

自動化の難問

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website (www.isaca.org/journal), find the article and click on the Comments link to share your thoughts.



「コンピュータは愚鈍である。そして、ツールが愚鈍であればあるほど主人はより賢くなければならない」頻繁に引用された1967年の記事でPeter Drucker氏はこう主張しています。¹ この文章は少し誇張に聞こえますが、当時、コンピュータの役割は事務的な雑用を補う程度のものでしたのでこの議論は的を射ておりおそらく関連性もありました。

50年後、計算能力が指数関数的に増加する人工知能（AI）システムがビッグデータと連携することにより多くの分野において人間よりも優れた能力を発揮しています。これらのインテリジェントシステムは、あらゆる産業分野に浸透し続けており新しいビジネスチャンス、より深い顧客ニーズの発掘、効率の向上、迅速性の向上などの形で莫大な利益をもたらしています。

米国のMemorial Sloan Kettering Cancer Centerは、IBM Watsonを使用して膨大な数の治療ガイドライン、研究発表、医療ジャーナル記事、医師の

メモ、その他の見解と患者の医療情報を比較し信頼スコアを付した提案を医師に提供しています。² カナダでは、モントリオール銀行が顧客に自動化されたアルゴリズムベースのポートフォリオ管理アドバイスを提供するロボ・アドバイザーを配置しました。³ マサチューセッツ工科大学（MIT）（米国）は、36億行以上のログファイルのデータを毎日見直し、疑わしいものについては通知することでサイバー攻撃の85%を検出できるAIシステムを開発しました。⁴

AIシステムの採用は今後数年間で加速すると予想されます。バンク・オブ・アメリカのメリルリンチ・リサーチの2015年12月のレポートによると、ロボティクスおよびAIソリューション市場は2020年までに1530億ドルに増加すると予測されています（ロボティクス向けには830億ドル、AIベースのアナリティクス向けには700億ドル）。同報告書では、この指数関数的成長が生産性を最大30%向上させ製造業の賃金を18~33%削減できると推定しています。⁵

重要性の低いビジネスタスクを使用してAIを実験している組織もあれば、AIアルゴリズムにミッションクリティカルな役割を託して野心的な進歩を遂げている組織もあります。このような例には、香港のベンチャーキャピタル会社ディーブ・ナレッジ・ベンチャーズ（Deep Knowledge Ventures）があります。この会社は2014年5月、取締役会にAIアルゴリズムを任命しました。⁶ Vitalという名前のアルゴリズムは、財政、臨床試験、知的財産、先行する企業の資金調達ラウンドによるデューデリジェンスを自動化し企業に投資するかどうかについて投票するという重大な責任と結果を伴う役割を果たしています。

AIの普及は興味深い機会をもたらしています。しかし、関連するリスク要因が存在し、それらが顕在化した場合、その影響は重大な結果をもたらすこともあります。AIの普及に関する戦略上の懸念は数多く出版されていますが、この記事ではビジネスでAIを採用する際にリーダーが直面する3つの重大なリスクの懸念事項に重点を置き、AIの可能性を最大限に利用しつつビジネスエクスポージャーを最小限に抑

Phillimon Zongo

Phil Zongoは、オーストラリアのシドニーを拠点に活動するサイバーセキュリティコンサルタントです。10年以上の技術リスクコンサルティングとガバナンス経験を有し経営コンサルティング会社や大手金融機関と協力しています。複雑な技術変革プログラムで重大なリスクをどのように管理するかについて、ビジネス上および技術上の関係者にアドバイスする実践的な経験を有しています。また、ISACA® *Journal*の2016年第4版に掲載されている「Managing Cloud Risk Top Considerations for Business Leaders」の執筆も担当しています。

えるための実用的な洞察を提供します。これらのリスク要因には次のようなものがあります。

- 欠陥のある、または誤ったAIアルゴリズムに基づく重要なビジネス上の意思決定
- 自動化に対して無抵抗な職務を担当する従業員からの文化的抵抗
- より重要なビジネス機能がAIに置き換えられることに伴うサイバー脅威の更なる拡大

欠陥がある、または誤ったAIアルゴリズム

緻密に設計されたAIシステムは、生産性と品質の大幅な向上を実現します。が、慎重に導入しなければ財務的影響および社会的影響は深刻なものになる可能性があります。銀行や金融業界では、アルゴリズムの不備が過度のリスクを招き組織を破産に導く可能性が危惧されます。ヘルスケア分野では、アルゴリズムの不備により薬を誤って処方し患者の容体をさらに悪化させてしまう可能性が危惧されます。法律分野では、アルゴリズムの不備により誤った法的助言が提供され厳しい規制違反をもたらす可能性が危惧されます。2012年、米国のマーケットメーカーであるナイト・キャピタル・グループ（Knight Capital Group）は、テスト検証なしで高頻度取引アルゴリズムに変更を加えたことにより、わずか30分で4億4,000万ドル以上の損失を被っています。こうした潜在的リスクの影響が現実のものとなった不幸な一例です。「あらゆるソフトウェア不備の母」とも呼ばれたこの事件により、同社は2011年の純利益の4倍のコストを損失しました。⁷

最小限のビジネス・インパクトでエラーをロールバックできる従来のルールベースのシステムとは対照的に、重要なAIアルゴリズムの中の軽微なエラーが重大な結果を招くことがあります。AIシステムは人間や外部環境と対話するときに予期せず動作する可能性がありこのリスクをさらに複雑にしています。インテリジェントシステムがますます重要なビジネス上の役割を果たすようになるにつれ、アルゴリズム不備に起因する重要なビジネス上の意思決定リスクは常に上昇します。従って、AIシステムがより強力かつ自律的になるに伴いその概念を人間の設計者の概念と一致させる必要性が増加するのです。⁸

リスクを管理しながら、AI価値を最大化するために役立つ3つの重要ステップ：

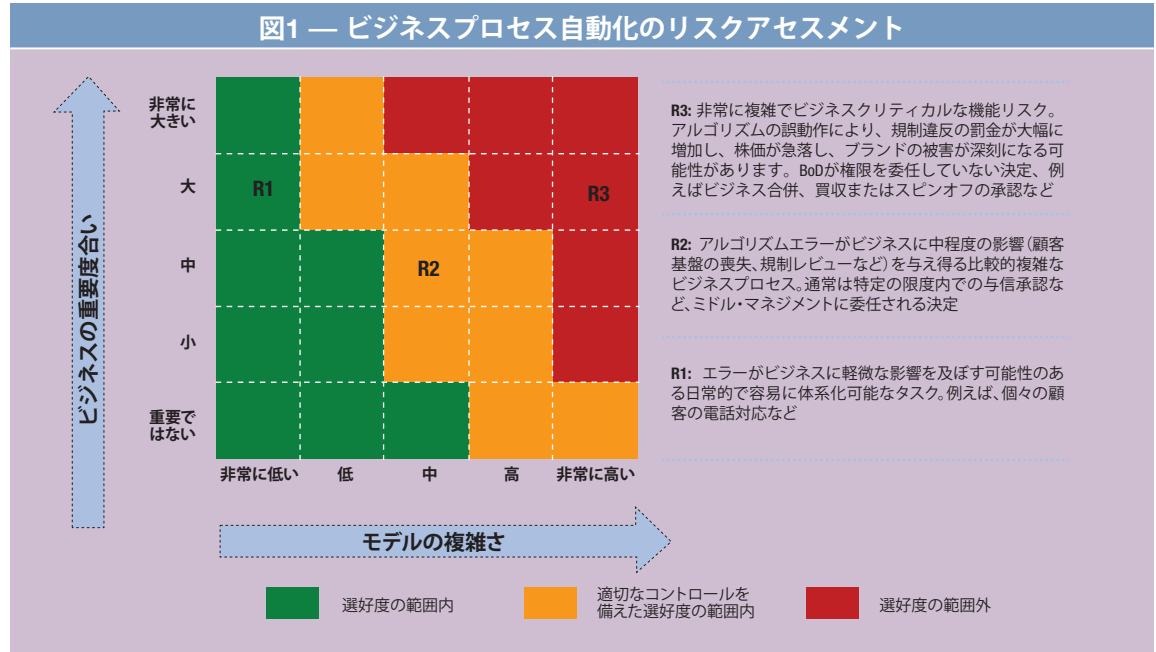
- AIの導入をビジネス戦略とリスク選好度に合わせる
- 低リスク機能で実験すること
- 厳密にテストすること

AIの導入をビジネス戦略とリスク選好度に合わせる
ビジネスリーダーは、AIの導入に内在する重要なリスクに留意して適切な監督を行い部分的または完全に自動化できるビジネス分野を明確化する原則を策定する必要があります。同様に重要な点として、取締役会は高リスクのビジネス機能の自動化を承認することにより、管理能力を超えるようなリスクやビジネス戦略に寄与しないリスク等に組織が晒されないようにする必要があります。

“ 最小限のビジネス・インパクトでエラーをロールバックできる従来のルールベースのシステムとは対照的に、重要なAIアルゴリズムの軽微なエラーは重大な結果を招くことがあります。 ”

このアセスメントを実施する簡単な方法を図1に示しています。ここでは、2つの要因によるリスクエクスポージャーをモデル化しています。自動化されたビジネス機能の重要性、および関連するモデルの複雑さ図1の例では、金融機関は異なるリスクエクスポージャーに基づいていくつかのコールセンター機能（R1）を自動化する一方で、ビジネスの買収またはスピンオフ承認（R4）の自動化を回避することを決定する場合があります。日常的な職務は、自然かつ簡単に自動化することができ知性的推論、創造性、対人関係のスキル、情緒的な知性などの複雑な機能に比べてもたらされる業務上のリスクは小さくなります。

図1 — ビジネスプロセス自動化のリスクアセスメント



原典：P. Zongo.の許可を得て掲載

特定の行政管轄下では、一部のビジネス機能の完全自動化が禁止される可能性があるため特定のビジネス機能を管理する規則を明確に理解することも不可欠です。例えば、2016年4月、マサチューセッツ州（米国）証券部門はロボ・アドバイザーに対して公認登録投資顧問として機能する能力への疑問を投げかける政策声明を発表しました。証券監督当局は、「現在の構造では完全に自動化されたロボ・アドバイザーは、公認登録投資顧問の信託義務を本質的に遂行することができない可能性がある」と発言しました。⁹ 当局の主張は、完全に自動化されたロボ・アドバイザーが顧客にとって最善の利益を提供しないばかりか、十分なデューデリジェンスも行っておらず自然人が提供するアドバイスとはほど遠いもので高水準のケアを満たすことができない可能性があるというものです。¹⁰ この政策立案は、プロジェクトの資金を投入する前に予定された改革を含むビジネス機能の自動化に関連する法的な影響を注意深く検討することの重要性を強調しています。

効果的なリスクアセスメントでは、ビジネスリーダーは以下の重要な質問に答えるよう求められます。

- インテリジェントシステムはいかにして企業のビジネス戦略を進めることができますか？ また、何をもって成功と考えますか？
- AIシステムが誤動作した場合の財務的、社会的または規制上のリスクはどの程度ですか？ また、経営陣はリスクが顕在化した場合、拡散した事態を収拾するのに十分な能力を備えていますか？
- この分野において、競合他社は何をしていますか、そしてこれらの目標を追求するために、彼らはどれだけ先行していますか？
- 経営陣はリーダーシップの役割を果たそうとしていますか？ それとも、AIの利点が十分に証明されるまで待ちますか？
- リスク管理に関して組織には実証可能な専門能力が備わっていますか？ これを外部委託する場合、特定されたベンダーは類似またはそれ以上の規模のAI転換プログラムを正しく提供しましたか？

AIの導入には大きな課題があるもののリスク削減の手助けをすることもあります。1961年、米国の発

明家George Devol氏によって開発された最初の産業用ロボットUnimateはこの目的のために設計されました。4,000ポンドのロボットアームは、ダイキャストを組立ラインから運び、これらの部品を自動車のボディに溶接しました。これは、排気ガス中毒に陥る可能性や不注意により手足を失ってしまう可能性のある労働者にとって高リスクを伴う仕事でもありました。¹¹ これに類似した現代の例としてIBM Watsonシステムがあります。これは、当局からの規制が厳しい業界で事業を展開する企業が絶え間なく変化する法令やコンプライアンス基準に対応するために使用されています。¹²

低リスク機能を用いて実験する

関連する結果の論理的理解を得る前に重要な作業を委ねるとリスクが高まります。¹³ 従って、組織は低リスク、低コストで簡単に変更可能なタスクを使用して実験、学習を重ねてから適応する必要があります。基礎となる仮定の検証、能力の証明、主要な不確実性の解消の後、組織はより複雑な機能を徐々に自動化することができるようになります。

厳密にテストする

インテリジェントシステムにおいては、不確実性の度合いが高まるため従来のアプリケーションよりも広範なテストを必要とします。現実のすべての複雑さを学習し相互作用するインテリジェントシステムを構築する場合、アルゴリズムがテスト仕様通り正常に動作することを検証するだけでは不十分です。システムが実際の環境で意図したとおりに動作することを確認するには追加作業が必要です。¹⁴ このテストは適切な資格と動機を有する従業員が実施すべきでしょう。同様に、詳細テストはAIシステムが変更された後、または新しいインテリジェンスを取得した後に実行されなければならずこれらのテストの実行条件には現実の環境を反映する必要があります。

文化的抵抗

重要な変革プログラムは従業員を深刻な不安状態に陥らせることがあります。AIプログラムは、このリスクを増幅します。なぜなら、自動化されやすい職種につく従業員の雇用が危ぶまれるからです。（特

に、熟練度が低く、反復性の高い業務につく）従業員は、自分の仕事の将来を心配することになります。その結果、彼らは、AIプログラムの成功を妨げ自分の仕事を守るために変化に対して反発することでしょう。革新に対する反発は今に始まったことではありません。最も有名な例として、19世紀初頭のラッドライト運動があります。英国の職人グループが一部の機械を破壊し繊維生産の自動化に抗議したのです。¹⁵ 更に、リーダーからの明確で一貫したコミュニケーションの欠如は、重要なAI変革プログラムに対する従業員の混乱と不信感を募らせる結果となります。

“ AIの変革を成功させるためには、ビジネスリーダーは信頼できる環境を作り、従業員を参加させて支援、サポートを高いレベルで確保する必要があります。 ”

2011年の報告書では、「従業員の態度や行動の再構成は、プロセス変革の実施による変革の成功と同様に重要である」ことが強調されています。¹⁶ AI変革を成功させるためには、ビジネスリーダーは信頼できる環境を作り従業員を参加させて支援、サポートを高いレベルで確保する必要があります。これを実現するためにビジネスリーダーは以下に取り組む必要があります。

- 従業員の意欲を高め、自動化の将来に関する共有ビジョンを推進し且つ説得力のある変革シナリオを伝えること。
- 自動化の影響を受けやすいセグメントを特定すること 従業員への影響を評価し代替雇用機会を特定すること。
- 上級ビジネスリーダー、人事、および変革の専門家からなる専任の変更管理チームを設置し、変革の課題を伝えて課題を予測し人員削減率を最小限に抑えること。また、変更管理コミュニケーションにおいては、従業員のフィードバックを汲み

上げる仕組み造りを目標として掲げなくてはなりません。

- 従業員がAIシステムと連携して作業する機会を特定し、そのシナジー（相乗効果）を最大限に引き出す戦略を策定すること。専門的な知的業務は一般的に幅広いタスクで構成されているため、1つのアクティビティを自動化してもポジション全体が不要になるわけではありません。¹⁷ 例えば、アルゴリズムはルーチンタスクを実行し、人間が顧客関係を管理したりより深いビジネスの洞察を導き出す時間を作ります。また、高度に規制されたタスクは完全に機械に置き換えられないかもしれません。
- プログラムがある仕事を完全に自動化しようとしている場合、適切な雇用保護法と適切な対応を理解するための法務チームをデューデリジェンスに従事させること。
- 行動の変化を促進し人々の関わりを維持するためのインセンティブを確立すること。

“AIシステムがビジネスを完全に変革する能力は、セキュリティとプライバシーコントロールの有効性に左右されます。”

企業は、コストを削減し効率を改善して、運用上のエラーを減らすため従来は人手で行っていた業務を引き続き自動化していくことでしょう。組織の最も貴重な資産である従業員に自動化が及ぼすマイナスの影響を考えると、ビジネスリーダーは潜在的なリスクを早期に予測し悪影響を最小限に抑えることが不可欠となります。また、従業員にもすべきことがあります。将来が絶望的と思われるような革新に直面しても、自分自身のスキル向上に励み組織にとって必要な人材であるように努めること研究者は、「技術競争が進むにつれ、低技能の労働者はコンピュータ化の影響を受けにくいタスク、すなわち創造的かつ社会的な知性を必要とするタスクに再配分され

る。しかし、労働者が競争に勝つためには創造的な社会的スキルを身に付ける必要がある。」と予測しています。¹⁸

サイバー攻撃の拡大

AIシステムがビジネスを完全に変革する能力は、セキュリティとプライバシーコントロールの有効性に左右されます。これらの保証を提供しなければその受容が妨げられる可能性があります。バンク・オブ・アメリカのメリルリンチ・リサーチの報告によると、自動運転車の導入への主要な障害はサイバー・セキュリティとプライバシーと規制、保険、コストなどその他の重要な要素への懸念であるとされています。同レポートによると、購入者の54%は、接続された車（connected cars）がハッキング可能となることを懸念し、30%はプライバシー問題を考慮し接続された車を使用したくないと述べています。¹⁹ 2015年、バージニア（米国）に拠点を置く研究者グループが、無人運転車システムをハッキングしてそのコントロールに成功し、アンセキュアなAIシステムには重大な脅威があることを浮き彫りにしました。

サイバーリスクの頻度と事業への影響は引き続き増加しており、取締役会、規制当局、政策立案者からの注目を集めています。公的および民間部門の企業は、執拗かつ狡猾で資源豊富なサイバー犯罪者に対抗する努力を続けています。次のセクションの解説をご覧ください。AIがこの問題をさらに複雑化していることをご理解頂けるでしょう。

脆弱性

今日まで、AIシステムの安全な開発とメンテナンスを導く業界標準は存在していません。この基準の欠如をさらに悪化させるのが、新興企業がAI市場を依然として支配しているという事実です。最近のMITの報告によると、IBMやPalantir Technologiesのような大手企業を除きAIは2,600もの新興企業による市場です。これらの新興企業の大部分は、市場投入の早期化、製品の機能性、投資収益率の高さに重点を置いています。彼らにとって製品にサイバー耐性を組み込むことは優先事項ではありません。

ベンダーは、無意識のうちに基本的なセキュリティコントロールとデフォルトのパスワードや弱い認証技術などの悪用されやすい脆弱性を持つソリューションを出荷しています。これらの弱点は、容易に悪用できるターゲットをサイバー犯罪者に提供してしまうだけでなく、既存のネットワークセキュリティコントロール層を潜在的に反駁する可能性もあります。Verizon 2016 Data Breach Investigations Reportは、確認された違反の63%が脆弱なパスワード、デフォルトのパスワード、または盗用されたパスワードに関連していることを強調しています。²⁰

AIシステムの自己学習機能にも独自の課題があります。サイバー犯罪者は、アルゴリズムの訓練を通して意図的にその行動を操作するために使用されるデータを設計目的に反して的確に予測することができます。AIチャットボット（Tay）を使った最近のMicrosoftのライブ実験の結果では、脆弱なAIシステムをインターネットに公開する危険性について警告しています。2016年3月、Microsoftは組織的攻撃により実験的AIアルゴリズム内の脆弱性が悪用された際に重大な過誤があったことを認めました。Tayは10才代の少女を模して造られており、ソーシャルメディア上の人々と交流して学習するように設計されています。不運なことに、Microsoftの見落としによりTayは攻撃によって特定の脆弱性が公にさらされることになりました。結果、Tayは、Microsoftの価値観やTayのデザインに対する誤解を招くような人種差別的なものを含む非常に不適切で攻撃的なツイートや画像を送信してしまったのです。

ゼロサムゲーム

インテリジェントシステムは、自動詐欺検出やスパム検出などサイバー犯罪との戦いにおいてすでに重要な役割を果たしています。しかし、この役割はゼロサムゲームになる可能性も秘めています。類似の技術が主要システムへの狡猾な回避型サイバー攻撃の実行にも使用できるためです。この所感に対して、最高情報責任者（CIO）、最高リスク責任者（CRO）、最高技術責任者（CTO）、規制当局およびビジネスユニットの役員を含めてマッキンゼーと世界経済フォーラム（WEF）が2014年に共同実施した調査では、75%以上の回答者から反響があ

りました。彼らは、サイバー攻撃の狡猾性やペースが自社の防御能力よりも急速に成長することを認めています。²¹

つまり、次の問いかけが非常に重要となります：このような犯罪者たちは、セキュリティベンダーの裏をかくて優良かつ巧みなAIプログラムを開発し、重要なシステムに対する高度かつ永続的な脅威となって株式市場を操作し、高額な詐欺を犯し継続的に知的財産を盗み出すことで関連するフォレンジック証拠を隠滅してゆくのか？

現在のサイバー犯罪の傾向がこのまま続けば、残存するビジネスサイバーリスクのエクスポージャーも引き続き上昇することになります。

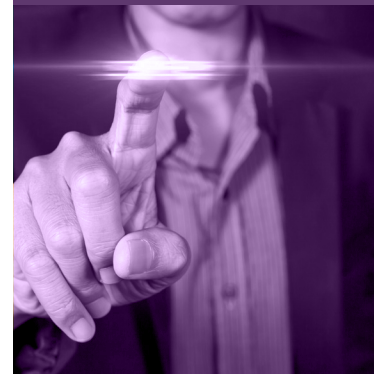
サイバー耐性インテリジェントシステムの構築

ビジネスイノベーションをサポートし、その価値を最大化するためにはインテリジェントシステムに対する包括的なサイバー耐性が不可欠となります。方針立案者、ビジネスリーダー、規制当局、ベンダーが一体となり取組むことが長期的な成功の前提条件です。しかし、これらの協調基準が実現する前にビジネスリーダーが行うべきことがあります：

- 可能なら受容されている既存の業界標準を使用すること。これらはインテリジェントシステム向けに特別に設計されたものではありませんが、企業が共通のセキュリティリスクを特定し新しい技術を確認するための確実なベースラインを確立するのに役立ちます。注目すべきフレームワークには次のものがあります。
 - オープンWebアプリケーションセキュリティプロジェクト（OWASP）トップ10²² — Webアプリケーションを設計によりセキュアにする推奨事項、および最新の主要Webアプリケーションセキュリティにおける10の欠陥リスト。
 - アメリカ 国立標準技術研究所（NIST）サイバーセキュリティフレームワーク²³ — 重要なサイバーインフラストラクチャの保護を促進するための標準、ガイドライン、実践で構成されています。
 - 情報セキュリティのためのCOBIT® 5²⁴ — 重要な情報セキュリティを管理し、新しい技術およびそれに伴う脅威に対する意識を維持しな

Enjoying this article?

- Learn more about, discuss and collaborate on cybersecurity in the Knowledge Center. www.isaca.org/cybersecurity-topic



がら、より多くの情報に基づく意思決定をするための詳細および実用的なセキュリティ専門家のためのガイドラインを提供します。

- 経験豊富なセキュリティコンサルタントがAI製品の重要なコントロール（詳細な侵入テストを含む）をレビューし、本番運用になる前に悪用可能なセキュリティ上の脆弱性を修正します。
- ベンダーのセキュリティ機能、製品のセキュリティロードマップ、セキュリティアップデートの頻度を決定するためのデューデリジェンスの実施 — 製品のセキュリティに対する長期的なコミットメントが重要な成功要因となります。

“今日のダイナミックなビジネス環境において、組織は新しいデジタル能力を試し、新しい製品を追求するリスクを受け入れ顧客との関係を維持しなければなりません。”

- AIシステムと重要なレコード間のセッションを危殆化させることなく保護する堅牢な暗号化を導入します。（一般に中間者攻撃と呼ばれる）
- 最小限のシステム権限を付与し、AIシステムが重大なタスクを実行するために使用するサービスアカウント、特に管理者と同等の権限を持つアカウントを悪用から保護します。
- 1つのコントロールレイヤで障害が発生しても、システム違反が発生しないように多層防御を採用します。

結論

インテリジェントシステムの完全な採用には各種の新興技術と同様に多くの課題が残っています。これらの課題はAIがもたらすと考えられる収益機会と比較すればたいへん見劣りするものです。

今日のダイナミックなビジネス環境において、組織は新しいデジタル能力を試し新しい製品を追求するリスクを受け入れ顧客との関係を維持しなければなりません。そのためには、イノベーション戦略をリスク選好度と整合させ、先行する大きな危険を予測し適切なガバナンス構造を変革プログラムに組み込む必要があります。役員の関与と監督がAIの成功に最も重要となります。

著者の注釈

著者は、この記事の改善に役立つGina Francis、Innocent Ndoda、Shingi Muvonge、Kathleen LoおよびAndrew Strongからの貴重なフィードバックに感謝します。

後注

- 1 Drucker.F. P., 「The Manager and the Moron」, *McKinsey Quarterly*, 1967, www.mckinsey.com/business-functions/organization/our-insights/the-manager-and-the-moron
- 2 IBM Corporation, 「Memorial Sloan-Kettering Cancer Center: IBM Watson Helps Fight Cancer With Evidence-Based Diagnosis and Treatment Suggestions」 (2013年1月), www-935.ibm.com/services/multimedia/MSK_Case_Study_IMC14794.pdf
- 3 Alexander, D., 「Bank of Montreal Jumps Into Robo-Advising Ahead of Other Lenders」, *Bloomberg Technology* (2016年1月18日), www.bloomberg.com/news/articles/2016-01-18/bank-of-montreal-jumps-into-robo-advising-ahead-of-other-lenders
- 4 Conner-Simons, A., 「System Predicts 85 Percent of Cyber Attacks Using Input From Human Experts」, マサチューセッツ工科大学、米国 (2016年4月18日), www.csail.mit.edu/System_predicts_85_percent_of_cyber_attacks_using_input_from_human_experts%20

- 5 Bank of America Merrill Lynch, 「Thematic Investing: Robot Revolution—Global Robot and AI Primer」、プレスリリース (2015年11月)、www.bofaml.com/content/dam/boamlimages/documents/PDFs/robotics_and_ai_condensed_primer.pdf
- 6 Wile, R, 「Venture Capital Firm Just Named an Algorithm to Its Board of Directors—Here's What It Actually Does」、*Business Insider* (2014年3月14日)、www.businessinsider.com.au/vital-named-to-board-2014-5
- 7 Philips, M, 「Knight Shows How to Lose \$440 Million in 30 Minutes」、Bloomberg (2012年8月2日)、<http://www.bloomberg.com/news/articles/2012-08-02/knight-shows-how-to-lose-440-million-in-30-minutes>
- 8 Sotala, K, 「Concept Learning for Safe Autonomous AI」、Machine Intelligence Research Institute (2015年)、www.aaai.org/ocs/index.php/WS/AAAIW15/paper/download/10131/10137
- 9 Massachusetts Securities Division, 「Robo-Advisers and State Investment Advisor Registration」、Policy Statement、(2016年4月1日)、www.sec.state.ma.us/sct/sctpdp/Policy-Statement--Robo-Advisers-and-State-Investment-Adviser-Registration.pdf
- 10 Ibid
- 11 Mickle, P, 「1961: A Peep Into the Automated Future」、www.capitalcentury.com/1961.html
- 12 Kelly, E, 「Computing, Cognition and the Future of Knowing How Humans and Machines are Forging a New Age of Understanding」、IBM (2015年)、www.research.ibm.com/software/IBMResearch/multimedia/Computing_Cognition_WhitePaper.pdf
- 13 Soares, N.; B. Fallenstein, 「Aligning Superintelligence With Human Interests: A Technical Research Agenda」、Machine Intelligence Research Institute (2015年)、<https://intelligence.org/files/TechnicalAgenda.pdf>
- 14 Ibid
- 15 Autor, H. A, 「Why Are There Still So Many Jobs? The History and Future of Workplace Automation」*Journal of Economic Perspectives* (2015年)、<http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.3.3>
- 16 Aiken, C.; D. Galper; S. Keller, 「Winning Hearts and Minds: The Secrets of Sustaining Change」、McKinsey & Company (2011年)、www.ru.is/media/opni/frettir/Winning-hearts-and-minds-McKinsey.pdf
- 17 Manyika, J.; M. Chui; J. Bughin; R. Dobbs; P. Bisson; A. Marrs, 「Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy」、McKinsey Global Institute (2013年)
- 18 Frey, C. B.; M. A. Osborne, 「The Future of Employment: How Susceptible Are Jobs to Computerisation?」(2013年9月17日)、http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf
- 19 Op cit, Bank of America Merrill Lynch
- 20 Verizon, 「2016 Data Breach Investigations Report」(2016年)、www.verizonenterprise.com/verizon-insights-lab/dbir/2016/?utm_source=pr&utm_medium=pr&utm_campaign=dbir2016
- 21 Bailey, T.; J. Kaplan; A. Marcus; D. O'Halloran; C. Rezek, 「Beyond Cybersecurity: Protecting Your Digital Business」、Wiley, USA (2015年)、www.wiley.com/WileyCDA/WileyTitle/productCd-1119026849.html
- 22 The Open Web Application Security Project, 「Category: OWASP Top Ten Project」(2016年)、https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- 23 National Institute of Standards and Technology, 「Framework for Improving Critical Infrastructure Cybersecurity」、USA (2014年)、<https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>
- 24 ISACA®, 「COBIT® 5 for Information Security」、USA (2012年)、www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx