デジタル運用モデルの5種類のリスク プロファイル

デジタル変革は、何らかの形ですべての組織に影響を及ぼしています。今日の組織にはさまざまなセグメントが存在しており、従来のアナログ型のプロセスから、はるかに接続性の高いデジタル型のアプローチへ移行しようとすることは珍しくありません。これらのイニシアティブが主に既存のプロセスを含む場合でも、ほとんどの組織は、ビジネスまたはミッション全体にわたってさらなる価値を引き出す助けとなるテクノロジーを求めています。

世界経済フォーラム（WEF）は、「業界のデジタル トランスフォメーション」において5種類のデジタル運用モデルを特定し、組織内で実施されているデジタル イニシアティブのさまざまな形態を説明しています。

	お客様中心型 お客様中心型のモデルは、フロント オフィス指向であり、あらゆるビジネス モデルをサポートするために使用可能です。	超倹約型 構造およびプロセス指向であり、高レベルの一元化、低コスト、および標準化型のモデルです。	データ基盤型 分析およびデータ主導という点に重点を置くコンピューター型モデルです。	「スカイネット」 マシンを多用することで、製造における生産性と柔軟性を高めることが可能です。	オープン型および流動型 エコシステムを構築してお客様の提案内容を強化、あるいはいくつかのアクティビティを実施します。
組織	分散型	標準的	センター オブ エクセレンス/ハブ アンド スポーク	標準的	ローカル
プロセス	フロント オフィスのプロセス	供給および製造におけるプロセス、サポート機能	高度な分析機能を必要とするすべてのプロセス	製造プロセス（危険な環境を含む）	外部世界との継続的なダイアログのフローがあるすべてのプロセス
人	フロントラインの強化	プロセスの最適化	俊敏性のテストおよび学習	自動化	コラボレーション、クラウド ソーシング
文化	クライアント最優先	少ない装備で充実した機能	セレンディピティ	「エンジニア」	共有
KPI	正味現在価値	コスト	投資収益率	フルタイム社員の割合	正味現在価値

出典：世界経済フォーラム

図1：世界経済フォーラムのデジタル運用モデル

組織がクラウド コンピューティング、ロボティクスおよび自動化、データ分析、IoT、モバイルの製品およびサービス、ソーシャル メディアなどのデジタル テクノロジーを活用して拡大と最適化をますます進めるにつれ、これらの運用モデルは企業内のさまざまな導入段階で使用される可能性があります。さらに、たとえばお客様中心型のプロジェクトにおいて、お客様との交流を通してより多くのデータが生まれたため、データ基盤型のプロジェクトを推進して新しいインサイトを得ようとするなど、複数のモデルが重なり合う場合もあります。これらのモデルは必ずしも相互に排他的なものではなく、むしろ組み合わせることで、デジタル イニシアティブによって生み出される潜在的なリスクを興味深い視点から考察し、理解できるようになります。

RSAは、デジタル リスクを「デジタル変革、デジタル型のビジネス プロセス、および関連するテクノロジーの採用に起因する、望ましくない、かつ通常は予期しない結果」と定義しています。言い換えると、一般的にリスクが対象に関する不確実性の結果と定義されることを考慮して、デジタル リスクは、デジタル変革に起因する対象の不確実性の結果に重点を置いているといえます。これらの新しいデジタル運用モデルが組織内で優先されるにつれ、リスクが混在する（および複数のリスクの性質が結びつく）状態は、デジタル イニシアティブの推進に伴う戦略的な進歩を妨げる最大の障害となります。デジタル ビジネスの不安定かつ超接続的な性質によって、新規のビジネス運用、および発展的なビジネス運用のリスクを管理しつつ、イノベーションを実現できる統合型戦略が求められています。

デジタル運用モデルのリスク プロファイル

リスクは非常に広範なトピックである一方、RSAが定義するデジタル リスク ドメインは、デジタル イニシアティブに関連するリスクの主要な側面を捉えています。

- **サイバーセキュリティ：**サイバー攻撃のリスク
- **プロセスの自動化：**自動化のプロセス変更に関連するリスク
- **耐久性：**ビジネス運用の可用性に対するリスク
- **サードパーティのリスク：**外部の関係者に関連する継承されたリスク
- **クラウド：**新しいデジタル ビジネス運用のアーキテクチャ、実施、導入および/または管理の変更によるリスク
- **ワークフォース/人材：**今日のワークフォースの動的な性質に関連するリスク
- **データ プライバシー：**個人情報に関連するリスク
- **コンプライアンス：**新しいテクノロジーによって決定されるコンプライアンス要件に関連するリスク

リスク エクスポージャについて理解し、デジタル イニシアティブのメリットを得ながらも、デジタル リスクから組織を保護するうえでの投資額を判断するために、リスクおよびセキュリティのリーダーは、ビジネスに合った持続可能かつ発展的なリスク管理戦略を実施する必要があります。5種類のデジタル運用モデルにはそれぞれ、ある程度の微妙な違いがあり、デジタル リスク管理戦略を形成するうえでの優先度が示されています。

お客様中心

組織がデジタル変革を進めるなか、お客様中心型のプロジェクトは最も注目を集める傾向にあります。これらのプロジェクトは、その範囲によっては多くの成長戦略のカギとなるため、戦略的目標を達成するうえで大きなプレッシャーが生まれます。さらに、お客様向けという側面により、世評という膨大なリスクが発生します。これらのタイプのイニシアティブで失敗が起きると、短期的および長期的な影響が広範囲に及びます。

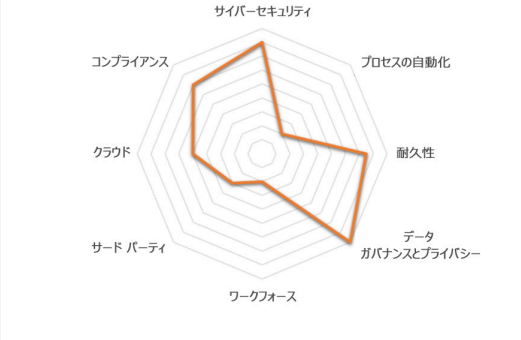


図2：お客様中心型モデルのリスク プロファイル

お客様向けのイニシアティブでは、多くの場合、個人データの収集と処理を行うことになります。そのため、サイバーセキュリティ、コンプライアンス、およびデータ プライバシーのリスクが上昇します。個人データには、GDPR、HIPAA、およびGLBAをはじめとするコンプライアンス要件の負担だけでなく、重大なレベルの世評リスクも伴います。データ侵害は非常に一般的であり（サイバーセキュリティの脅威が常に発生している状況では特に）、典型的な事例では一般に公開されてしまい、最悪のケースでは、全国的なニュースとなる場合があります。さらに、高可用性システムに対するお客様の期待と、お客様向けのシステムに関連するビジネスの停止が及ぼす経済的な影響を考慮すると、耐久性は、同様に優先すべきリスク管理の分野であるといえます。

超倹約型

多くの組織は、デジタル変革に取り組む際に、既存のプロセスを最適化するためのプロジェクトから着手します。WEFのモデルで「超倹約型」と呼ばれるこれらの最適化プロセスは、コスト コントロールを目標としており、範囲によって内容が大きく異なる場合があります。例としては、サービスのアウトソーシングまたはスペシャリストのスキルの利用や、仮想化テクノロジーの導入によって、ITコストを削減することなどが挙げられます。

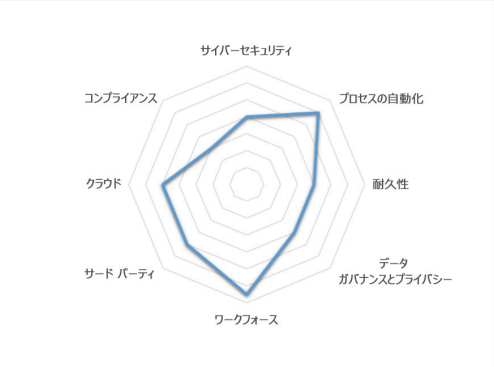


図3：超倹約型モデルのリスク プロファイル

これらの広範なプロジェクトを考えると、リスク プロファイルは、イニシアティブの性質に基づいて変動することになります。組織がこれらのプロジェクトに対して一般的にどのような取り組みを行っているかを見ると、リスクの側面のうちいくつかが、他よりも優先されていることが分かります。これらのプロジェクトの多くは、既存のプロセスをよりデジタル化された運用に移行することに目を向けているため、プロセスの自動化に関するリスクは重要な要素といえます。たとえば、サービス センターにおける手動タスクを排除するためにロボティクス プロセス オートメーション（RPA）を実装した結果、複雑さが生じた場合は、これを管理し、適切なモデルと処理手順が利用されていることを確認する必要があります。さらに、これらのプロジェクトの多くは社員ベースに影響を及ぼすため、ワークフォース関連のリスクは、社員の役割変更を管理することから、スキル セットを維持し、人員減に対処することまで、多岐にわたります。最後に、ほとんどの最適化プロジェクトにはクラウド テクノロジーとサード パーティの両方のエレメントが含まれており、それら両方の分野のデジタル リスクが強調されています。

データ基盤型

データを主軸としないデジタル イニシアティブは、基本的に考えられません。一方、データ基盤型のイニシアティブは、新しい革新的な方法で価値を引き出すために、データの使用率に対して全面的に重点を置いています。このような取り組みの多くは、組織の「バック オフィス」で行われており、既存または新規のデータ ストアを活用して複雑な分析を重ね、ビジネス プロセスを最適化する方法を模索しています。

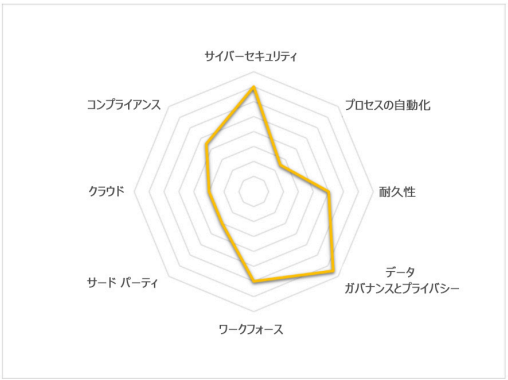


図4：データ基盤型モデルのリスク プロファイル

結果として得られるリスク プロファイルは、予測どおり、データ関連のリスクに偏っています。データ ガバナンスとプライバシー リスクは、データの性質によって異なり、たとえば、個人識別情報（PII）と知的財産（IP）の違いを挙げることができます。PIIの場合、プライバシーとコンプライアンスのリスクが増大するものの、データ ガバナンス（処理されるデータの内容、処理方法、およびデータの責任者などを把握すること）は、いずれのデータ基盤型イニシアティブにおいても必要となります。また、サイバーセキュリティは、データ基盤型イニシアティブのリスクを管理するうえで主要な役割を果たします。データの機密性と整合性は、保護されなければなりません。これには、データ アクセス（ワークフォース関連のリスクを増大させるもの）が適切であると保証することが含まれます。

スカイネット

WEFは、「マシンの台頭」と負荷の高い自動化をターゲットとするデジタル イニシアティブについて表現する際に、映画『ターミネーター』で登場する人工知能（AI）主導型のテクノロジーにちなみ、親しみを込めて「スカイネット」という用語を使用しています。一般に、このタイプのプロジェクトは製造業者と物流企業で見られます。ロボティクスは製造分野ですでに広く使用されていますが、自律走行車や拡張現実をはじめとするプロジェクト分野では、製造施設を最適化するために、さらに多くのデータが使用されています。

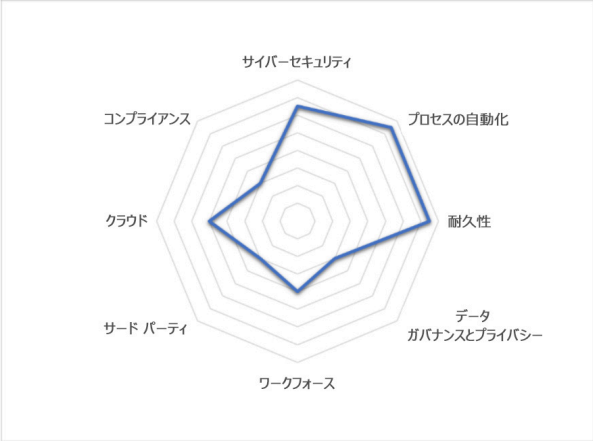


図5：スカイ ネット型モデルのリスク プロファイル

これらのイニシアティブのリスク プロファイルは、プロセスの自動化、耐久性、およびサイバーセキュリティに偏っています。自動化が製造のライフサイクルにおいて一層重要な部分を占めるようになったことで、少しのシステム停止であっても、重大な経済的および世評的な影響が生じることになります。また、これらのイニシアティブは、システム（特に、運用テクノロジー（OT）およびITシステムなど、従来のセグメント化されたインフラストラクチャ）の接続性向上に依存しています。この接続性により、セキュリティ侵害の潜在的な影響が製造フロアにまで広がり、サイバーセキュリティというエレメントがますます重大なものとなります。

さらに、AIの適用は大きな変化を伴うため、政府および規制機関は、AI対応の新しいテクノロジーをどのように規制すべきかについて、理解し始めたばかりにすぎません。スカイネット戦略を推進している組織は、該当する新しい法律および規制を慎重に予測し、モニタリングする必要があります。

オープン型および流動型

最後の運用モデルでは、パートナーのエコシステムと、さらなるデジタル戦略との関係が強調されています。これらの関係は多岐にわたり、外部関係者との全面的な共同事業、クラウド サービス プロバイダーの使用、サプライ チェーンへのより緊密な技術統合、スペシャリスト

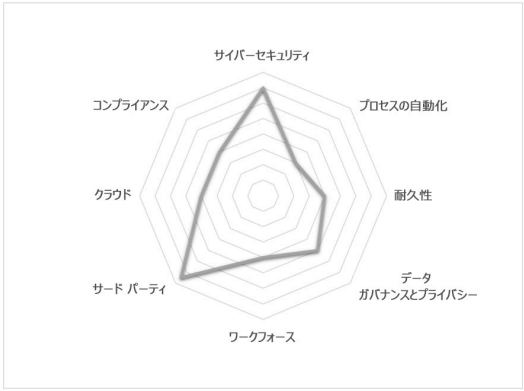


図6：オープン型および流動型モデルのリスク プロファイル

のスキルの選択的な使用などが挙げられます。WEFが呼び掛けているエレメントの1つは、異なるエンティティが共同で作業することでカスタマー エクスペリエンスを強化するという、お客様共通型の概念です。お客様向けのイニシアティブであっても、サプライチェーンの統合イニシアティブの一部であっても、通常これらのイニシアティブには、双方にメリットを生むためにデータフローと接続型のシステムが含まれます。

組織と複数の外部関係者間の接続性を考慮すると、サードパーティのリスクとサイバーセキュリティを管理することは、紛れもなくこれらの関係によって生じる悪影響を軽減するための主要な目標といえます。ガバナンス プロセスによって、サードパーティとの関係における所有権と説明責任を確立し、既知のリスクと課題を評価および追跡し、データおよびアクティビティの適切なアクセスとモニタリングを確実に行うことは、重要なエレメントとなります。エコシステムの性質によっては、耐久性が、特にサプライ チェーンの自動化の観点から見て要因の1つとなり得ます。データに起因する関係においては、データのガバナンスとプライバシーも懸念事項となります。

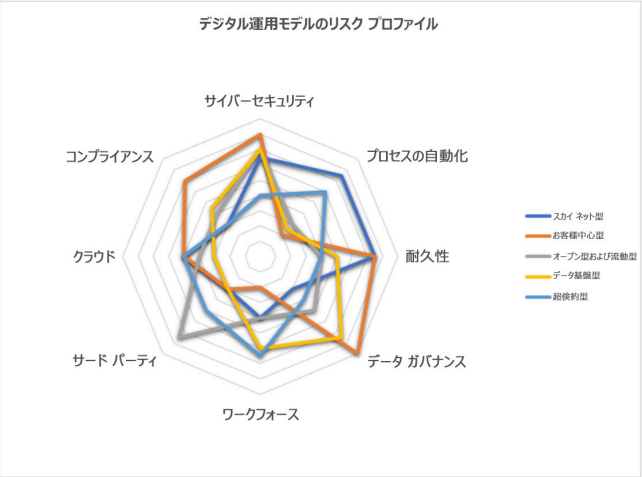
デジタル運用モデルの微妙な相違点についての説明

これらのリスク プロファイルは、デジタル運用モデルの一般的な特性に基づいています。しかし、それぞれのデジタル イニシアティブには、全体的なデジタル リスク プロファイルに影響を与える独自の要因が存在します。容量にかかわらず、クラウド テクノロジーを使用することで、デジタル リスクのエレメントは様変わりします。また、サード パーティ、業界や規制条件に関する幅広いコンプライアンスの影響、または、一時的あるいは季節限定の人材などを含む動的な社員ベースなどの要因も同様です。

重要なアクションは、運用の変更に関連するリスクを系統的に特定、評価、および処理することです。デジタル イニシアティブが展開されるにつれ、プロジェクトの固有の属性によって優先順位が決定されます。これらの一般的なプロファイルを適用することで、より詳細な分析を行うべき分野に着目することができます。重要な点は、継続的なリスク管理のライフサイクルとしてこのプロセスに取り組むことです。デジタル イニシアティブにより、ビジネス運用は今後も継続的に変化します。リスクの特定、評価、および処理のサイクルも、継続的に取り組む必要があるアクションとなります。デジタル運用は一般的に緊密に連携しているため、1つの分野で障害が発生すると、すぐに別の分野で課題が生じかねません。たとえば、サイバーセキュリティ攻撃はサード パーティ（サードパーティのリスク）によって発生し、ビジネスの中断（耐久性リスク）とデータ侵害（プライバシー違反またはコンプライアンス違反）につながる可能性があります。したがって、これらの分野に比例して対処するための統合型戦略が必要です。

まとめ

デジタル イニシアティブには、さまざまな形態が考えられます。ビジネスの運用に関する変更は、微小なものから大規模なものまで、多岐にわたります。いかなる場合でも、デジタルを基盤とする社内プロセスや、外部の製品およびサービスへと移行する流れにより、今日の組織は変革を余儀なくされています。それぞれのデジタル イニシアティブには、ビジネス運営



に及ぼす独自の影響力があり、結果として組織にもたらされるリスクもさまざまです。テクノロジーの導入によって成長を後押しし、イノベーションを促すというプラス面がある一方で、リスクというマイナス面を常に管理する必要があります。

デジタル運用モデルのさまざまなリスク プロファイルを理解することで、リスクを効果的かつ効率的に特定、評価、および処理するために優先すべき分野を明らかにすることができます。これらのリスク ドメインから事前に抜け出すことで、潜在的な障害を明らかにし、リスク管理のプラクティスをビジネスとともに進化させることができます。デジタル変革を成功させるための取り組みにより、事前にリスク管理に対応することができ、組織は、高度に最適化され、変革されたリスク管理機能によってサポートされるデジタル運用モデルの可能性を認識できるようになります。

誰もが抱えるデジタル リスク管理を私たちがサポート

RSAはBusiness-Driven Securityソリューションを提供し、さまざまな組織が、統合的な可視性、自動化されたインサイト、および組織的なアクションを使用してデジタル リスク管理のための統合的なアプローチを採用できるようサポートしています。RSAのソリューションは、高度な攻撃の効果的な検出および対応、ユーザーのアクセス制御の管理に加え、ビジネス リスク、不正行為、およびサイバー犯罪の削減を目的として設計されています。RSAは、世界中の数百万人のユーザーを保護し、Fortune 500の企業の90%以上をサポートして、これらの企業が成長を遂げ、引き続き革新的な変化に適応できるように支援しています。

動的かつ高リスクのデジタル世界で成長を遂げるための方法を学びましょう。 japan.rsa.com