーでサポートしている非差別化プロセスは何か。よりコストパフォーマンスに優れた、業界に特化したソリューションが協業先のベンダーから提供されていないか。

2 今後数年間の成功に不可欠なテクノロジーは何か。これらの分野により多くの資金と開発人材を振り向けるにはどうすればよいか。それらを組織内に残しておくべきなのか、それともクラウドに移すべきか。

3 「急速に近づく」未来への準備はできているか。システムやプロセス横断で変化への対応力を生み出し、育成するために、デジタルトランスフォーメーション戦略をどう見直すべきか。

執筆者

Ranjit Bawa
US cloud leader
Deloitte Consulting LLP
rbawa@deloitte.com

Brian Campbell
Strategy principal
Deloitte Consulting LLP
briacampbell@deloitte.com

Mike Kavis
Chief cloud architect
Deloitte Consulting LLP
mkavis@deloitte.com

Nicholas Merizzi
Cloud strategy principal
Deloitte Consulting LLP
nmerizzi@deloitte.com

SENIOR CONTRIBUTORS

Steve Rayment
Partner,
Deloitte Australia

Benjamin Cler
Senior manager,
Deloitte Luxembourg

Jorge Ervilha
Manager,
Deloitte & Associados SROC, S.A.

Senthilkumar Paulchamy
Manager
Deloitte Consulting LLP

参考文献

1. According to the Flexera 2021 report *Cloud computing trends: 2021 state of the cloud report*, 90% of enterprises expect cloud usage to exceed prior plans due to COVID-19.
2. Kash Shaikh, "Industry clouds could be the next big thing," *VentureBeat*, March 28, 2021.
3. Ford Motor Company, Autonomic, and Amazon Web Services, "Ford Motor Company, Autonomic, and Amazon Web Services collaborate to advance vehicle connectivity and mobility experiences," April 23, 2019.
4. *Analytics Insight*, "HIPAA compliance, big data and the cloud—a guide for health care providers," September 15, 2021.
5. Brian Campbell, Nicholas Merizzi, Bob Hersch, Sean Wright, Diana Kearns-Matatlos, *Reimagining digital transformation with industry clouds: Organizations can leverage industry clouds to enable strategic transformation and stay on the cutting edge*, Deloitte Insights, November 23, 2021.
6. Bill Briggs, Stefan Kircher, and Mike Bechtel, *Open for business: How open source software is turbocharging digital transformation*, Deloitte Insights, September 17, 2019.

日本のコンサルタントの見解

本レポートでは、「インダストリークラウドの潮流」と題して、一般的な業務プロセスだけでなく業界固有プロセスにもクラウドを活用することで、リソースやエネルギーの効率化が可能であること、そして、クラウド活用で浮いたリソースやエネルギーは競争上の差別化に集中させるべきであること、という2つの示唆が述べられている。

グローバルでは、デジタルトランスフォーメーションの推進とクラウドの活用が切っても切り離せないことをいち早く理解し、積極的にクラウド活用を進めて成長してきた企業がいくつも存在している。一方、我が国では、令和3年版情報通信白書「企業におけるクラウドサービスの利用動向」によると、インダストリークラウドどころか、一般的なクラウド活用そのものがほとんど進んでいないことが示されている[1]。

本稿では、国内企業がインダストリークラウドを使いこなし、競争優位性をもたらす差別化領域を具現化するために組織が行うべき準備について述べていく。

組織が行うべき準備1：全社ITインフラのクラウド化

組織が行うべき準備として、インダストリークラウドを使いこなしていくために必要となるのが、全社ITインフラのクラウド化である。

本レポートで述べられているインダストリークラウドは、技術的にはSaaS（Software as a Service）の形態で提供されている。このため、組織がインダストリークラウドを使いこなすためには、まず初めに、さまざまなSaaSを利用可能とする全社ITインフラのクラウド化が必要となる。現在の国内企業の全社ITインフラは、例えば巨大なデータセンターがあり、さまざまな機器を配置し、社内ネットワーク境界でセキュリティー対策をするといった構成になっていることが多い。このような仕組みのままインダストリークラウドを利用しようとした場合、クラウドへのアクセスのキャパシティを処理できない、あるいはセキュリティー対策がクラウドに対応できていないといった理由により、十分に活用することは困難であろう。

全社ITインフラのクラウド化とは、クラウド上で提供される仮想サーバーのことではなく、ネットワークや認証、セキュリティーなどを含むITインフラ機能について、クラウド上で提供される複数の機能を組み合わせて実現することを意味している。これは、ゼロトラストの考え方に基づくクラウドセントリックなアーキテクチャーへの転換であり、最先端テクノロジーを迅速に活用し、利便性とセキュリティー高度化を両立できるものである。

全社ITインフラのクラウド化にあたっては、多様なビジネスニーズを踏まえ、ゼロトラストやグローバルガバナンスなどの観点を持ち、ITインフラ領域全体を俯瞰して検討することが必要となる。なぜなら、クラウド上で提供される機能群を取捨選択し「組み合わせて」全体を実現することが求められるためである。

この際、ある特定の要件しか見ずに部分的な機能導入をしてしまうと、技術要素間の整合がとれず、ほかの要件を実現できなくなってしまうリスクが高くなる。これを避けるためには、複雑に関連するテクノロジー要素間の関係性を抜け漏れなく把握し、全体感のあるITインフラのデザインを行うことができる、目利き力をもったアーキテクトの存在が必要不可欠となるであろう。

組織が行うべき準備2：ランディングゾーンを備えた基盤の構築

組織が行うべき準備として、競争優位性をもたらす差別化領域を具現化していくために必要となるのが、ランディングゾーンを備えたクラウドコンピューティング基盤の構築である。

本レポートで述べられているように、インダストリークラウドを活用する真の目的は、リソースとエネルギーを競争上の差別化に集中させることである。この、競争優位性をもたらす差別化領域については、スクラッチのプログラム（自家製のコード）で実現していくことが必須であり、この「自家製のコード」を実行できる環境をきちんと準備することが求められる。この準備として必要なことが、ランディングゾーンを備えたクラウドコンピューティング基盤の構築だ。

業務プロセスを実現する際に複数SaaSアプリケーションを組み合わせてリソースやエネルギーを省略するのと同様に、競争優位性をもたらす差別化領域では、PaaSやFaaS（Function as a Service、サーバーレスでアプリケーション開発を行うことができるサービス）と呼ばれるクラウドネイティブなサービスを組み合わせることで、柔軟で素早い具現化を可能にすることが肝要である。旧来の仕組みのように仮想サーバーを立てて必要な製品をひとつひとつインストールしていくのではなく、クラウドプロバイダーが用意するPaaSやFaaSの機能を組み合わせて1つのシステムを実現していくのである。このための環境をクラウドコンピューティング基盤と呼ぶ。

複数サービスの組み合わせでシステムを実現し、素早く新たな製品、サービス、ビジネスモデルを市場に展開して成長を遂げるためには、クラウド上のサービスを利用することに足枷がなく自由にサービスを選んで組み合わせを試行錯誤できる環境が必要である。この際、システム開発担当者へある程度高い権限を割り当てることが必須となるが、クラウド環境のすべての管理者権限を開発担当者に付与するのではなく、一定のセキュリティー品質を保ちつつ開発の推進を阻害しないレベルで権限を付与する「自由度と統制を両立」する運営が求められる。この、自由度と統制の両立のために必要となるのがランディングゾーンである。ランディングゾーンというのは、ハイパースケーラーのPaaSやFaaSサービスを用いる際に、利用する環境の基礎構成要素を適用させる仕組みであり、複数のシステム横断で、組織共通のセキュリティーやガバナンスルールを自動的に適用する技術である。ランディングゾーンを備えたクラウドコンピューティング基盤を前もって準備しておくことで、競争上の差別化を、より効果的に推進できるようになるであろう。

自組織内で手の内化するべき対象

先に述べた全社ITインフラのクラウド化や、ランディングゾーンを備えたクラウドコンピューティング基盤は、一度構築したら終わりではなく、そのときどきの環境要因や要件に応じて、常に変化させ続けることが求められる。

例えば全社ITインフラのクラウド化においては、リスクの見直しを定常的に行い、動的に連動させる機能の見直し（クラウド認証機能とクラウドネットワークセキュリティー機能に加えて、エンドポイントセキュリティーとの動的な連携も新たに検討するなど）を定常的に行うことが必要となる。また、ランディングゾーンについては、クラウドサービスでセキュリティー強化のための機能改善がなされた際に、自組織のシステム開発において当該機能の利用を必須とする制約を追加し、当該機能が自動的に組み込まれるように変更することが必要となる。

こういった変更が発生するごとに外部のITベンダーに頼みひとつひとつ要件定義をしているようでは、素早く新たな製品、サービス、ビジネスモデルを市場に展開し成長を遂げることはできなくなってしまう。このため、全社ITインフラのクラウド化や、ランディングゾーンを備えたクラウドコンピューティング基盤について、自組織内で手の内化できるようにしておくことが肝要である。

まとめ

我が国では、インダストリークラウドどころか、一般的なクラウド活用そのものがほとんど進んでいないことが現状であるが、インダストリークラウドの潮流を迎えた今、いち早くクラウド活用の歩みを進める必要がある。しかし、多岐に渡る検討範囲に対して全体俯瞰の視点を持ち進むというハードルを乗り越えながら進めるためには、すべての検討を自組織のリソースだけで行うことは現実的ではなく、外部リソースの活用も視野に入れて検討することも良いと考えられる。外部の支援サービスを用いつつ、それらを手の内化することを見据え、外部業者に丸投げするのではなく、伴走してもらう中でそのノウハウを自組織に貯めながら、推進していくことが重要である。

本レポートで登場する先進企業群同様、インダストリークラウドを使い倒し、従来のIT化にかけていたリソースやエネルギーを、競争優位性をもたらす差別化領域へ集中させることができるよう、必要な取り組みを推進していただきたい。

執筆者

佐藤 岳彦　ディレクター
Technology Strategy & Transformation

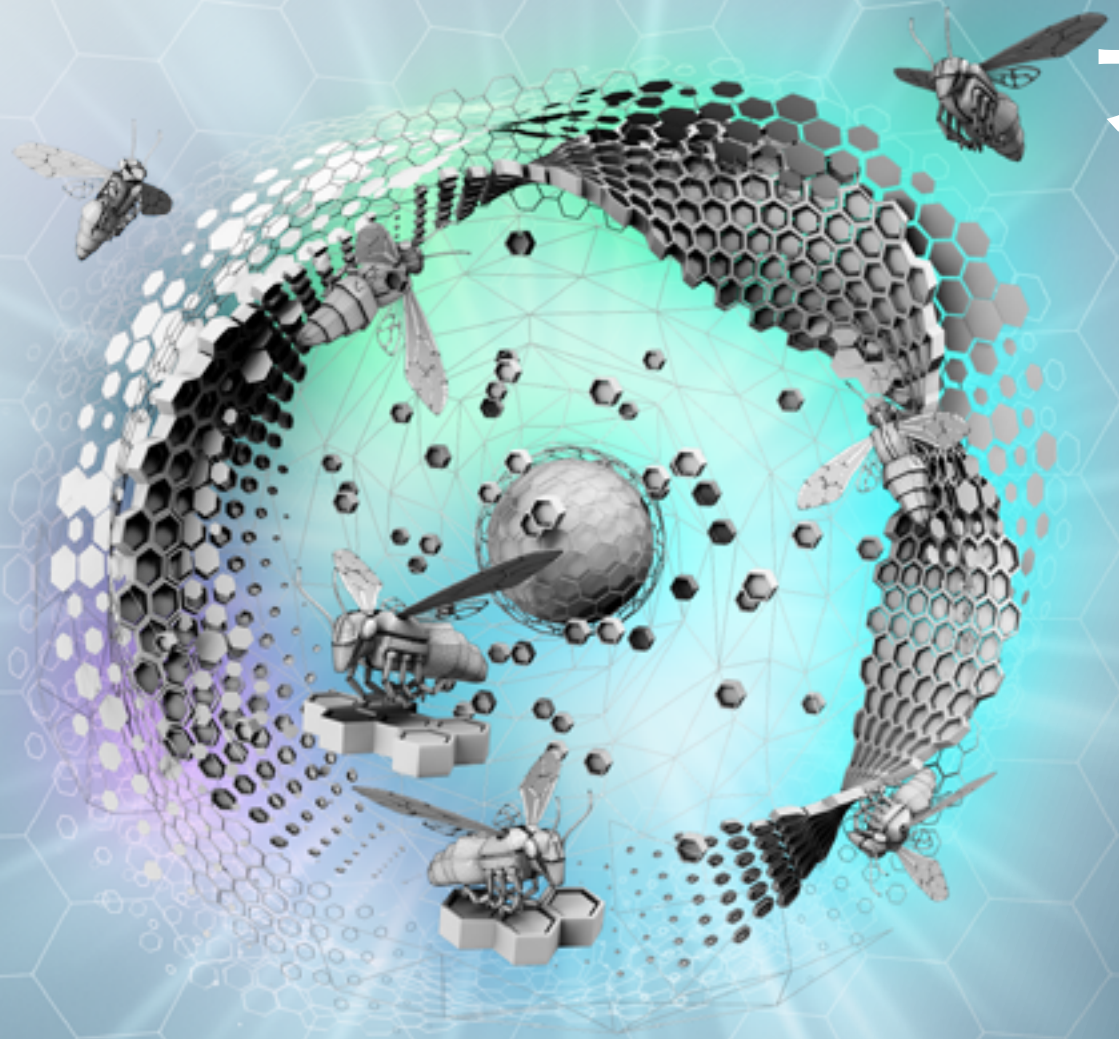
外資コンサルティングファームを経て現職。官公庁、金融、製造業を中心に、IT構想策定、次世代ITインフラグランドデザイン、大規模ITプロジェクトのマネジメントなど、テクノロジーコンサルタントとしてクライアントの変革を支援。ゼロトラスト、クラウドインフラに関するエキスパート。

南野 香澄　マネジャー
Technology Strategy & Transformation

外資コンサルティングファームを経て現職。IT構想策定、大規模システム構築案件、内部IT監査などを経験。専門は、IT構想策定、次世代ITインフラグランドデザイン、クラウドコンピューティングなど。主な担当プロジェクトに、「働き方改革・次世代ITインフラロードマップ策定支援」など多数。

参考文献

1. 総務省, “令和３年版情報通信白書,” July 2021, p. 313.



ブロックチェーン：ビジネス利用への期待

ブロックチェーンの加速度的普及

テクノロジーの成熟、標準化と、新たなデリバリーモデルが企業における普及を促進している

ウォールストリートを越えて

ブロックチェーンを活用したビジネス上の試みとして、多くの業界で創造的なユースケースが生まれている

ニーズ主導

既存企業であれ新興企業であれ、ブロックチェーンの実用化は、真のニーズへの取り組みから始まる

トレンド3

ブロックチェーン：ビジネス利用への期待

ビジネスの本質を変えつつある分散型台帳テクノロジーが、
デジタル資産だけでなく有形資産の管理手法を再考する機会を企業に提供している

昨今の暗号通貨とNFT（Non-Fungible Token、非代替性トークン）の流行はメディアを賑わせ、それを目にする人々の想像力を掻き立てているが、こうしたブロックチェーンやDLT（Distributed Ledger Technology、分散型台帳技術）といった技術はエンタープライズ領域でも関心が高まっている。企業間のネットワーク通信を支えるTCP/IP通信と同様に、共有台帳は、不可視ながらもビジネスにとって不可欠な基盤となり、業界を牽引する伝統的な企業が新たな収益源を創造してポートフォリオを拡大することや、スタートアップ企業が刺激的で新たなビジネスモデルを考え出すことを可能にする。

ブロックチェーンとDLTプラットフォームはハイプサイクルにおける幻滅の谷を越えて、真に生産性の向上を実現する段階に差し掛かっている。組織間の境界を越えてビジネスの本質を変え、企業がアイデンティティ、データ、ブランド、原産地情報、認証、著作権、そのほか有形無形を問わない資産をどのように創出し、管理するかを再考する機会を提供している。事実として、パンデミックにおいて投機的なプロジェクトが中止されている間も、利益をもたらすことが実証できているプロジェクトへの投資は倍増した[1]。

「*Tech Trends*」が前回ブロックチェーンを取り上げた際、我々はその採用と商用化の道筋を明らかにするための技術、プロセス、スキルセットそれぞれの標準化の必要性を考察した[2]。今日では、特にプライベートなネットワークやプラットフォームにおける技術的な進歩と規制基準の策定が、金融サービスを超えた組織での普及を促進し、成熟するテクノロジーとプラットフォームが、相互運用性、スケーラビリティーとセキュリティーを兼ね揃え、その普及を推し進めている。企業がブロックチェーンとDLTプラットフォームを使い慣れるにつれ、多くの業界で創造的なユースケースが生まれ、組織間の境界を越えて行うビジネスの本質が変わっていく。

ブロックチェーンの加速度的普及：進化するテクノロジーとスタンダード

第1世代のブロックチェーンとDLTは、暗号資産取引、清算、決済といった用途での実現可能性が実証されているが、スピードの遅さ、エネルギー消費量の多さとスケールすることの困難さもまた証明されている。

当初、マーケットには有象無象のプラットフォームやプロトコルが存在していたが、技術もしくはプロセスに於いて基準が欠如しており、相互運用性も無かったために企業は複数のプラットフォーム間でのやりとりを実現することができなかった。初期のユースケースは、あるユーザーから別のユーザーへの単純な価値移転に限定されており、ユーザーは契約の合意に必要な条件付きの取引や、不測の事態への備えを設けることができなかった。

さらに、トランザクションの検証に関連する固有の課題によって実装が制限されていた。例えば、暗号資産やそのほかのユースケースでは、大量のエネルギーを浪費し、トランザクションあたりのコストが高く、時間もかかる（トランザクションあたり10分以上）複雑で冗長な計算プロセスであるプルーフオブワーク（PoW：proof-of-work）によりトランザクションを検証していた[3]。

このような課題は、ほとんどのテクノロジーの普及の初期段階においてつきものである。起業家、企業、学術機関がブロックチェーンやほかのDLTプラットフォームの産業化に着手している今日では、テクノロジーの成熟、標準化の進化、新しいデリバリーモデルが企業における活用を促進している。具体的な事例は以下の通りだ。

プライベート／パーミッションド型ネットワーク
初期のDLTプラットフォームの多くは、誰でも参加できる信頼性の低いパブリックネットワークであった。結果として、不正を働くユーザーもネットワークにアクセスが可能で、プライバシーと匿名性が欠如していた。今日では、リスクに対抗する企業には、より信頼性の高い安全な選択肢も存在する。プライベートネットワークでは認証を得たユーザーのみが参加できる。また、パーミッションド型ネットワークでは認証されたIDを持つすべてのユーザーのみが参加できるが、その行動は役割の権限設定によって制御される。

技術の進展
使いやすさとスピードを重視する傾向が強まり、第1世代のアプリケーションではサポートされていなかった、より実用的なユースケース（例：自己実行型の契約やコンティンジェンシー）の確保が可能になった。トランザクションを検証するための新しいタイプの暗号化プロセスは、PoWよりもはるかに消費エネルギーが少なく、ボトルネックを取り払い、トランザクション速度の向上、およびトランザクション当たりのコストとエネルギー消費の削減を可能にした。例えば、プルーフオブオーソリティ（PoA：proof-of-

authority）は、企業が好むプライベート／パーミッションド型ネットワークの多くでトランザクションを検証するために使用されている。

インターオペラビリティ（相互運用性）の改善

エンタープライズ領域での活用に適した多くのDLTプラットフォームが登場した。Polkadot、Cosmos、Wanchainをはじめとする多くの新しいプロトコルやプラットフォームにより、企業は複数のブロックチェーンを接続し、多数のプラットフォーム上で複数の相手と円滑に対話、協力、共有、取引を行うことが可能になった。これにより、複数のユースケースとカスタマイズされたアプリケーションをサポートする基盤インフラを開発できる。アーキテクチャー、合意メカニズム、トークンの種類などの特性はプラットフォームによって異なり、組織は目的と用途に応じて複数のプラットフォームを検討する必要がある。

イノベーションエコシステム

DLTプラットフォームの増加に伴い、イノベーションが活性化し、広範で活力あるエコシステムが生まれている。エコシステムの参加者たちは、ID管理やサプライチェーンマネジメントなどの特殊な機能を提供する分散型アプリケーションを開発している。

今日では、テクノロジーの成熟、基準の発展、新しいデリバリーモデルが企業における普及を促進している。

ウォールストリートを越えて

金融業界は、より安全で効率的なトランザクションの実現を目指し、ブロックチェーンやほかのDLTプラットフォームのユースケース開発の先陣を切っていた[4]。しかし、特に複数の組織が同じデータを利用し、トランザクション履歴の可視化を必要とするユースケースにおいては、金融業界以外のプレイヤーもその多大なメリットを享受できる。このようなユースケースは従来一般的に、信頼とセキュリティーを欠いた高価で非効率的なプロセスとされてきた。ブロックチェーンやほかのDLTがビジネスオペレーションの効率性を強化し、価値を提供する新たな方法を生み出す可能性が顕在化するにつれ、ほかの業界の多くの先進的な企業は、これらの技術を導入し、既存のインフラやロードマップに統合していくであろう。

事実、「デロイト グローバル ブロックチェーンサーベイ2021」の参加者の大多数（80%）は、ブロックチェーン、デジタル資産、暗号資産ソリューションから新たな収益源が業界にもたらされると考えている[5]。世界的なブロックチェーンに対する支出は急増しており、ある調査会社は2021年の53億米ドルから2026年には340億米ドルに増加すると予測している[6]。別の調査によると、ブロックチェーンの実装においては銀行業がリードしており、通信、メディア、エンターテインメント、製造業、医療・ライフサイエ

ンス、小売、消費財、そして政府がそれを追いかけている。また、小売と消費財は、現在から2024年の間にブロックチェーン関連の支出が最も急速に増加すると予測されている[7]。

次のようなユースケースが注目を集めている。

自己主権型データ管理とデジタルID
ブロックチェーンやDLTプラットフォームを利用して安全なデータ格納と管理を行うことで、ユーザーは個人データの所有権を取り戻し、改ざんのないデジタルIDを作成して管理することができる。これにより、個人を特定できる情報のセキュリティーが強化され、偽造IDや盗難IDの作成が防止される。アプリケーションには、接触者追跡、電子医療記録と認証情報、電子投票などが含まれる。

第三者間での安全なデータ共有
「*データシェアリング時代のはじまり*」で述べたように、第三者間でのデータのアクセスと共有は、通常、テクノロジーのサイロやプライバシーの問題が原因で制限されている。プライベート／パーミッションド型ネットワークを使用することで、組織はデータを安全に利用・交換できるようになる。これにより、検証済みの信頼できる第三者へ、必要な特定のデータアクセスのみを提供できるようになる。これは、データの整合性やプライバシーを犠牲にすることなく、企業と業界の境界を越えてデータを共有し、エコシステムやパートナー間での協力と信頼を強化できることを意味する。例えば、医療提供者間の安全なデータ共有は、患者の健康情報の交換を改善する可能性があり、情報機関の間では、国際的な境界を越えて、脅威情報やそのほかの有益な情報の交換を促進することができる。

グラントファンディング
助成金や融資といった資金調達に関する支援者と被支援者の双方にとって、ブロックチェーンやそのほかのDLTプラットフォームは、財務および効果の監視と報告に伴う管理上の負担を軽減することに役立つ。連邦政府機関の取り組みに関するある調査では、ブロックチェーンを使用して、実行、追跡、監視することで、報告の質と透明性が向上し、支払いと報告の効率性が向上したことが明らかになった[8]。

会社間勘定
特に大規模かつグローバルな組織や、多数の事業体が存在する組織では、多くの場合、複数のERP、スプレッドシート、手動プロセスを用いて、企業間取引の決済や消去を行う。トランザクションの完了後、それらの管理ツール間の数値の整合性が確認されるまでに何週間も時間を要することが往々にしてあり、ブロックチェーンやそのほかのDLTプラットフォームを用いて共通かつ不変の記録を検証し作成することで、特に合併や買収における会社間移転会計のトレーサビリティ、透明性、監査性を向上させることができる。

サプライチェーンの可視化
今日のグローバルサプライチェーンでは、ブロックチェーンやそのほかのDLTプラットフォームが製品追跡と原材料のトレーサビリティを向上させ、偽造製品や違法または粗悪な原材料や部品の削減、原

産地証明（七面鳥、ダイヤモンド、ワインなど）、政府による関税や貿易政策の実施を後押しすることができる。また、資産と出荷の追跡にも役立ち、発注からサプライチェーン、請求書作成、支払いに至るまで、調達プロセス全体の透明性を高めることができる。

顧客（ファン）エンゲージメントの向上

NFTをコレクションとして販売することで、個人や組織はデジタルコミュニティーを構築し、ファンや顧客を引き付け、ブランドを構築することが可能になる。COVID-19によりスポーツやエンターテインメントのライブイベントが制限された際に、NFTは、エンターテイナーやスポーツのパーソナリティ、チーム、リーグが収益を多様化し、ファンや顧客とのコミュニケーションを保つことを助けた[9]。また、ブロックチェーンとNFTをイベントのチケット発行に用いることで、チケットの不正や改ざんを排除できる可能性がある。

クリエイターへの正当な収益還元

アーティスト、ライター、発明家、そのほかのクリエイターは、ライセンス、特許、著作権を通して知財（IP：intellectual property）の所有権を証明し、収益化することに苦心している。ブロックチェーンやほかのDLTプラットフォームを使えば、クリエイターは、IPをダウンロードするたびに実行されるスマートコントラクトに自分のIPを埋め込むことができる。ユーザーIDに基づいた自動支払を実現することができれば、大企業に個人消費者よりも高い支払いを求めるといった処理も可能になる。

ビジネスと顧客ニーズを牽引

今日のDLTプラットフォームと1990年代半ばのインターネットとの間にはいくつかの類似点を見出すことができる。また、インターネットが業界やエコシステム全体のビジネスプロセスにもたらした変化についても同様に類似点があるといえる。

黎明期、インターネットは遅く、醜く、誤解されていた。一部の伝統的な企業はインターネットを無視し、オンラインショッピングや映画ストリーミングの市場はないと結論づけた。その一方で、多くのスタートアップは熱心に参加し、社名の最後に「.com」を付け、ビジネスや製品の立ち上げに多額の費用を費やした。

2つのおとぎ話はいずれも凄惨な結末を迎えた。しかし、インターネットを無視して路頭に迷ったすべての業界リーダーにとって代わるように、抜け目のない企業が最終的にオンラインの巨人となった。そして、持続不可能で欠陥のあるビジネスモデルを持ったスタートアップが短命で終わった代わりに、堅実なビジネス戦略と実行力を持つスタートアップは大成功を収めた。ドットコムバブルが収まったときに生き残ったのは、目に見えるビジネスと顧客のニーズを中心にビジネスモデルを構築した（あるいは再構築した）企業群であった。

繰り返しになるが、ブロックチェーンやほかのDLTプラットフォームの現状は、1997年のインターネットのそれと類似している。不格好で、インターフェースは洗練されていないが、エンタープライズアプリケーションのための多くの可能性がある。インターネットと同様に、企業や組織がビジネスプロセスとオペレーションを合理化し、新しいデジタルビジネスモデルの構築と価値創出を実現する後押しができる。従来型の仲介者を利用せずに、組織の境界外で信頼を築くことができる特性は、価値の創造と提供の方法を大きく変えるであろう。そしてインターネットのように、彼らは産業やエコシステムを越えてビジネスが行われる方法を変えている。1つの組織でも変革は困難だが、それが複数の組織や業界にまたがる場合は、さらに難しくなる可能性がある。DLTを使用する障壁が低くなるにつれ、*ビジネスと顧客のニーズをリード*している既存企業と新規参入企業の両者が、この変革をよりスムーズに進めることができる。

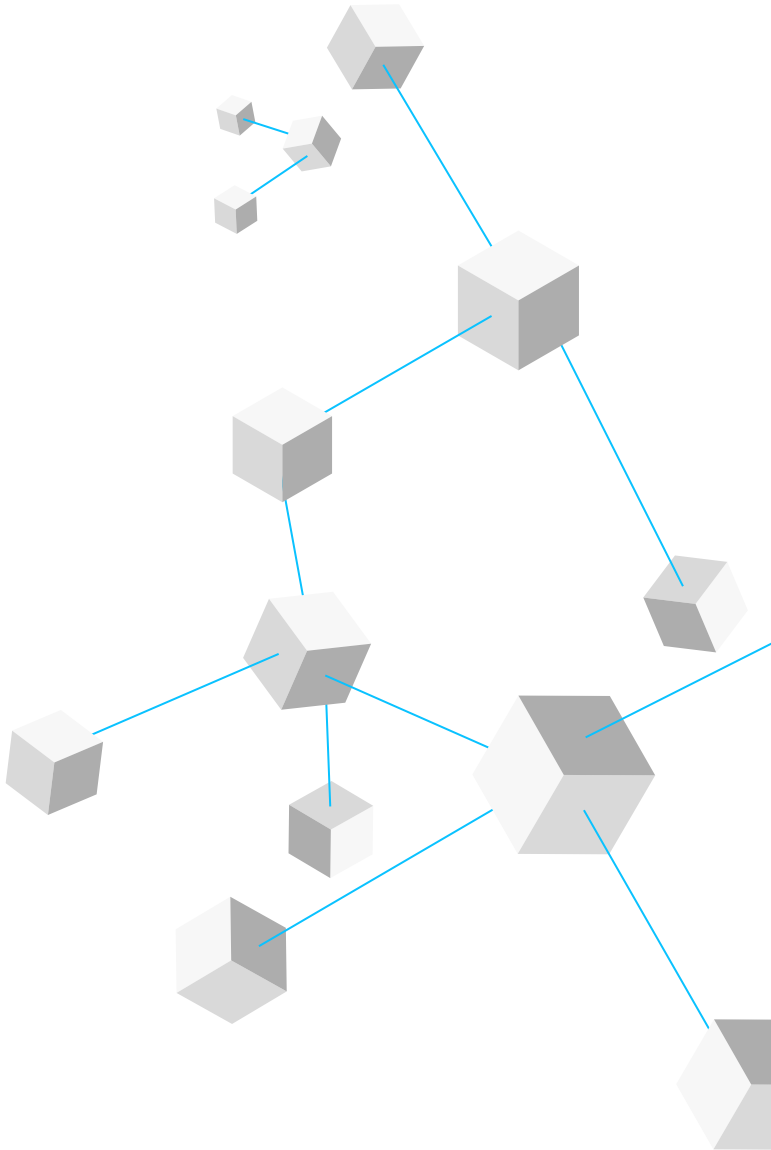
多くの起業家やスタートアップは、ブロックチェーンやほかのDLTをベースにした新たなユースケースやビジネスモデルを開発し、投資家を惹きつけようとしている。例えば、いくつかのスタートアップがオーサーシップの基盤となる共有台帳を構築しており、そうしたプラットフォームは芸術家、作家、音楽家が直面する著作権、帰属、著作権管理、著作権使用料支払いに関する課題を解決することができる[10]。しかし、既存のマーケットリーダーもこれらのトレンドを静観している訳ではなく、信頼できるサービスプロバイダーとしての評判を活用し、DLTを用いたビジネスモデルを取り入れている。例えば、Microsoftはブロックチェーンを活用して同社のパートナー企業に対するゲームのロイヤルティ契約と支払いの記録を提供している[11]。

進むべき道

今日、成熟しつつあるテクノロジー、発展する基準、新たなデリバリーモデルが、ブロックチェーンやそのほかのDLTプラットフォームの普及を促進している。多くの企業ユースケースが出現し続けており、さまざまな業界の組織が、あらゆる種類の物理的およびデジタル資産の価値創造を変革し、組織の境界を越えてビジネスプロセスを合理化するだけでなく、新しいビジネスモデルを開発できるようになっている。共有台帳への信頼が高まるにつれ、ブロックチェーン上の記録は、いつの日かブロックチェーン外の記録よりも信頼できると認知されるようになるかもしれない。

革新的なビジネスモデルは、スタートアップが新天地を切り開き、レガシー企業が「信頼を必要としない」共有台帳エコシステム内においても信頼できるブローカーとしての評判を維持するために、既存のビジネス戦略を進化または補完することを可能にする。成功するためには、新参者も古参も、まず顧客やビジネスのニーズを正確に特定する必要があるであろう。

組織がブロックチェーンやほかのDLTプラットフォームを活用して新しいビジネス価値を創出する際には、どのプラットフォームやプロトコルが業界や検討しているユースケースに最も適しているかを理解し、将来にわたって複数のプラットフォームで運用できるよう、エンタープライズアーキテクチャーを進化させる必要があるであろう。そして、これらのテクノロジーとプラットフォームがもたらす組織や業界を横断した変革をサポートするため、組織にビジネスプロセスの改善に向けた切迫感を醸成するとともに、チェンジマネジメントのケイパビリティーを強化することが必要であろう。



最前線からの学び

Caisse des Dépôtsは、フランスの金融業界におけるブロックチェーン活用を加速度的に普及させる

フランスの公的金融機関であるCaisse des Dépôts et Consignationsは、いくつかの成熟したブロックチェーンイニシアティブを打ち出している。いまだ、多くの企業がブロックチェーンとは何か、どのように役立つのかを解明しようとしている一方で、205年の歴史を持つこの公的金融機関は、ブロックチェーンを活用することで、新たな機会と新たなオペレーションへの扉を開けようとしている。

しかし、一夜にしてそこにたどり着けたわけではない。Caisse des Dépôtsのブロックチェーンおよび暗号資産プログラムの責任者であるNadia Filaliは、2015年にBitcoinと暗号資産を支えるセキュリティープロトコルについて初めて聞いたとき、その可能性を認識した一方で、幅広いパートナーエコシステムとともに、多様な専門知識を持つチームが必要になることに気づいた。「ブロックチェーンの活用は1社ではうまくいかない。協力する必要があるのだ」とFilaliはいう[12]。

Caisse des Dépôtsは、複数の金融機関やブロックチェーンのスタートアップと話をした後、ほかの10の組織と提携し、LaBChainを立ち上げた。LaBChainは、金融サービスにおける分散型台帳技術の活用機会調査に特化したコンソーシアムである。コンソーシアムメンバーすべてが訓練と実践を通じてこの技術について共通の理解をひとたび確立すると、LaBChainは、担保管理、顧客確認情報（KYC：Know Your Customer）の共有、ユーロトークン化などのユースケースに関するPoCプロジェクトの実現を可能にした。規制当局や研究者を含む35人以上のメンバーを抱えるLaBChainは、フランスのブロックチェーンエコシステムへの入り口となった。「重要なのはシンクタンク（考える組織）を作ることだけでなく、ドゥタンク（実行する組織）を作ることだった」とFilaliはいう。

ブロックチェーンと暗号資産プログラムの1つの使命が技術導入をサポートすることであるとするならば、もう1つの使命は、ビジネスや顧客のための潜在的な応用分野を探ることである。Filaliは、ブロックチェーンとその潜在的なインパクトを理解している社内

チームを編成し、法務、IT、財務部門のスタッフを含めて、ソリューションの実装を開始した。Filaliのチーム（関連スタッフ含め）は、今では、社内のブロックチェーン製品を開発するだけでなく、規制当局と相談することや、ブロックチェーンを活用するほかの公的機関の支援も行う。彼らの仕事は、EU Blockchain Observatory and Forumとの提携につながり、Filaliは2021年4月以来、INATBA（International Association for Trusted Blockchain Applications）の理事長を務めている。

Filaliのチームは、デジタルIDに関連するより広範なプロジェクトにも取り組んでいる。フランスの郵政公社とエネルギー会社2社とともに、Caisse des DépôtsはArchipelsというスタートアップを設立し、文書認証サービスを提供している。エネルギー供給者は、認定された請求書のハッシュ（存在証明）をArchipelsのブロックチェーンにて提出することができる。これにより、銀行や管理者は顧客から提供されたドキュメントを検証し、不正行為を減らすことが可能となる。Archipelsは現在2,000万件以上の文書のハッシュを保持しており、台帳内のエントリを作成および更新している。Filaliは、この最初のサービスが、デジタルウォレットなど、より多くの本人確認サービスにつながると期待している。

これらのイニシアティブは、いずれも、フランスの各省や業界団体、銀行との間で緊密な調整を必要とした。Filaliは次のように語る。「大規模なブロックチェーンプロジェクトはいずれもこのような機関と連携する可能性が高いため、パートナーとの密連携が重要であり、トップマネジメントによるスポンサーシップも我々が成長するためにとても重要だった」

ブロックチェーンが成熟するにつれ、こうしたパートナーシップの構築は容易になっていくかもしれない。2019年と2021年に、フランス議会は一連の暗号資産規制を可決した。これらの規制は、ブロックチェーン関連企業が金融規制当局に登録し、とりわけマネーロンダリング防止およびKYCに関する規則に従うことを要求する。「ある意味で、これは暗号資産とブロックチェーンに大きな正当性を与えた」とFilaliはいう。いまでは、これまで暗号通貨やブロックチェーンに懐疑的だった機関がデジタル資産を活用する方法やトークン化と自己主権型IDに関する具体的なユースケースを模索している。

「惑星が並んでいるようなものだ。我々は、エネルギーを持っている。我々には能力がある。そして、今行動しなければ時機を逸するかもしれないということを人々は理解している」とFilaliはいう。

ブロックチェーンは宝石商にとって永遠のパートナー

香港を拠点とする宝石商のChow Tai Fookは、世界でも有数のダイヤモンド販売業者である。定義上、同社は物理的な資産を売買しているが、だからといって新しいデジタルツールを活用できないわけで

はない。同社は現在、デジタルセールスおよびマーケティングプラットフォームを運営しており、顧客データ分析を活用するとともに、生産ラインの多くを自動化している。そして今、ブロックチェーンをデジタルポートフォリオに加えた。

Chow Tai Fookの商品の主なバリュープロポジションの1つは、アメリカ宝石学会（GIA：Gemological Institute of America）の認証、およびダイヤモンドの倫理的調達のガイドラインを定める国連のキンバリープロセスの要件を満たすダイヤモンドを販売しているという事実である。問題は、良心的でない販売業者が定期的にこれらの基準を掻い潜り価格を下げたダイヤモンドを売るため、消費者はその違いを見分けるのに苦労していることである。

このような問題をうけて、Chow Tai Fookは、ダイヤモンド認証情報のデジタル化にあたり、ブロックチェーンを採用した。ダイヤモンドをカットして研磨した後、Chow Tai FookとGIAによって管理されている2者間ブロックチェーン台帳の特定のエントリに記載されたシリアルナンバーとダイヤモンドをリンクさせる。これにより、原産地や等級など、ダイヤモンドの最も重要な情報の不変でデジタルな記録が保存される。顧客はダイヤモンドを宝石店に持ち込み、シリアル番号と関連する記録を調べてもらい、専用のモバイルアプリケーションを通じてこの記録にアクセスすることができる。

Chow Tai Fookの宝石商グループにてGeneral manager of business analytics and technology applicationsを務めるJade Tin Hei Leeは次のようにいう。「これが顧客を守る方法である。ブロックチェーンによって、ダイヤモンドの情報（品質・履歴）について完全な透明性を持つことができる[13]」

このような情報をブロックチェーンに記録することは、Chow Tai Fookが独自の内部プロセスを構築することにも役立つ。同社には5,000を超える宝石店があり、その約65%は加盟店が所有・運営している。これらの店舗では年間約50万個のダイヤモンドを取り扱っており、0.3カラット以上のダイヤモンドのほとんどについて独自に認証している。これらの各店舗を経由したすべてのダイヤモンドについて認証結果と照合することは、以前は非常に難しいプロセスであったが、今では、ダイヤモンドのシリアル番号をブロックチェーンの元帳エントリーと照合するだけで済む。

同社は、金融取引を容易にするにあたってもブロックチェーンを利用しようとしている。同社の加盟店は、在庫購入のコストを賄うために銀行融資を必要とすることがあるが、銀行はその融資を行う前に、店舗の売上高や収益、そのほかの業績に関する情報を確認する必要がある。Chow Tai Fookは現在、加盟店のデータをブロックチェーンに入力することで、処理を高速化し、店舗が必要なときに必要な分の在庫を確保できるようにする方法を模索している。

「ブロックチェーンを使って業績情報を記録し、銀行が簡単に検証できるようにすることを目指している。我々は加盟店の営業効率化に貢献したい」とLeeはいう[14]。

ダイヤモンドは非常に流動性の低い資産である。高い価値がある一方、現金や株式などの資産に比べ、売買や取引が困難な場合がある。Leeによると、ダイヤモンドの価値をデジタル化して記録することで、この問題の一部を減らすことができる。また、デジタル証明書を信頼する可能性が高い若い世代の購入者を引き付けるのにも役立つ。デジタルに精通した若い顧客層の期待に応えることが、同社の重要な優先事項でもある。

「Chow Tai Fookは92年前に創業した企業で、ダイヤモンド業界はそれよりもさらに古いが、ブロックチェーンなどの技術を活用した新しい機会によるメリットを模索している。我々は古い会社だが、何十年にもわたって革新を続けている」とLeeはいう。

いかにしてブロックチェーンはアメリカ財務省においてミステリーからメインストリームに変わったのか

アメリカ連邦政府は、大抵の一般企業より詳細に支出を追跡することに力を注いでいる。透明性と説明責任は、納税者のお金を扱う際に最も重要である。そのため、財務省はブロックチェーンによる新たな記録保持の自動化の可能性を調査している。

毎年、さまざまな連邦機関が数十億ドルの補助金を拠出している。これらの補助金の受給者は、より小規模な2次受給者へ補助金を配るケースが多い。補助金の流れについて追跡する必要があるが、歴史的に見て、これは大量の報告と事務処理を意味してきた。

こうした負担を軽減するため、米財務省の財政局は、補助金の分配と資金の流れを追跡するプロセスの簡素化を目的としたブロックチェーンソリューションの開発に取り組んでいる。このプロジェクトは、補助金の支払いを実際のお金を表すデジタルトークンに変えるものである。補助金の受給者は、政府機関との間でトークンを換金するか、トークンを分割して2次受給者へ配布することができる（2次受給者もトークンを実際のお金に変えることが可能）。これらの過程で、各トークンの取引の際にブロックチェーン上にて、送金額および送金目的に関する情報が更新・記録される。

このような情報の大部分は自動的に生成されるため、この自動化されたプロセスが、受給者および2次受給者が政府資金を受け取る際に必要な事務処理の大部分を置き換えることになる。研究機関は、報告などの管理業務に44%以上の時間を費やしていると推定され、ブロックチェーンを使って支払いを追跡することで、管理業務の多くを削減できる可能性がある。

財務省のInnovation program managerであるCraig Fischerは、次のように語る。「すべての補助金に関する情報に資金の出元を加えることができる。つまり、我々は、その資金は誰から得たものなのか、何のためのものか、そして資金調達の意図を知ることができる。ブロックチェーンによって、記録と報告は同義になる[15]」

このプロジェクトはまだPoCの段階である。現時点では、このアプリケーションは補助金をトークン化し、ブロックチェーンに大本の補助金とその分配を記録できる。最後に必要なピースは、ブロックチェーンと従来の支払システムをつなぐ汎用APIである。

補助金支払いプロジェクトは、Fischerと彼のチームが既に運営しているほかのブロックチェーンPoCの成果に基づいている。1つ目は、ブロックチェーンを利用して職員が使用するスマートフォンを追跡するプロジェクトである。2つ目は、ソフトウェアライセンスを管理するプロジェクトで、どの職員が活発にライセンスを使用し、どのライセンスを無効にしても問題ないかを追跡したものである。

Fischerによると、これらの取り組みはいずれも、同部門内でブロックチェーンの認知度を高め、ブロックチェーンの持つ暗号資産以外の用途を実証することを目的としているという。政府機関でブロックチェーンを使用するには、いくつかの課題がある。例えば、Fischerの知る限り連邦政府内でほかに成熟したブロックチェーン決済プロジェクトはないため、彼のチームがアクセス制御やセキュリティー基準などのサポートプロセスを設計・開発しなければならないことである。

しかしFischerは、彼らのPoCが連邦政府全体でブロックチェーンを利用するさきがけになっていると確信している。当初、最も困難だったのは、ブロックチェーンとは何かについて人々を教育することであったが、今では理解が浸透し始めており、彼は付加価値を示すことに集中することができている。「以前は、私はブロックチェーンを使ってこの問題に対処している、と説明する必要があった。今では、私はこの問題に対処している、というだけで済む」とFischerはいう。

私の見解

Andre Luckow
PhD, head of emerging technologies, BMW Group IT

20年間、新しいテクノロジーを研究してきた経験から、誇大宣伝と希望の違い、つまり真に変革的なテクノロジーとそうでないテクノロジーの違いを認識することができるようになった。

2018年、私はブロックチェーンがハイプサイクルのピークにあったとき、ブロックチェーンの潜在的なユースケースを検討するよう求められた。当然ながら、私は健全な懐疑心を持って検討を進めたが、我々の組織が可能性を絞り込むにつれて、変革のための正しいユースケースを見つけるに至った。

ビジネス上の問題はデータのレンズを通して見えるが、BMWグループの事業の中でより良いデータを必要としていたのは複雑なサプライチェーンであった。BMWグループでは、複雑なグローバルサプライヤーネットワークを活用し、15ヶ国31工場で1日約1万台を生産している。少し前までは、我々はまだスプレッドシートと電子メールに依存していた。詐欺やセカンドティアサプライ

ヤーにおける可視性の制約、供給と需要のミスマッチは、生産の混乱と品質問題を引き起こす可能性がある共通の問題だった。私のチームは、BMWグループと少数のサプライヤーがブロックチェーン上でより簡単にサプライチェーンデータを共有できるようにするPoCから始めた。すべてのサプライチェーン参加者間で共有されたリアルタイムの可視性により、在庫の過不足を防ぐことにつながった。また、透明性のおかげで、部品の出所に関する情報が増えただけでなく、サプライヤーは改善の機会を見つけることもできた。

BMWグループは、リーダーやサプライヤーパートナーにプロトタイプを披露した後、明確な事業機会を見出し、ブロックチェーンの取り組みをより多くのサプライヤーに拡大するための投資をした。以前はPartChainとして知られていたこの取り組みは、ほぼシームレスな透明性を実現し、「Catena-X」や「Automotive Network e.V」のような、より広範なデータ共有イニシアティブに影響を与えた。Catena-Xは、自動車のバリューチェーンに沿って共同データエコシステムを構築し、OEM、中小企業、リサイクル企業などが、安全なデータに基づいた経済圏を最大限に活用できるようにした。誰の目にも明らかなように、このテクノロジーは、バリューチェーン全体でデータの可視性を向上させるためのイニシアティブを推進する上で有益であることが証明されている。

また、ドライバーの操作性を向上させるブロックチェーンのユースケースも模索している。製造とサプライチェーンにおける当社の進歩にもかかわらず、消費者への自動車の販売やレンタルは依然として紙を大量に使った困難なプロセスである。我々は、最近ドイツ政府と提携し、運転免許証情報の共有と購入プロセスの簡素化にあたりブロックチェーンを利用している。自己主権型IDは、ドイツ国民が最小限の手間と最大限の安全性のもとに、ライドシェアや保険会社との頻繁な免許証情報のやりとりを可能にし、売り手にはID詐欺を減らす簡単な方法を提供する。そう遠くない将来、車の購入はQRコードをスキャンするのと同じくらい簡単になるであろうと我々は考えている。

2018年のブロックチェーンに関する誇大宣伝と、それ以降のBMWグループの進展を振り返ってみると、2つのことが明らかである。1つは、ブロックチェーンは変革をもたらすものであり、やがてブロックチェーンを基礎とする技術をそれと気づかずに使うようになる程に、より優れたビジネスプロセスと顧客体験を築くことができるであろう可能性を秘めていること。もう1つは、変革には皆が予想していたよりも長い時間がかかる可能性があること。企業は、どの新しい市場やエコシステムがブロックチェーンによってサポートされ、簡素化されるかについて、より広い考え方を持つ必要がある。適切なユースケースを見つけるためには、データに基づき適切に問題を設定することが必要である。この技術をあらゆる方面から推進していけば、さらに素晴らしいアイデアが出てくるはずだ。

今後の展望

ストラテジー

CEOには、ITリーダーと協力し、ブロックチェーン技術の可能性を理解するまたとない機会が提供されている。今日のブロックチェーン技術の進歩は、30年前、TCP/IPの標準化によりインターネットが急速に普及した状況と類似している。ブロックチェーン技術に対する広範な理解はいまだ限定的であるものの、ビジネスモデルに影響を与える可能性は非常に大きい。データベースが組織内のビジネスプロセス再構築を可能にしたように、DLTは組織間のプロセスの合理化を可能にする。CEOはテクノロジー採用ライフサイクルに乗るスピード感を決める必要がある。

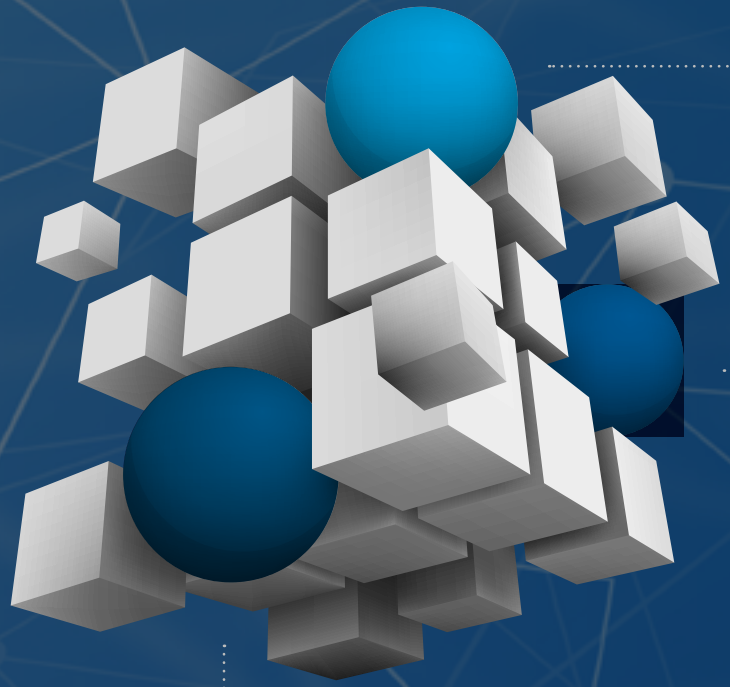
ファイナンス

多くのCFOは、ブロックチェーンなどのデジタル台帳技術の理論的な有用性を認めているが、本格的な採用には消極的である。その場合は、アジャイルの手法を用いて、DLTのユースケースをテストし、効果と安全性を検証することをお勧めする。CFOは、テストケースの特定や検証の実施、結果の確認にあたり、ITリーダーと密に連携しながら進め、ユースケースの検証が成功した後、企業全体や企業間への展開へ移行する前に、規制や財務上のリスクを見直すといいであろう。

リスク

企業によるブロックチェーン利用は十分には普及しておらず、この技術のリスクに関する理解は始まったばかりである。CROはIT部門と協力し、新しいテクノロジーに対する組織の準備状況を改善する必要がある。技術採用のためのロードマップを策定し、ブロックチェーンのユースケースを特定することに加え、リスクを主体的に減らすことができる。例えば、新しい暗号化アプリケーションは、トランザクションの検証における効率性と信頼性を大幅に向上させるが、ブロックチェーンベースのデジタルIDソリューションは、秘匿性の高いトランザクションにおけるセキュリティーを強化することができる。さらに、ブロックチェーンの採用準備に関する計画は、量子コンピューティングなどの新しい技術の採用の際にも応用可能である。

さあ、はじめよう



要点

1 成熟しつつあるブロックチェーン技術、DLTプラットフォームや基準などにより、どのような新しいデリバリーモデルや収益源、ビジネスプロセスの改善が可能になりうるか。

2 分散化は、ほかの組織やエコシステムパートナーとのコミュニケーションや協力、データ交換の方法をどのように改善しうるか。

3 製品やサービスの開発、製造、流通の透明性やトレーサビリティの確保にブロックチェーンを使うことで顧客の信頼を得る、あるいは高める機会を特定できるか。

執筆者

Wendy Henry
Government & Public Services Blockchain leader
Deloitte Consulting LLP
wehenry@deloitte.com

Linda Pawczuk
Global Blockchain & Digital Assets leader
Deloitte Consulting LLP
lpawczuk@deloitte.com

SENIOR CONTRIBUTORS

Hiroki Akahoshi
Director, Deloitte Tohmatsu Consulting LLC

Marie-Line Ricard
Partner,
Deloitte France

Tyler Welmans
Director,
Deloitte MCS Limited

Claudina Castro Tanco
Senior manager,
Deloitte Consulting LLP

Jesus Pena Garcia
Senior manager,
Deloitte Luxembourg

Wiktor Niesiobędzki
Specialist lead,
Deloitte Poland

Ruchir Dalmia
Senior consultant,
Deloitte MCS Limited

Lily Pencheva
Senior consultant,
Deloitte MCS Limited

Nicklas Urban
Senior consultant,
Deloitte Consulting GmbH

参考文献

1. Martha Bennett and Charlie Dai, "Predictions 2021: Blockchain," Forrester, October 28, 2020.
2. Deloitte Insights, *Blockchain to blockchains: Broad adoption and integration enter the realm of the possible—Tech Trends 2018*, December 5, 2017.
3. John Schmidt, "Bitcoin's energy usage, explained," *Forbes*, June 7, 2021.
4. KBV Research, *Global blockchain technology market by type (public, private and hybrid), by component (infrastructure & protocols, application & solution and middleware), by enterprise size (large enterprises and small & medium enterprises), by industry vertical (BFSI, IT & telecom, healthcare, retail & ecommerce, government & defense, media & entertainment, manufacturing and others), by regional outlook: Industry analysis report and forecast, 2021–2027*, May 2021.
5. Linda Pawczuk, Richard Walker, and Claudina Castro Tanco, *Deloitte's 2021 Global Blockchain Survey: A new age of digital assets*, Deloitte Insights, 2021.
6. Yahoo.com, "Global Blockchain Market (2021 to 2026) - by Component, Provider, Type, Organization Size, Deployment, Application, Industry and Geography," accessed November 29, 2021.
7. Fortunebusinessinsights.com, "Blockchain Market Size, Share & Covid-19 Impact Analysis, 2021-2028," accessed November 29, 2021.
8. MITRE, *Assessing the potential to improve grants management using blockchain technology*, 2019.
9. VISA, *NFTs: Engaging today's fans in crypto and commerce*, accessed November 2021.
10. 101 Blockchains, "Real world blockchain use cases—46 blockchain applications," July 6, 2018.
11. Rachel Wolfson, "Game time? Microsoft adopts Ethereum blockchain for gaming royalties," *Cointelegraph*, December 18, 2020.
12. Nadia Filali (head of the blockchain and cryptoassets program, Caisse des Dépôts), interview, October 15, 2021.
13. Jade Tin Hei Lee (general manager of business analytics and technology applications, Chow Tai Fook Jewellery Group), phone interview, September 23, 2021.
14. Ibid.
15. Craig Fischer (innovation program manager at the US Department of the Treasury), interview, October 29, 2021.

日本のコンサルタントの見解

デジタル資産国内本格デビュー

2021年、NFT“元年”

2021年はブロックチェーン技術が国内でも注目された年となった。その立役者の1つが流行語大賞にもノミネートされたNFTである。NFTはビットコインなどの暗号資産と同じくブロックチェーン上で発行されるトークンの一種である。個々のトークンに識別子を付与しデジタルデータに固有性を持たせることができる点がNon-Fungible（非代替性）と呼ばれる所以だ。

ゲーム・絵画・音楽・映画などのデジタル作品とユーザーを紐づけることで、ユーザーが保有していることを証明できる点が新しい。あらゆるプレイヤーが参入し、一部の高値での取引はバブルと評されている。また、「デジタル所有権」という概念は日本国内法にはない。ビジネスで活用する際は法的論点を踏まえた精緻な商品設計が必要である。

同じくアセットのデジタル化では、株式・債権・不動産などを対象に配当を有するものとしてSTO（Security Token Offering、セキュリティートークンオファリング）が先行しルール整備が行われた。2022年には大阪で取引所の設立が予定されており、今後の動向に注目したい。

暗号資産（仮想通貨）

アメリカでは若い成人男性の43%が何らかの暗号資産（仮想通貨）を利用したことがあると回答しているなど一定の広がりを見せつつある[1]。ビジネスでもアメリカ電気自動車大手Teslaが暗号資産決済を導入、アメリカ大手決済事業者Block（旧Square、Twitter創業者Jack DorseyがCEO）が運営する決済アプリケーションCash Appでビットコイン売買を可能にするなど、海外では成長企業が続々と参入している。エルサルバドルが2021年9月に法定通貨にビットコインを採用するといった驚くニュースもあった。

一方、国内では投資意欲が海外ほど高くないことも影響し、これまでの暗号資産（仮想通貨）に対しては消極的であった印象であるが、2022年に入り、LINE PayがLINK（傘下企業が発行する暗号資産）決済を試験提供することを発表するなど変化が見えつつある。また、メタバースや前述NFTが今後拡大していくなかでおのずと国内でも利用が増えることが予測される。

中央銀行デジタル通貨

CBDC（Central Bank Digital Currency、中央銀行デジタル通貨）による法定通貨の革新も進む。先行した中国では2022年北京五輪会場で「デジタル人民元」を利用可能としている。一部報道では2021年10月時点で個人ユーザー登録数が1億4,000万件に達したなど、国の本気度が伺える。なお、すでにカンボジアでは2020年10月より「バコン」という名のデジタル通貨が正式運用されており、この技術を実は日本のブロックチェーン企業であるソラミツが提供している。

日本の中央銀行である日銀は、現時点において発行する計画はないとしているが、実証実験を並行して進め、2026年を目途に判断する想定である。

国内企業が取り組むべきこと

「なぜブロックチェーンか」ではなくどう活用するか、に発想の転換を

デジタル資産が躍進する中でビジネス取引を支える基盤技術としてのブロックチェーン活用も進んだ。プライベート型ブロックチェーンは、あらかじめ承認された企業のみが参加するため、暗号資産（仮想通貨）などパブリック型ブロックチェーンと比較して、不正な参加者を排除することができる。

「なぜブロックチェーンか」という問いに対して、透明性・改ざん耐性・可用性などいくつかの回答が挙げられるが、技術点のみに着目した回答は難しい。どう活用するかに発想を転換して検討することが重要だ。例えば、業界の垣根を超えたエコシステム型ビジネスである。必須機能としての「送金・決済」「本人確認・ID」「健康・医療記録」などのセンシティブ情報の共有、企業間をまたがる「取引履歴」の保管など、どれも多くのユースケースがすでに生まれている。通常、企業間でデータを連携する場合、両者のシステムに合わせてデータを突合し、形式を揃えて各々が格納する。この調整と開発に多大な費用を要して先に進まず、断念するケースが現場では起きている。ブロックチェーンはsingle source of truth（唯一の情報源）の概念を持ち、この情報源が参加者監視の下に正しく記録され続ける。この特性を活かすべきである。

本文でも用いられたデロイトのグローバルサーベイでは、経営陣のブロックチェーンに対する前向きな姿勢が明確に伺われた。技術点のみで検証するフェーズは終わり、ビジネスへ取り入れられるフェーズに差し掛かっている。

本番運用に向けた準備は整っているか

今後国内企業においても、実証実験の枠組みを超えて本番運用を迎えるブロックチェーンシステムが多く発表されるであろう。ブロックチェーンは、企業間を跨るエコシステム型ビジネスにおいて有効であり、技術だけでなく関連ステークホルダー（座組）に対する強い推進力やガバナンス態勢が不可欠である。
デロイトはグループで事業企画・設計／開発・運用（コード診断などセキュリティー含む）まで一貫してブロックチェーンシステムをサポートするチームを組成しているが、さまざまなテーマでの相談が増えている。潮目が変わり、まさに本番に向けた準備を整え活用する局面である。

社会課題の解決に向けて

脱炭素、エシカル消費などあらゆるものの トレーサビリティをブロックチェーンで

ビジネスだけでなく社会課題の側面でもブロックチェーンの活用が期待されている。脱炭素やエシカル消費など社会課題に対するアプローチが経営の主アジェンダとなる中で、情報共有基盤として採用する事例が先行する海外ではいくつも生まれている。国内でもデロイトがJICAと取り組む「コートジボ

ワール国ブロックチェーン技術を活用した児童労働の防止に係る情報収集・確認調査」では、現地の正しい申請情報を改ざんなく格納する基盤としてブロックチェーンを活用した。

国連開発計画（UNDP）は、Beyond Bitcoinと題したサイトで、SDGsの解決に向けてブロックチェーンの6つの活用ドメイン（「金融包摂（Financial Inclusion）」「エネルギー・アクセスの環境向上」「生産と消費責任」「環境保護」「法的アイデンティティの提供・維持」「寄付の効果向上」）を定め推進している[2]。

欧米・中国など先進他国はブロックチェーンを国家戦略として表明（・議論）している。日本でも昨年6月に閣議決定された成長戦略計画に「ブロックチェーンなどの新しいデジタル技術の活用」が明記された。これにより、国内ビジネス活用あるいは社会課題解決に向けて、ますます拡大が期待される。

執筆者

赤星 弘樹　ディレクター
Core Business Operations

IT系コンサルティング会社を経て現職。ペイメント／ブロックチェーンリード。専門は、金融分野（含む異業種）の新事業開発、Fintech活用、デジタル戦略、組織改革など。担当プロジェクトに、「決済事業戦略」（小売／通信）、「ブロックチェーン技術研究・実証」（銀行）など多数。

参考文献

1. Forbes, “Crypto’s Super User: Young Men. 43% Of U.S. Males Aged 18 To 29 Have Bought The Currency,”accessed February 17, 2022.
2. United Nations Development Programme, “Beyond bitcoin Using blockchain to advance the SDGs,”accessed February 17, 2022.

IT組織の再構築：加速する自動化

インフラの自動化	プログラムによるインフラ管理を実現する
システムとソフトウエア管理の自動化	プログラムによるシステム・ツール、ソフトウエア管理を実現する
自動化の最適化	重要業務に機械学習を適用する（障害の予測、防止の実現）

トレンド4

IT部門の再構築：加速する自動化

先進的なIT部門は、「ITバックオフィス」という立ち位置から セルフサービス化と自動化に基づく変革型の組織へと移行している

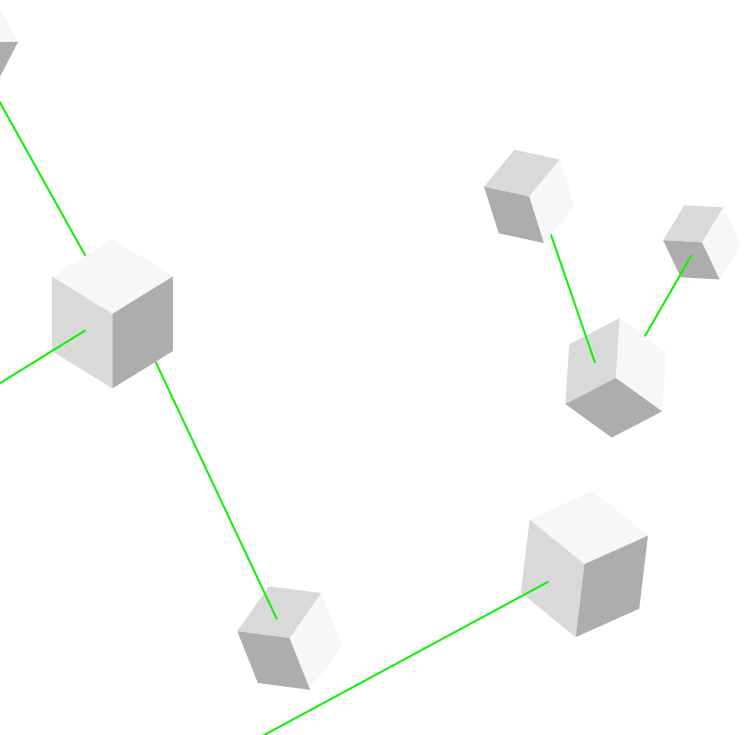
多くの組織において、未だに膨大な量の反復的な業務が人の手を介して行われている。例えば、システム管理、監視、点検、起票されたチケットへの対応などが挙げられる。過去10年間で、クラウドベンダーは反復作業の自動化により、全体の効率をどれだけ向上させることができるかを示してきた。自動化された業務は一貫性が担保でき、監査も可能になるため、ミスの削減と品質の向上につながる。また、ITスキルが高い人材を反復作業から解放し、より付加価値の高いタスクに集中させることもできる。

ITリーダーはさまざまな理由から、このような自動化の取り組みを後回しにしてきたが、そういった状況は変わり始めている。一部の先駆的なCIOは、システム開発の中で手作業が多く発生してしまっている組織や技術者の文化、業務を変革し始めている。

このようなCIOは、クラウドサービスを有効に活用して変革を加速させるだけでなく、クラウドベンダーのベストプラクティスを参考に、インフラ、ソフトウエア、セキュリティーやアプリケーション開発に係るプロセスの標準化や改善にも取り組んでいる。こういった継続的な改善への取り組みが定着している組織においては、AIや機械学習といった先進技術を活用したサービス開発や運用業務の最適化、また業務運用の完全自動化といったことにも取り組んでいる。

こういった継続的な改善活動や業務の自動化に早くから取り組んでいる企業では、すでに業務効率の向上や人件費の抑制といった効果を実現している。ITリーダーを対象とした最近の調査では、回答者の74%が自動化により業務生産性が向上したと回答している。また、業務の自動化を推進したチームの59%が、最大30%のコスト削減効果が得られたと回答している[1]。さらに、品質やセキュリティー面への効果も期待できることから、回答者の95%が業務の自動化を優先事項と回答しており、そのうち21%は最優先事項と位置付けているということが調査から明らかになった[2]。

事業環境の変化のスピードは増すばかりで、それと呼応するようにビジネス部門はIT部門に対し、より多くのことを今まで以上に早く実現することを求めるようになってきている。一方で、経営の期待に応えられる高度なスキルを持った人材は恒常的に不足している状況で、多くの企業において人材獲得が課題になっている。このような変化の激しい環境下で生き残っていくために、どの企業も最小限の経営資源で最大の成果を得たいと考えている。



このような状況を踏まえると、IT部門の変革には今すぐに着手していかなければならない。

変革への道のり

自動化は最近新たに出てきたトレンドではない。実際、過去の「*Tech Trends*」でも、サイバーセキュリティーやネットワーク、ハードウエアとソフトウエアの動的なプロビジョニングといった領域における自動化のトレンドを取り上げている。では、今回のトレンドは何が違うのか。端的にいうと、競争優位性である。COVID-19はこれまでの労働環境を一変させている。その中で注目すべきは、デジタルネイティブな企業は当然の如く、業務を可能な限り自動化していることだ。そのため、スタートアップ企業は既存の競合企業よりもより低いコストで、より高いスケーラビリティー、信頼性、効率性とレジリエンスを実現できている。こういった企業は、手作業を強いるような技術的な負債や組織的な課題とは無縁である。デジタルネイティブな企業にとって、旧態依然とした手作業は日常的なものではなく、むしろ最後の手段なのだ。このような組織文化は歴史や実績を持つ企業とは全く異なる部分である。今日のような競争環境下においては、ITを徹底して活用する姿勢が必要であり、それが結果的に競争優位性につながっていくのである。

自己変革を推進したいと考える組織は、次の3つの領域に注力して取り組んでいただきたい。

オンプレミスインフラの標準化と自動化

自動化の第一歩は、すべてのインフラ基盤と管理機能をプログラムで制御できるようにすることである。インフラ基盤上のリソースをプログラムによって制御することで、一貫したポリシーを適用できるようになるほか、手動で構築していた環境を自動化プログラムと構成ファイルで管理できるようになる。このような自動化は、コンピューティング技術（コンテナ、仮想サーバー、機能）、ネットワーキング技術（ソフトウ

エア定義ネットワーク）、ストレージ技術を組み合わせながら実現していく必要がある。

自動化領域を拡大していくためには、組織全体でプロセスを標準化する必要がある。しかし、多くの組織における運用状況を見ると、個別に設計されたプロセス、アプリケーションや障害時の業務運用が混在したままである。サーバーによって処理方法が異なる場合や環境によって設計や構成が異なる場合、ネットワークによって動作が異なる場合などは、業務運用が高コストかつ非効率となる可能性が高い。

このような状況に心当たりがあるならば、ソリューションやコンポーネントの開発からデプロイ、保守までの標準プロセスを整備することを検討すべきである。クラウドベンダーは、プログラムで制御できるコンピューターリソースを増やすことで、インフラ基盤全体をプログラムで管理できるようになると早くから気づいていた。現在、世の中で利用されているIaC（Infrastructure as Code）プラットフォームは、初期のクラウドでの自動化構想がルーツになっているものが多い。

IaCの検討が進むにつれ、セキュリティー（Security-as-Code）や運用（Operations-as-Code）への応用が進み、設定ファイルやプログラムで制御できる領域が拡がっていった。この「as-code」の取り組みが目指すのは、最適化されたルールに基づきすべての環境が構成されている状態である。もちろん、独自仕様で開発されたシステムもその例外ではない。もし統一されたルールに基づきすべての環境が構成されていれば、現在は数人の管理者で運用されているような大規模な環境であっても、1人のエンジニアで管理できるようになる。そうすれば、インフラ基盤の運用チームは運用管理業務から解放され、クラウドプロバイダーのように自動化やセルフサービス化を推進できるようになる[3]。

自動化による運用管理の効率化を図る際は、環境構築の基本的なプロセスから見直す必要がある。従来は、新しいインフラの構築に際して、いくつもの承認が必要な厳格な調達プロセスが必要であった。しかし、今日の環境構築においては、新たな仮想インスタンスを追加する程度であれば、従来ほど厳格な事前承認は必要ない場合もある。従来の環境では統制上必要であった引き継ぎ業務や承認手続きを整理し、自動化、もしくは業務の見直し、簡素化を行うことで、運用の効率化、開発者の生産性向上と、組織のアジリティ向上を図ることができる。

計画的、かつ戦略的に取り組むことで、自動化は経営に大きなメリットをもたらす。加えて、以下のような利点も得ることができる。

- **精度の向上：**ドキュメント、クエリ、フォームの解釈において属人性が排除される。
- **セキュリティーと耐障害性の向上：**ルールを一貫して適用することができる。Security-as-Codeという新たなトレンドは注目に値する。
- **信頼性の向上：**プログラムで修正された問題は基本的に再発しない。

プロバイダーの「as code」サービスを利用する組織への助言が1つあるとすれば、これらの機能を最大限に活用するために、既存の業務は必ず整理しておくことだろう。さもなければ、新しい環境においても、現在と同様の状態を再現するだけになってしまうかもしれない。

ソフトウエア・管理ツール・アプリケーションの標準化と自動化

先進的なIT部門は、もはやインフラ基盤を管理するのではなく、インフラ基盤を管理するプログラムを開発することで、スケーラビリティーや効率性、環境の一貫性を高める取り組みを推進している。このような考え方は、ソフトウエア、管理ツールやさまざまなアプリケーションにも適用できる。現在、多くのIT部門は、開発や保守・運用、セキュリティーを管理するためにソフトウエアを活用している。複数のソリューションを手動で管理するよりも、1つのプログラムで管理する方が簡単なためである。例えばIaCは、ソフトウエア開発のような俊敏性をインフラ基盤管理で再現している。デプロイメントの観点からも、システムの構成要素ごとに複数のチームと個別に調整を行うような人手での運用よりも、すべてを包括的に管理ができるソフトウエアの方が管理や運用が行い易い。

インフラ基盤の管理と同様に、オンプレミスで稼働している一部のソフトウエアも自動化の有力な候補となる。例えば、データベース管理、統合ツール、セキュリティー管理、システム管理やOSへのパッチ適用は容易に仮想化や抽象化ができる。

クラウドを活用している企業には、クラウドベンダーから自動化機能やプログラミングインターフェース、統合ミドルウエアや各種管理機能などがPaaSの機能として提供されており、それらの機能はクラウドベンダーによって日々拡張も図られている。

では、何から着手していけば良いのだろうか。まず、最初に取り組むべきは「ユーザージャーニー」の作成である。具体的には、ユーザーに機能提供をしようとしている担当者の一連のプロセスと想定される課題を整理していく。その際に、不要な承認手続きや引継ぎ作業を徹底的に削ぎ落とした上で、開発されたプログラムが本番環境にデプロイメントされるまでの作業の自動化、またはセルフサービス化を行っていけば良い。最後に、自動化が進むと既存の業務評価指標ではパフォーマンスが測定できなくなる可能性がある。その場合、目指す組織像と業務の評価指標を再定義することで、「自動化を推進する文化」を奨励していくことが重要である。

機械学習（ML）とルールで自動化を最適化

一般的に、自動化の第一段階はルールの定義であり、例えば「プロセスXが応答しない場合、プロセスを

再開する」などのルールである。クラウドベンダーが10年前に取り組んだように、IT担当者は停止や誤動作の原因となる問題を特定し、それらの問題に対処できるように自動化ツールを最適化していけばよいのだ。そうすれば、いずれはルールベースの自動化を超えて、機械学習ベースの自動化に移行していくことができるであろう。未成熟な状態から始まる自動化への対応も、徐々に洗練させていくことができるのだ。

キャパシティ予測や障害予測など、機械学習はさまざまなIT業務を支えている。しかし、多くの企業においては、障害を早期に発見する、または予測モデルを活用して将来の障害を防止することが機械学習の最優先事項となっている。これらの分野に焦点を当てることで、機械学習の適用／実装を担うチームは稼働時間を大幅に改善し、業務に深刻な影響を与える障害を抑制することができるであろう。最近は、PaaS製品に機械学習機能を組み込んだものも増えてきている。例えば、以前は開発者や運用管理者が手作業で行っていた定型業務を最適化できるような機械学習機能を提供しているPaaS製品も出てきている。その結果、開発と運用がより効率的に行えるようになってきている。

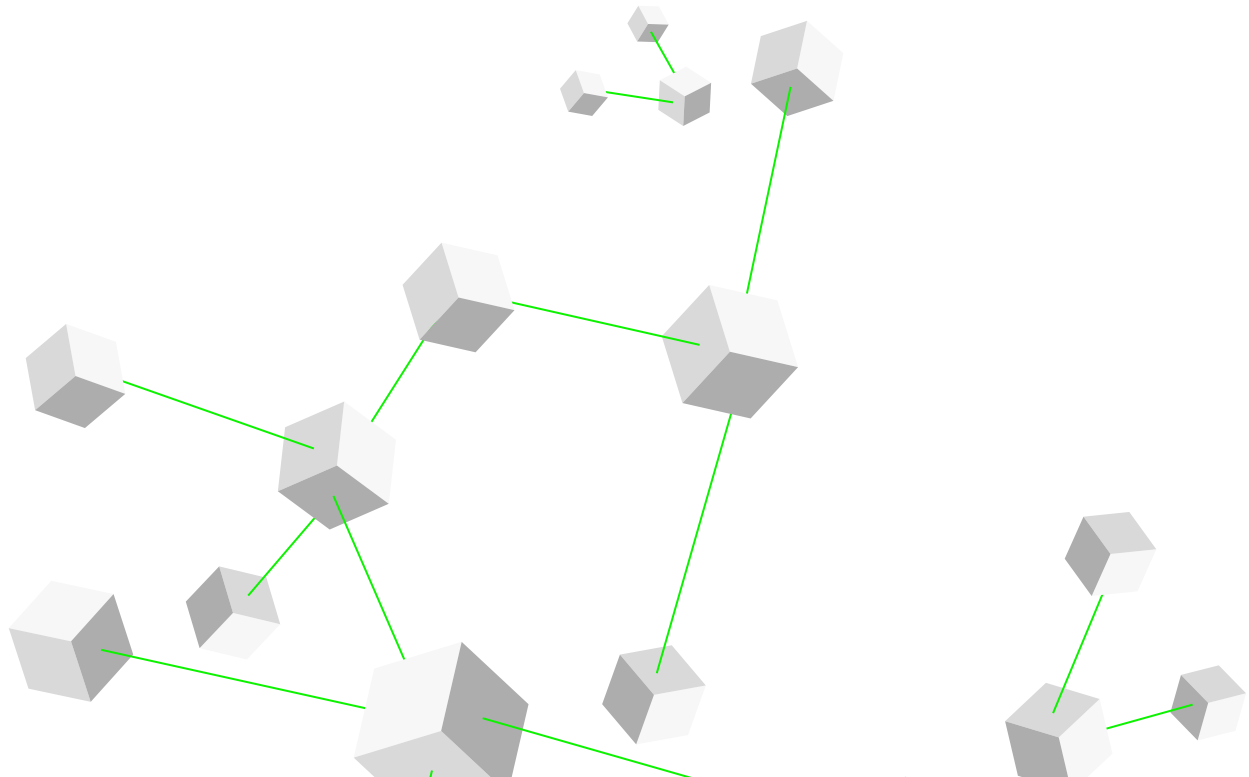
もう1つの最適化手法は、一貫したルールの適用である。たとえば、エンタープライズアーキテクチャーは、何をどのように使うかに関する一連の意思決定であり、その結果得られたルールは、アーキテクチャー設計や機能配置を決定するための最適な判断軸となる。自動化を進めていく際にも一貫性を重視する必要があり、そのためには、これらのルールを企業全体のシステムとプロセスへ体系的に組み込む必要がある。一貫性こそが最適なパフォーマンスを実現するのである。

進むべき道

自動化の機会を模索しているCIOやそのほかのリーダーにとって、時間は最も重要なものである。今日のように急速に技術革新が進む中、サーバーやデータセンターの運用保守に人手を割くことにビジネス上の価値を見出すことは難しい。CIOが自動化によってIT部門の変革を推進していけば、従業員をパッチ適用や監視といった運用保守業務から、より付加価値の高い業務へシフトしていくことができるであろう。自動化の可能性は開発、導入、保守、セキュリティーなどの領域にも及び、より多くのIT業務で効率化と一貫性を高めることができるであろう。

モノを管理することから、モノを管理するプログラムを管理することへの変革は、一朝一夕では実現できない。例えば、技術者や役員からの文化的な抵抗や、レガシーシステム上で手動で設定がなされているような仕組みが自動化を難しくすることもあるであろう。たとえ機敏なITチームでさえも、変わっていくことは容易ではない。対面でのやりとりに慣れている人は、セルフサービスや自動プロビジョニングへの適応に時間を要するかもしれない。これから自動化を推進していこうとしている組織では、標準プロセスの自動化を推進する専門チームの組成が有効である。このチームが、実績を積み上げつつ、段階的に対象範囲を広げていくことで、より多くの業務を変革していくことができるであろう。

幸いなことに、必要な自動化の一部は、クラウドベースのソリューションを活用しての実現が可能である。残りの部分は、自動化の将来像の実現に向けて計画的に、かつ一貫性を持って取り組むことで実現できるであろう。



最前線からの学び

クラウドにおける自動化が開発者の機敏性とイノベーションのスピードを解放

2015年、Capital One（アメリカの金融グループ）は、新しいアプリケーションをすべてクラウド上で構築・実行し、既存のアプリケーションはすべてクラウドに移行すると宣言した。当時は野心的な目標とみられたであろう。何故なら、同社のオンプレミスのインフラの規模は巨大、かつ当時はビジネスを完全にクラウドで運用することは稀であったからだ。しかし、同社は目標を達成し、レガシーのデータセンターを廃止してパブリッククラウドへ全面的に移行できた。これはアメリカの銀行として初の成功事例となった[4]。クラウド移行によるメリットはもちろんあるが、最も重要なのは、自動化の機会が増えたこと、またとそれに伴い迅速に拡張ができるようになったことである。

Capital Oneがより多くのデータとアプリケーションをクラウドに移行していく際に、テクノロジーチームのメンバーは、既存のシステムとプロセスを単純に複製したくないと考えた。彼らは、より現代的なテクノロジーを駆使し、クラウドのあらゆる可能性を発掘したいと考えていた。その中には、マイクロサービスや自動化、リアルタイムデータ、機械学習などの先進技術の採用も含まれている。

「コンピューティングとストレージは、クラウドにとって氷山の一角に過ぎない」と、Capital Oneのテクノロジー部門でクラウドと組織の生産性向上に向けた技術開発を担当するSenior Vice PresidentであるChris Nimsは述べている[5]。「アプリケーションをクラウドに移行するだけでは、すべてのメリットを得ることはできない」

Capital Oneは現在、サーバーレスコンピューティングモデルを活用することで、開発者がコンピューティングリソースの発見や、アプリケーションを提供するコンテナ、必要なライブラリー、そのほかの依存関係を探すことにかける労力を省くことができている。チームはまた、オープンソース化したルールエンジンを構築し、自動化されたガバナンス、セキュリティー、コンプライアンス、効率性によってクラウド環境をより良く管理するためのポリシーも定義できるようにしている。

一見すると複雑そうに見えるが、稼働時間の改善につながったこ

とをチームは実感した。最新のテクノロジーを活かすことで、自動監視ツールが導入できるようになったのだ。機械学習アプリケーションがリアルタイムにサーバーデータとシステムアプリケーションを監視し、それらがスムーズに動作していることを確認しながら、ほとんどのユーザーが気づく前に技術者に異常のアラートを上げている。

「監視対象が細かくなっており、手作業で監視するという従来の方法ではスケールできない」とCapital Oneのfinancial services divisionのCTOであるArjun Dugalはいう[6]。「我々は、高度でクラウドネイティブなモニタリングツールを利用し、機械学習ベースの異常検出を活用することで、アプリケーション監視の方法を再構築した。戦略が功を奏し、潜在的な障害ポイントの数は大幅に増加しているにもかかわらず、インシデントは実際に減少している」

インフラの自動化により、Capital Oneはテクノロジー分野の人材獲得競争においても、より魅力的な企業になった。Nimsによると、コンピューターエンジニアリングのスクールに通うほとんどの生徒の志望動機は、難問を解くことが好きだからだという。卒業後は、上司への手続きの承認依頼や、サーバーのパフォーマンス監視、旧式のデータベースの保守といったことに時間を費やしたいと考えていない。自動化によって、エンジニアたちはよりインパクトのあるプロジェクトに時間を費やすことができ、Capital Oneは雇用の面でも有利になっている。「優れたエンジニアは、先進的なインフラに携わりたいと考えている。また、彼らはテクノロジーの最先端に触れていたいとも思っている。であれば、我が社はエンジニアが最も重要だと考えていることに時間を割かせる」とNimsはいう。

開発者の仕事に対する満足度を向上させることの効用は、人材を引き付けることに留まらない。ビジネス価値の向上にも寄与するのだ。Dugalによると、Capital Oneは11,000人の技術者を雇用しており、そのうちの85%が開発者であるため、アジリティのわずかな向上でさえ、同社にとって大きなメリットになるという。

また、彼は「重要なのは、エンジニアが最も価値の高いタスクに集中できるように、無駄な仕組みを排除すること。そして、開発者の生産性の向上は、顧客の利益とイノベーションのスピードを大きく向上させることにも直結する」と述べている。

UiPathがIT自動化の成功への道を開く

RPA（ロボティック・プロセス・オートメーション）プラットフォームのリーディングプロバイダーであるUiPathは、2005年以来、自動化で実現できることを戦略ビジョンに据え置くことで、顧客企業の自動化を支援してきた。また、同社は、自動化の仕組みを継続的に改善しながら顧客価値を創出する運用モデルを構築している[7]。UiPathのcustomer strategy and solutionsのsenior vice presidentであるJay Snyderは、「自動化はITによって推進・管理されるが、ビジネスによって実現される。IT部門とビジネス部門がお互いを補完し合うことが成功の要因である」と述べている。

UiPathはこれまでに数百もの組織におけるビジネスプロセスの自動化を実現しており、IT業務に対する専門性もますます深化させている。Operations and partnersのsenior vice presidentであるEddie O'Brienによると、ITのシニアリーダーが変革に関与するほど、IT部門内での自動化の取り組みは拡大する傾向がある。「多くの場合において、人々は自動化の取り組みを開始するものの、次にどこを目指すべきかを見失う。IT部門と緊密に連携するほど、適切なデジタルトランスフォーメーションが実現できる」という。

Snyderによると、ITを適切に活用することで、自動化プラットフォームの制御のみならず、チケット作成、ライセンス管理、サイバーセキュリティー対応などのIT業務の自動化も可能になるという。さらに、個々のプロセスの自動化のみならず、DevOpsやデータ管理といった業務重要度の高いITサービスを自動化することで、ゼロタッチIT（人手を介さないIT運用）の実現を目指すこともできるという。Snyderのチームは IT部門と協力して、自動化のユースケースに関するプレイブックを作成しており、タスクボリュームが多く、付加価値の低いタスクから優先的に整備を行っている。また、Snyderのチームメンバーは、システム管理者などのペルソナを作成して、まさにこれまでIT部門の従業員が担当していたようなさまざまな業務プロセス・部門を跨いだ一連のタスクを、RPAプラットフォームで実装可能なように学習をさせている。そうすることで、組織のITスタッフは、より付加価値の高いタスクや、さらなる自動化の設計に専念できるようになる。「多くの人は、自動化によってスタッフを削減することに重点を置いているが、実際のメリットは生産性を向上させることにある」とSnyderは述べている。

結果として、IT部門では自動化拡大の好循環が生まれることになる。デジタルアシスタントのサポートを受ける従業員が増加するほど、チームメンバーはより多くの自動化のアイデアを生み出し、そのアイデアは自動化のプロセスに組み込まれていくことになる。さらに、プラットフォーム内のAI/MLにより組織の自動化状況を分析し、改善や拡張のリコメンドをすることも可能である。O'Brienによると、継続的なITの自動化を達成するための鍵は、適切な戦略の導入から始めることである。目標は、デジタルとビジネスの変革を推進するend-to-endの自動化を実現することである。O'Brienは「完全に自動化された企業というビジョンを掲げることで、今日におけるITの管理手法とその効率性に大きなインパクトを与えることができる」と述べている。

Anthemは自動化を梃子に保険業界をリード

全米で約4,000万人に健康保険サービスを提供しているAnthemにとって、被保険者の健康維持への取り組みは最優先事項である。Anthemは近年、主要なインフラの大部分を自動化することで被保険者中心のサービスを実現し、IT部門の役割を見直すと共に、エンジニアがビジネス上の優先順位が高いプロジェクトに集中できる環境を実現した。

同社のCloud Center of Excellenceのstaff vice presidentを務めるSrinivas Yamujalaは、「保険業界のIT部門の役割は管理から構築へとシフトした」と語る[8]。また、「Anthemが競争力を維持するには、デジタル化を進め、俊敏性を高める必要があった。変革の取り組みを促進するため、end-to-endの自動化に注力している。インフラサービスと共有プラットフォームの提供の簡素化と迅速化を図ることで、アプリケーションやプロダクトの構築とリリースをより速くできるようにしている」と語る。

この取り組みにおける注力領域の1つとして、クラウド化がある。「以前までは、手作業による繁雑な調達・構築プロセスに基づいてインフラを準備していた」とYamujalaはいう。新規顧客のためにサーバー増強が必要となった場合、従来はハードウエア調達や構築作業に3〜6ヶ月かかっていた。しかし、今ではビジネスプロセスの大部分がクラウド化されており、数ヶ月かかっていたインフラの準備をわずか2時間で完了できるようになった。ヘルスケア分野の規制とセキュリティーポリシーに準拠した、オーケストレーションとプロビジョニングの自動化プラットフォーム（特許出願中）を開発したことにより、アプリケーション開発チームは必要なリソースを数分で準備できるようになった。

Anthemはイノベーションと変革への取り組みを推進するために、クラウドベンダーのサービスを、同社の厳格なセキュリティー基準に基づいて堅牢化し、利用可能としている。こういった事前設定済みのサービスをサービスカタログに纏めることで、アプリケーション開発者は法規制やセキュリティーコンプライアンス基準を満たしたクラウドサービスを利用できる。これまでは、開発チームが特定のサービスを利用する際は独自に準拠対応をする必要があり、結果として異なるアプローチや冗長な実装が発生していた。

また、以前はアプリケーション開発の際、特定のファイアウォールの通信ポートを許可し、システムやアプリケーション間の通信を確保するため、セキュリティーチームに対してチケットを起票する必要があった。AnthemはマイクロサービスとAPIの仕組みにより、それをすべて自動化プラットフォームに組み込むことで、開発者にとって面倒なファイアウォールの変更依頼の必要性を最少化した。さらに、ゼロトラストを導入することで、ファイアウォール設定を完全になくすことに取り組んでいる。これにより、開発者の生産性は大幅に向上し、今後もさらなる向上を目指している。

「我々は開発者コミュニティーに力を与えたい」とYamujalaはいう。「我々が取り組む自動化の大部分は、アプリケーションの開発とデプロイメントの簡素化に関するものだ。昨今の自動化の多くはIaC（Infrastructure as Code）に関するものだが、我々はそれを超えて、開発者がビジネスニーズへの対応を迅速化するための方法を考えている」

すべてを自動化することのもう1つのメリットは、システム稼働の安定性向上である。エンジニアは、オンプレミスのインフラを維持するために、サーバーやその上で稼働するアプリケーションを監視する必要がある。アプリケーションとハードウエアの間には相

互に依存関係があるため、エンジニアは障害防止への取り組みに苦労してきた、とYamujalaは語る。現在はそれらをクラウドサービスに任せることができ、システムのパフォーマンスも向上している。

アプリケーションの開発・デプロイメントの自動化と併せた、インフラとプラットフォームの自動化の推進は、IT以外にも大きなメリットをもたらしている。Yamujalaによると、「ビジネス全体が、変化するビジネスニーズと顧客の期待に対し、より迅速に対応できるようになっている」

「業界や顧客ニーズなど、さまざまな環境変化の中でビジネスを継続する我々の対応力は、俊敏性、アジリティとスピードの面で強化されている」と、Yamujalaはいう。

私たちの見解

Bill McDermott
President and CEO of ServiceNow

C.J. Desai
Chief operating officer
at ServiceNow

ServiceNowでは、我々が持つ
プラットフォームを企業全体の
デジタル変革の司令塔だと考えている。

デジタル化が進んだ現在では、ITはビジネスの仕組みそのものであり、テクノロジーインフラ全体にわたる一貫した自動化のアプローチが過去に類を見ないほど重要になっている。

そう考える理由は、ServiceNowでは我々自身が「ファーストユーザー」であるためだ。我々が世に出すものはすべて、まず社内で利用する。それにより自動化がもたらす効果の把握と、デジタル化されたプロセスを連携させることのメリットの理解が容易になる。また企業全体のデジタル変革の実現を支えるIT部門において、自動化をどのように活用すべきかを理解する上でも有用だ。

プラットフォームの開発当初は規定に沿ったワークフローをサポートするのみで、その数もごくわずかであった。それが現在では機械学習を利用した自動化をサポートするまでに成長しており、今後は整備されたインターフェースを持た

ないシステムにもRPA機能を提供できるようにする予定だ。

しかし、顧客接点となる個別のフロントエンドプロセスを自動化することが、デジタル変革の取り組みにおける最終目標ではない。真の目標は、複雑化したミドルエンドやバックエンドのシステムを整理し、自動化した個々のフロントエンドプロセスと統合することだ。企業はこれまでフロントエンドのシステムと顧客体験の改善に、何十億ドルと投資してきた。その一方で、多くの企業は手作業のプロセスが多いバックエンドのシステムや、それらを支える技術への投資を抑制してきた。そのことが業務全体の効率を下げ、結果としてフロントエンドでの優れた顧客体験の妨げとなっている。

しかし、顧客はそのような状況には満足せず、必要なときに必要なものをすぐに提供してほしいと考えている。そしてプロセスに透明性があることを期待している。素晴らしい注文システムがあっても、顧客が注文の状態を追跡できない場合は全体的な顧客満足度が低下する。

このような背景により、ServiceNowは旧来のSoR（System of Record）から、より現代的な「System of Action」というアプローチへのシフトを支持している。顧客接点の部分だけでなく、販売プロセス全体を通じて顧客とつながる必要がある。手作業による取り組みでは拡大は難しいが、自動化を使うことで拡大が可能となる。

自動化は顧客の期待に応えるだけではなく、従業員満足度の向上においても重要だ。毎日同じ機械的な作業を好む従業員はほとんどいない。開発者やエンジニアは特にその傾向が強く、単調なシステム監視といった作業よりも、付加価値の高い複雑な問題の解決に時間を割きたいと考えている。同時に、あらゆる業界の企業が必要な人材の確保に苦心しており、過熱する人材争奪戦に多くが悲鳴を上げている。付加価値が低いタスクを自動化することで、従業員はより付加価値が高い問題に取り組むことができるようになる。これは従業員満足度を向上させ、定着率を高めるための最良の方法の1つだ。

すべては価値実現のスピードを高めることに尽きる。達成すべき目的が顧客とのつながりの強化であれ、従業員の高付加価値業務へのシフトであれ、自動化に対する一貫したアプローチは、より迅速にビジネス価値を実現することに役立つ。業務の自動化を達成することで、価値実現までの期間は数ヶ月から数年ではなく、数週間から数ヶ月に短縮できる。

今後の展望

ストラテジー

ITの自動化により、効率性、耐障害性、スケーラビリティーを向上させることができる。CEOは、ITリーダーと綿密に連携し、業務上および戦略上の目標を達成するための計画を理解すべきである。そうすることにより、IT担当者はより付加価値の高い仕事に専念できるようになるため、CEOはCIOと協業しながら、IT人材要件の再定義と再教育を行うことができる。ITの変化に不安を抱くのではなく、個人の成長と学びに対して喜びを感じながら、組織におけるテクノロジーの役割に新たな可能性を与えていかなければならない。

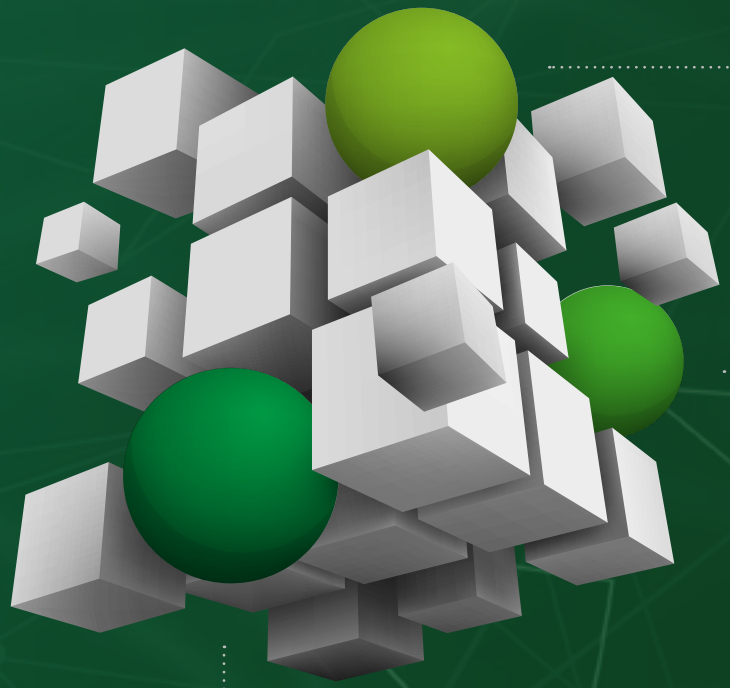
ファイナンス

IT人材の需要は従来から引き続き高いことを踏まえると、CFOは自動化の推進が加速していることを歓迎すべきだ。また、定型的なIT業務を自動化するには、人材と資金の両方の先行投資が必要であることを理解しなければならない。IT担当者が定型業務から解放され、より高度な自動化が可能になれば、レジリエンスの向上やコストの削減も実現することができるのである。スキルアップや組織の改革は必要だが、自動化の推進によって、多様なIT人材を獲得するための選択肢が増えることになる。

リスク

企業が自動化を進めていくにつれ、新たな攻撃経路が開かれてしまう可能性がある。従来の環境では、システム停止やインシデントの復旧後に運用管理者が手動でシステムをオンラインに戻す形になっていたが、自動化に伴う適切な計画が策定されていなければ、課題が生じてしまうであろう。CRO（最高リスク管理責任者）は、ITプロセスのデジタル化と自動化を推進する際に、レジリエンスを重視する必要がある。組織が自動化を推進していく際には、最初にリスク管理の原則を組み込んでおくことが望ましい。そうすれば、リスク管理の原則に基づき、AIを活用して差し迫った脅威に対しても、先を見越した対応が行えるようになる。

さあ、はじめよう



要点

1. 現在、マニュアル操作が必要なインフラ基盤と管理機能はどれか。このうち、標準化と自動化が可能なものはどれか。
2. 各従業員が行っている最も付加価値の低い業務は何か。それは自動化すること、または無くすことはできないか。
3. 最適化の対象となる自動化機能はどれか。ルールベースの意思決定から機械学習での最適化にどのように移行するか。

執筆者

Kacy Clarke
Cloud architecture go-to-market lead
Deloitte Consulting LLP
kaclarke@deloitte.com

Ken Corless
Cloud engineering managing director
Deloitte Consulting LLP
kcorless@deloitte.com

Glen Rodrigues
Foundry services market leader
Deloitte Consulting LLP
grodrigues@deloitte.com

Lars Cromley
Cloud engineering technology fellow
Deloitte Consulting LLP
lcromley@deloitte.com

SENIOR CONTRIBUTORS

Julien Kopp
Partner,
Deloitte France

Andreas Zachariou
Director,
Deloitte MCS Limited

Alice Doyne
Senior manager,
Deloitte MCS Limited

Kelly McLaurin
Senior manager,
Deloitte Consulting LLP

Naoki Morinaga
Senior manager, Deloitte
Tohmatsu Consulting LLC

João Sanches
Senior manager, Deloitte &
Associados SROC, S.A.

Takashi Torii
Senior manager, Deloitte
Tohmatsu Consulting LLC

Bertrand Polus
Manager, Deloitte Tohmatsu
Consulting LLC

参考文献

1. Salesforce, *IT leaders fueling productivity with process automation*, accessed November 9, 2021.
2. Ibid.
3. David Linthicum et al., *The future of cloud-enabled work infrastructure: Making virtual business infrastructure work*, Deloitte Insights, September 23, 2020.
4. "How Capital One Moved Its Data Analytics to the Cloud," *Harvard Business Review*, February 23, 2021.
5. Chris Nims (senior vice president for cloud and productivity engineering in the technology division, Capital One), interview, October 25, 2021.
6. Arjun Dugal (CTO of the financial services division, Capital One), interview, October 25, 2021.
7. Jay Snyder (SVP customer strategy and solutions, UiPath) and Eddie O'Brien (SVP operations and partners, UiPath), interview, October 27, 2021.
8. Interview with Srinivas Yamujala, staff vice president of cloud center of excellence, Anthem, Inc., November 5, 2021.

日本のコンサルタントの見解

運用自動化というテーマはよく聞く話題であるが、本編で議論されている内容は単純な運用負荷軽減のための補助的なツール導入といったものではない。IT, disrupt thyselfという原題は「IT部門は変革を迫られている」といったニュアンスであり、これが意味するところは、以下のようなホラーストーリーである。

クラウド事業者によって開発されてきた自動化ツールや技術の普及により、運用はオペレーターがキーボードをたたく作業から、コードを記述してソフトウエアで実行するスタイルに変わった。この技術が広がり、エンタープライズでも活用され始めてきたことで、従来のオペレーターとしての運用作業は無くなり、運用者は別の職種へ転換していく。しかしその一方で、テクノロジーがレガシーであることで変革ができず、従来のやり方のままの運用を続けざるを得ない組織もある。するとそのような会社や組織は若いエンジニアにとって魅力がないため、若い人が入ってこなくなり、やがてシステムの維持ができない状態になっていく。これが、自動化による影響の負の側面である。そうならないためには、CIO自らが変革を率先して進めていく必要がある。もし現場の抵抗があるようであれば、別組織を作るという手段も検討するべきだ、といった内容である。

日本における認識のギャップ

しかしこのストーリーは、日本の読者にとっても腹落ちしやすいものだろうか。率直にいって、ピンとこないという感想をお持ちの方も多いのではないだろうか。その原因として、日本固有の事情も考慮すると以下の2点が考えられる。

まず1点目は、日本における多くのユーザー企業では、IT運用をベンダーに委託している部分が大きい傾向があることである。委託先のベンダーは人が作業することを前提に見積りを行っており、またそれがビジネスとして成立しているため、敢えてコストをかけて自動化をするインセンティブが働きにくい。ユーザーにとってもベンダーにとっても、現状維持が最も都合がよい選択となってしまいやすい。

2点目はIT人財のコストである。欧米におけるIT人財とは大学でコンピューターサイエンスを履修したようなスペシャリストであり、専門職としての報酬も高い。一方、日本におけるIT人財のハードルは相対的に低く報酬も低いため、コストをかけて自動化をするメリットが小さい。結果として、人手でやってしまった方が短期的なコスト効率が高くなってしまう場合も珍しくない。

しかしこのような現状も、足元をよく見ると変化は確実に起き始めている。IT業界における人財の流動化は急速に進んでおり、スキルやナレッジを積んだ人財が転職していってしまうことは珍しくなくなっている。また、能力の高いエンジニアに対して高給を準備するという傾向も外資系企業を中心に広がりつつある。従来型の手作業や非効率な運用を変えようと

しないベンダーからは、徐々に優秀な人財の流出がおき、いずれ品質の低下につながってくるだろう。ユーザー企業からすると、ずっとお願いしている保守ベンダーからある日突然、「今までと同じサービスは今後提供できない」といわれることになるかもしれない。今は想像し難いかもしれないが、そういう事態につながる変化が水面下で着実に進んでいることは認識しておくべきである。

自動化からAI活用、働き方の改革へ

日本でもこの変化にいち早く気づき、自動化を取り入れて変革へと進みだしている企業はある。ここでは、いずれも日本を代表する企業である2社の例を紹介したい。

1つ目は、ネットワーク運用の自動化を導入し、5年をかけて“匠の技”を見える化し、システムに落とし込んだ事例である。ネットワーク運用は複雑性が高く、これまでは熟練した要員でなければ運用はできなかったが、自動化により人員を半減させることができている。注目すべきは自動化に伴ってリモート監視がしやすくなり、在宅勤務など多様な働き方が可能になったという点である。自動化の取り組みから働き方改革につながり、さらに優秀な技術者の確保にも効果が出てくることが期待される。また、さらにAIを活用した障害の予測や検知の実証を進めており、これにより障害復旧の時間を従来の4～18時間から1時間未満に短縮することを目論んでいる。障害復旧は運用現場にとって最もストレスがかかり、心的な負担も大きい。AI活用により負担が軽減されれば、現場の人間にとっても嬉しいことといえる。AIは人間の仕事を奪うのではなく、助けになるという好例ともいえるだろう。

2つ目は、自社サービスを支える5,000台を超えるサーバーからなるサービス基盤において自動化の導入を進めている事例である。そのインフラの設計から構築、テスト、リリースまでの全体の流れに対し自動化を導入してきており、実際に効果も現れてきている。今後に向けて、多様な業務バリエーションの標準化を目的とした、業務プロセスの変革に取り組んでいる。

どちらの事例においても、従来は人がやっていたことをソフトウエアにやらせることで自動化を行っている。だがこれは、ソフトウエアも人と全く同じように動くことができる、という意味ではない。人は状況に応じて柔軟に判断し、曖昧な表現や事象であっても考えて動くことができる。多くの企業において、手順書が必ずしも正確かつ網羅的に記載できていない場合でも運用が大過なく回っているのは、手順書に書かれていない隙間を人が埋めてくれているからだ。しかしソフトウエアは違う。気を利かせてくれることや、行間を読んでくれることはしない。あくまでコードで書かれたロジックに従って動くだけだ。では、人とは同じように動かないソフトウエアでどうやって自動化をするか。その鍵となるのが「プロセスの標準化」である。

鍵は標準化にある

プロセスの標準化とは、端的にいえばバリエーションを減らすということである。

日本のITシステムの特性として良く挙げられる点は、カスタマイズが多いということだ。人間がコミュニケーションやあうんの呼吸で行っていた現場の業務プロセスをIT化しようとすると、カスタマイズや例外的な処理が避けられない。日本では、この属人的なプロセスをある種忠実にシステム化してしまい、標準化に取り組んでこなかったケースが多い。標準化されていないプロセスを自動化しようとすると、多様なパターンに対応する必要があり、自動化スクリプトやプログラムの開発に多くのコストがかかる。最悪の場合、コストをかけても自動化が完成しないこともありえる。

ITの自動化が目指すものは、単に作業を自動で行うことではない。大事なのは、プロセスを標準化し、バリエーションを減らすことである。IT部門の担当者の大半の時間は、調整作業に費やされている。そこを減らすためにはプロセスを変革していくことが必要となる。そうすれば実効性のある自動化となり、業務プロセスの変革につながっていく。マネジメント層はこのことを強く意識し、自動化と同時にいかに標準化を進めるか、バリエーションを減らしていくかを課題として認識し、現場の意識も含めて変えていくようにドライブしていくことが重要である。

目に見えれば標準化が進む

プロセスの標準化を進め、バリエーションを減らそうとした場合、どこから手を付けるべきだろうか。ともすると、日本企業はそういった取り組みは苦手だと思われる方もいるかもしれないが、少し思い出してほしい。日本の企業は元来、自動化や標準化による改善は得意領域だ。カンバン方式に代表されるように、プロセスの改善を続ける事例は多くある。しかしITの分野になると、どうも同じようにいかない。なぜだろうか。

原因として考えられるのは、ITは目に見えにくいため、プロセスについても見えにくいということである。目に見えないものをモデル化し構造化し定義するという点については、確かに欧米が得意とする領域であり、日本がやや不得手とする部分かもしれない。しかし逆に言えば、可視化さえできれば改善は得意であるともいえる。例えば、VSM（Value Stream Mapping）という手法でプロセスを可視化し、そこから標準化のきっかけをつかんでいる例もある。このような取り組みを通じてプロセスを見える化し、標準化と自動化を両輪で回していくことが重要である。

崖から落ちないために

経産省が発表したレポート、「2025年の崖」についてはご存じの方も多いだろう[1]。2025年に向けて、IT人財の引退やSAP ERPのサポート終了などにより、日本企業はDX（デジタルトランスフォーメーション）が実現できないだけではなく、最大12兆円／年の経済損失が生じるといった内容である。

では、この「2025年の崖」レポートがいつ発行されたかは覚えておられるだろうか。実は2018年のことであり、もうすでに4年も経つのだ。発表当時は2025年までだいぶ余裕があると思われたかもしれないが、もうあと3年しかない。大規模なITシステ

ムプロジェクトであれば構想からサービスインまで2年や3年かかることは珍しくないことからすると、2025年はすでに目前といっても過言ではない。IT部門の変革はすでに待ったなしである。先送りはもうできない。あと3年でできることは限られると思われるかもしれないが、動き出せばその先には従来にはないスピードで大規模までスケールしていく世界は見えている。

まだ遅くはない。動き出すための一歩を踏み出す時が来ている。

執筆者

森永 直樹　ディレクター
Systems & Cloud Engineering

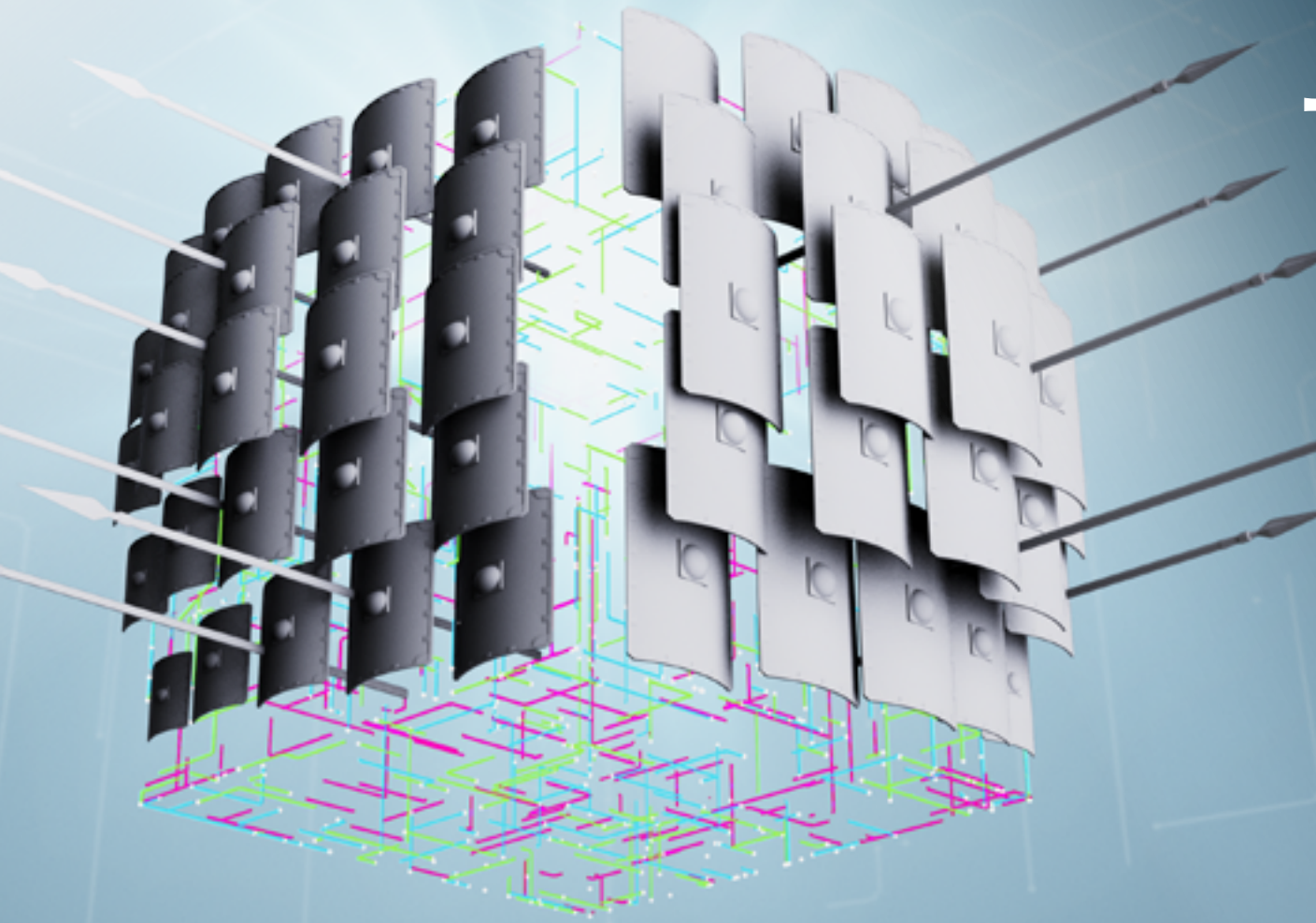
IT系コンサルティング会社を経て現職。IT戦略立案、全社システム改革など多数の大規模プロジェクトに従事。システムアーキテクトとしての豊富な経験に基き、実行性の高いIT戦略立案やシステム構想策定、クラウドマイグレーション戦略策定に強みを持つ。

鳥居 隆史　シニアスペシャリストリード
Systems & Cloud Engineering

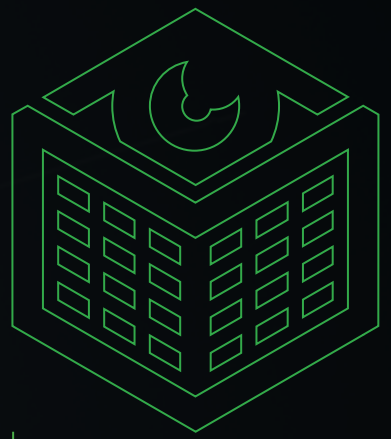
ITベンダーコンサル部門を経て現職。ハードウェアからシステム、クラウドまで幅広い技術領域に加え、コンテナや自動化といった先行技術の知識と経験も豊富。確かな技術力をベースに、システム全体構想から構築運用の実行までカバーする。

参考文献

1. 経済産業省, “DXレポート ～ITシステム「2025年の崖」克服とDXの本格的な展開～,” September 2018.



サイバー AI：真の防御



拡大する攻撃対象の保護

企業の脆弱性は多くのシステムやデータがオンラインにさらされることで増加している

サイバー人材不足の解消

AIが慢性的なサイバー人材不足を解決する助けとなる

AIによる攻撃にAIで対抗

AI主導のセキュリティツールはAI主導の脅威に対する最良の防御策になる

トレンド5

サイバーAI：真の防御

データとマシンインテリジェンスによってセキュリティーチームを強化する

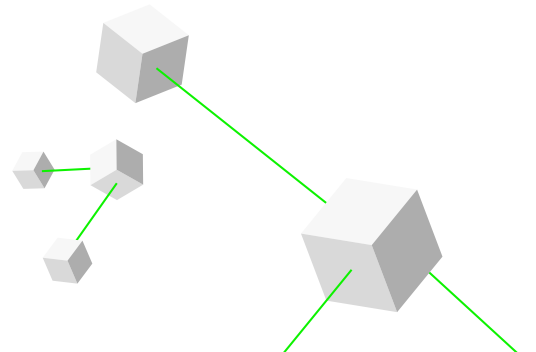
セキュリティー技術に多額の投資をしているにもかかわらず、企業はセキュリティー侵害に悩まされ続けている。攻撃者はすぐに戦術を進化させ、技術の進化を先取りしている。近い将来、人間はサイバー攻撃の膨大な量とその巧妙さ、検出の困難さに圧倒されるであろう。

SOC（セキュリティー・オペレーション・センター）に流入してくる多くのセキュリティーデータの効率的な分析はすでに課題となっている。これらのデータには、新たな攻撃経路を探す糸口や新たなマルウェアの使用機会を探す高度な攻撃者の標的になることが多い、ネットワークデバイス情報やアプリケーションデータ、そのほか幅広いシステムからの情報は含まれない。また、ビジネスがファイアウォールの垣根を超えて拡大するにつれ、セキュリティーアナリストは絶えず拡大する攻撃対象領域を保護する責任を負うことになる。

一方、サイバー犯罪のコストは上昇し続けており、2015年の3兆米ドルから2021年末までには6兆米ドルに倍増し、2025年までには10兆5,000億米ドルに増加すると予測されている[1]。2021年の1件あたりのデータ侵害の平均コストは424万米ドルと、2019年から10%増加している[2, 3]。保険会社AIGによると、ランサムウエアによる請求だけでも2018年以降150%増加している[4]。

すでにAIの助けを借りる時が来ている。サイバーAIは攻撃者の動きを上回るスピードで対応できるだけではなく、彼らの動きを予測し事前に行動できるため、戦力を倍増させる可能性を秘めている。サイバーAI技術やツールは導入の初期段階にあり、世界市場は2021年から2025年の間に190億米ドルの成長が見込まれている[5]。

AIの適応学習およびパターン検知の能力は、検知や抑制、応答を加速させる。これによりSOCアナリストは負担が軽減され、能動的な行動をとれるようになる。結果として、AIによるサイバー犯罪の発生にも備えることができる。



企業における攻撃対象領域の拡大

企業における攻撃対象となる領域は急激に拡大している。「*技術スタックは物理化する*」で述べているように、5Gの採用とネットワーク接続の増加は、従業員の分散化とエコシステムの拡大とともに新たなリスクをもたらす可能性がある。企業活動はファイアウォールの外にさらされ、顧客のデバイスや従業員の自宅、パートナーのネットワークにまで拡大している。

リモートワーカーの増加。COVID-19以前は、従業員の約6%しか在宅勤務をしていなかったが、2020年5月には約35%になっている[6]。2020年のロックダウン直後の6週間で、在宅勤務者への攻撃割合は12%から60%へと5倍に増加した[7]。ある調査によると、51%の回答者が、リモートワークに移行した後にフィッシングメールが増加したと回答している[8]。

多くの従業員にとって、リモートワークは例外的ではなく今後も続くことが予想され、サイバー犯罪者に多くの機会を提供することになる。例えば、企業のファイアウォールやWebセキュリティーゲートウェイの外では、リモートワーカーはターゲットにされやすい。彼らはホームネットワークとVPN接続に依存しており、クラウドベースのアプリケーションやデータにアクセスするために、安全ではないデバイスを使用することが多い。また、従来のオンプレミス型のセキュリティーデバイスは一般的に、家庭でのインターネットアクセスではなくエンタープライズクラスのネットワークをサポートするように設計されている。

企業活動が従業員の自宅にまで拡大するにつれて、ユーザーの行動やデータ活動は多様化し、これまでの常識から逸脱するようになる。従業員が通常とは異なる場所や通常とは異なる時間にログインすることで、異常な動作を特定することがより困難になり、誤検知の増加につながる可能性がある。

ネットワーク接続デバイスの増加。5G、IoT、Wi-Fi 6などのネットワーク技術の進歩により、ネットワークに接続されたデバイスが増加している。ある推計によると、2023年までに293億台に達するという[9]。これら増加しているデバイスはサイバー犯罪者が攻撃経路を探す際の候補になりうる。

これらネットワークに接続された膨大な数のデバイスは、処理を必要とするデータを生成しかつセキュリティーによる保護も必要とするため、SOC内の処理を詰まらせる一因となっている。特にサービスオーケストレーターによって管理されている場合、アクティブな資産、その目的、期待される動作を把握し管理することは困難である。

これらデバイスの多くは、一元的に配置、管理されるのではなく、さまざまな遠隔地に分散され、複数のエッジ環境でデータを収集して企業に送信する。適切なセキュリティー対策を講じなければ、これらデバイスは危険にさらされ、ネットワーク上で正常に動作しているように見せかけながら、実際は侵入者

によって制御されたボットとなり、悪意あるコードを放つことや、スウォーム攻撃を行う可能性がある。

特にサービスオーケストレーターによって管理されている場合、アクティブな資産、その目的、期待される動作を把握し管理することは困難である。

第三者・パートナーの広範なエコシステム。拡大するグローバルサプライチェーンや保有データ、インフラ、サービスは、以前から第三者リスクを高める一因となっている。また、外部のアプリケーションやデータを組み込む企業が増えるにつれて、APIに対するセキュリティー上の懸念が高まっている。Gartnerの予測では、2022年においてAPIの悪用が企業の最も狙われる攻撃経路になるという[10]。

第三者による情報漏えいはますます複雑化している。5年前であれば、特定のシステムを標的に、広く出回っているマルウエアを用いて、契約者の認証情報を取得し顧客データを盗む事例などがよく見られた。確かに厄介ではあったが、出所が明確で被害を監視し、復旧することができた。

このような攻撃は、1つの企業から盗まれた情報を使用して数千もの顧客やサプライヤーを危険にさらすことができるような高度な侵入に比べると軽微に感じられる。サプライチェーン攻撃は、複雑なサプライネットワークの最も安全性の低い組み込みコンポーネントを悪用することで、同じことができてしまう。境界のない侵害は、監視や復旧がほぼ不可能であり、漏えいは何年も続く可能性がある。

5Gネットワークの採用。5Gは新しい接続や機能、サービスにより企業ネットワークを完全に変革すると期待されている。しかし、分散ハードウエア、ソフトウエア定義型ネットワーク、オープンアーキテクチャー、仮想化インフラが混在するため、5Gへの移行は攻撃対象の拡大と新たな脆弱性を生み出す。そのため、より動的なサイバーセキュリティーによる保護が必要となる。

4Gネットワークでは1平方キロメートルあたり10万台しか接続できないが、5Gネットワークでは、最大100万台のデバイスを接続できるため、スケーラビリティーに優れ、高密度に接続されたデバイス環境を実現できる[11]。市場関係者は、2025年までに5Gモバイル接続件数（IoTを除く）は18億件と、2021年の5億件から大きく増加すると予測している[12]。また、セルラーIoT接続数は2020年の約170万件から、約37億件に増加すると予測している[13]。

公共の5Gネットワーク拡大に合わせて、政府、自動車、製造、鉱業、エネルギーやそのほかのセクターも含め、低遅延でデータプライバシーを遵守し安全なワイヤレス接続といった企業要件を満たすプライベート5Gネットワークの投資を始めている。自動運転車やドローンからスマートファクトリーデバイス、携帯電話に至るまで、公共および民間の5Gネットワークのエコシステム全体（接続されたデバイスやアプリケーション、サービス）が、ハッカーにとって新たな侵入ポイントとなる可能性がある。各資産は、特定のセキュリティー要件を満たすように構成する必要があり、デバイスの種類が増加するにつれて、ネットワークはより多様になり監視と保護が困難になる。

今日のサイバー脅威に対するAI防御

攻撃範囲が拡大し、サイバー脅威の深刻さと複雑さが増加している中、サイバーセキュリティー人材が慢性的に不足している。世界的に300万人以上のサイバーセキュリティー専門家が不足していると推定されており、解消するためには、この分野の雇用を約89%増加させる必要がある[14]。AIがこのギャップを埋めることを助けてくれる。

脅威検知の高速化。脅威検知は、サイバーAIにおける最も初期の応用例の1つである。AIによって既存の攻撃対象領域の管理技術を強化しノイズを減らすことで、限られたセキュリティー専門家が最も強力な攻撃のシグナルや危険な兆候の検知に注力することができる。また、迅速な意思決定と行動、より戦略的な活動に集中することもできるようになる。

高度な分析と機械学習プラットフォームは、セキュリティーツールの大量データを素早く判別し、標準からの逸脱を特定、ネットワーク上の何千もの新しい接続先からのデータを評価できる。また、正当なファイルと悪意あるファイル、正規な接続、正規なデバイス、正規なユーザーを区別できるように訓練できる。

AIを活用したネットワークとIT資産のマッピング・可視化プラットフォームは、拡大する攻撃対象をリアルタイムで把握することができる。また、コンテナ化されたシステムを含めたアクティブな資産を識別・分類し、不正な資産の状態も可視化することができる。AIと機械学習を組み込んだサプライチェーンリスク管理ソフトウエアは、物理的およびデジタルなサプライチェーン環境を監視し、資産がどのように構成され接続されているのか追跡するプロセスを自動化できる。

抑制と対応の強化。AIは、セキュリティーチームの手間がかかる作業を自動化し、抑制と対応の効率化を大きく加速することにも役立つ。機械学習、ディープラーニング、自然言語処理、強化学習、知識表現といったさまざまなAIのアプローチの活用が考えられる。これらを自動化された評価や意思決定と組み合わせることで、アナリストは複雑化し、増加するセキュリティー上の脅威を管理し、取り組みの大規模化を図ることができる。

例えば、5Gはこれまでと同様に、攻撃者が意図的にシグナル転送を妨害するジャミング攻撃に脆い。5Gネットワークセキュリティーの設計と実装を共同研究しているバージニア工科大学のCommonwealth Cyber Initiativesとデロイト グローバル（デロイト）の研究者らは、ネットワークをダウンさせる前に低レベルの信号妨害を特定することに取り組んでいる。AIベースの干渉方式と機械学習モデルを実装することにより、低レベルの信号干渉の有無を検出し、妨害パターンを分類できるリアルタイムの脆弱性評価システムを開発した[15]。

自動化は、AIの影響を最大化し、検出から修復までの時間を短縮することに役に立つ。AIと機械学習が組み込まれたSOC自動化プラットフォームは、特定のデータへのアクセスをブロックするなど自律的な予防措置を取ることができ、さらなる評価のためSOCに問題をエスカレーションさせることができる。APIアクセスを制御するAPI管理ソリューションに重ねることで、ユーザーのアクセスパターンについて訓練された機械学習モデルは、すべてのAPIトラフィックを検査し、異常の発見・報告・対処をリアルタイムでできるようになる。

積極的なセキュリティー体制。適切に訓練されたAIは、より積極的なセキュリティー体制を実現し、サイバーレジリエンスを促進する。これにより、攻撃を受けている場合でも業務を継続し、攻撃者がシステムに侵入している時間を短縮できる。

例えば、コンテキストに富んだユーザー行動分析を教師なしの機械学習アルゴリズムと組み合わせることで、ユーザーの行動を自動的に調べることができる。ネットワーク活動やデータアクセスの典型的なパターンの認識、異常の特定・評価・フラグ設定（誤検知の無視）や、対応・介入要否の判断が可能になる。また、人間であるセキュリティー専門家に情報を提供し、攻撃者の追跡に積極的に関与できるようにすることで、AIは自発的な脅威ハンティングを可能にする。

組織はAIと機械学習を活用して、セキュリティーポリシーの設定、コンプライアンスの監視、脅威と脆弱性の検出と対応などの分野を自動化できる。例えば、機械学習を活用した特権アクセス管理プラットフォームは、ゼロトラストセキュリティーモデルの実現に必要なセキュリティーポリシーを自動的に策定・維持することができる。これらのモデルは、ネットワークトラフィックパターンを分析することで、正規な接続と悪意ある接続を区別し、アプリケーションとワークロードを保護するためにネットワークをセグメント化する方法を助言してくれる。

脆弱性解析と強化学習を組み合わせることで、セキュリティー専門家は複雑なネットワーク構造をモデル化した攻撃グラフを生成し、最適な攻撃経路を明らかにすることができる。ネットワークの脆弱性をより深く理解し、テストを実施するために必要なスタッフの数を減らすことができる。同様に、サイバー攻撃のシミュレーションツールは、高度な脅威の戦術や手順を継続的に模倣して、インフラの脆弱性や潜在的な攻撃経路を浮き彫りにすることができる。

人間のセキュリティーアナリストの役割を進化させる。セキュリティーアナリストを対象にしたある調査では、回答者の40%が、最大の悩みとしてアラートの多さを挙げた。47%の回答者は、インシデント対応において優先すべきアラートの判断が難しいと述べている[16]。また別の調査では、アナリストの役割はセキュリティー脅威の分析や対処ではなく、アラート調査の時間や量の削減である、と考えるアナリストが増えていることが明らかになっている。アナリストの離職率は10%以上だとする回答者が4分の3以上を占めており、半数近くが離職率は10%から25%であると回答している[17]。

AIは人間のセキュリティー専門家に取って代わることはできないが、彼らの仕事を強化し、仕事の満足度を高める可能性がある。平均的なSOCでは、AIと自動化により、Tier1とTier2アナリストの面倒な業務を排除することができる（Tier1では受信データの評価と問題のエスカレーション、Tier2ではトラブルチケットへの対応、脅威の範囲の評価、対応策と改善策の決定と、必要に応じたエスカレーションを行う）。これらのアナリストは、最も複雑なセキュリティー課題に対処し、脅威や脆弱性の積極的な特定と監視に重点を置く、より高度なTier2やTier3といった、戦略的で採用が困難な役割を担うように成長させることが可能となる。

未来のAIによるサイバー犯罪に対抗するために最低限必要な武器

高速なデータ分析やイベント処理・異常検知・継続的学習・予測知能などは、セキュリティー脅威に対するAIの重要な機能であるが、同時に犯罪者にとっても新たな攻撃の開発やより効果的な攻撃、システムの弱点を検出する機能として悪用することができる。

例えば、研究者たちは敵対的生成ネットワーク（訓練データに似たデータセットを生成するための競合する2つのニューラルネットワーク）を使用して、何百万ものパスワードの解読に成功した[18]。同様に、GPT-3として知られるオープンソースの深層学習言語モデルは、振る舞いや言語のニュアンスを学習で

きる。サイバー犯罪者がこれを悪用することで、信頼できるユーザーになりすまし、電子メールといった通信などにおいて正規と不正の区別を困難にすることが可能である[19]。フィッシング攻撃の文面は信憑性が増し、攻撃が成立する可能性がより高くなる[20]。

高度な敵対者は、標的を定めた上で目立たないように慎重に行動し、長期間検知されることなくネットワークに侵入していることがすでにできている。これにAIマルウエアが加わると、侵入者は多くのユーザーを危険にさらして価値あるデータセットを高速で特定しながら、素早く偽装して検知を回避する方法を習得するかもしれない[21]。

同様に、「GPT-3」として知られるオープンソースの深層学習言語モデルは、振る舞いや言語のニュアンスを学習できる。

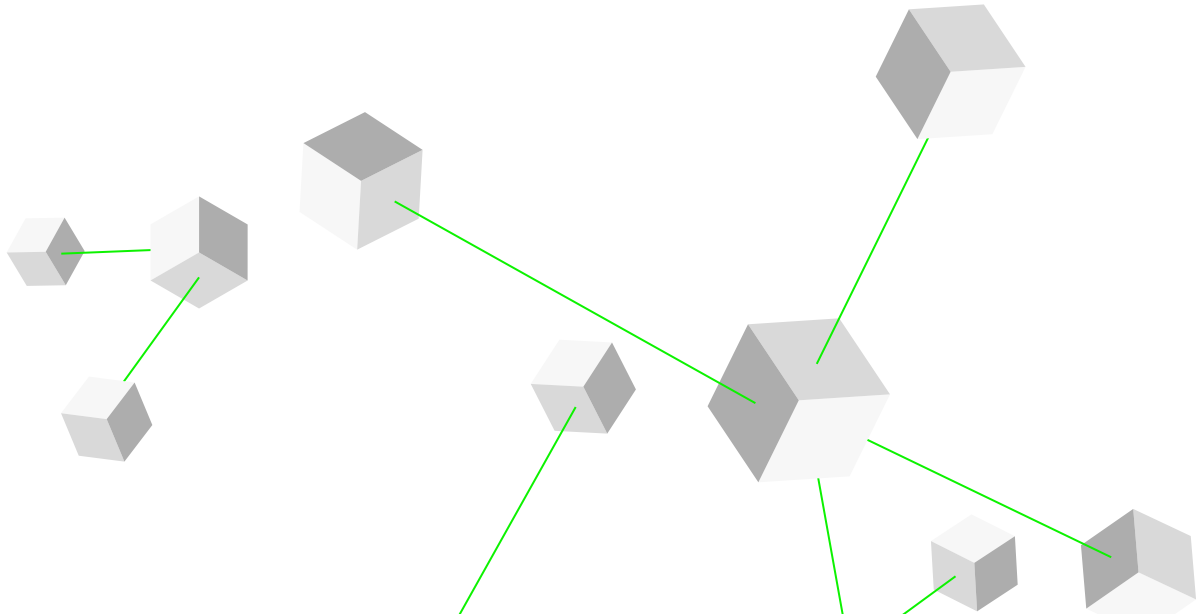
組織は、攻撃者と同様の手段を用いることでこのような侵入を防ぐことができる。十分なデータがあれば、AIを活用したセキュリティーツールは、AIによる脅威を効果的に予測し、リアルタイムで対処できる。例えば、セキュリティー専門家は研究者がパスワードの解読に使用したものと同じ技術を活用してパスワードの強度を測定することや、おとりパスワードを生成して侵入の検知を支援することができる[22]。また、コンテキストに基づく機械学習を活用して、電子メールユーザーの行動や関係、時間パターンを理解し、異常な行動やリスクの高い行動を動的に検知することが可能である[23]。

進むべき道

人間とAIは、これまでもセキュリティー侵害の検知、防止のために協力してきたが、多くの組織においてサイバーAIの活用はまだ初期段階にある。しかし、従来の企業ネットワーク以外の攻撃対象領域が増え続ける中で、AIはより多くのものを提供できるようになっている。

機械学習や自然言語処理、ニューラルネットワークなどのアプローチは、セキュリティーアナリストが信号とノイズを区別することに役立つ。パターン認識や教師あり・なしの機械学習アルゴリズム、予測・行動分析を使用することで、AIは攻撃の特定と撃退を支援し、異常なユーザー行動やネットワークリソースの割り当ての自動検出を支援できる。AIは、オンプレミスのアーキテクチャーとエンタープライズクラウドサービスの両方のセキュリティー確保に活用できるが、クラウドにおけるワークロードとリソースのセキュリティー確保は、従来のオンプレミス環境ほど難しくはない。

AI（あるいはほかの技術）単体では、現在や将来の複雑なセキュリティー課題を解決することはできない。AIがパターンを識別しリアルタイムで適応的に学習する能力は検知、抑制、対応を加速させ、SOCアナリストの負担を軽減し積極的に行動できるようにする。このような人材は今後も高い需要が見込まれるが、AIによってその役割もかわることになるであろう。組織はアラートのトリアージなどの下位レベルのスキルから、より戦略的で積極的な行動ができるスキルへとアナリストを再教育する必要がある。AIや機械学習によるセキュリティー脅威の要素が明らかになりつつある今、AIによって引き起こされるサイバー犯罪の発生に備える上でAIはセキュリティーチームの助けとなる。



最前線からの学び

Sapper Labsはソフトウエアにソフトウエアで戦う

Sapper Labs Cyber Solutionsは、カナダやアメリカの軍、政府、重要インフラ事業者のセキュリティー課題解決を支援するため、サイバーセキュリティーのソートリーダーシップやインテリジェンス、研究開発、実装、運用セキュリティープラットフォームや高度なトレーニングを提供している。AIは、Sapper Labsの技術ツールキットの中でますます重要なツールとなっている。

オタワに拠点を置くこのサイバー防衛企業は、監視、偵察、防衛工学といった積極的な防衛活動で地上部隊を支援する戦闘エンジニアの軍事用語からその名を取っている。すべてのネットワークやシステム、機能はすでに危険にさらされており、組織はこれを防御し対策を行う人材を持っていないという前提ですべてのプロジェクトに着手する。Sapper Labsの共同設立者兼CEOであるAl Dillonは、「人材パイプラインの成長は、攻撃対象の拡大、企業・政府のイノベーション計画の拡大のいずれにも追いついていないため、組織や資産を守ることができる人材を十分に育成できていない」と述べている。「そこでAIが活躍してくれるのだ」[24]

そのために、Sapper Labsはカナダとアメリカの複数の安全保障や防衛、諜報機関と協力して、進化する敵の脅威戦術や手順にリアルタイムで対応することを目的としたAIシステムを開発している。これらのシステムは意思決定者に情報を提供するだけでなく、人間の関与にかかわらず脅威から身を守る方法を学習することができる。「現在、機械学習やAI、自動化を利用するサイバー防御は、主に人間主導のサイバーエンゲージメントに焦点を当てている」とDillonはいう。「今日の技術革新のペースと、特に組織外でのネットワークやデバイスの普及を踏まえると、組み込み型の自動化システム機能が必要になる」

Dillonは、国家安全保障や防衛組織、官民組織が共通の目標とすべきなのは、軍事レベル相当のソフトウエア主導のエンゲージメントにシフトすることであると述べている。AI主導のソフトウエアは、AIを悪用した敵から守り反撃する。「我々は皆、国家主体の攻撃や、同様の意図、専門知識とツールを持つそのほかの悪意ある攻撃の脅威にさらされている」と彼は説明する。

例えば、Sapper Labsと政府機関は多層型脅威検知システムを開発している。このシステムは、衛星や陸上、海上に設置されたセンサーからソーシャルメディアなどのデジタルソース、そのほかパ

ブリック／プライベートネットワーク情報に至るまで、さまざまなソースからの情報やデータフィードを融合する。このようなデータを従来の方法で調査するには、人間が率いるセキュリティーチームでは数ヶ月から数年かかる。このデータとインテリジェンスを統合し、アルゴリズムを適用するプロセスを自動化することで、従来の10倍から15倍の速さで評価と意思決定を行うことが可能になる。Dillonは、3年以内にサイバーAIと自動化技術が大きく進歩し、インテリジェンスの評価や結論、意思決定を従来よりも50倍速く行えるようになると予想している。

Dillonによると、そこにはサイバーAIの最大の問題があるという。「サイバーAIに対する人間や社会的、文化的な問題を克服することは、技術的な問題を解決することよりもはるかに難しいであろう」と述べている。「最大の難関は、AIによる意思決定を人々に信頼してもらうことである。人々は、たとえ決断を下すのに50倍の時間がかかったとしても人間のリーダーが下した決断の方が安心できると考えている」

教育はこの信頼を築く鍵の1つである。Sapper Labsは、ほかの民間企業や公的機関、学術機関との連携を通して、自動化されたサイバーセキュリティーについてより広く認知してもらえるよう取り組んでいる。「我々は技術の導入と革新という点でエキサイティングな転換期にいるが、国家安全保障や個人データ、知的財産、そのほか重要資産を守るための社会的影響についてまだ十分に理解していないことは憂慮すべきである」とDillonは述べている。「AIを活用したセキュリティープラットフォームが、攻撃者の先を行くことができる唯一の方法となる可能性があることを、我々は認識しなければならない」

私の見解

Mike Chapple

Information security leader and IT, analytics, and operations teaching professor, University of Notre Dame

この１年間で、
サイバーセキュリティー攻撃の特質は
大きく変化した。

以前は、組織にとっての主な懸念事項の１つはランサムウエア攻撃であり、攻撃者はフィッシングやマルウエアを通じて企業データにアクセスし、そのデータを暗号化して身代金を要求した。このような攻撃は、マルウエアの餌食となった人物を利用することになり、組織がデータのバックアップを用意していた場合には必ずしも成功せず、場当たり的なものであった。

しかし昨今、国家によるサイバー戦争に匹敵するような組織的犯罪が行われており、その危険性は高まりつつある。COVID-19による感染拡大の際には病院が標的となったケースや、パイプラインが標的となり燃料を供給できなくなったケースなど、高度な標的型攻撃が行われている。攻撃者の新たなパラダイムは、盗んだ企業データに対して「データを人質に取る」「顧客情報や知的財産などの機密情報を漏えいする」という２つの恐喝を行うことである。これら脅威は、サイバー犯罪者が望むような資金とデータを保有している大規模組織にとって特に顕著である。さらに、5Gモバイルネットワークの採用や在宅勤務

などが拡大し、エンタプライズテクノロジーは従来の境界を越え、犯罪に狙われる攻撃対象が拡大し続けている。

このようなリスクの高まりに組織はどのように対処すればよいのか。2つの選択肢がある。1つは、人を増やすという選択肢。しかし人材市場におけるスキル格差が深刻化しているため採用は困難である。もう1つの選択肢はAIや自動化などによりリアルタイムで脅威を検知し分析、対応することである。最近の技術変化により、後者の選択肢であるサイバーAIはますます効果的になっている。

AIとサイバーセキュリティーの交わりは、10年近く前から話題になっている。これまではバズワードやルールベースの製品が中心だったが、計算能力とストレージ容量の進歩により、サイバーセキュリティーベンダーは自社製品に機械学習とAIを本格的に組み込み始めている。今日では、大企業は脅威に対するインテリジェンスを進化させるために、このようなサイバーセキュリティーベンダーに頼ることができるようになった。

主要なサイバーセキュリティーベンダーは多くの企業で製品を展開しており、それらがデータを収集するためのセンサーとして機能している。各顧客の匿名化されたデータにAIを適用することで、ベンダーはある組織からの脅威データを使用して、ほかの場所で同様のセキュリティー侵害の兆候を探すことができる。そのネットワーク効果は指数関数的である。データセットが大きく多様化するほど、これらのベンダーの検知機能は向上し、保護機能も向上する。このため、中規模企業も大規模企業も、マネージドサービスプロバイダーと連携することでメリットを得ることができる。あるいは、データサイエンスチームとサイバーセキュリティーチームが協力して、自社のサイバーセキュリティーウエアハウスでAIモデルを訓練することもできる。

今日のコンピューティング能力は、攻撃者のシグネチャや通常の動作からの逸脱を検出する高度なUEBA（ユーザーエンティティの動作分析）を開発できる。UEBAは、例えば、土曜日の朝にテラバイト級のデータをダウンロードするユーザーを検出しフラグを立てるかもしれない。このようなプロファイルとパターンを結びつけることで、脅威をより精密に識別することができる。

このようなシグナルはこれまでも存在していたが、以前はそれを分析して意味のあるパターンを導き出すことは非現実的だった。現在では、これらフラグをつけたAI関連の脅威をSOAR（Security Orchestration, Automation, and Response）プラットフォームに送り込み、アクセスを遮断するなど即座に対応することができるようになった。

サイバーセキュリティーの歴史はセキュリティーの種類を問わず、古くからいたちごっこである。我々が自己防衛のためにAIツールを開発しているように、攻撃者も攻撃をさらに複雑にするためにAIを開発している。国家はすでにこの領域に参入しており、今後1年半から2年の間に、民間のサイバー犯罪者がさらに参入してくる可能性がある。組織が被害者になりたくないのであれば、ユーザーやシステム、データを将来にわたって保護するためにAIを活用する機会を

模索し、行動することである。そうすることで、サイバー攻撃の特質が再び変化するときにも、企業は備えることができるだろう。

私の見解

Adam Nucci

Deputy director of strategic operations, US Army

アメリカ陸軍はモダナイゼーションの真っ只中にあり、データ主導の考え方を受け入れ、デジタル変革を推進する必要がある。

その目的は、兵器システムやプラットフォームだけでなく、プロセス、労働力や文化も進化させることである。

モダナイゼーションに伴い、すでに複雑化している技術環境はさらに動的に変化しており、我々はさまざまな巧妙な敵に囲まれている。野心的なモダナイゼーションの目標を達成するためには、セキュリティー体制の強化が不可欠であり、そのために必要なツールは、今ここにある。しかし、それらをセキュリティーだけではなく、ネットワーク、組織機能や人材に関するデリバリーアプローチの変革にも活用するためには、集中した取り組みが必要である。データを迅速に分析し、アクションにつなげるためのプラットフォームを構築することが極めて重要である。また、クラウドコンピューティングを幅広く導入すること

で、リアルタイムのデータ共有だけでなく、あらゆる種類のデータやネットワークの管理、制御、可視化も可能になる。

基礎的要素は揃っている。データ、アナリティクス、クラウドコンピューティングの強力な組み合わせは、ネットワークではなくデータを中心としたゼロトラストベースのセキュリティーアプローチの基盤となる。これは、ネットワークベースのID・クレデンシャル管理から、データおよびデバイス中心のIDアクセス管理と最小権限アクセス原則へのシフトを意味する。これにより、サイバーAIを大規模に活用する場が整うことになる。

機械学習やディープラーニングといったAI技術により、複数のハードウエアおよびソフトウエアプラットフォームを横断したサイバーセキュリティー環境を理解することができる。例えば、データがどこに格納され、どのように動作し、誰がアクセスしているのかを知り、攻撃者のプロファイルを構築してネットワーク環境全体で認識させることができる。AIと予測分析は、サイバーセキュリティーの人に関連する側面を理解することにも役立つ。運用環境から社会全体まで、情報の次元はあらゆるものと密接に絡み合っている。高度な機械学習とAIは、情報がユーザーに与える影響、我々が意思決定を行う方法や、敵の行動パターンなどの理解に役立つ可能性を秘めている。

今日のAIは汎用的ではない。狭い範囲を対象として構築された目的型のソリューションが中心であり、ほとんどが特定の用途向けである。しかし、サイバーセキュリティーはテクノロジーだけで解決できるような狭い問題ではなく、主には人の問題である。我々の敵は多様で創造的だ。何が彼らを動かすのだろうか。サイバーAIを進化させるためには、サイバー人材にも同じような多様性と想像力を持たせる必要がある。従来のSTEM教育を受けた、直線的な思考を持つサイバー人材と、曖昧な関連性から推論を導き出すことができるアプリケーション開発の異端児的な人材や多面的な思考ができる人材の力を掛け合わせる必要がある。これは、AIモデルの構築とトレーニングに人間的な側面を加えるだけでなく、サイバーセキュリティーの戦力増強にもつながる。

AIに基づくサイバー戦略により、データやアナリティクス、クラウドを活用して、侵入の予測、検出と対処を自動的に行うことができる。モバイル環境や低帯域幅環境においては新たな課題と機会の両方が存在するものの、テクノロジーの基盤は整っている。

サイバーAIのさらなる実現のためには、官民の連携強化も必要である。サイバーセキュリティーは国家安全保障そのものであり、サイバーセキュリティーを後付けするという発想から、すべての商業システムや政府システムに根幹として組み込むという発想に、社会全体でシフトする必要がある。これは公共部門だけで実現できることではない。官民の強力なパートナーシップと、業界、学術機関、国際的なパートナー間の相互交流により、センサー内蔵システム、

データや、AIを活用した予測分析に基づく、揺るぎないサイバーセキュリティー基盤を構築することができるのだ。

今後の展望

ストラテジー

サイバーリスクはこれまで以上に重要な戦略的関心事である。組織が収集するデータの量やパートナーシップ、労働力の幅が広がるにつれ、保護はますます複雑化している。サイバーAIは、近年のサイバー攻撃の規模とその巧妙さに対抗するための最良の手段となっている。CEOは、CRO、CISOやCIOなどから現在のセキュリティー体制を理解し、見直しの必要性を確認する必要がある。AIをセキュリティーおよび戦略上の優先事項として位置づけることで、リーダーは防御の強化とリスク管理の重要性について、組織の足並みを揃えることができる。

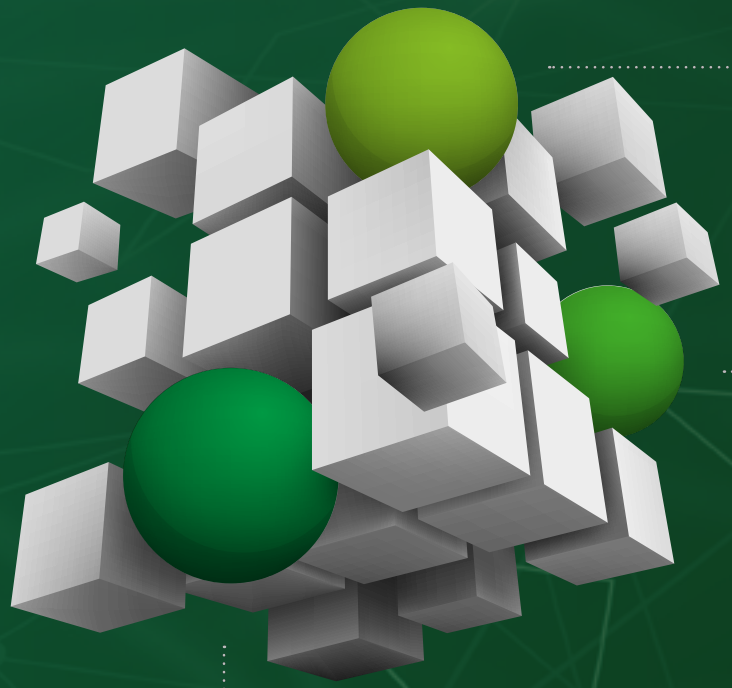
ファイナンス

サイバー攻撃の蔓延と経済的影響の増大に合わせ、CFOはリスク管理の監督についてより重要な役割を果たすようになっている。CFOは、経営層におけるその役割を活用し、AIで強化したサイバー防御の全社的な導入を提唱すべきである。また、サイバーセキュリティーチームと協力し、サイバーAIの実現に必要な投資やスケジュール、リスク、メリットを理解し、その情報を重要な優先事項として取締役会に提示すべきである。

リスク

攻撃者は何年も前からAIを活用してサイバー攻撃を行っている。CROは、AIによる防御とインテリジェントなセキュリティーオペレーションでそういった攻撃と戦うという新たな日常に備える必要がある。企業は、そのための新しい組織機能を社内リソースで構築すべきか、セキュリティーチームを強化するためにサイバー保護のアウトソーシングを活用すべきかを評価する必要がある。当然、AI防御には独自の脆弱性があり、脅威の状況は今後も進化を続けるであろう。手遅れになってから対応するのではなく、今すぐ行動を起こし、防御を徐々に向上させることが、顧客とそのデータを守る手助けとなる。

さあ、はじめよう



要点

1 リモートワーカー、ネットワークに接続されたデバイス、および第三者リスクの増加により、攻撃対象はどのように拡大しているか。また、それを保護するためにどのような対策を講じているか。

2 現在、AIツールをどのように使用してサイバー脅威を検出し、封じ込め、対応しているか。AIの利用をどの分野に拡大すれば、より積極的なセキュリティー体制を構築できるか。

3 現在のサイバーセキュリティー目標を達成するために必要なスキルセットと組織体制を持っているか。2年後にはどうなっているか。どのようにしてこれらのスキルを習得できるか。

執筆者

Curt Aubley
Cyber & Strategic Risk groups managing director
Deloitte & Touche LLP
caubley@deloitte.com

Ed Bowen
Advisory AI CoE leader
Deloitte & Touche LLP
edbowen@deloitte.com

Wendy Frank
Cyber 5G leader
Deloitte & Touche LLP
wfrank@deloitte.com

Deb Golden
US Cyber & Strategic Risk leader
Deloitte & Touche LLP
debgolden@deloitte.com

Mike Morris
Cyber & Strategic Risk managing director
Deloitte & Touche LLP
micmorris@deloitte.com

Kieran Norton
Cyber & Strategic Risk infrastructure security solution leader
Deloitte & Touche LLP
kinorton@deloitte.com

SENIOR CONTRIBUTORS

Wil Rockall
Partner,
Deloitte LLP

Jan Vanhaecht
Partner,
Deloitte Belgium CVBA

Sam Holmes
Senior manager,
Deloitte LLP

Ryan Lindeman
Senior manager,
Deloitte & Touche LLP

PaPa Yin Minn
Specialist master,
Deloitte Tohmatsu Cyber LLC

参考文献

1. Steve Morgan, "Cybercrime to cost the world $10.5 trillion annually by 2025," Cybersecurity Ventures, November 13, 2020.
2. IBM, *Cost of a data breach report 2021*, accessed November 17, 2021.
3. Ibid.
4. *CNBC*, "Cybercrime could cost $10.5 trillion dollars by 2025, according to Cybersecurity Ventures," March 9, 2021.
5. *PR Newswire*, "Artificial intelligence-based cybersecurity market grows by $19 billion during 2021-2025," June 21, 2021.
6. NCCI, "Remote work before, during, and after the pandemic: Quarterly economics briefing—Q4 2020," January 25, 2021.
7. Jasper Jolly, "Huge rise in hacking attacks on home workers during lockdown," *Guardian*, May 24, 2020.
8. Fleming Shi, "Surge in security concerns due to remote working during COVID-19 crisis," Barracuda, May 6, 2020.
9. Cisco, *Cisco annual internet report (2018–2023) white paper*, accessed November 17, 2021.
10. Gartner, "API security: What you need to do to protect your APIs," accessed November 17, 2021.
11. David Flower, "5G and the new age of fraud," *Forbes*, December 30, 2020.
12. GSMA, *The mobile economy*, accessed November 17, 2021.
13. Steve Rogerson, "Cellular IoT connections grew 12% in 2020, says Berg," IoT M2M Council, August 4, 2021.
14. (ISC)², "(ISC)² study reveals the cybersecurity workforce has grown to 3.5 million professionals globally," accessed November 17, 2021.
15. Wendy Frank (Cyber 5G leader at Deloitte & Touche LLP), interview, October 1, 2021.
16. Palo Alto Networks, *The state of incident response 2017*, accessed November 17, 2021.
17. Critical Start, *The impact of security alert overload*, accessed November 17, 2021.
18. Matthew Hutson, "Artificial intelligence just made guessing your password a whole lot easier," *Science*, September 15, 2017.
19. Lily Hay Newman, "AI wrote better phishing emails than humans in a recent test," *Wired*, July 2021.
20. William Dixon and Nicole Eagan, "3 ways AI will change the nature of cyber attacks," World Economic Forum, June 19, 2019.
21. Ibid.
22. Matthew Hutson, "Artificial intelligence just made guessing your password a whole lot easier."
23. Tony Pepper, "Why contextual machine learning is the fix that zero-trust email security needs," Help Net Security, February 16, 2021.
24. Al Dillon (cofounder and CEO, Sapper Labs Cyber Solutions), phone interview with authors, October 19, 2021.

日本のコンサルタントの見解

AIを加速するために

近年、AIはビジネスの加速やサイバーセキュリティーの強化、安全保障関連など多様な領域において積極的に利活用できなければ時流に取り残される時代となった。しかし、AIの普及が進むにつれ、AIを取り巻く新たな脅威も次々と登場している。よりAIの利活用を加速させるためには、安全・安心なAIの開発および利活用するための対策が必要不可欠と示唆される。

AIを取り巻くセキュリティーは、総務省「サイバーセキュリティータスクフォース」でも議論されている通り、Attack using AI（AIを利用した攻撃）、Attack by AI（AI自身による自律的な攻撃）、Attack to AI（AIへの攻撃）、Measure using AI（AIを利用した対策）の4つの観点が取り上げられている[1]。特に昨今では、さまざまな学習モデルのAIが実社会で広く利用されている背景もあり、それらを標的とした新たなAIへの脅威が顕在化している。Attack to AIへの現実的な対策が今まさに希求されている。

Attack to AI（AIへの攻撃）

AIシステムは、一般的には学習データの収集フェーズ、学習データセットの生成フェーズ、AIモデルの学習フェーズというサイクルを経て、実際にAIが利活用されるAIモデルの運用フェーズとなる。これら各フェーズにおいてさまざまな攻撃手法が確立されており、AIが脅威にさらされる可能性がある。現在約50以上の攻撃手法が報告されており、大きく4つに分類される。Attack to AIの概要を図1に示す。

Poisoning攻撃。学習に利用するデータやロジックを汚染することで、誤分類など含む期待と異なる学習モデルを生成させる攻撃である。間接的汚染や直接的汚染などいくつかの攻撃手法がある。例えば、間接的汚染では、攻撃者がターゲットモデルの加工済みデータにアクセスできない場合でも加工前のデータを改ざんすることで間接的に汚染する。また、直接的汚染では、データインジェクションやデータマニピュレーションによるデータの汚染や、ロジックコラプションによるモデルの汚染を行う。

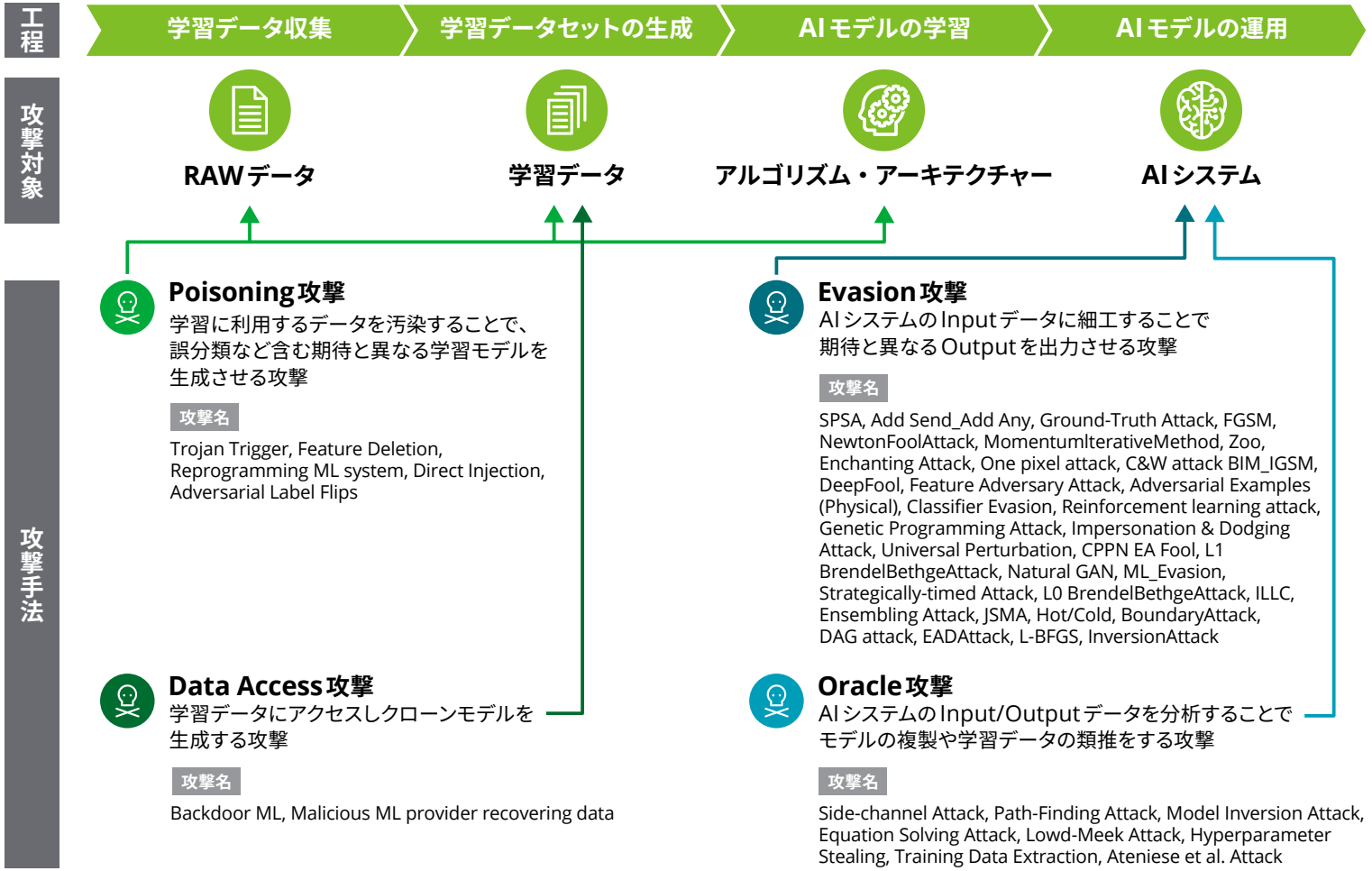
Data Access攻撃。学習データにアクセスしクローンモデルを生成する攻撃である。この攻撃では学習データの一部またはすべてにアクセスし、AIのクローンモデルを作成することが可能である。また、この攻撃は潜在的な入力の有効性をテストしてEvasion攻撃のための準備としても使用できる。

Evasion攻撃。AIシステムのInputデータに細工することで期待と異なるOutputを出力させる攻撃である。この攻撃では、L-BFGS（Limited memory Broyden–Fletcher–Goldfarb–Shanno）やFGSM（Fast Gradient Sign Method）、JSMA（Jacobian-based Saliency Map Attack）といった勾配ベースの検索アルゴリズムを利用し、入出力ペア全体の損失関数の勾配を計算するために、モデルの知識や代替モデルが必要となる。

Oracle攻撃。AIシステムのInput/Outputデータを分析することでモデルの複製や学習データの類推をする攻撃である。攻撃者は、APIを使用してモデルに入力を与え、その出力を観察する。これにより、攻撃者がモデル自体を直接知らない場合でも、取得した入出力ペアを使用して、ターゲットモデルと類似した動作のクローンモデルを訓練することができる。Oracle攻撃には、抽出攻撃や反転攻撃、メンバーシップ推論攻撃が含まれており、これら攻撃では、出力値や信頼度などの情報を収集してモデルやパラメーター、特性を推測する。

注目したいポイントは、図1からも分かる通り各フェーズにおいて攻撃手法が存在するが、特にEvasion攻撃およびOracle攻撃はAIモデルの運用フェーズ、つまり実際に利活用しているAIに対しても攻撃が可能な点である。では、攻撃によって引き起こされる具体的な脅威にはどのようなものがあり、顕在化しているのであろうか。

図1 Attack to AIの概要



顕在化する脅威

AIに対する攻撃により顕在化した脅威を、研究などの実証実験の側面、実社会で発生した事象の側面からまとめる。図2にその一例を示す。

Adversarial Attack。数多くあるAIに対する攻撃の中で、大きなインパクトを与えたものは敵対的学習である。Adversarial Attackは先のEvasion攻撃に含まれる。AIシステムのインプットに対して細工したデータ（摂動）を与えることで、期待と異なる結果をアウトプットさせる攻撃となる。図2の例では、道路標識に細工したシールを貼り自動運転AIの判断を誤認させている。「STOP」サインにノイズとして計算された形のシールを貼ることで、AIは「STOP」サインではなく、「Speed Limit 45」サインと誤認識してしまう[2]。

また、デロイト トーマツ サイバーセキュリティー先端研究所の研究成果として報告された手法では、自然界における暗黙のバイアスを利用することでAIシステムからオブジェクトを隠すことが可能であることが実証された[3]。この事例では「STOP」サインとダイニングテーブルを合わせることで、「STOP」サインをAIから隠すことに成功している。一般的に「道路標識は道路のそばにあり、ダイニングテーブルと一緒に存在しない」というような暗黙のバイアスを利用し、攻撃を実現している。

Clone Attack。AIシステムは一般的にブラックボックスであるが、インプット・アウトプットの両データを分析することで学習モデルのクローンや学習データの再構築、学習データの類推が可能である。Clone Attackは先のEvasion攻撃に含まれる。この事例としては、AI顔認識サービスのAPIから学習データに使用した画像を類推した例が論文で公開されている。当該サービスのAPIアクセスを通してインプット・アウトプットデータを分析し、元の画像を復元している[4]。また別の事例では、ある学習モデルにおいて、合成データを使用することでモデルを模倣することが可能なことが示されている[5]。模倣する行為そのものが脅威ではないが、悪意をもって模倣され利用されると大きな脅威となる。

Ethics。AIに対する攻撃だけではなく、AIが学習したモデルの倫理に関する問題も顕在化している。ある企業はAIチャットボットを開発し公開したが、程無くしてそのチャットボットが差別主義者となったため公開を停止した[6]。公開情報を通じて人種差別や性差別、陰謀論など不適切な内容を学習した結果、倫理的に問題のあるAIに変わり果てた事例であり、社会的に大きなインパクトを残すことになった。

Deep Fake。AIを悪用した攻撃や犯罪も登場している。2019年にAIを悪用した犯罪が実際に発生している。ある犯罪者がAIを使用してターゲット会社のCEOの声になりすまして、22万ユーロを騙し取るという詐欺事件が起きている[7]。ターゲット人物の声質やアクセント、文の区切りなども模倣していたとのことで、AIによって生成された声の完成度の高さも注目される。

これら顕在化した脅威の一例から、実社会への影響を議論する必要がある。

脅威の顕在化がもたらす実社会への影響

最後に、実社会においてすでにAIはさまざまな分野で利用され、技術に組み込まれているという背景のもと、顕在化した脅威が実社会へ及ぼす影響について議論する。議論の概要は図3に示す。

生命に対する影響。自動運転や医療診断支援といった分野においてAIが利活用されている。自動運転のAIが道路標識や車線を誤認識することで自動車が暴走し運転者や歩行者などが危険にさらされる。また、医療診断支援システムのAIが陽性を陰性と誤認することで患者の治療方針が変わり健康維持に影響が及ぶ可能性も考えられる。つまり、AIの脅威は生命を脅かす脅威にもなり得ることが分かる。

経済に対する影響。金融業界においてAIを活用した取引が行われている。アルゴリズムの取引に利用される優秀なAIを悪意をもって複製、悪用することで不正に収益を上げるといったことが示唆される。さらに、信用評価や異常検知に利用されている学習

図 2 顕在化する脅威の一例

Adversarial Attack

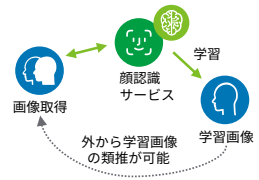
道路標識にノイズが載ったシールを貼ることで自動運転のAIを誤認させる事例

出所：Robust Physical-World Attacks on Deep Learning Visual Classification, https://arxiv.org/pdf/1707.08945.pdf

自然界における暗黙のバイアスを利用することでAIシステムからオブジェクトを隠す事例

出所：デロイト トーマツ サイバー サイバーセキュリティ先端研究所, hhttps://i.blackhat.com/asia-21/Thursday-Handouts/as-21-PaPa-Ziegler-Hiding-Objects-From-Computer-Vision-By-Exploiting-Correlation-Biases.pdf

Clone Attack



顔認識サービスのAPIを使用して学習データに使用した画像を類推した事例

出所：Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures, Matt Fredrikson Carnegie Mellon University, Somesh Jha University of Wisconsin–Madison, Thomas Ristenpart Cornell Tech, 2015
https://www.cs.cmu.edu/~mfredrik/papers/fjr2015ccs.pdf

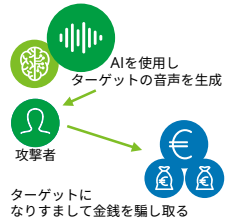
合成データを使用することでモデルを模倣する事例

出所：Stealing Knowledge from Protected Deep Neural Networks Using Composite Unlabeled Data,
https://ieeexplore.ieee.org/document/8851798

Ethics / Deep Fake

AIチャットボットが人種差別や性差別、陰謀論など不適切な内容を学習して、倫理的に問題のあるAIに変わる事例

出所：Microsoft and the learnings from its failed Tay artificial intelligence bot, https://www.zdnet.com/article/microsoft-and-the-learnings-from-its-failed-tay-artificial-intelligence-bot/



犯罪者がAIを使用してターゲット会社のCEOの声になりすまし詐欺を行う事例

出所：Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case , https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

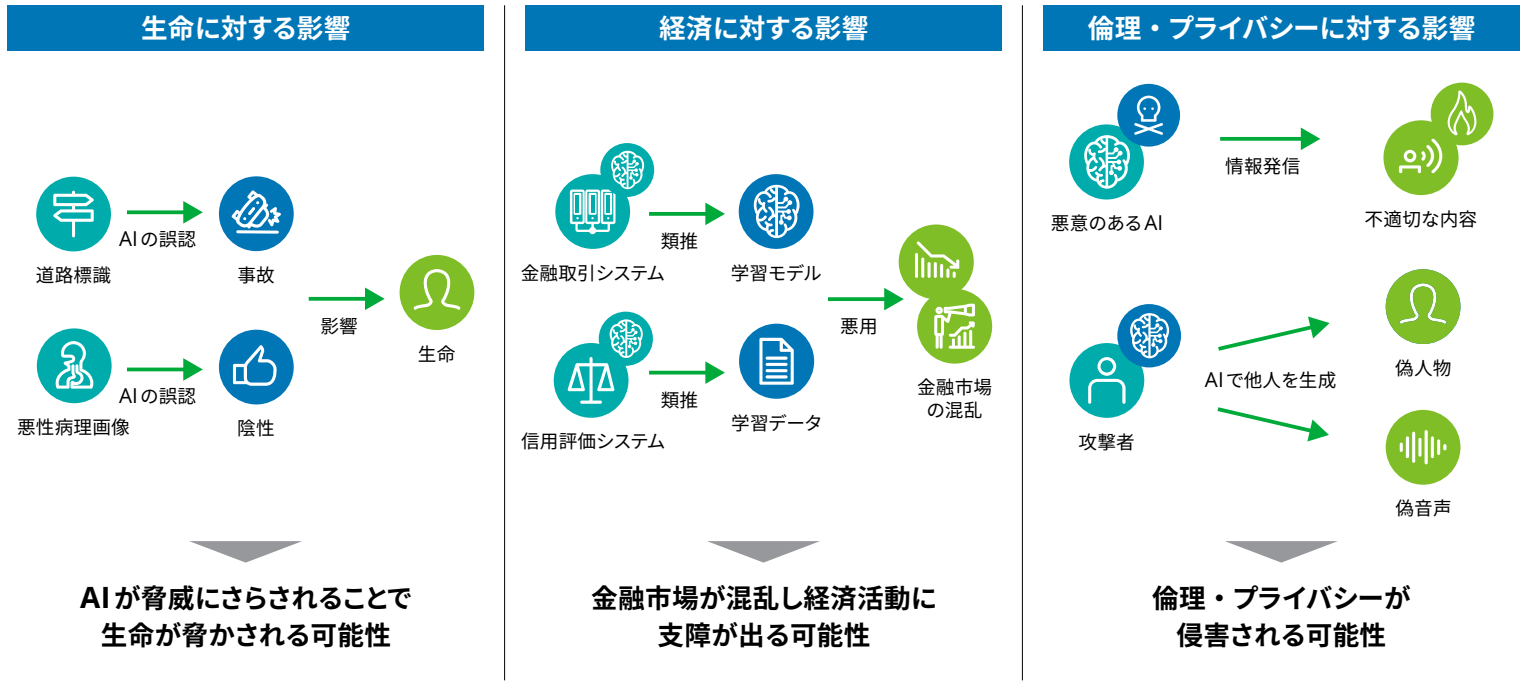
データを類推、悪用することで市場に影響が及ぶ可能性が考えられる。つまり、AIの脅威は経済を脅かす脅威にもなり得ることが分かる。

倫理・プライバシーに対する影響。AI自体が攻撃者になることや、AIを利用して攻撃するということも考えられる。倫理的に問題のあるAIが不適切な情報を発信しそれが真実として拡散することや、攻撃者がAIを利用して他人になりすましプライバシーを侵害することなど、人間社会に大きな影響が及ぶ可能性が考えられる。

攻撃者の一歩先へ

AIへの攻撃手法、攻撃により実際に顕在化した脅威の一例、最後に実社会へ及ぼす影響について議論してきた。これからもAI技術は間違いなくビジネスを加速させ、組織のサイバーセキュリティーを強化する上でも、必要不可欠な存在である。同時に、攻撃が成功すれば大きな脅威となり、悪意のある第三者からのターゲットにもなる。

図3 脅威の顕在化がもたらす実社会への影響



しかし、AIの開発から運用までのサイクルを把握し、チョークポイントを抑え、攻撃の仕組みを理解することでセキュアなAIを開発することができるのではないだろうか。攻撃者にとってもAIは重要な武器になりつつある今日、その一歩先へ進むためには、安全・安心なAIを構築して武器や防御として、さらにビジネスや社会を加速させるツールとして利活用することが重要である。

執筆者

神薗 雅紀　執行役員
チーフテクニカルオフィサー／サイバーセキュリティ
先端研究所 所長 サイバーセキュリティリード

セキュリティベンチャー企業や政府研究機関を経て、2019年より現職。研究開発を主軸とし、新たなソリューションやアセットの開発、研究開発事業支援、テクノロジー特区の立案および支援など、多数の新たなテクノロジー領域やオポチュニティーの立案に従事。上記貢献により、2018年 総務大臣奨励賞を受賞。

熊谷 裕志　サイバーセキュリティ先端研究所
上席研究員

セキュリティ関連の非営利団体やベンチャー企業、コンサルティングファームを経て、2019年より現職。脆弱性の解析や調査研究に従事し、現在は主にコア技術などの研究開発や新規ソリューション開発をリードしている。

Yin Minn Pa Pa　サイバーセキュリティ先端研究所
主任研究員

サイバーセキュリティ関連の研究に10年以上従事。主にネットワークセキュリティやマルウェア分析、IoTセキュリティ、Webセキュリティ、AIセキュリティに関して強みを持つ。また海外サイバーセキュリティカンファレンスやジャーナルなどにて研究成果の発表を行いエミネンス向上にも貢献。

参考文献

1. サイバーセキュリティタスクフォース事務局, “今後重点的に取り組むべき研究開発課題について,” accessed February 8, 2022.
2. Road Signs, “Attack on a Stop Sign using Black/White Art Stickers,”September 5, 2017.
3. Y. M. P. Pa, P. Ziegler, and M. Kamizono, Hiding Objects from Computer Vision by Exploiting Correlation Biases, May 7, 2021, p.37.
4. M. Fredrikson, S. Jha, and T. Ristenpart, Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures, October 2015, p.1322–1333.
5. Mosafi, E. O. David, and N. S. Netanyahu, Stealing Knowledge from Protected Deep Neural Networks Using Composite Unlabeled Data, July 2019, p.1–8.
6. Barbaschow, “Microsoft and the learnings from its failed Tay artificial intelligence bot,” accessed February 8, 2022.
7. C. Stupp, “Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case,”August 30, 2019.

技術スタックの物理化

システムの耐障害性の実現

ミッションクリティカルな物理システムは停止することが許されない

ガバナンスの再考

スマートデバイスが新たなガバナンスの課題をもたらす

技術知見のアップデート

スマートデバイスの管理、監視、保守のためにはこれまでとは異なる新しいITスキルが必要である

トレンド6

技術スタックは物理化する

CIOは物理的な技術スタック※を管理する必要性が高まっている

先進的なプロセッサーやセンサー、産業用ロボット、機械学習の普及に伴い、あらゆるデバイスがスマート化、オンライン化され、データの収集が可能になっている。デバイスから収集したデータを製品やサービスにフィードバックするサイクルを確立することで、企業は製品やサービスの改善につなげ、新たな収益源を生み出している。物理的なデバイスと機能が増えるにつれて、CIO（Chief Information Officer、最高情報責任者）の権限は、デジタルの範囲を超えて、これらの新しい物理的な資産を幅広くカバーするように再び拡大しつつある。

何十年もの間、IT部門は、テクノロジー、ツール、アプリケーション、フレームワーク、データエコシステムなど、主にデジタルな技術スタックの管理に重点を置いてきた。これまで、物理的な技術スタックは主に従業員のアクセスポイントとデータセンターのインフラが中心で、それが変わることは少なかった。

しかし、テクノロジーが現場や事業に浸透するにつれて、テクノロジーはビジネスの実現手段から価値創出の推進手段へと進化し、企業活動の要となっている。今日、企業内にあるすべてのスマートデバイスを管理するには、セキュリティー、自動化、データに基づく分析と意思決定、AIと機械学習といったデジタル機能が必要とされている。例えば、アナリティクスとAIによる最先端の推論機能が組み込まれた産業用制御システムは、2021年には5%未満だったが、2025年には30%まで増加することや、コネクテッドカーが2025年までに毎月10エクサバイトのデータを生成することが予想される[1, 2]。

製造工場のフライス盤、病院の心臓モニター、インフラの検査用ドローン、レストランのロボット調理器、オフィスビルのスマートセンサー、新しい「Phygital（Physical-Digital、物理デジタル）」な一般消費者向け製品など、新しい世代の物理資産には、ビジネスに不可欠な機能を実現する高度なデジタル技術が組み込まれている。これら資産の管理、監視、測定、保護に関するIT部門の責任は大きくなってきている。CIOは、アプリケーション、デバイス、セキュリティーの要件を満たす適切なテクノロジーを選択し、デバイスおよび社内システムの中で最も長い連続稼働時間と高い冗長性を必要とするネットワークテクノロ

（※注）：技術スタック（またはテクノロジースタック）は、ビジネス目標を達成するためにIT部門が管理する、最適なテクノロジーの組み合わせ。
例えばプログラミング言語、ライブラリー、インフラ、ミドルウェア、データベース、ソフトウェア、ツール、ユーザーデバイスなどが含まれる。

ジーをどのように導入、管理、および保守すべきかを検討する必要がある。また、デバイスのガバナンスと監視についても再検討し、IT部門に所属するメンバーのチーム構成、役割定義、管理方法、トレーニング方法を見直す必要がある。

稼働時間、冗長性、セキュリティー水準を高める

新しい物理的な技術スタックに含まれるデバイスの多くは、顧客向けのビジネスに不可欠なアプリケーションとサービスを提供している。これらのデバイスは、大量のデータと動画を生成、利用することが多く、リアルタイムで重要な意思決定を行うためには、それらのデータを迅速に転送し、分析する必要がある。

以前の物理デバイスとは異なり、システム停止はユーザーに不便を強いること以上の意味を持つ可能性がある。例えばレストランの注文システムがダウンし、空腹の客がほかのレストランに移るといったビジネス上の損失から、埋込み型心臓モニターがオフラインになり、重要な患者のデータが記録できなくなるといった生命に関わる脅威まで、さまざまな可能性が考えられる。

耐障害性は非常に重要であり、最高レベルのシステム稼働時間、信頼性、およびセキュリティーが要求される。物理的な技術スタックがビジネスに与える影響が増大し続ける中、企業は最高水準の事業継続性を確保するために新世代のコネクテッドデバイス、無線ネットワーク、エッジコンピューティングをどのように管理・維持するのか、検討する必要がある。次に重要な領域をいくつか示す。

デバイスとデータの管理

デバイスとシステムのパフォーマンスを最適化するために、多くの場合、IT部門は複数のベンダーのコネクテッドデバイス、アプリケーション、ネットワークのエコシステムを導入および管理する必要があり、作業はリモートとなるケースも多い。デバイスの状態監視、問題の検出とトラブルシューティング、およびソフトウエアとファームウエアの更新管理には、新しいプラットフォーム、ツール、およびアプローチが必要になる場合がある。またデバイスに何重もの冗長性を持たせる必要がある。

特に大規模な導入において、繰り返し手作業によるデバイス管理を避けるためには、自動化が重要となる。自動化されたデバイス管理ツールは、デバイスの登録、構成、プロビジョニング、メンテナンス、リモートや無線によるファームウエアとソフトウエアの更新、および監視を拡張することに役立つ。

パフォーマンスの向上や、新しい製品やサービスの開発を行うためには、これらのデバイスによって生成される大量のデータを管理する必要がある。IT部門は、データの取得頻度、処理時間、精度、形式などの課題を考慮する必要がある。データを保存するストレージは非常に重要であり、リモート環境の場合は、分散ストレージとエッジコンピューティングが有力となる。

ワイヤレスネットワーク

これらの機器をネットワークに接続するための最も効率的で耐障害性の高いソリューションを選択するために、IT部門は、消費電力、信号強度と範囲、物体または天候や環境要因に関連する干渉、電気または無線周波数の干渉、コスト、接続する機器の数、周波数共有、セキュリティー、回復力、および一定のインターネット接続の必要性などの属性を評価する必要がある。

多くのスマートデバイスは、顧客の施設やそのほかリモートの実環境で動作し、5G、Wi-Fi 6、Bluetooth Low Energy（BLE）、メッシュネットワーク、衛星などの高度な無線接続によって実現されている。このようなテクノロジーは、高スループット、低遅延、大容量を実現し、データ転送効率の改善も実現する。

デロイト グローバル（デロイト）が2020年に実施した調査によると、パンデミックにより企業が新しい無線ネットワーク技術、特に5GとWi-Fi 6に対する投資を加速したことが分かった。調査の参加者は、これらのテクノロジーをビジネス推進において最も重要な無線技術と見なしている[3]。どちらの技術も、パフォーマンスと運用面が向上しており、デバイス、ユーザー、トラフィックを大規模にサポートし、現実に限りなく近い環境を再現するとともに、組織の耐障害性を高めることが期待されている。5GとWi-Fi 6のおかげで、IoTをはじめとする低遅延技術を活用した新しいアプリケーションが、エッジコンピューティングデバイス側で大量のリアルタイムデータを収集し、共有することができるようになる。

ワイヤレスネットワーク技術は補完的なもの、つまり複数の技術を組み合わせてさまざまなユースケースに対応することができるものである。多くの組織が、災害級の嵐の中でも継続的な運用を保証するためにエネルギー技術や発電源を多様化することと同様に、冗長性を保証するために無線ネットワーク技術の使用も多様化する必要があるかもしれない。

エッジコンピューティング

5GとWi-Fi 6の性能がアップグレードしたにもかかわらず、クラウドは自律走行車やスマート工場、AR（Augmented Reality、拡張現実）やVR（Virtual Reality、バーチャルリアリティー）など数十ミリ秒から数ミリ秒以内のネットワークレイテンシーが必要なアプリケーションに対し、許容可能なレスポンス時間やデータ転送速度を保証できない。デバイスが生成する分散データをリアルタイムで処理する必要がある場合、パブリッククラウドやデータセンターよりも、エッジコンピューティングのような分散型コンピューティングの方が効率的である。

データソースに近いところで計算能力を発揮するエッジコンピューティングアーキテクチャーは、膨大な量のデータをリアルタイムで管理、処理し、そして価値を引き出すために必要なレイテンシーと帯域幅を提供することができる。しかし、これをエッジコンピューティングの復活と呼ぶのはふさわしくない。

エッジコンピューティングは何年も前から存在しているからだ。最近の調査によると、ITリーダーの72%がすでにエッジコンピューティングを利用しており、ガートナーは、2025年までに企業が管理するデータの50%以上がデータセンターやクラウドの外で生成、処理されるようになると予測している[4, 5]。エッジコンピューティング市場の成長は目前に迫っている。あるエッジコンピューティングの業界団体は、2019年から2028年の間に、エッジコンピューティングのデバイスや設備機器への累積支出額が8,000億ドルに達すると予測しており、その中でも製造業と医療分野での最も顕著な増加が見込まれるとしている[6]。

ITリーダーの72%はすでにエッジコンピューティングを利用している。

エッジコンピューティングサイトは多くの場合無人施設であり、その業務上不可欠な性質を考慮すると、電源、冷却装置、およびネットワーク接続の冗長化が重要であり、物理的なセキュリティーとリモート監視・管理も同じく重要となる。

ガバナンスと監視に対する新しいアプローチ

ガバナンスや監視の戦略やポリシーは、新世代のコネクテッドデバイスのニーズに合わせて進化させる必要があるかもしれない。IT部門にとっては、物理的なデバイスやネットワークの利用に関連する規制や基準は馴染みがない故に対応に際しての課題であり、しかも何年にもわたって確定しない可能性がある。例えば、アメリカの裁判所がつぎはぎだらけの州税法から、電子商取引における売上税について明確な判決を下すまでに、20年近くを要したことからも推察される。

ここでは、デバイス、データ、およびセキュリティーに関連する、ガバナンス上の重要な検討事項を紹介する。

デバイス

特定の物理的資産を操作することは、国家、政府、州や地域の法令によって規制されている場合がある。例えば、屋外でドローンを使用するアメリカの組織は、ドローンを登録し、アメリカ連邦航空局から空域の承認を得る必要がある。また、特定の種類のドローンは、無線識別システムを搭載しなければならない[7]。

同様に、自律走行車の使用を規定する法律は、国によって、さらには州によっても異なる。アメリカでは、連邦政府の規則は存在せず、商用車の使用、運転者の免許、車内での運転者の要件、速度制限、賠償責任保険などを規定する州法が乱立しているだけである[8]。

責任の所在はますます複雑になる可能性がある。例えば、コンピューターで作動するスマートデバイスがミスを犯して人間に危害を与えた場合や、財産に損害を与えた場合は、販売ベンダーと運用ベンダーのどちらが責任を負うのか。また、AIによる判断で被害が発生した場合、どうなるのか。特定のデバイスに対する保険が推奨、あるいは必須とされる可能性がある。

また、もう1つの問題として、リモート管理されたデバイスの所有権とメンテナンスがある。これには、セキュリティー、保守、および修理の責任と、サービスレベルへの影響が含まれる。IT資産の廃棄はデバイスのライフサイクル管理に含める必要があり、単一または複数のIT資産のリプレイス、証明書の失効、データのアーカイブ、機密情報の削除などの計画を策定する必要がある。

デバイスの調達では、エンタープライズ向けのスマートデバイスと、厳密なエンタープライズ仕様を満たさないマスマーケットのスマートデバイスとを区別するなど、新たな課題が生じる可能性がある。従来のITベンダーのエコシステムが、運用技術や産業用IoTのサプライヤーにまで拡大するにつれて、調達の性質と文化は変化するであろう。

データ

CIOやチーフデータオフィサーは、ネットワークに接続されたデバイスから生成されるデータやメタデータの所有権について検討しなければならないかもしれない。例えば、データやメタデータをコピーすること、それらを配布すること、二次的著作物を作成することを誰が法的に許可されていて、それを誰が管理するのか、などである。

従来のコネクテッドデバイスやアプリケーションと同様に、データのプライバシーを確保することは依然として最優先事項だ。EU一般データ保護規則（GDPR）、国際標準化機構（ISO）、アメリカ標準技術研究所のサイバーセキュリティーフレームワーク（NIST CSF）、医療保険の相互運用性と説明責任に関する法律（HIPAA）、連邦情報セキュリティー管理法（FISMA）、そのほかの業界や地域の規制やガイドラインにしたがってエンドユーザーデータを収集し、保護することは、最低限必要となる。また、センサーやカメラを搭載したデバイスは、通常、エンドユーザーの明示的な認識や許可なしに、継続的にデータを収集・共有している点を考慮しなければならない。例えば、生きている人間を識別するために使用できる静止画や動画は、GDPRの下では個人データに該当するため、それに応じて収集され、保護されるべきである[9]。

セキュリティー

これらの物理資産は、多くの場合独自のオペレーティングシステムや通信プロトコルで開発されており、内蔵されているセキュリティーも弱く、機器のメモリーや演算能力も限られているため、保護することが非常に困難である[10]。100万台以上の企業や医療機関のIoTデバイスを対象とした最近の分析では、全デバイスのトラフィックの98%が暗号化されておらず、57%のデバイスが中程度または高強度の攻撃に対して脆弱であることが明らかになった[11]。企業のファイアウォールの外部に配置された業務上不可

欠な資産は、特にデータ、機械学習アルゴリズム、およびそのほかの知的財産が埋め込まれている場合、新たなセキュリティー上の脅威となる。

従来のネットワーク機器と同様に、これらのコネクテッドデバイスも、クラウドとそのほかのネットワーク機器やエンドポイントと安全に通信でき、データを暗号化し、ネットワーク認証される必要がある。ほとんどの主要クラウドプロバイダーは、デバイス管理プラットフォームにセキュリティー機能を搭載している。もしくは、IT部門がカスタムのセキュリティー保護を開発・導入することで、すべてのデバイスが積極的に監視・保護されるようにしている。

デバイスの調達プロセスでは、セキュリティーと第三者によるデータアクセスを考慮する必要がある。一部のIoTデバイスでは、メーカーに情報を送信するためのバックドアが隠されていることがセキュリティー研究者によって発見されているので、ベンダーの選択は慎重に行うことが推奨される[12]。

プロダクトエンジニアリングサービス：スマートなコネクテッドプロダクトの研究開発

技術スタックが物理的になっていくにつれて、製品の研究開発の重点は、必然的にスタンドアロン製品（スピーカー、サーモスタットや自動車など）から、リアルタイムで移動・分析する必要があるデータ、および柔軟な消費モデルを備えたスマートなコネクテッドプラットフォーム（クラウド上のサービスから音楽を直接再生するスピーカー、温度の自動調整機能とアプリケーションからの操作機能を備えたサーモスタットや、リモートでの診断・サービス・アップグレード機能を備えた自動車など）へと進化している。このような製品は複雑であり、多くの場合、実現にはビジネスモデル、ITシステムと、ビジネスプロセスを同時並行で転換する必要がある。

PES（Product engineering services、プロダクトエンジニアリングサービス）は、概念設計からソフトウエア・ハードウエアの開発・製造に至るまで、これらの複雑な製品を構築するための統合プロセスである。PESは、例えばCPUやGPUなどのハードウエアコンポーネントの開発・統合を含むこともある。ソフトウエアにはハードウエアを操作するために使用されるオペレーティングシステム、デバイスドライバー、ファームウエア、およびそのほかの組み込みソフトウエアと、機能やUIを提供するアプリケーション・ソフトウエアも含まれる。PESにおけるもう1つの重要な取り組みは、スマート製品を企業のITシステムやクラウド上のプラットフォームと接続して、利用状況の追跡や課金、パフォーマンスの監視、アナリティクスの収集を行うことだ。そして、PESは、センサーやそのほかハードウエアの構築・監視や、アプリケーションストア、eコマースサイト、そのほかの流通チャネルで使用するアプリケーション開発に必要となる第三者ベンダーやパートナーの豊富なエコシステムを製品チームが活用することに役立っている。

必要な新しい専門知識とスキル

物理資産がビジネス上重要となり、企業の敷地外に設置されることになると、それらを維持・管理・監視するために新しいスキルセットが求められる可能性がある。

例えば、IT部門は、重要な技術的要件・セキュリティー要件・耐障害性要件をデバイスやネットワークに組み込む必要があり、信号処理・センサー調整・通信プロトコルなどのタスクを実行する低電力電子機器をプログラムできるシステムエンジニアや、無線ネットワークの計画・分析・設計・最適化に役立つ無線周波数スペクトル管理を理解しているエンジニアが求められることになる。産業施設では、接続されたセンサーベースの装置・機器を、従来の製造システム、産業用アプリケーションや命令・制御・監視システムと統合する必要がある。

組織がデータを管理し、示唆を出し、意思決定を自動化し、そのアルゴリズムとモデルを改良するためには、動画や画像の分析を専門とするデータサイエンティストやAI・機械学習のエンジニアが必要になる。データの取得、保存、交換、プライバシー保護や所有権に関する問題に対処するには、さらにほかの領域の専門家も必要になる。

ITプロジェクトマネジャーは、通常のマネジメントスキルやソフトスキルに加えて、デバイスのセキュリティー、運用プロセス、業務プロセス、変更管理やエンドユーザートレーニングに関する知識も必要になる場合がある。

CIOは、高度なスキルを持つ社内チームをゼロから構築するか、アウトソーシングするか検討する必要がある。既存のビジネス人材やテクノロジー人材をリスキル（再教育）するため、社内のコンピテンシーセンターやトレーニングアカデミーの設置や、そのアウトソーシングを検討する必要もある。

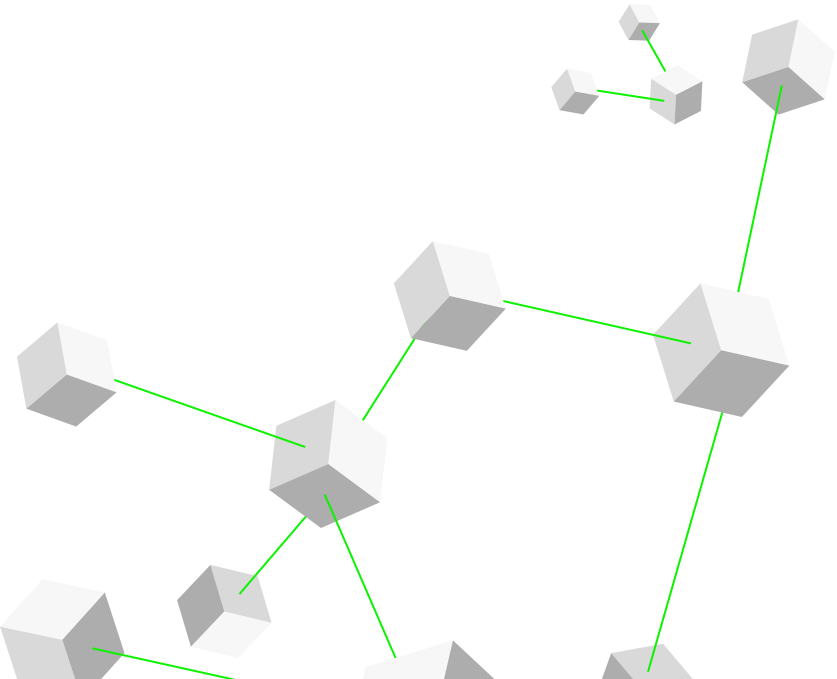
進むべき道

物理的な技術スタックの拡大は、企業が価値を創造し提供する方法を劇的に変える可能性を秘めている。ビジネス的な洞察や、人間と機械のやりとりを収益化する手段を得ることで、企業のビジネスモデルが進化する可能性がある。例えば、デバイスのモニタリングとメンテナンスのサービスを、デバイス販売時にas-a-serviceとして付加する、顧客が使い切れなかった容量を売り戻す共有資産モデルを開発する、プリンターカートリッジなどの消耗品を、センサーを使って自動的に再注文するプログラムを開発する、リセラーモデルからD2C（ダイレクトツーカスタマー）モデルに拡大する、あるいはデバイスのデータをマネタイズする、といったことが考えられる。

ビジネスリーダーは、さまざまなビジネス分野における物理的な技術スタックの影響を評価する必要があるであろう。特に安価なデバイスが多数ある場合には、デバイスが故障した際に交換することで、デバ

イスの管理とメンテナンスのコストが潜在的な利益を上回ってしまう可能性もあるため、ビジネスケースを慎重に検討する必要がある。

上記のようなセンサー内蔵のデータドリブン資産は、多くの場合、ビジネスに不可欠であるため、IT部門は最高レベルの耐障害性を確保する必要がある。また、ワイヤレスネットワーク機能とエッジコンピューティング機能をアップグレードして、厳しいレイテンシーとスループットの要件を満たし、新しいデバイスに適用可能な資産管理とガバナンスに精通する必要がある。そして、そのためにも、CIOはテクノロジー組織の編成、定義、管理やトレーニングの方法を再検討する必要がある。必要な技術スキルを見つけるには、CIOは既存の人材をリスキルするか、新しいテクノロジー人材を採用するか、必要なスキルをアウトソースするかを検討しなくてはならない。



最前線からの学び

不可能はない：IoTを通じた航空業界におけるデータ利活用の方法

カスタマーサービスに特に注力していることで知られているSouthwest Airlinesは、チケットの購入、チェックイン、搭乗に関する顧客取引データを長年にわたって収集し、カスタマーエクスペリエンスを継続的に向上させ、業務プロセスを改善してきた。しかし、取引データをつなぎ合わせていくうちに、データの欠落があることが分かった。多くのやりとりが取引システムの外で行われていたため、それらがログに記録されず、測定できなかったことが原因である。

このデータの欠落を解決するため、SouthwestはIoTのテストを開始した。Southwestは最初に航空機のターンタイム（乗客の降機から、次の便の出発準備、乗客の搭乗完了までの時間）を改善する取り組みを実施した。Southwestは、航空機の搭乗時間を短縮するために、7年前から搭乗口でビデオカメラとコンピュータービジョンを使用する取り組みを顧客のプライバシー確保に留意しながら試験的に行ってきた。それ以来、Southwestは乗客のカスタマーエクスペリエンスを改善するために、資産活用および運行管理、運用と保守などのIoTのテストを続けている。旅客輸送の分野では、SouthwestはBluetoothとWi-Fiビーコンを使い、空港での乗客の混雑具合を確認することで保安検査の待ち時間を見積もるテストを行った。テスト中、Southwestのモバイルアプリケーションで顧客がこのサービスを選択すると、空港内を移動するユーザーの携帯電話に対してシステムから信号が送られる仕組みになっている。

これは、高度な機械学習と物理インフラを組み合わせることで、これまで非実用的だったアプリケーションの展開が促進されることを浮き彫りにしている。しかし、Justin Bundick（Director of data science and automation）によると、この傾向は、新しいユースケースを可能にするだけでなく、稼働時間と信頼性の向上に加えて、新しいスキルも必要とする、拡大する物理インフラの管理にも役立つという[13]。

Bundickによると、IoTインフラを構築する上で最も重要な課題の1つは、「多対多の関係」の複雑さを管理することだという。従来のITインフラは、多様なユースケースをサポートするために、さまざまな物理デバイスやアルゴリズムを補完する必要があったが、それはIoTインフラにも当てはまる。「同一モジュール内に複数の機

能が含まれていないこと、スケーラビリティーがあること、適切なITインフラプロバイダーと提携して耐障害性を備えていることを確認する必要がある」とBundickは述べている[14]。

Southwestのチームにとってもう1つの重要な発見は、テストに関するものだ。開発者はどこからでもシステムを修正することができるが、特に空港などのセキュリティーの高い環境では、物理的なインフラの修復はより複雑になる。そのため、SouthwestがIoTインフラを製品化するには、堅牢で信頼性の高いものでなければならない。「実際の環境でテストを行うことにより、特定のソリューションの実行可能性についてより多くの情報を得られるとともに、重要な洞察を得てリスクを理解することもできる」とKevin Kleist（Emerging trends advisor）は述べている[15]。

IoTを適切なものにするには、さまざまな人材とスキルセットが必要である。設備導入のためには設備エンジニアが必要であり、物理デバイス特有の脆弱性を緩和するにはサイバーセキュリティーの専門家が必要である。さらに、Bundickが指摘するように「IoTデバイスによって生成されるデータは、それを分析するデータサイエンティストがいない限り、膨大な量のビットとバイトにすぎない」ことを忘れてはならない。

Angela Marano（Managing director of business transformation）は、独自の価値を付加できる分野と、ベンダーと提携する意味がある分野を評価することが重要であったと述べている。チームが新しい問題を解決する必要がある場合、彼女は市販の製品よりも優れたものを作るためにどのようなスキル、データ、または能力が必要かを評価する。市販の製品よりも優れた独自の価値を付与できる場合もあれば、既存のソリューションを使用する方が有利な場合もあるからだ。

「今日、我々は冒険と実利の健全なバランスを保っている。つまり、新規のソリューションはビジネスに本当に寄与しているのかを問い続け、我々の真の競争優位性がどこにあるのかを確実に理解する必要がある」とMaranoは述べている[16]。

ドローンは電気インフラの検査に革命をもたらす

SCE（Southern California Edison）はドローンを使って電力インフラを検査するパイオニアである。約50,000平方マイルの供給区域において、電柱、電線、鉄塔、変圧器、そのほかの配電および伝送構造物の点検にドローンを使用する。ヘリコプターよりも安全かつ軽量で、操縦性が高く、コスト効率に優れたドローンは、特に山火事の危険性が高いと考えられている地域で、SCEの作業員が検査を迅速化し、より正確なデータを収集することに役立つ。

2021年には、山火事の危険にさらされている地域にある約200,000棟の建造物のうち75%がドローンを使用した検査を受けており、前年と比べて25%増加している。これはドローンが、より徹底的で、より迅速で、より正確な検査を可能にする能力を備えているためである。「ヘリコプターに比べて、ドローンは構造物に近づいて、さまざまな角度や視点から

写真を撮ることができる。ドローンの使用によって、より近くで多くの良い写真を撮ることができるため、潜在的な設備の問題、植生の危険性、そのほかの発火リスクの可視性が向上する」とVibhu Kaushik（Director of inspections）は述べている[17]。

加えて、「ドローンの使用により検査する建造物の数を加速度的に増やすことができる。ヘリコプターよりもコスト効率が高く、ドローンのパイロットを雇うことや、ドローンを飛ばすために検査官を訓練することもより簡単である」とKaushikは述べている。

ドローン検査プログラムの急速な拡大は、SCEにさまざまな課題と機会をもたらした。例えば、当初、検査官はノートパソコンに画像を保存していたが、高解像度画像の数が急速に増加したため、ノートパソコンへの保存は不可能になった。ゆえにSCEはクラウドプラットフォームに移行し、2人のドローン作業員が現場で撮影した画像は直接クラウドに転送され、オフィスの検査官が閲覧、評価を行うようになった。

Kaushikのチームは現在、検査官自身がドローンを飛ばせるように訓練する新たなプロセスをテストしている。ドローン検査チームが検査を行う際、画像はクラウドに保存され、タブレット端末を活用して現場で評価される。ドローンの飛行はGPS座標を使ってあらかじめプログラムされているため、検査官は画像の評価に集中できる。

収集される画像の膨大な件数そのものが、さらなる課題をもたらす。SCEの供給区域には、約1,400,000本の配線柱と140,000本の伝送構造物があり、検査には各構造物につき10〜12枚の画像が必要になる。より大きな送信塔を検査するには、400〜600枚の画像を収集する必要がある。「長期的に考えると、すべての画像を人間の検査官により評価し続けることは難しい」とKaushikは述べている。

この画像収集および評価の課題を解消するため、SCEはAIモデルの開発・訓練を行っており、電柱、絶縁体、変圧器などの構造物の欠陥を検知し、修復が必要な構造物を自動的に特定できるように、AIモデルに数千枚の写真を学習させている。このAIモデルは、まず検査画像の評価を行い、異常が検出された場合に人間の検査官に通知する。「人間の検査官は、何百万枚もの画像を検査することなく、欠陥、あるいはその可能性があると特定された画像に優先順位をつけることができる。これによって、より迅速に欠陥を見つけて修復できるようになる」とKaushikは説明する。

Kaushikによると、SCEのAIモデルが成熟するにつれ、欠陥を検知する精度は向上している。

また顧客の認知度と受け入れ態勢の確立も、ドローン検査の課題だった。SCEは包括的なコミュニティー支援プログラムを開発し、地域の法執行機関と協力してコミュニティーメンバーの教育と情報提供を実施した。「我々はブランディングがいかに重要であるかも認識した。SCEとの関連が明確でない場合、なかなか受け入れてもらえないが、我々がSCE

ブランドを活用し、地域社会の意識を高めるために積極的に働きかけると、人々は概して前向きに受け入れてくれるようになる」とKaushikは述べている。

SCEは今後、ダムやそのほかの発電構造物の検査や、損傷調査、修理検査においてメンテナンスや修理を行う作業員の補助にもドローン活用を拡大していく。「SCEはドローンを使って送電網の回復力、安全性、効率性を改善することに取り組んでいる。ドローンやスマートセンサーなどの技術は、脱炭素化、分散化、非中央集権化、および自動化された未来のエネルギーグリッドの開発を支援していく」とKaushikは述べている。

Sheba Medical Centerが打ち立てるスマート病院の標準

イスラエルのSheba Medical Centerは、スマートデバイスやそのほかのデジタル技術の活用などが成果を上げ、長年にわたり世界で最も優れた病院に位置づけられている[18]。毎年200万人近くの患者が治療を受ける、ラマトガンに本拠を置く医療センターでは、Shebaの臨床医と医療スタートアップのための、75の研究ラボおよびARC（Accelerate、Redesign、Collaborate）イノベーションプログラムが提供されている。

患者のケアを改善するために、Shebaはセンサーやカメラを活用した遠隔医療、CTスキャンを診断するためのAIなど、さまざまな医療分野におけるイノベーションをリードしている[19]。例えば、多くのスマート病院の医師が医療機器からの通知の多さに圧倒される「アラート疲れ」に対処している一方で、Shebaは医療スタッフの注意を妨げずに品質、安全性、および効率の向上を実現する技術の統合アプローチを開発した。ShebaのChief Innovation Officerであるeyal Zimlichman博士は、「スマート病院は医師の自律性を奪うためではなく、医師のより効果的な業務遂行を支援するためにAIとスマートデバイスを活用するべきだ」と述べる[20]。

Shebaは、不確実性の高いデータ集約型の環境において、医師が複雑で重大な患者の問題に対処することを支援するため、集中治療室（ICU）におけるAIベースの意思決定支援を提供している。動脈血圧センサーなどのICUにおける患者用センサーが生成した大量のデータをShebaのAIプラットフォームが分析し、治療に関する重要な警告や提案を医師に提供する。リスクの高い環境では、適切な洞察がなければ多くの間違いを犯しかねない。「ICUにおけるあらゆる意思決定は、患者の健康と病院の効率性に大きな影響を与える可能性があるため、我々はICUのリスク改善に意思決定支援を集中させている」と

Zimlichmanは述べる。

また同医療センターは、業務上の課題対処にもAIと病院機器からのデータを活用している。どの病院でも、管理者は業務と患者の流れを監督する必要があるが、意思決定はデータに基づいていないことが多い。Shebaのチームはいくつかのスタートアップと連携し、患者のベッドからのリアルタイムデータを使用して、病床割り当てと患者配置の効率を最大化するコントロールタワーアプリケーションを構築している。また、チームは慢性疾患の患者を観察するため、スマートウォッチなどのウエアラブル技術を活用した継続的ケアのアプリケーション開発にも取り組んでいる。「患者のニーズに合ったデジタル環境を構築することで、従来の方法を補完するとともに、入院を減らすことができる」とZimlichmanは述べる。

現在、ARCのチームは、切開の場所が適切か、出血が安全基準値を越えていないかを執刀中の外科医に知らせる、AIを活用した映像分析機能の開発に取り組んでいる。技術が進歩すると、将来的には手術ロボットが患者の腹部を開くといった（比較的）簡単な処置から始め、いずれは単独で手術を行うようになるだろう。Zimlichmanは、10年から20年以内に最も複雑な外科的処置や遠隔手術をロボットが執刀できるようになると考えている。「将来的に、飛行機のオートパイロットのように、ロボットが外科手術の95%を完了させ、外科医がその監視と、残りの5%の執刀を行うようになるだろう」とZimlichmanは述べる。

現在、医療費の多くが病院から発生しているが、病院は技術の進歩によって高度化し、効率性と安全性を向上できることをShebaは証明した。Zimlichmanによると、テクノロジーのさらなる進展に伴い、医師による治療のほとんどが病院外でできるようになるため、病院の役割は小さくなり、物理的にも縮小する可能性がある。「COVID-19は病院の変革を加速させており、我々は生きている間にその新しい姿を見ることができるであろう」とZimlichmanは述べる。

私の見解

Brad Chedister

Chief technology and innovation officer, DEFENSEWERX

より優れた新サービス・新製品を提供するため、組織におけるコネクテッドデバイスへの依存は高まりつつあり、無人航空機システム（UAS）を利用した配達や鉄道の点検、偵察などが行われるようになっている。

工場やファストフード店から、病院や防衛機関に至るまで、ロボットを活用したプロセスの自動化により、効率と品質を改善している。しかし、スマートでコネクテッド、かつ自動化された組織の時代において、人間がハードウエアよりも重要であることを我々は決して忘れてはならない。

私の組織の技術開発と技術革新の取り組みは、防衛機関による困難な問題の解決を支援するために設計されている。我々はアメリカ各地でいくつかのイノベーションハブを運営し、国を守るためのソリューション開発に役立つイノベー

ションエコシステムの形成を進めている。私の仕事では、組織がデータとデバイスに依存するようになるにつれ、人と技術が交わるところでしばしば問題が発生する。

例えば、レガシーシステムとプロセスの専門知識を持つ人々が新しい技術と新しい働き方に移行しなければならない場合、人材開発はいうまでもなく重要だが、時にはカルチャーの転換が必要な場合もある。イノベーションの取り組みを展開する際、「こういった理由でできない」という否定的な気持ちから入る人もいるかもしれない。例えば、レガシーシステムとの相互運用性がないため、または導入と実装に時間がかかりすぎるため、それはできない、といったことである。

私はチームに対して、彼らの思考プロセスを「こういった理由でできない」から「もしできるとしたら」へシフトすることを勧めている。例えば、夢のような話かもしれないが、85,000以上のイノベーションから成るエコシステムをふるいにかけて、戦闘機に関する問題を解決するための革新的なツールを発見できるような、自動CRMツールを開発できるとしたらどうだろうか。「もしできるとしたら」という思考プロセスとカルチャーがなければ、スマートな自動化ツールとシステムが出発点を越えることはおそらくないであろう。

このようなカルチャーの変化は、組織がイノベーターになるために必要な技術的スキルを備えた人材を見つけ、採用する一助になる。組織は、単に関連性を維持するだけでなく、UASやそのほかの無人機、ロボット工学、センサー、AIと機械学習、データ分析、そのほかの鍵となる技術に携わる人材を引き付ける必要がある。

人と技術に関連するもう1つの課題、特に民間企業における自動化とロボティクスに関する課題は、技術が人の仕事を奪うという考え方である。防衛産業で最も重要な資産は戦闘員であり、装備や技術ではない。そのため、我々は人を守るために技術を利用することに重点を置くのである。

例えば、UASを使用して未知の領域を偵察する場合、兵士に危害が及ばないようにする機能がある。諜報・監視・偵察ソフトウエアと短波赤外線画像機能を備えたUASは、人間の10倍の距離を「見る」ことができる。同様に、企業は従来は人間が行っていた危険な任務を、スマートデバイスや自動化を活用して達成する方法を検討することができ、その過程で効率化やそのほかの改善も実現する可能性が高い。

民間部門であろうと公共部門であろうと、いくつかの活動は本質的に人間的なものである。信頼と思いやりを必要とするタスクには個人的な交流が必要であり、決してAIやロボットに取って代わられることはない。しかし、職場をより安全で効率的にすることに役立つ限り、タスクを自動化しシステムをロボット化する傾向が鈍化することはないであろう。

今後の展望

ストラテジー

テクノロジーを活用したカスタマーエクスペリエンスに対するCEOの関心は高まっており、その実現においてはIT機能と物理的なテクノロジーの統合がますます重要となる。物理的なテクノロジーには、耐障害性についてこれまでとは異なる基準が求められる。例えば、自動運転車の停止や故障が乗客や通行人に深刻な危険をもたらす可能性があることはその良い例である。特に人間の安全が最優先される分野において、CEOは、各担当チームが新しい物理的なテクノロジーの活用に際して求められる基準を満たす能力を有しているかどうか検証すべきである。また、IT部門のリーダーと協力し、物理的なテクノロジーを活用する際は顧客の利便性に加えて、安全性やセキュリティーを優先する文化を確立していくことも重要である。

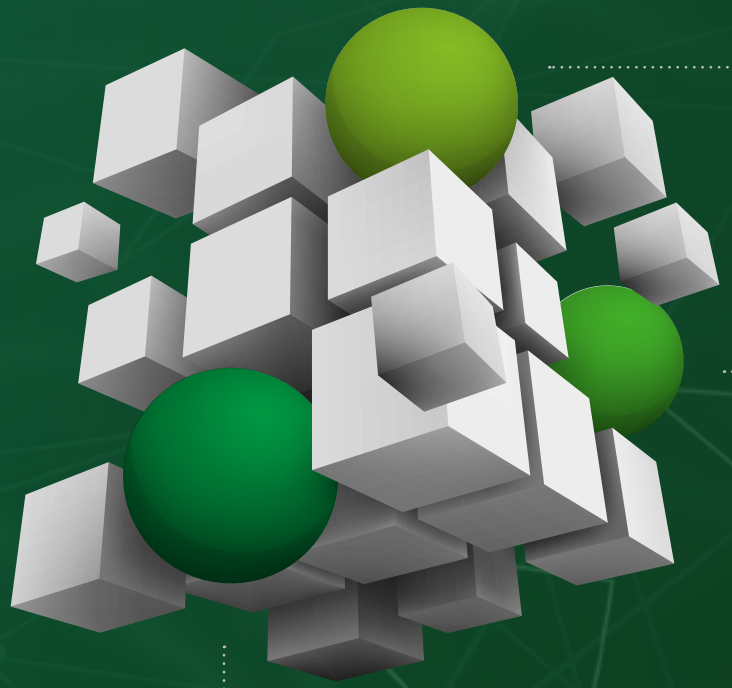
ファイナンス

スマートデバイスの重要性が高まってきたことにより、IT部門はかつてないほど多様なデバイスを管理している。CFOはこの機会に、障害やセキュリティー違反が発生した場合のレピュテーションや株主価値への潜在的な損害を含め、コスト面での影響やリスクエクスポージャーの変化を確認すべきである。また、CFOは、IT部門がリスク、コンプライアンス、そのほかの部門と部門横断的に連携することも支援できる。さらには、ソフトウエア、ハードウエア、物理的なテクノロジーの適切な予算水準を把握するために投資状況を確認することも有効であろう。

リスク

コネクテッドデバイスや5Gネットワークのようなイネーブラーは多くの注目を集めているが、それらの多面的なセキュリティー要件の詳細はまだ定義されていない。医療機器や工場のロボットなど、物理的なテクノロジーの重要性が高まるにつれて、障害発生時のリスクは劇的に上昇している。CROは、IT部門やビジネス部門と協力して、潜在的なセキュリティー上の懸念とそれに対応するリスク要件を特定しておくべきである。また、CEOやCIOと協力して、信頼性を重要視するリスク管理の文化を醸成することも重要であろう。

さあ、はじめよう



要点

1 新世代のコネクテッドデバイスと物理資産の保守に必要な稼働時間、冗長性、セキュリティーを提供するためには、どのようにテクノロジーインフラを強化すればよいか。

2 複雑さを増す多数の物理資産の管理には、どのような規制やコンプライアンス要件が影響を与えうるのか。

3 複雑かつ多様な接続デバイスを管理・保守・保護するために、組織はどのようなスキルセットを必要とするのか。組織はそれらのスキルセットを保有しているか。保有していない場合には、どのようにスキルを獲得するか。

執筆者

Peter Liu
Unmanned Aerial Systems (UAS) and Counter-UAS (CUAS) technologies leader
Deloitte Consulting LLP
peteliu@deloitte.com

Robert Schmid
Internet of Things practice leader
Deloitte Consulting LLP
roschmid@deloitte.com

Sandeep Sharma, PhD
Deputy chief technology officer
Deloitte Consulting LLP
sandeepksharma@deloitte.com

SENIOR CONTRIBUTORS

Brian Greenberg
Principal,
Deloitte Consulting LLP

Britta Mittlefehldt
Director,
Deloitte Consulting GmbH

Tim Paridaens
Partner,
Deloitte Belgium CVBA

Andreas Staffen
Partner,
Deloitte Consulting GmbH

Thierry Cazenave
Senior manager,
Deloitte France

Gabriel Goïc
Senior manager,
Deloitte France

Adam Niedbała
Manager,
Deloitte Poland

Hugo Araujo
Senior consultant,
Deloitte MCS Limited

Nigel Forlemu
Consultant,
Deloitte MCS Limited

参考文献

1. Gartner, *Market guide for edge computing solutions for industrial IoT*, accessed November 17, 2021.
2. Phil Marshall and Philippe Cases, *Enabling the connected vehicle market to thrive*, Topio Networks, accessed November 17, 2021.
3. Jack Fritz et al., *Accelerating enterprise innovation and transformation with 5G and Wi-Fi 6*, Deloitte Insights, March 22, 2021.
4. Intel, *The edge outlook*, accessed November 17, 2021.
5. Thomas Bittman, Bob Gill, Tim Zimmerman, Ted Friedman, Neil MacDonald, Karen Brown, *Predicts 2022: The Distributed Enterprise Drives Computing to the Edge*, Gartner, October 20, 2021.
6. The Linux Foundation, *State of the Edge 2021: A Market and Ecosystem Report for Edge Computing*, 2021.
7. Jaclyn Diaz, "U.S. announces new rules for drones and their operators," *NPR*, December 29, 2020.
8. IIHS, "Autonomous vehicle laws," accessed November 17, 2021.
9. University College London, "Guidance note on the use of images and videos under data protection law," accessed November 17, 2021.
10. Mary Shacklett, "IoT projects demand new skills from IT project managers," TechRepublic, July 14, 2021.
11. Palo Alto Networks, *2020 Unit 42 IoT threat report*, March 10, 2020.
12. Internet of Business, "Security researchers find backdoor in Chinese IoT devices," accessed November 17, 2021.
13. Justin Bundick (director of data science and automation, Southwest), interview, September 8, 2021.
14. Ibid.
15. Kevin Kleist (emerging trends advisor, Southwest), interview, September 8, 2021.
16. Angela Marano (managing director of business transformation, Southwest), interview, September 8, 2021.
17. Vibhu Kaushik (director of inspections, Southern California Edison), phone interview with authors, October 22, 2021.
18. *Newsweek* editors, "The top 10 hospitals in the world," *Newsweek*, March 6, 2020.
19. Sheba Medical Center in Israel, "ARC – The center for digital innovation at Sheba Medical Center," accessed November 20, 2021.
20. Dr. Eyal Zimlichman (chief innovation officer at Sheba Medical Center), phone interview, November 11, 2021.

日本のコンサルタントの見解

本編でも紹介したように、スマートフォンを始めとする端末はますます賢くなり、種類や利用方法も多様化している。その状況に追随するべく、端末そのものの管理、IoTを始めとする各種デバイスから生み出される膨大なデータの管理、セキュリティー管理などのガバナンスが求められているのは、日本でも同様といえる。

従来は、デバイスが取得したデータをインターネット経由でクラウド環境に転送し、クラウド側で集中的に処理していた。最近では、取得したデータをクラウド環境に送らずにできるだけデバイス側で処理するエッジコンピューティングが登場している。さらには、デバイス上にAIモデルを組み込み、デバイス上でAIモデルを用いた予測まで実施する「エッジAI」が注目されている。

エッジAIとは

エッジAIが注目されている背景について、簡単に触れておきたい。IoTの普及により、これまでは取得困難であったさまざまなデータを取得することが可能となった。一方、データ量が指数関数的に増加することに起因して、膨大なデータ量を集中処理することに伴う分析パフォーマンスの低下、および膨大なデータをクラウド環境へ転送することによる通信コストの増加が課題として浮き彫りになってきている。

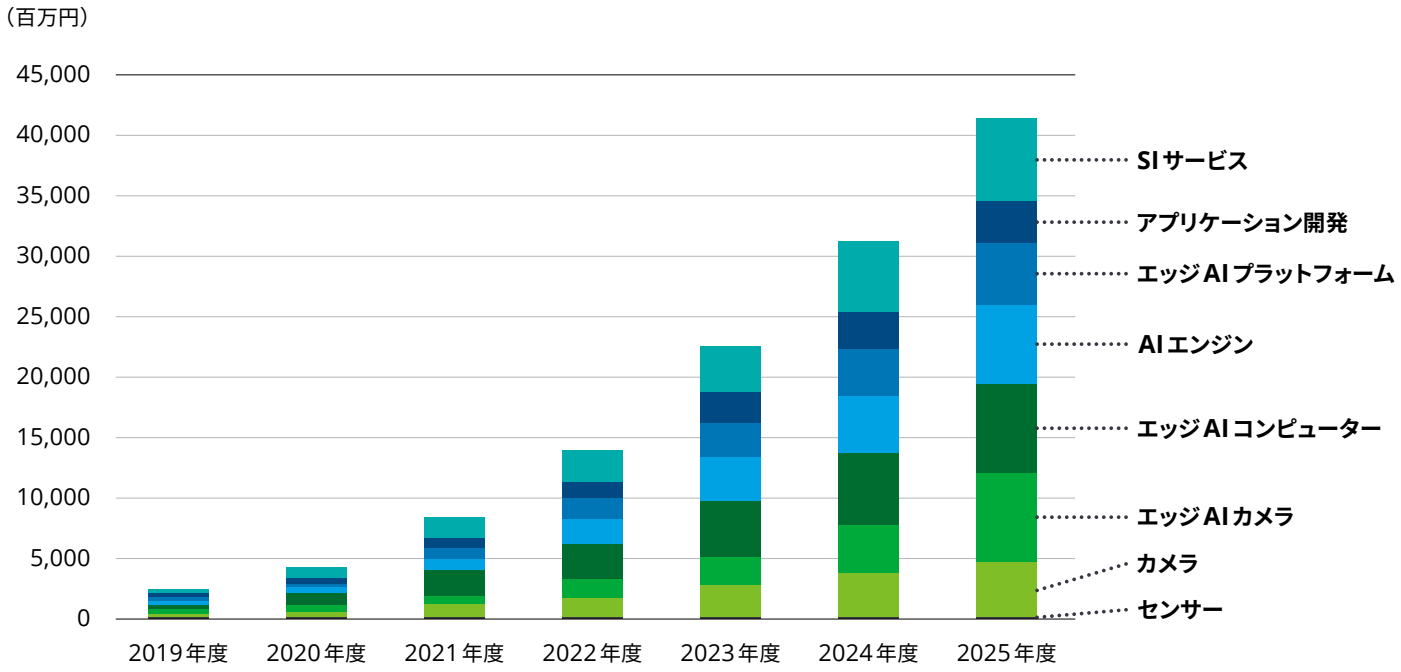
デバイス上にAIモデルを組み込み、デバイス上でデータを処理することで、クラウド環境へのデータ転送が不要となり、リアルタイムに近いレスポンスの実現が可能となった。また、クラウド環境へ転送するデータ量の削減により通信コストを削減しつつ、ハッキングなどのセキュリティーリスクも低減されることになった。そのほかにも、クラウド環境でシステム障害が発生した際も、デバイス側で処理をしているため、影響を受けにくくなるなどのメリットもあり、注目を集める要因になっている。

エッジAIの市場規模

デロイト トーマツ ミック経済研究所の調査によると、エッジAIに関連するソリューションの市場規模について、2020年度は43億円弱と市場規模が小さかったが、2022年度からは本格的に立ち上がり、2025年度には約10倍の413億円規模にまで拡大すると予想している[1]。特に、エッジAIカメラは年平均成長率95.8%と最も高い成長率が見込まれている。最近ではエッジAIカメラを利用して、病院や店舗の混雑状況を可視化するソリューションが出始めている。

また、デロイトが発刊している「TMT Predictions 2022」では、2022年に世界で3億2,000万台の消費者向け健康・ウェルネスウエアラブル機器が出荷され、2024年にはその数が4億4,000万台に達するだろうと予測している[2]。センサーとAIの進歩により、これらの機器は手首や1円玉サイズのパッチに装着できるほど小さくなり、急成長を見せている。

図1. エッジAIソリューションの市場規模推移



出所：デロイト トーマツ ミック研究所の独自調査・予測

エッジAIがもたらす将来像

エッジAIの実用化に向けて、様々な分野で研究や取り組みが実施されている。最も期待されている分野の1つが自動運転であろう。車両に搭載したカメラやセンサーを用いて歩行者、周辺車両、標識などの構造物を認識すること、車線変更や合流などで車両同士が協調することや、リアルタイムに高精度な状況判断をすることが必要となる。まだ取り組み段階のため、事故などのネガティブなニュースが先行してしまっているが、本技術が確立することで、新たな世界観をもたらしてくれる。MaaS（Mobility as a Service）が代表的なところであろう。利用者の好きなところで乗って降りることができるオンデマンド交通サービスや自動運転する店舗型車両をスマートフォンで自宅や職場に呼ぶ購買サービスなど、様々な新しいサービスが検討されている。

医療分野も大きく期待されている分野の1つである。病院でさまざまな検査を受けることができるが、検査機器にAIデバイスを搭載することで、熟練の医師

でも診断が難しい症例を検査しながらAIで予測し、的中率の向上を図ることが可能になる。また、医師や検査技師の負荷を軽減することで、ヒューマンエラーによる医療事故の防止にもつながっていく。すでに医療現場におけるAI活用は始まっており、例えば、AIと画像認識を組み合わせた早期がんの検出が挙げられる。このAI技術を内視鏡カメラと組み合わせた内視鏡検査AIも登場してきている。

以上の2分野からも分かるように、エッジAIがさまざまなシーンで活用されることで利便性や信頼性が向上し、我々の生活スタイルは大きく変わっていくことであろう。

日本企業での取り組み状況

上記では、エッジAIの展開状況とその展望について述べた。では日本での取り組みはどのような状況だろうか。残念ながらこのテクノロジーをフル活用して業務に活かしている企業はまだごく少数である。その中でも先進的な取り組みを行っている事例をいくつか紹介しよう。

エッジAIの代表的なユースケースの1つがスマートファクトリーである。これを体現しているのが電機製造企業のA社だ。同社の工場ではエッジAIを利用した外観異常のリアルタイム判定を実現している。部品や製品の外観を目視してチェックする検査工程は熟練者の技術への依存度が高くノウハウの継承が喫緊の課題だったが、熟練者の技術に相当するチェックをAIで行う。同社は実証実験の中で、作業ミスの見逃し“0”化とともに、製造工程全体の作業時間を15%削減する効果を確認したという。

また大手総合化学メーカーB社では、生産現場のDXを行い撹拌機の異常予兆検知、火力発電所の破断予兆検知、動力プラントにおける異常予兆検知など、数々のエッジAIのユースケースを実現している。同社では、生産部門にDXチームを配置し現場業務に精通した担当者が改革を推進することで効果的なデジタル活用を狙ってきた。トライアル＆エラーを重ねることによりエッジAIをはじめとしたデジタル技術活用のノウハウが現場に蓄積しており、今後も改革の加速が期待される。

エッジAIの活用の可能性は製造現場だけではない。顧客が訪れる店舗や町中においても、エッジAIを活用した世界観は広がりつつある。

小売C社では、エッジAIによる顧客体験の工場を体現している。店舗内に設置したネットワークカメラで撮影した画像をAIで処理し、来店者の性別・年代といった属性、消費者の行動パターンを分析し、商品の前にとどまる滞在時間をその商品への興味指数として捉える。出品者であるメーカーはこのような情報を把握し、顧客からの生のフィードバックを受取り、製品開発やマーケティング、広告戦略などに役立てることができる。またD社では、ポストコロナ時代や人手不足社会にも柔軟に対応できる魅力あるまちづくりを推進するため、大手町・丸の内・有楽町エリア（以下、丸の内エリア）を舞台にエッジAIの活用を進めている。同社は次世代カメラシステムを導入し、混雑状況の把握・対応、会員施設などでの顔認証チェックイン、通行人の見守り、刃物などの異常検知などの実現を推進している。

医療業界においてもエッジAIの取り組みは広がっている。通信企業E社は、エッジAIを活用した遠隔医療の実証実験を行っている。医師や看護師による遠隔モニタリングのほか、患者容体悪化の兆候検知の実現を見据えている。

このように国内でも生産部門や医療、小売りなど様々な領域・ユースケースでエッジAIの世界観が広がりつつあることが分かるであろう。

以上のように、エッジAIの先端性と取り組み事例について紹介してきた。最後に、リスクについても触れておかなければならない。

まず、AIの特性上異なる環境や条件下で学習をすると、端末によって異なる振る舞いをすることがある。これはAIが導き出した根拠が一見すると分からないことが原因で、一般的に「ブラックボックス問題」と称されるものである。これがどういう問題を引き起こすかというと、人間が望んでいる振る舞いをエッジAIがしてくれない可能性があるということである。端末が多くなればなるほど蓄積されるデータも膨大になり、ブラックボックス化した端末が増えることが考えられる。

次に、エッジAIの利活用に関する倫理性である。エッジAIは自らが置かれた環境に順応すべく学習する上に、大量生産が可能なため、例えば軍需産業におけるロボット兵器などに悪用されると、特に紛争地帯で甚大な被害が予想される。AIや機械学習をロボット兵器に活用しないとする国際的な枠組みはすでに何年も前から存在しているが、批准していない国々やそれを破って秘密裏に開発している国も、一般的に考えてないとはいえないかもしれない。

最後に、エッジAIを最終的に管理するのは人間だということを忘れてはいけない。先に挙げたブラックボックス問題やロボット兵器の転用も、人間が適切に管理していれば平和利用が可能になる。また、エッジAIから生み出される膨大なデータも緻密に管理する必要がある。エッジAI任せにするのではなく、その使い方からアルゴリズムの設計、データの管理に至るまで、人間がしっかり関与することがこれからの時代は特に重要になってくるであろう。

ますます賢くなったデバイスのガバナンスについて、現状の国内企業の状況はどうだろうか。全体観としては、基本となるデバイスの台帳の整備から必要なケースが多い。例えば工場においては、経理的な資産管理はなされているものの、ガバナンスを目的としたデバイス管理がなされているところはまだ少ない。上記で触れたようなリスクを回避し、エッジAIがビジネスにもたらす効果を享受するには、まずは基本的な資産管理から始めることが必要である。

執筆者

田中 大地　シニアマネジャー
Technology Strategy & Transformation

外資系ITメーカーを経て現職。金融・消費財業界を中心に、経営統合、グローバルITガバナンス立案、グローバルロールアウトなど、多数のグローバルプロジェクトをビジネスとITの両面から手がけている。

四ッ家 昭胤　マネジャー
Technology Strategy & Transformation

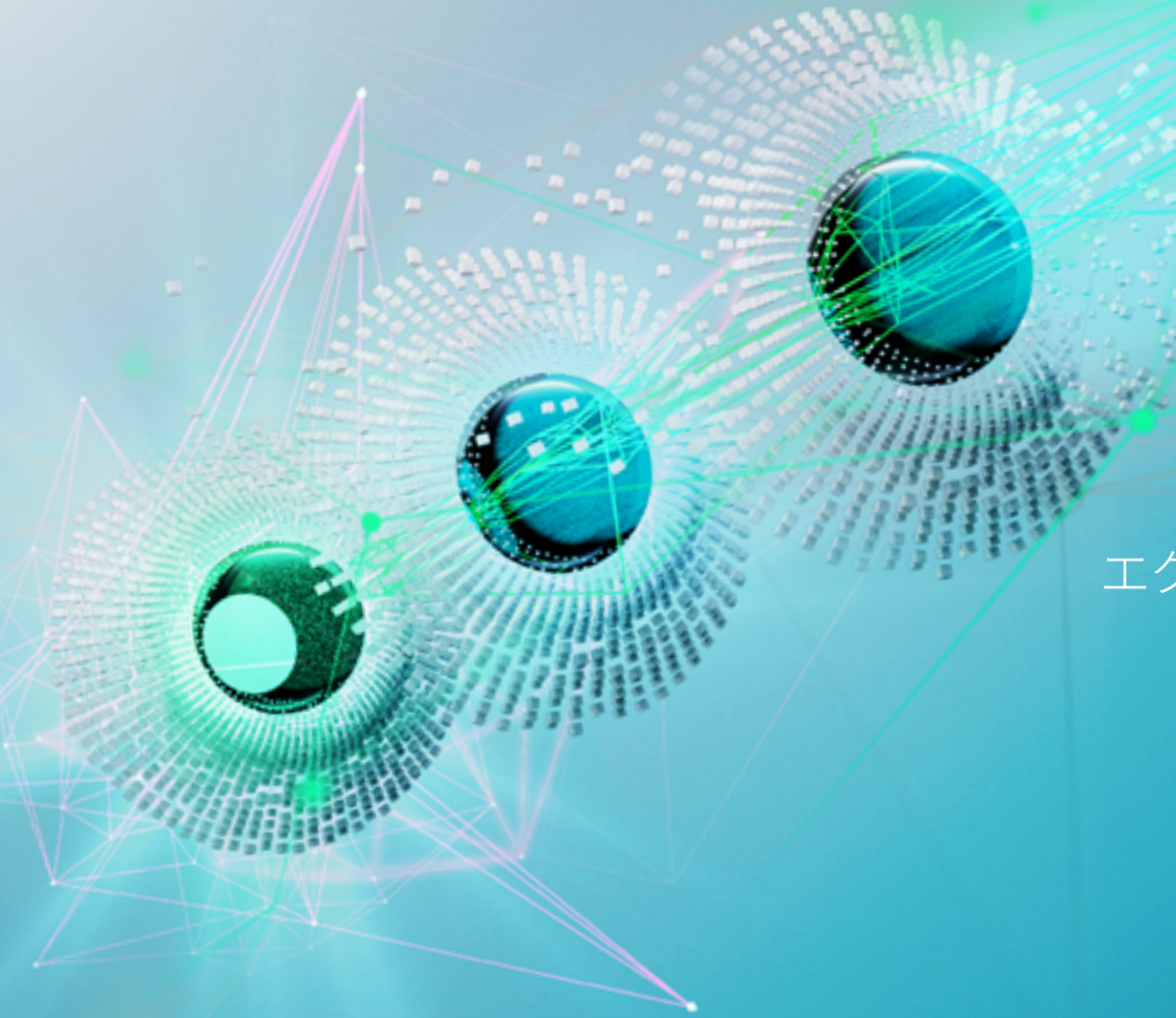
独立系SIer、ユーザー系SIerを経て現職。損保、証券、資源・エネルギー系の大手企業向けに、BPR、IT戦略立案支援、および基幹システム刷新・構築プロジェクトを数多く経験。ICT知見、プロジェクトマネジメント領域に強みを持つ。

石川 智美　シニアコンサルタント
Technology Strategy & Transformation

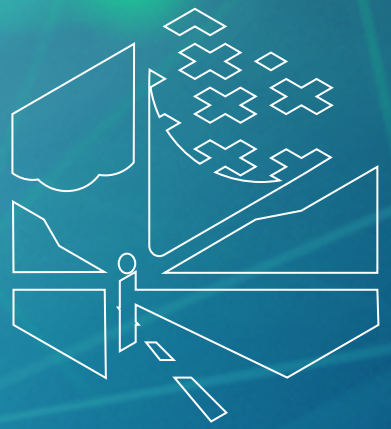
事業会社のIT企画部門を経て現職。IT／デジタルトランスフォーメーション戦略策定、IT組織設計を中心としたアドバイザリーに従事。

参考文献

1. デロイト トーマツ ミック経済研究所, “エッジAIコンピューティング市場の実態と将来展望 2021年度版,” November 30, 2021.
2. Deloitte Insights, “TMT Predictions 2022,” accessed February 16, 2022.



未来のフィールドノート



「量子」の展望

「量子」は今後10年で研究段階から実用化へ

エクスポネンシャルインテリジェンス：もう一度、AIに感性を込めよう

AIが人間の感性を理解する

アンビエントエクスペリエンス：スクリーンを超えた日常

誰でもどこでも使えるテクノロジー

トレンド7

未来のフィールドノート

今後注目すべき3つのテクノロジー

グローバルにエンタープライズテクノロジーが紡ぎだす領域においては、楽観的な意見が多数派だ。我々は、動きの速いイノベーションや、それによって引き起こされている破壊的な変化に期待を膨らませている。テクノロジーの進化に対して、我々は揺るぎない確信を持ってきたといえる。それはまるで、小さなどんぐりから大きな樫の木に育つように、この好意的な捉え方は拡大していくであろう。

このたとえには、将来の成果を楽観的に過大評価してしまうという問題がある。AIの急速な進化により、5年後には魅力的な新しいビジネスモデルが生み出されるはずだという期待は、次の四半期報告書に頭を悩ませているCFOにとっては、何の慰めにもならないであろう。

多くのリーダー、ストラテジスト、そして技術者たちが、「内容や実現時期が不確実な出来事に対して、今どのようなことができるのか」と疑問に思うことは当然だ。今後10年の間に多くの新しいテクノロジーが登場し、何か驚くような発展を遂げるということは、現実的にあり得ることだ。実際にどのようなことが起こるかは、もちろん誰も知ることはできない。しかし、この「*Tech Trends 2022*」の最終章では、現時点では小さな兆しに留まるテクノロジーの可能性について、戦略的に検討するフレームワークを提供していく。

ここでは特に重要な、3つの可能性を紹介する。

- **量子技術**
  今後10年以内にコンピューティング、センシング、通信に変革をもたらす

- **エクスポネンシャルインテリジェンス**
  人間の感情や意図を理解する次世代AI技術である

- **アンビエントコンピューティング**
  職場や家庭環境など、生活のあらゆる場面においてテクノロジーが存在し、相互協調して動作する

末尾では、デロイト コンサルティングのChief futuristであるMike Bechtelが、過去を振り返り未来を瞥見する。

「量子」の展望

量子コンピューティングは急速に成熟しているものの、依然としていくつかの難解な問題が議論の的となっている。1つは、マヨナラフェルミオン粒子が存在するかの議論である。確かに、大半の人たちには関心事ではないが、研究者にとっては長年の論点であり議論が尽きていない。この議論における一方の陣営は、マヨナラフェルミオン粒子（理論的にはそれ自身の反粒子を含む）は、驚くほど安定した量子ビットを作ることができると主張しており（実在主義）、片や反駁側はマヨナラフェルミオン粒子が存在し有効である証拠は見つけることができていないとして、マヨナラフェルミオン粒子は量子力学上で存在する可能性のみである（実証主義）と反論している[1]。

ある意味、理論上の粒子をめぐるこの議論は、今日の量子コンピューティングの状況を要約しているともいえる。量子コンピューティングのすべては信じられないほど興味深く将来の展望を期待されているものの、いまだ発展の初期段階であり、実社会での活用へと至るには未解決の課題もあり見通しは立っていない。

しかし、これら量子力学上の問題がすべて解明した暁には、人類の未来に大きな影響を及ぼすことは疑いようがない。実際、量子力学の研究は加速しており、この10年以内に研究段階から商業利用に向けて発展していくことが期待される[2]。大手テクノロジー企業、政府機関、スタートアップなどが、飛躍的な進歩を目指し、数十億ドルを投じて競い合っている[3]。

重点的に取り組まれている分野：

- **コンピューティング**
  量子コンピューターは、高度な計算問題を解決するための特定の目的に特化したコンピューターである。その原理は、量子力学の現象を利用して情報を処理し、高度に専門化された計算を実現している。すなわち、量子コンピューターは従来のコンピューターの後継者ではなく、むしろ従来のコンピューターと共存し、複雑な計算に対して高度なコンピューティング能力を提供する形となるであろう[4]。量子コンピューターの可能性を示す最近の事例として、従来のスーパーコンピューターでは数千年かかるといわれてきた特殊な計算を、量子コンピューターが5分で完了させ話題となった[5]。

- **通信技術**
  量子通信は、量子力学の原理を利用し、傍受や盗聴が理論的に改ざんされない通信ネットワークを構築するハードウエアベースのソリューションである。セキュアな通信を実現する技術として、光ファイバー上で暗号鍵を交換するQKD（Quantum Key Distribution、量子鍵配送）がある。QKDは、当事者間で安全性の高い暗号化キーを交換して、光通信を介してデータを通信する技術である。QKDを実現する技術は発展の途上にあり、いくつかの量子コミュニケーションネットワークは実現されているものの、引き続き研究開発が進められている[6]。

- **センシング**
  素粒子の感度により、量子センシングデバイスは従来のセンシングデバイスより高い応答性と正確性を備えることができる。今後10年以内には、一部の応用分野において従来のセンシングデバイスを量子センサーが置き換える可能性がある。実際に、エネルギー、運輸、ヘルスケアなどの分野が有望なユースケースとなっている。量子センサーは利用可能であるが、現時点での利用場面は限られている。研究者たちは、より安く、より軽く、よりポータブルで、よりエネルギー効率の高いセンサーの実現に取り組んでいる[7]。

量子力学は気の遠くなるような課題を抱えているが、量子テクノロジーの進歩にともない、技術の細部にまで注目が集まるようになってきている。粒子を凍結するレーザーや宇宙よりも低い温度などについて考えないでいられる技術者がいるであろうか。同様に、量子テクノロジー企業の上場に対する投資熱を見逃すビジネス戦略家がいるであろうか。

新たな景色は5年の歩みで見えてくる

量子にまつわる議論の旅路において終着点は杳として知れないが、向かうべき方角は見出しつつあり、今後5年での歩みによって、より多くの新しい景色が見えてくるであろう。コンピューティング、通信技術、センシングから化学に至るまで、あらゆる領域が量子技術による最適化の恩恵を受けると予想される。さあ、今がその未来への第一歩を踏み出す時機だ。競争相手はすでに踏み出している。この機会を指をくわえて見ているだけで良いのであろうか。

エクスポネンシャルインテリジェンス：もう一度、AIに感性を込めよう

データマイニングの世界では、ビールとおむつにまつわる逸話が語り継がれている。スーパーマーケットの客の購買履歴を分析したところ、ビールをおむつの隣に並べると売上が伸びることが分かったという話だ。おむつとビールの売上にどのような関係があるのだろうか。あるデータサイエンティストの説によると、妻は仕事帰りの夫におむつを買ってくるように頼むそうだ。夫は、頼まれたおむつを手に取りながら、そのおむつを履いた小さな子どもの世話を想像しながら、ビールでも飲んで体の疲れを癒したいと思うのだという[8]。

子育てにはストレスがつきものだということはいうまでもないが、ここには重要な教訓が隠されている。機械的な売上分析が示唆するのは、おむつとビール

の間の売上の関係性までである。売上を左右する顧客の感情や心理を推測し説明する洞察力を備えるには、人間の脳が必要だ。言い換えれば、圧倒的な分析力のあるAIを使っても、これまでは統計的な関係性について*意味のあるもの*と*意味のないもの*を区別することができなかった。

今後10年間で、この状況は劇的に変化する可能性がある。以前の「*Tech Trends*」レポートでは、「感情コンピューティング」「感情AI」と称される新たな分野のAIソリューションが、テクノロジーのIQに対して感情指数（EQ）をどのようにして大幅に取り入れてきたのかを調査した[9]。今後10年間、イノベーターたちが次世代の深層学習技術を使ってAIモデルを訓練し、カリスマ性、魅力、感情といった人間の特徴を認識・模倣できるようにすることで、感情コンピューティングは変化し成長を続けるであろう。さらに、「シンボリック」や「コネクショニズム」技術を駆使して、AIや人工ニューラルネットワークに演繹的推論や論理的推論機能を組み込むようにもなるであろう。近い将来、これらの技術は統計的な相関関係を調べ、人間の脳と同じように、そこに意味があるのか、それとも本質的な意味を持たないデータのランダムな特徴に過ぎないかを判断できるようになるであろう。言い換えれば、機械は世界を、文脈のないゼロイチの集合体としてではなく、人間のようにより理にかなった形で理解することができるようになる。

ここからAIと人間の関係が変化していることが読み取れる。1950年代にAI分野が登場して以来、我々はこの興味深い技術について、何ができるのかと同じくらい何ができないのかを評価してきた。AIはデータから洞察を導出する能力を飛躍的に向上させてきたが、認知や感情については人間の優位性が疑いのないものだった。しかし、マシンのパワーと能力は指数関数的に向上している。現在研究者が設計しているAIは、開発の効率性と洞察力、すなわち人間らしい鋭い感性の実現に焦点が当てられている。

先駆的な研究者は現在、AIアプリケーションを、汎用性と細部へのこだわりが両立するよう、極めて人間的な方法で訓練している。例えばコールセンター、レストラン、銀行では、AIを搭載したボットが、よくある質問を質問される順に認識することで驚くほど人間らしいやりとりを顧客と行っている。次のステップは、例えば、ナイトテーブルから落ちたランプと、倒れて助けが必要な人間を見分けるセンサーを搭載した、高齢者介護用ロボットを開発することになるかもしれない。今後10年間でAIの直感・感情に関わる能力が成長すれば、教育者、作家、医師、さらにはCIOとして働くロボットが出てくるかもしれない。

こうした開発、訓練、展開のプロセスは、今後10年間およびその先も引き続き急速に進展していくと考えられる。今まで人間にしかできないと思われてきたことが、次第にプログラムコードとして表現されるようになる。こうなれば、ビジネスリーダーたちはAIによる完全な自動化が実現できると考え、結果としてバリューチェーン、ビジネスモデル、戦略に変革がもたらされる。10年という時間は遥か先のことと映るかもしれない。特に、目の前の四半期報告書の作成に忙殺されている意思決定者にとってみるとなお

さらである。しかし、それでは「エクスポネンシャルインテリジェンス」、すなわち指数関数的なAIの進展に乗り遅れてしまう。今こそ、組織内の着手しやすい業務の自動化から始めるべきである。

SF作家が長い間語ってきた、恐ろしいディストピア的な世界についてはどうだろうか。心配は無用だ。実際のところ、ソフトウエアは常に中立であり、開発者の明示的な命令や暗黙の偏見を表しているだけだ[10]。最近、デロイトの未来学者たちは、世界経済フォーラムと共同で、「*Technology futures: Projecting the possible, navigating what's next*（テクノロジーの未来：可能性を予測し、次に来るものを導く）」を出版した[11]。この本では、未来の可能性とそれを実現するためのアプローチを鮮やかに検証している。AIの未来について、著者はこう書いている。「情報技術が、機械に計算させるものから、機械に識別を教えるものへと進化し続ける中で、組織、政府、規制当局が『カリキュラム』を注意深く監視することがますます重要になってくる。我々が明確に共有しているといえる価値観、つまり金銭的な価値、社会的な価値、倫理的な価値を理解し、表現するAIを開発するにはどうすればよいのだろうか。我々は、感性を持つようになる、今はまだ小さな子どものようなAIを、目指すべき価値観に沿うよう訓練しなければならない。必ずしも従来の我々のやり方を踏襲する必要はないのだ」

アンビエントエクスペリエンス：スクリーンを超えた日常

1960年代にコマンドラインインターフェースが登場して以来、テクノロジーがスクリーンの陰に隠されるのではなく、あらゆるところで目に留まる世界を思い描いたのは、未来学者とSF作家だけのように思われた。ほとんどの人にとって、コンピューターの能力とインターネットには長方形のスクリーンを通してアクセスするものだという理解が定説となった。

時間が経つにつれて、このスクリーンはずっと小さくなり、今ではポケットや手首に収まるようになった。さらに、これらの縮小された画面の背後にある計算処理やネットワーク技術は、飛躍的に強力かつ洗練されたものになっており、我々はスクリーンを介さずにクラウドに直接接続し始めている。スマートスピーカーを例に考えてみよう。今日、スマートテクノロジーを利用している家庭で育った子供たちにとって、天気予報を得るために「部屋に向かって尋ねる」以外の選択肢は考えられないであろう。

今後10年間のうちに、アンビエントコンピューティング（ユーザーがいつでもどこでもデジタルリアリティを利用できるようにする、成長しつつある技術分野とその手法を表す包括的な用語）が、我々にとって標準的で当たり前になるにしたがって「スクリーンを超えた日常」の時代が幕をあけるであろう。

「スクリーンを超えた日常」とはどのようなものだろうか。以下のようなシナリオを考えてみよう。

- **フリクションレス**
  デスクトップコンピューターとの最初の出会いを思い出してみよう。おそらく、それには分厚い紙のマニュアルが付いていた。対照的に、今日のモバイルデバイスに必要なのは、それ自体がデジタルアプリケーションとなっている「クイックスタート」機能だけである。基盤となるテクノロジーはより複雑になっているが、体験はよりシンプルになっている。アンビエントテクノロジーは、新しいツールを習得して使用するために必要な手間をさらに減らすことを約束している。なぜなら、子供たちが天気予報を部屋に向かって尋ねるように、話すだけ、またはジェスチャー、はたまた一瞥するだけでことが済むためだ。もはやコンピューター室に行くことや、ノートパソコンにログインすること、モバイルデバイスをチェックすることの必要はなくなった。実際、アンビエントインターフェースは常に待機状態であり、次に必要なステップを持続的に推測し、ユーザーの目的を達成するための最も効率的な方法を積極的に提供するからだ。

  我々は、数多くのテクノロジーが我々の環境を継続的に観測し、仕事と個人の生活を自動化、あるいは少なくとも合理化するために協調して働く未来を思い描いている。もちろん、セキュリティーやプライバシーに関する懸念もあるであろう。しかし、より合理的でフリクション（摩擦）レスな生活が、今日の我々の大多数にとって、そして間違いなくその子どもたちにとって現実のものになるであろうと確信を持っていうことができる。シンプルは何事にも勝るのだ。

- **よりプロアクティブで直感的**
  誰もがパーソナルアシスタントを持っている世界を想像してみてほしい。これらの高性能アシスタントはデジタルで、さまざまなセンサー、音声認識、分析、指数関数的に発達するインテリジェンス機能によってバックアップされており、24時間365日環境を監視し、可能な限りユーザーの手間を減らす。例えば、デジタルアシスタントによって、空港への出発時刻が通知されることもあるであろう。目的地にたどり着くための最善の方法を決めてからモバイルアプリケーションを使ってチェックインするのではなく、アシスタントはあなたのスケジュールや好み、目的を知っており、すべてを代行してくれる。通知されてからバッグを手に取って家の外に出ると、デジタルアシスタントは不必要な機器の電源を切り、エアコンを最適な設定に調整し、ホームセキュリティーシステムを起動する。

- **「見たら分かる」が成立する**
  個人の物理的な体験をデジタル情報で拡張することは、「スクリーンを超えた日常」のもう1つの大きな次元になるであろう。我々はすでに、アーリーアダプターたちがスマートグラスやVRまたはARのヘッドセットを使って、デジタル情報を労働者の視界に重畳していることを知っている。これは、現実そのものをオンライン化することだと考えてほしい。あるいは、原始的なブラシを用いて、原子をビットで描くことだともいえるかもしれない。研究者も起業家も、スマートコンタクトレンズや埋め込み型の脳チップを使って人間の

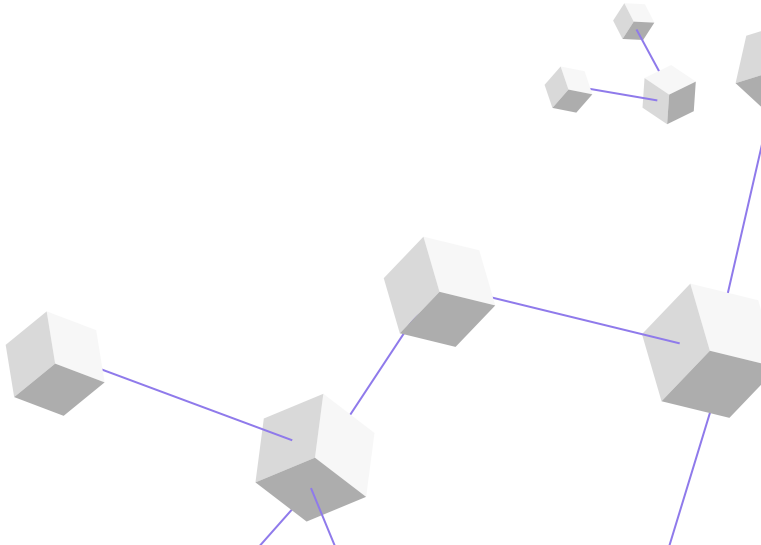
感覚を向上させ、（文字通り）人間の心を読み取ることの可能性をすでに模索している。考えてみれば、太陽を見て、日没まで何時間かを知るのは自然なことではないか。またはバス停を見て、次のバスが到着するまで何分か知ることもそうだ。人間を見てその心を読み取ることは不思議ではあるが、我々が一日中スマートフォンを見つめているよりはましかもしれない。

**より合理的で
手間のかからない生活が、
今日の我々の多くにとって、
そしてもちろん
その子供たちにとって
現実となるであろう。**

アンビエントワールドへの我々の旅はどのように展開するのだろうか。先行する組織が、まずは手堅く達成できる目標に焦点を当てつつ、時間の経過とともに、より変革的なプロジェクトに着実に移行しており、漸進している。最初のステップとして、これらの先駆者たちはすでに、自分たちの組織のどこに余計な手間が存在しているのかを突き止めようとしている。それは、人と人とのやりとりや、長い硬直化した面倒なプロセス、さらには従業員がテクノロジーを利用する方法の中にあるかもしれない。そして、現在利用可能な技術を使って手間を減らす方法を模索している。積極的な取り組みのひとつの例として、航空業界を考えてみよう。航空会社はこの10年間で、チケット販売から手荷物の取り扱い、座席の選択に至るまであらゆることを再考し、デジタル化によって顧客体験を完全に変えてきた。この取り組みはまだ進行中だが、20年前に商業飛行を経験したことのある人なら、航空券から滑走路までの経路が以前よりもシンプルな顧客体験になっていることを否定できないであろう。小売業、接客業、金融業などほかの多くの分野でも同様の取り組みが進んでいる。

顧客にとっても従業員にとっても、「より簡単」なことは大きな意味を持つ。アンビエントな欲求のすべてをサポートするために必要なテクノロジーは、現時点では提供されていないかもしれないが、実現の兆しが見え始めていることは明らかだ。

さぁ、「スクリーンを超えた日常」を今すぐ始めよう。



私の見解

Mike Bechtel
Chief futurist, Deloitte Consulting LLP

我々のチームは、
未来学者として未来を予見するために、
過去を研究することに注力している。

過去の歴史からはさまざまな考え方を引き出すことができるのだ。具体的には、さまざまなテクノロジーの歴史を研究し、それが世界の仕組みや生活の中にどのように影響を与えたか、あるいは与えるにいたらなかったか、などを調査している。25年に及ぶイノベーション研究の結果、ひとつの未来のみを予測することは価値がないと分かっている。過去に起きたパターンを考慮し、ありそうな未来を予測していくことは、組織にとって逆風を回避し、追い風を利用して、より戦略的に次のステップを描くことにつながるのだ。

1840年における最初のコンピューターの特許について振り返ると、基礎的な要素は今日まで変化がない。本編で概説したように、インタラクション（ユーザーインターフェース）、情報（データ）、そしてコンピューティング（処理）という、これら3つの要素がITにおける進歩の基礎であると考えるならば、その次の到達点が何なのかは把握できる。モバイルデバイスやバーチャルリアリティーを超えたインタラクションが、アンビエントコンピューティングにつながり、スクリーンを介さずに物理的な世界とデジタル世界を同時に体験できるようになる

であろう。情報はAIを超えるエクスポネンシャルインテリジェンスをもたらし、変数を計算することと同じように、機械が愛らしくなり、詩を作る方法を学習するような未来が訪れるであろう。最終的には、デジタルビットを超えた計算は量子技術につながり、物理学を応用することで、数学では解決できない問題を解くことができるようになる。

このような未来が実現するまでに、エンタープライズITに影響を与える、多くの技術革新が生まれてくるであろう。それらは、企業で適用される前に、よりリスクを取ることのできる芸術や娯楽の領域で広がると考えられる。「いいねボタン」のようなアイデアは、消費者の間で受け入れられ、その後に企業向けのチャットプラットフォームに導入されてきた。同じように、ソーシャルメディア上で拡散されているような動画が、職場でのトレーニングなどで活用されるかもしれない。将来のIT部門では、ナレッジ共有の最適な手段としてメタバースを活用している可能性もあるが、それは今日的な視点ではまるで遊んでいるように見えるであろう。

また、コンテンツ作成が一般化されてきたように、過去綿々と続いてきたITにおける大きな負担も、徐々に軽減されてきている。データベース管理の課題はクラウドによって抽象化され、ソフトウエア開発はオープンソースのテクノロジーやコードアクセラレータによってより簡易化されている。未来のIT部門では、さまざまな種類の部品を組み合わせることでアプリケーション開発ができ、自前でゼロから開発を行う必要が少なくなるであろう。結果として、将来のIT部門では、限られた用途のために新しいシステムを作り出すのではなく、既存の製品を組み合わせて最適にシステムを構成して作り出す役割を担うことになる。

ITチームにおける役割の変化に伴って、ITリーダーシップの果たすべき役割も進化していく必要がある。テクノロジーやツール類が、課題解決の手段として急速に広がり続けることで、CIOは情報そのものよりも、テクノロジー自体を重視することになるであろう。技術者として時間を使うのではなく、市場やビジネスのなかで、重要な示唆を得るために時間を費やしていくことになる。将来のCIOは、CEOの右腕として信頼できる相談役となり、新しいものが何であり、次にどのようなことが訪れ、何に投資すべきかなど、組織を導くサポートをしていくことになる。

将来を見つめ、地に足をつける

変革を実現するためには、ITチームはより探索に注力していく必要がある。そうしないと、すべてのリソースを現状のオペレーションに向けてしまう恐れがあるからだ。ITチームでは、労働力の5%から10%を次に来るものの探索活動にあて、15%から20%を有望なイノベーションを継続的に実装する取り込みに専念させるべきである。ビジネス書のベストセラー作家であるOren Hararіが「電球はローソクを改善し続けた結果として生まれたのではない」と述べたように、費やすコストは膨大になるかもしれないが、次の電球を作ることの成果は指数関数的なものとなるであろう。現在すべきことと、将来への取り組みを両立させ、バランスをとることで、未来の成功に近づくことができるのだ。

執筆者

Mike Bechtel
Chief futurist
Deloitte Consulting LLP
mibechtel@deloitte.com

Scott Buchholz
Government & Public Services chief technology officer
Deloitte Consulting LLP
sbuchholz@deloitte.com

SENIOR CONTRIBUTORS

Doug McWhirter
Senior manager,
Deloitte Consulting LLP

Caroline Brown
Manager,
Deloitte Consulting LLP

Amy Golem
Manager,
Deloitte Consulting LLP

Raquel Buscaino
Senior consultant,
Deloitte Consulting LLP

Nelson Launer
Senior consultant,
Deloitte Consulting LLP

Abhijith Ravinutala
Senior consultant,
Deloitte Consulting LLP

Lucas Erb
Consultant,
Deloitte Consulting LLP

参考文献

1. Sergey Frolov, *Quantim computing's reproducibility crisis: Majorana fermions*, *Nature*, April 12, 2021.
2. Scott Bucholz, Deborah Golden, and Caroline Brown, *A business leader's guide to quantum technology*, Deloitte Insights, April 15, 2021.
3. Daphne Leprince-Ringuet, "The global quantum computing race has begun. What will it take to win it?," *ZDNet*, February 9, 2021.
4. Deloitte analysis.
5. Frank Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nature* 574 (2019): pp. 505–10, Daniel Garisto, "Light-based quantum computer exceeds fastest classical supercomputers," *Scientific American*, December 3, 2020.
6. Deloitte analysis.
7. Bucholz, Golden, and Brown, *A business leader's guide to quantum technology*.
8. Gregory Choi, Data mining: Association rules in R (diapers and beer), blog post, Data Science Central, August 22, 2016.
9. Tamara Cibenko, Amelia Dunlop, and Nelson Kunkel, *Human experience platforms: Affective computing changes the rules of engagement*, Deloitte Insights, January 15, 2021.
10. World Economic Forum, *Technology futures: Projecting the possible, navigating what's next*, April 5, 2021.
11. Ibid.

日本のコンサルタントの見解

「量子」の世界、その展望

いま何が起きているか

コンピューター技術は、ムーアの法則にしたがい日進月歩で進歩してきたが、量子コンピューターの出現により、このムーアの法則自体は終焉を迎えることになるであろう。量子コンピューターの有用性、実用性はいまだ確証を持たれているわけではない。しかしながら、次世代のデジタル社会を迎えるにあたり、その処理性能が膨張し続けるデータの処理解析に有効活用できるのでは、という期待が急速に高まっている。

本文で触れた「コンピューティング」「通信技術」「センシング」は個別のテーマではなく、量子コンピューターの優れた計算能力を支える上で不可欠な要素であり、多くの企業が提供側として取り組んでいる。

コンピューティングセンシング分野では欧米・中国が先行しているものの、日本も研究開発・実用化を推進し、一部の企業では製品化に至っている。他方、通信技術分野では、QKD製品化やQKDネットワークの国際規格をリードするなど、日本は世界に対して存在感を示している[1]。実用化という点では各クラウドベンダーが実際に量子コンピューティングサービスを提供しており、利用者目線でのハードルは下がる一方である。

何をすべきか

日本企業に対しては次の3点を提言する。まず、量子コンピューターの活用以前に、デジタル時代の重要テーマであるデータ活用を推進するにあたり「何をすべきか」というビジネスアジェンダが必要と理解すべきである。次に、量子コンピューティングが研究段階から実用化へと流れが加速するに伴い、市場の投資および人材確保の活発化が進むと考えられ、その波に乗り遅れないためにも投資領域検討・人材育成に備えるべきである。最後に、特別なことではないが、自社・他社の立ち位置や動向把握、そこからの差別化や協業によるイノベーションといった価値を生み出すため、引き続き量子コンピューティングの動向は注視すべきである。

来るべき未来への展望

昨年末18年ぶりに最新作が上映された映画「MATRIX」、1999年の第一作では、拳銃の弾丸を超高速でよけきる、まさにあの処理の世界観が、この量子コンピューティングの世界観かと感じている。人の五感を代替する技術要素（AI、RPA、IoT、ロボティクスなど）に加え、これらをつなぐ神経伝達速度を代替すると期待される量子コンピューター技術、さらには6Gといった次世代高速通信技術との組み合わせにより物理距離の壁を取り払い、どこにいても誰もが「MATRIX」の世界を体験できるようになる未来が見える。

量子技術の発展によって加速する次世代DXの実現は、空想の遠い未来ではなく、現在の延長線上にあり、近未来にたどり着くためのさらなる取り組み、試金石になるであろう。

エクスポネンシャルな世界の到来に向けて、我々は何をすべきか

現在のAIに対する認識

AIはデータから統計的に有意な相関関係や特徴的なパターンを解析するものと認識されてきた。「AIが人間の感性を理解する」という本文の見解に実感が沸くであろうか。現在目にしているAIとは違うものであり、遠い将来の話と映るかもしれない。

従来、AIは複雑・大量のデータを分析し予測する目的で利用されてきた。本文の「ビールとおむつの関係」をはじめとして、AIは数値化された情報から重要な相関関係やパターンを導出し、その背景にある人間の意図・行動心理は、人が解釈を加えた上で判断してきた。いうなれば、AIは高性能な計算機の役割を与えられてきたといえる。現在多くのAIは限定的なデータと機能を持ち目下の作業を楽にする目的で用いられている。集積・分析するデータは、数値にせよ音声・画像にせよ、ほとんどの場合は人の内面を映すことは意図されておらず、AIに意思決定に関わる役割は与えられていない。

将来のAIを見据えて

今後AIは人間の感性にまで技術進化を遂げるという。こうした未来は、これまでのAI活用の認識・取り組みの延長線上に来るのだろうか。感性を持つAIの到来を想定するとすれば、現在のAIの役割の認識を変えていくこと、そしてその上で必要となりうるデータの範囲も再定義をしていく必要がでてくるであろう。

例えば業務アシスタントAIを想像してみよう。AIは昨日までの実績を分析し異常を警告してくれるが、次に何をすべきかの示唆は与えてくれない。AIに気づきや意思決定の結果、マーケットからの反応を与えることで、異常の警告だけでなく、いくつかのシナリオに沿った示唆を出すようになる。そこにはいくつかの失敗も含まれるかもしれないが、精度向上につながる新たなフィードバックとなるはずだ。

IoH（ヒトのインターネット）など、人のデータはますます活用されるであろう。そうなればAIはもはや単なる計算機ではなく、一緒に働くパートナーである。

今後何をすべきか

エクスポネンシャルな世界がどうなるのかは我々の手の中にある。AIは我々の行動履歴を学習している以上、自分のコピー以上には成り難く、成長の方向性とスピードも限界がある。今後、AIを指数関数的に進化させるためには、オルタナティブデータや他者のチャンピオンモデルと掛け合わせるといったことに果敢に取り込んでいくことが重要になるであろう。

アンビエントな社会の夜明けに直面する、我々が持つべき認識

我々はプロセス社会にストレスを感じて生きている

本文で語られている「アンビエントエクスペリエンス」などのアンビエント○○という表現は日本ではあまり一般的でない。一方で、「スクリーンを超えた日常」という表現については、感覚的に理解しやすいのではないだろうか。今日、我々はスクリーンを前提とした圧倒的なプロセス社会、目的達成までにスクリーンを経由することを当たり前とする社会に生きている。そして我々はそのプロセスで生じる「手間」に意識的、無意識的にストレスを感じている。だから本文で語られる「スクリーンを超えた日常」という表現は、比較的イメージしやすくポジティブな印象を与えやすい。

仕事や生活をより効率的に便利にするためにデジタル技術は発達してきたが、スクリーンを前提としたことで、人間的な感覚と一致しない不要なプロセスが生じて、それに我々がストレスを感じていることは皮肉だし強欲だと感じる人もいるかもしれない。しかし、より便利にシンプルに、自然に日常を送りたいという欲求の実現は、それを叶える技術がある限り止まらないであろう。精度や信頼性が変わらないのであれば、コーヒーを飲みたいと思ってからスクリーンを見て豆の種類の選択や注文の操作をするよりは、コーヒーを飲みたいと思って席に座ると気分にあったコーヒーが自動的に出てくる方が楽に決まっている。

現実のデジタル化とデジタルの現実化

「アンビエントエクスペリエンス」の実現に向けては、現実のデジタル化も重要な要素となる。例えば、人の気分や趣向、意識していない健康状態などはこれまで気軽な計測が難しかった。そういった現実の要素が、インプラントデバイスなどの観測技術やAIなどの分析技術の発達によりデジタルに変換、処理できるようになる。それにより、これまで実現できなかったプロセスの省略も可能となるであろう。また液晶画面以外の出力装置が発達することで、デジタルの現実化も進むであろう。現実と同様の体験をもたらすデジタル情報を、視覚以外の要素も含めて再現できれば、それは現実と変わらない価値を持つ。現実とデジタルの境界を意識しない時代が近い将来訪れるのかもしれない。

今後何をすべきか

「スクリーンを超えた日常」は静かに浸透して、一度置き換わると不可逆である。また複数の高度な技術の組み合わせにより実現されるため、特定の業務や顧客ニーズに対して最適化するには時間がかかるであろう。最適解が出された後で追いつくことは難しい。大多数の顧客や従業員がスクリーンを当たり前としている状態が長く続くものと考えず、部分的にでも「アンビエントエクスペリエンス」化に取り組み始めることが重要だ。近視眼的な費用対効果に捕らわれず、積極的に新技術の活用にチャレンジすることは日本企業の競争力に大きなアドバンテージを与えるであろう。来たるアンビエントな社会でも、早起きは得なのだ。

執筆者

室住 淳一　パートナー
Advance Artificial Intelligence

外資系・国内系コンサルティング会社を経て現職。AI技術を活用した新規事業創出、業務の高度化、AI基盤構築など、企業のDX推進へのコンサルティングに従事。AI中期経営計画策定、ユースケース創出、データマネジメント推進、データ利活用推進、AI人材育成支援に強みをもつ。

鈴木 紳吾　マネジャー
Technology & Business Operation

日系コンサルティングファームを経て現職。ITアーキテクチャーおよびSAPベーシス領域に強みを持ち、製造業・商社などのグローバル展開プロジェクトを担当、展開先現地でのデリバリーを実施した経験を持つ。

宍倉 剛　パートナー
Advance Artificial Intelligence

流通小売業及びAIスタートアップ（兼務として一般社団法人データサイエンティスト協会事務局長）及び、日系コンサルティングファームを経て現職。データサイエンス領域における戦略策定・業務変革、組織設計・人材開発に強みを持つ。

稲葉 貴久　マネジャー
Research & Technology Transformation

先端技術の研究と活用を支援するR&TTユニットのマネジャー。VR/AR/MR（XR）の専門家であり、この分野に関する深い理解、経験、コネクションを有する。また、XRチームのリーダーでもあり、チームのプロデューサーとしてソリューションの計画、提案、実装を牽引している。

参考文献

1. 国立研究開発法人情報通信研究機構, “国際標準化機関ITU-Tで初の量子鍵配送ネットワークに係る勧告が成立,”July 2, 2019.

Acknowledgments

監修

Scott Buchholz
Emerging technology research director and Government & Public Services chief technology officer
Deloitte Consulting LLP
sbuchholz@deloitte.com

As a leader and visionary in new and emerging technologies, Scott Buchholz helps clients use technology to transform their organizations, missions, and businesses. He works across industries to provide actionable advice and insights to use technology to improve performance, effectiveness, and efficiency.

He leads Deloitte Consulting's efforts in exploration of quantum computing and related technologies, working to solve customer challenges with these advanced technologies. In his role as CTO for Deloitte Consulting LLP's Government & Public Services practice, he works with government clients to use technology to innovate in their operations, technology, and mission delivery.

Mike Bechtel
Chief futurist
Deloitte Consulting LLP
mibechtel@deloitte.com

As chief futurist with Deloitte Consulting LLP, Mike Bechtel helps clients develop strategies to thrive in the face of discontinuity and disruption. His team researches the novel and exponential technologies most likely to impact the future of business, and builds relationships with the startups, incumbents, and academic institutions creating them.

Prior to joining Deloitte, Bechtel led Ringleader Ventures, an early-stage venture capital firm he cofounded in 2013. Before Ringleader, he served as CTO of Start Early, a national not-for-profit focused on early childhood education for at-risk youth. Bechtel began his career in technology R&D at a global professional services firm where his dozen US patents helped result in him being named that firm's global innovation director. He currently serves as professor of corporate innovation at the University of Notre Dame.

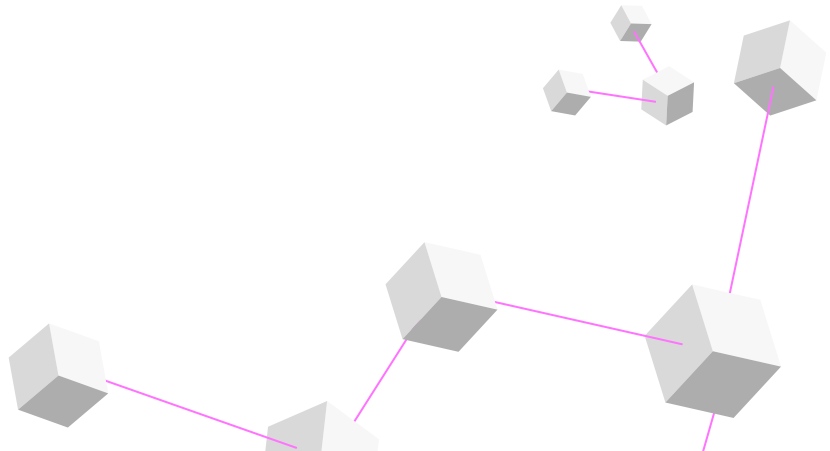
今後の展望の執筆者

ストラテジー

Benjamin Finzi
US and Global Chief Executive Program leader | Deloitte Consulting LLP

Anh Nguyen Phillips
Global CEO Program research director | Deloitte Touche Tohmatsu

Benjamin Stiller
Principal | Deloitte Consulting LLP



ファイナンス

Steve Gallucci
US CFO Program leader | Deloitte LLP

Patricia Brown
US CFO Program managing director | Deloitte LLP

Ajit Kambil, PhD
CFO Program global research director | Deloitte LLP

リスク

Deborah Golden
US Cyber & Strategic Risk leader | Deloitte & Touche LLP

Contributors

Anthony Abbatista, Jaime Austin, Stefan Babel, Blair Baillio, Arod Balissa, Amod Bavare, Rupesh Bhat, Douglas Bourgeois, Tobias Brenner, Morgann Carlon, Natalie Chatterton, Anthony Ciarlo, Emily Cole, Morgan Davis, Louis DiLorenzo Jr., Greg Dost, Emma Downey, Michael Eniolade, Michael Fancher, Nairita Gangopadhyay, Andreas Gentner, Adarsh Gosu, Kevin Govender, Stefan Graf, Dorothea Haas, Esther Han, Ariana Hannes, David Harrison, Nikolaus Helbig, Michele Herron, Alexander Hewer, Meirav Hickry, Karen Johnson, Khalid Kark, Tim Kelly, Tovi Kochav, Kelly Komisar, Ed La Hoz Miranda, Matthias Lachmann, Amar Lakhtakia, Rebecca Lalez, Kristi Lamar, Bjoern Langmack, Louis Librandi, Mark Lillie, Daniel Martyniuk, Carey Miller, Simham Mulakaluri, Derek Nelson, Timo Perkola, Dalibor Petrovic, Felipe Piccirilo, Florian Ploner, Dilip Kumar Poddar, Vishal Prajapati, Aparna Prusty, Asish Ramchandran, Hannah Rapp, Alison Rogish, Daniel Rotem, Sanaa Saifi, Peter Sany, Heather Saxon, Rakinder Sembhi, Sofia Grace Sergi, Sandeep Sharma, Sandro Sicorello, Paul Kwan Hang Sin, Nitingaurav Singh, Ranjeet Singh, Nicholas Smith, Tim Smith, Ramona Stordeur, Jan Stratman, Elisabeth Sullivan, Natalie Velazquez, Markku Viitanen, Aman Vij, Jason Wainstein, Jian Wei, Denise Weiss, Shani Weitz, Sourabh Yaduvanshi, Thaddeus Zaharas, Yihong Zeng, and the Knowledge Services team.

Research team

LEADS

Emma Copsey, Ankush Dongre, Mayank Gupta, Rani Patel, Pooja Raj, Katrina Rudisel, and Samantha Topper.

TEAM MEMBERS

Ayshvar Balasubramanyam, Anupama Balla, Srinidhi Bapu, Niko Brammer, Yi-Hui Chang, Krishna Chanthanamuthu, Gurmehar Cheema, Hannah Chen, Soham Dasgupta, Francisco de Ros, Chirag Dixit, Chetana Gururaj, Nidhi Kaushik, Jonathan Key, Ashley King, Mo Koneshloo, Dhir Kothari, Sahil Lalwani, Dong Li, Antaryami Mallick, Swetha Marisetty, Siddhant Misra, Deepashree Mulay, Rutuja Naik, Amruta Pawar, Anna Perdue, Harsh Raman, Vandhanaa Ramesh, Spandana Narasimha Reddy, Nikolaus Rentzke, Prateeti Sarker, Sai Krupan Seela, Bala Seshu Sesham, Kshitij Pratap Singh, Manpreet Singh, Rachel Spurrier, Brendan Stec, Raghul Surendran, Jack Suter, Alap Trivedi, and Falyn Weiss.

Special thanks

Stefanie Heng for grace under fire while masterfully conducting the *Trends* orchestra and managing the dynamic diva duo. Without your ability to keep dozens of plates spinning, we would've crashed and burned many times over. Thank you for all you do!

Doug McWhirter for your infallible leadership and wicked wit. In addition to wrangling words from smacks of SMEs, you grew and cultivated a subtlety of rock star designers and writers who went above and beyond. We appreciate you more than words can say.

Caroline Brown for poise under pressure. We appreciate your continued ability to transform streams of consciousness, reams of research, and an impatience of interviews into brilliant prose, all while dominating on other projects and tutoring teammates.

Adrian Espinoza, Ed Burns, and **Heather Mara** for a fantastic freshman year! Jumping straight into *Trends* is no mean feat. Your fresh perspectives and ideas were deftly transformed into wise words, gorgeous graphics, and a compelling creative vision. Bravo!

Natalie Martella for embracing every opportunity (and sharing levity with your joke-of-the-week). Thank you for coconducting, helping turn the cacophony into a symphony, and leaning into all facets of development, design, and marketing. Huzzah!

Aaron Gano, Abhijith Ravinutala, Kelly Gaertner, and **Maria Wright** for pitching in on all fronts. For relentless research to resounding reviews to intense interviews and more, you helped raise the bar (and the roof). We are beyond lucky to have you on the team!

Alison Cizowski, Cheylin Parker, Mary Hughes, and **Tracey Parry** for your relentless endeavors to get *Trends* to the public. We appreciate your support across all things marketing, communications, and PR!

Aditi Rao, Andy Bayiates, Blythe Hurley, Sarah Jersild, and the entire Deloitte Insights team. For the continued support, patience, and partnership, we thank you and appreciate your drive to improve and evolve *Tech Trends* every year.

Alexis Werbeck, Joanie Pearson, Mackenzie Odom, Matt Lennert, and the Green Dot Agency, thank you for another incredible year of collaboration and bringing our creative vision to life. It gets better and better.

日本版発行責任者

山本 有志　執行役員　パートナー
Japan Leader
Tech Strategy and Transformation

多様な業界に対して、IT戦略立案、IT組織改革、グローバルITガバナンス強化、IT投資コストマネジメント高度化などのテクノロジー ストラテジーに関するコンサルティングに従事。企業の戦略実現を左右する大規模ITプロジェクトのマネジメント経験も多く、戦略から開発・運用までITライフサイクル全般の知見を活かし、CxOに対してアドバイザリーサービスを提供。

千田 章貴　執行役員　パートナー
Asia Pacific Leader
Tech Strategy and Transformation

主に国内及び外資系金融機関に対して、各種改革やデジタルトランスフォーメーションプロジェクトに多数従事。ビジネス戦略立案からシステム化構想及び導入、定着、アウトソーシングを含む広範囲なコンサルティング領域を経験。アジアマーケットを中心とした海外戦略やグローバルオペレーションシステムの最適化などを含むグローバルプロジェクトに強みを持つ。

日本版発行担当者

データシェアリング時代のはじまり

三木 聡一郎
小林 胡桃実
栗田 遥
志村 知美
蓮池 由梨
小倉 康司
徐 漢邦
染谷 佳奈
藤本 真里絵

インダストリークラウドの潮流

佐藤 岳彦
金川 直弘
土田 泰徳
稲葉 高洋
北島 伊久美
秋田 修吾
佐藤 佑哉
南野 香澄
中澤 雄馬
久山 真宏

ブロックチェーン：ビジネス利用への期待

赤星 弘樹
横田 一生
川口 知宏
梅村 圭輝

IT部門の再構築：加速する自動化

森永 直樹
秋葉 洋毅
高畑 浩一
加藤 嵩大
新保 卓己
鳥居 隆史
楊 鵬
平田 真一
深井 雄介
Bertrand Polus
冨原 裕一
吉井 博香
今井 研太郎

サイバーAI：真の防御

桐原 祐一郎
Yin Minn Pa Pa
熊谷 裕志
神薗 雅紀

技術スタックは物理化する

斉藤 宏樹
丸居 玄明
四ッ家 昭胤
坂元 穂波
山下 雄輝
小野 礼夏
田中 大地
小坂 慶之
石川 智美
塚本 麻衣
岡野 利信

未来のフィールドノート

奈倉 太郎
小野沢 正樹
芳賀 健一
宍倉 剛
稲葉 貴久
坂口 直樹
鈴木 紳吾
室住 淳一
河原 弘宜

編集協力

古賀 友久
原田 直樹
武野 淳
細谷 彩恵
竹谷 剛史
清水 孝弘
四ッ家 昭胤

国内のお問合せ先

山本 有志／Yushi Yamamoto
Japan Technology Strategy & Transformation Leader
Partner

デロイト トーマツ コンサルティング合同会社
yusyamamoto@tohmatsu.co.jp

川嶋 三香子／Mikako Kawashima
Technology Strategy & Transformation
Senior Manager

デロイト トーマツ コンサルティング合同会社
mikawashima@tohmatsu.co.jp

Deloitte.
Insights

Deloitte Insightsの登録はこちらから www.deloitte.com/insights

@DeloitteInsightをフォローしてください @DeloitteOnTechをフォローしてください @deloitte_jpをフォローしてください

Deloitte Insights contributors

Editorial: Aditi Rao, Blythe Hurley, Andy Bayiates, Aparna Prusty, Dilip Kumar Poddar, Emma Downey, Nairita Gangopadhyay, and Rupesh Bhat

Creative: Alexis Werbeck, Adrian Espinoza, Heather Mara, and Jaime Austin
Promotion: Hannah Rapp
Cover artwork: Bose Collins

デロイトインサイトについて
デロイトインサイトはビジネスや公共サービス、そしてNGOに関わる人々にインサイトを与える、オリジナルの記事やレポート、定期刊行物を発行しています。私共のプロフェッショナルサービスを提供する組織とビジネスや学術に関わる共著者から研究結果や経験を引き出し、企業幹部や政府のリーダーとなる方々に、幅広い視野で議論を進めていただくことを目的としています。
デロイトインサイトはDeloitte Development LLC.によって発行されています。

本誌について

デロイト トーマツ コンサルティング合同会社
〒100-8361 東京都千代田区丸の内3-2-3 丸の内二重橋ビルディング
Tel 03-5220-8600　Fax 03-5220-8601
www.deloitte.com/jp/dtc