KPMG

顧客の信頼

顧客に信頼されるブランドの中核には
信頼されるテクノロジーがある

home.kpmg/jp/Future-IT

目次

デジタル時代における信頼の重要性

信頼というものは、デジタル時代といえども不変で広範囲に通用する重要な価値であり、顧客と固く信頼で結ばれている企業は、その効果を享受していることは明らかです。調査によると、信頼されているブランドは顧客から高いロイヤルティを寄せられ、顧客の支出額も増える一方で、顧客の信頼を喪失するとビジネスに大きな悪影響が生じることが分かっています。

デジタル時代になり、顧客との信頼関係はより重要になっています。顧客に信頼されることは、もはやビジネスの基本的な要素などというものではなく、顧客に自社の新製品やサービスを選択してもらうための必須要件であり、重要な差別化要因といえます。

多くの業界で、テクノロジーは顧客のニーズや期待に応えるために欠かせない要素になっています。バーチャルフィッティングルームでジーンズを試着したり、スマートサーモスタットで家の中を快適にしたりと、多くの顧客がブランドとの接点においてデジタルによる顧客体験を経験しています。また、顧客がウェブサイトやアプリを直接使わなくても、テクノロジーの恩恵を受けていることも多々あります。例えば、在庫切れと同時に在庫補充を発注することで商品の欠品期間を短縮させたり、ホテルでは、得意客の客室を自動的にアップグレードしたりしています。

数字で見る信頼

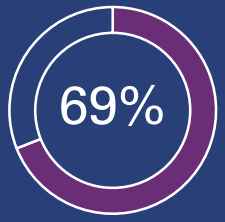
ブランドは信頼崩壊の危機に直面している

顧客の60%は、
企業が顧客にとっての最善の配慮を
行っていないと感じています

不信は取引を破綻させる

グローバルなブランドは、
信頼不足によって年間2兆5千億ドルの
コストが発生しています[4]

企業価値観の重要性

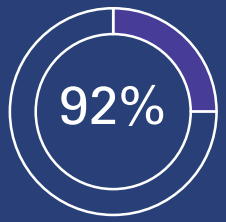


消費者の69%は、
倫理基準が高いとされる企業の商品を
購入しようと考えています[2]

透明性に対する価値

顧客の約40%は、
より透明性の高いブランドがあれば、
お気に入りのブランドから乗り換えるとしています[3]

プライバシーと信頼の関係性



顧客の92%は、顧客が提供した
プライバシー情報に対し、顧客自身が
管理できる企業を信頼する傾向にあります[5]

[1] State of the connected customer（Salesforce、2018年6月）

[2] An ethical compass in the automation age（KPMG米国、2017年）

[3] Trust is as important as price for today's consumer（Inc.、2018年5月18日）

[4] Lack of trust costs brands $2.5 million per year（Social Media Week、2018年2月6日）

[5] State of the connected customer（Salesforce、2018年6月）

技術革新によって、ビジネスも変革されます。新しいオペレーティングモデルが必要となり、それを支えるプラットフォームの需要も高まります。

世界の支出予測

2021年:

クラウドサービス：
2770億ドル[6]
（約29.9兆円*）

2022年:

IoT：
1兆ドル以上[7]
（約108兆円*）

人工知能：
776億ドル[8]
（約8.4兆円*）

ブロックチェーンソリューション：
117億ドル[9]
（約1.3兆円*）

*1ドル=108円

[6] Worldwide Semi-annual Public Cloud Services Spending Guide（IDC、2018年1月）

[7] Worldwide Semi-annual Internet of Things Spending Guide（IDC、2019年1月）

[8] Worldwide Semi-annual Cognitive Artificial Intelligence Systems Spending Guide （IDC、2018年9月）

[9] Worldwide Semi-annual Block chain Spending Guide（IDC、2018年7月）

テクノロジーは、企業と顧客の良好な関係を支える要素として重要性を増しています。しかしながら、41%の企業は明確なデジタルビジネスのビジョンや戦略を持っていません。また、50%の企業は、顧客とのやりとりを通じ、顧客に対して統一した評価や見解を持っておらず、49%の企業は個々の顧客データを利用した、顧客対応のパーソナライズを行っていません[10]。この状況は、破壊的な新しいテクノロジーとそれを活用しうる新しいスキルセット獲得のための投資によって変わろうとしています。今後3〜5年間で、人工知能（AI）、モノのインターネット（IoT）、クラウド、ブロックチェーンなどの破壊的テクノロジーへの投資は急増する見込みです。テクノロジーに基づくイノベーションが急速に進化し、企業はそれらを事業運営に深く組み込むようになるでしょう。続いて労働力に変化が起こります。CEOの76%は、先端技術のスペシャリストの採用を優先するとしています[11]。近い将来、テクノロジーは、製品やサービス、デリバリーモデルのほとんどを支えるバックボーンになるでしょう。

テクノロジーの進化とともに、顧客体験に与えるテクノロジーの影響も大きくなるでしょう。最先端技術によって、顧客とブランドの関係性が変わります。今では、巨大なテクノロジー系企業によって、高い技術障壁が築かれており、また、ほぼすべての業界において、機敏なスタートアップ企業による破壊的な変革が引き起こされています。これからのブランドは、過去データの自動分析に基づく対応と、顧客への最適な価値の提供のために、企業全体に革新的技術を導入していくことになるでしょう。

[10] Harvey Nash／KPMG 2018年度CIO調査
[11] KPMG U.S. CEO Outlook Survey 2018（KPMG米国、2018年）

このような局面では、テクノロジーリーダーは厳しい現実にさらされます。健全な顧客関係を維持するには、複雑で目に見えないことも多いコネクテッドなテクノロジーが必要になってきています。しかし、人々は直観的に、目に見えず触れられない、理解できないものには不信感を抱くものです。

多くの顧客がデジタル世界におけるビジネスリスクについて懸念するのもやむを得ないことです。ビッグデータ分析によって、ブランドは個々の顧客に合うサービスを提供できます。一方で、顧客は自分の情報がどのように使われているかをコントロールしたいと思っています。IoTによってアナログな製品がスマート化しネットにつながる一方で、利用者の極めて個人的なデータモデルが作られます。製品には新しい階層が加わり、複雑になるとともに、新しいサイバー脅威が生じます。AIはパーソナライズされた体験を生み出し、日常業務を合理化することができるものの、それが「気味が悪い」と感じられたり、単純な作業が思い通りにならず、フラストレーションを感じることもあります。

現在、テクノロジーを用いたブランドは、顧客と接する際に顧客が自社に盲目的に信頼することを求めていることが頻繁にあります。テクノロジーリーダーは、次のような難しい質問に直面しています。「機械学習のアルゴリズムがこれから私たちに代わって倫理的な選択をしてくれるとどうして言えるのか」、「車の自動運転システムが誤作動しないと言い切れるのか」、「個々人に合うサービスを受け取るため個人データを渡した場合、そのデータには誰がアクセス可能で、どのような用途で使われるのか」。

デジタルがビジネスのバックボーンになると、テクノロジーに付随する不確実性の取り扱いが、顧客との信頼を高めるための、ビジネスとテクノロジー双方における優先課題になります。

「デジタル時代の新しい製品やサービスにとって、顧客の信頼は最も重要な価値です。顧客からの信頼を確保するためのオペレーティングモデル（規範や行動からプロセス、ポリシー、ガバナンスまで）を確立するために、テクノロジーは重要な役割を果たし、将来の成功へ導くでしょう」

Steve Bates, Global Lead
CIO Center of Excellence, KPMGインターナショナル

テクノロジーリスクの状況

32%

企業の32%が、リスク管理とサイバーセキュリティがテクノロジーの商業利用にとって最大の障壁だとしています[12]。CEOの**9%**は、顧客データの保護は大きな関心事だと言っています[13]。

50%

テクノロジーリスクリーダーの50%が、先端技術によって自分たちの仕事の範囲は拡大していると述べています[14]。

33%

企業の3分の1以上が、AI、クラウド、IoT、モバイルに関連するリスクを評価することなく、速やかに採用しています[15]。

41%

企業の41%は、明確なデジタルビジネスのビジョンや戦略を持っていません[16]。

50%

企業の50%は、すべての顧客とのやり取りについて、統一的な見解を持っていません[17]。

49%

企業の49%は、顧客データを利用した顧客体験のパーソナライズを行っていません[18]。

76%

CEOの76%が、最先端技術のスペシャリストの採用を優先課題と位置づけています[19]。

[12] 変化し続ける破壊的テクノロジー（KPMGインターナショナル、2017年）

[13] KPMG U.S. CEO Outlook Survey 2018（KPMG米国、2018年）

[14] Disruption is the new norm: Tech risk management survey report（KPMG米国、2017年）

[15] Disruption is the new norm: Tech risk management survey report（KPMG米国、 2017年）

[16] Harvey Nash／KPMG 2018年度CIO調査

[17] Harvey Nash／KPMG 2018年度CIO調査

[18] Harvey Nash／KPMG 2018年度CIO調査

[19] KPMG U.S. CEO Outlook Survey 2018（KPMG米国、2018年）

KPMG

顧客の信頼獲得における テクノロジーリーダーの果たすべき役割

テクノロジーで顧客体験を強化する場合、デジタル製品・サービスの主要要素として信頼が備わっていることが必要です。実際、最高情報責任者、最高技術責任者、最高情報セキュリティ責任者、最高デジタル責任者、最高イノベーション責任者などのテクノロジー担当エグゼクティブにとって、「**技術的信頼**」と言われるテクノロジーへの信頼を築くことは、今や戦略的に不可欠です。

技術的信頼とは、デジタルによる優れた顧客体験――アクセスが容易で、わかりやすく、透明性に優れ、安全に体験できること――を提供できる技術的能力を企業が備えていることと言えます。技術的信頼の確立は、未来の顧客と良好な関係を築く基礎になります。すなわち、顧客はデジタルによって体験できるあらゆるメリットを求めながら、すべてのリスクを避けたいと考えているため、これらに応えることが顧客との関係の基礎となるのです。

デジタル時代において、企業が顧客に安全、かつ一貫したサービスを提供するには、技術的信頼に基づくことが不可欠です。

顧客との関係性を形成する際に、高レベルで技術的信頼を獲得した企業は強力にテクノロジーをコントロールしている様子を顧客に示すことができます。また、このテクノロジーのコントロール力が企業の真の競争優位を生み出すことにつながると言えます。企業による適切なテクノロジーのコントロールは、テクノロジーによって顧客の日常に生じる不安や恐怖を和らげ、より良い結果を導きます。顧客は自分が守られ、大切にされていると感じ、デジタル対応の製品やサービスを信用し、受け入れやすくなります。信頼があれば、優れたテクノロジーを取り込んだ製品は一時期の流行として消え去るのではなく、持続可能なプラットフォームへと進化することができます。

技術的信頼は、顧客による企業認識に直接的な影響を与える可能性があります。大手調査会社のForresterは、企業の印象は透明性、信頼性、能力によって向上すると結論付けています。これらの印象は、過去の相互作用を通じて時間をかけて形成されていくものです[21]。

技術的信頼という概念は、顧客向けの技術だけに当てはまるものではありません。それは、企業のあらゆるオペレーションにおけるテクノロジーを融合し連携することで、顧客の課題解決に向けて活動するということです。また、日常業務に新しいテクノロジーやデータソースを活用しなければならない社内顧客（つまり、従業員）も、技術的信頼があると当該サービスを積極的に活用するようになります。従業員は、テクノロジーの目的を理解し、従来の方法より優れた結果が得られると確信すると、業務に新しいテクノロジー――Eメールプラットフォームからワークフロー用のモバイルアプリ、そしてコラボレーションツールなど――を利用するようになります。

テクノロジー担当エグゼクティブは、技術領域のリーダーとして、フロントオフィス、ミドルオフィス、そしてバックオフィスにおける企業の重要な能力を有効に連携させることで、顧客からの技術的信頼の獲得に重要な役割を果たすことができます。ブランドのテクノロジーに信頼が寄せられるならば、ブランド自体にも信頼が寄せられます。テクノロジー担当エグゼクティブは、技術的信頼を確立することにより、顧客が好む体験を持続的に提供し、より大きなビジネス利益を導くことができるのです。

顧客をリスクから守りながらサービスを提供します。

技術的な信頼は、企業が顧客にポジティブな体験を提供するために必要な一連の技術的特性です。

企業を信じ、信頼します。

技術的信頼とは、企業に対する顧客の全般的な評価に直接影響を与えるもので、企業の透明性、信頼性、能力に対し、顧客が過去の相互作用を通じて形成するものです。[20]

[20] The mechanics of trust（Forrester、2018年12月）
[21] The mechanics of trust（Forrester、2018年12月）

技術的信頼の創出 → **技術的信頼の獲得**

テクノロジー担当エグゼクティブ
信頼獲得の触媒役

バックオフィス
- 企業と製品のセキュリティ
- 社内向け製品とアプリケーション
- アベイラビリティとレジリエンス
- サードパーティのガバナンス
- ITリスクマネジメント

ミドルオフィス
- コネクテッドサプライチェーン
- 製品イノベーションとエンジニアリング
- データに基づく分析と考察
- プロセスオートメーション

フロントオフィス
- 顧客体験
- デジタルチャネル（モバイル、IoT）
- 製品、プラットフォーム、サービス
- 販売とマーケティング

外部顧客

技術的信頼の構築方法

企業が顧客から信頼されるソリューションを提供するには、テクノロジーリーダーはどうすればよいのでしょうか。

顧客の信頼を呼び起こし、維持するために、組織全体でどのような能力を育成すべきでしょうか。

技術的信頼は、顧客が企業イメージを形成する上で最初に意識する重要な要素であり、**サービス、保護、統治**の3要素から成り立っています。顧客の信頼獲得に成功する技術チームとは、顧客に対し円滑で、ダイナミックかつ弾力性に富んだ相互作用を通じ、顧客に貢献するものです。そのようなチームは、顧客を不測の事態から**保護**し、事態が悪化した場合には迅速かつ透明性のある対処で、問題を解決するために様々な取組みを行います。予め製品デザインの中核にセキュリティとプライバシーを組み込み、データ利用においては、責任をもって倫理的に行います。

さらに、コネクテッドデジタルエコシステムが容赦なく急速に進化する中で、変化に柔軟なポリシーと実務によってテクノロジーを**統治**します。顧客の信頼を棄損する可能性のあるリスクは、IT組織が継続的に管理します。

これは単なる技術的な挑戦ではありません。顧客の目標達成に向けた推進役という、ITの新しい戦略的任務を遂行するため、IT組織の変革は勿論、自らの役割に対する認識を運用サポートから顧客サービスとソリューションの提供へとマインドセットを変える必要があります。

技術的信頼の創出

サービス

— Everything-as-a-Service
— サービスのレジリエンス
— 摩擦のない顧客体験

保護

— セキュリティとプライバシーの設計
— 資産としてのデータ
— ダイナミックなインシデント対応

統治

— 継続的な資産管理
— デジタルリスクマネジメント
— 統一的なコンプライアンス

技術的信頼の獲得

透明性

— 複雑化ではなく明確化を推進

信頼性

— 本物の価値を守る

コンピテンシー

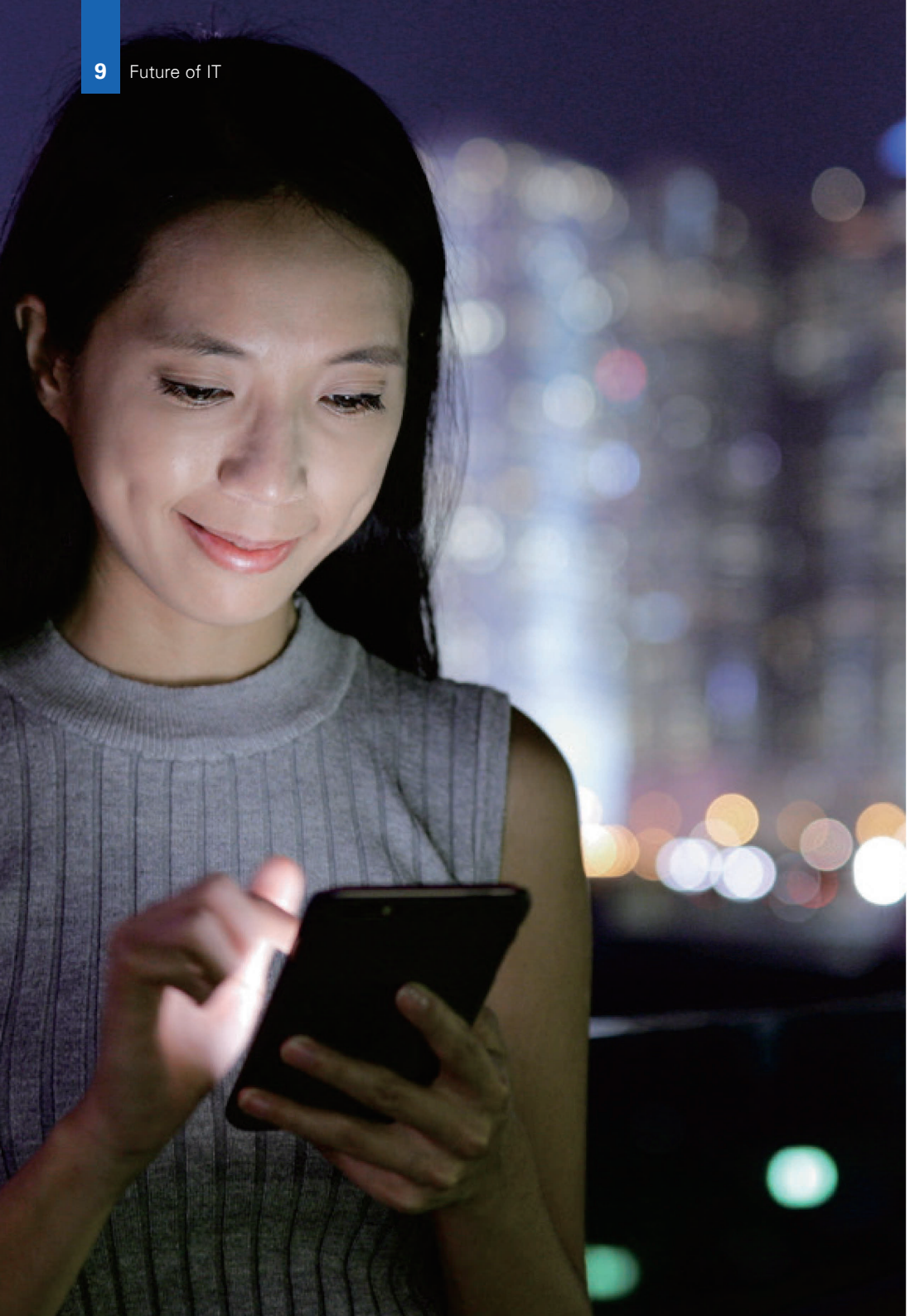
— 約束どおり実行する能力

The mechanics of trust（Forrester、2018年12月）

これまでのIT組織の主業務は、事業運営を支えるバックオフィスのシステム構築と管理でした。しかし、デジタル時代の展開とともに、テクノロジーは次第に顧客の体験にとって根本的に重要な要素になりつつあります。人やモノはますますつながるようになり、企業と顧客間で発生し、交換するデータ量は爆発的に急増します。顧客エンゲージメントは対面よりもデジタルーフィジカルの体験を通じて生じるようになるでしょう。

重要なビジネスの成果をサポートするには、テクノロジーリーダーの責務の中でも、顧客関係の構築・管理が重要になりますが、これは単純なバックオフィス用のツール管理ではありません。昔ながらのテクノロジープロジェクトの管理方法では、これらの責務に対応することは困難です。たとえ顧客向けの革新的なデジタルプロジェクトを迅速に稼働させても、単に製品やサービスを提供するだけでは顧客の信頼を獲得し、さらに高めることはできません。問題をもっと大きく企業活動全体的に捉え、大きなソリューションとして扱っていく必要があります。テクノロジーはもはやバックオフィスのITといった企業の能力向上のための存在ではなく、顧客が望む体験の実現を促進することを求められています。IT主導で事業運営、企業文化、ガバナンスに幅広い変革を起こしてこそ、顧客を尊重し安全確保ができる環境を創り出せるのです。

次頁以降の各セクションで、技術的信頼の各要素を構成する主な能力、つまり、デジタル時代の技術リーダーにとって優先すべき特性について解説します。



サービス: 顧客第一

サービス

— Everything-as-a-Service
— サービスのレジリエンス
— 摩擦のない顧客体験

行動は言葉より多くを語ります。顧客に高品質なデジタルサービスを提供することで、将来における顧客との対話の方向性が定まり、信頼関係の基礎が築かれます。

顧客は、意のままに自らのニーズを充足させ、価値を高めてくれるテクノロジー主導の体験を求めています。このような顧客体験を提供するには、テクノロジー部門は 3つの能力、すなわち、Everything-as-a-Service、サービスのレジリエンス、摩擦のない顧客体験の提供が必要です。

Everything-as-a-Service

タクシーを呼ぶ。食料品を買う。処方薬を調剤してもらう。テレビ番組を見る。小切手を換金する。車を修理する。テクノロジーインターフェースは顧客とブランドの接点として急速に広まり、好まれるようになっています。あらゆる業界において、ウェブサイト、アプリ、コネクテッド製品などの多種多様なモバイルやデジタルチャネルを通じて顧客エンゲージメントが提供されています。

ITには、どのような場所でもインターネット経由で動的な顧客とのやりとりを可能にする責任があります。一般的には、ITはデジタル製品・サービスの運用は勿論、変化する顧客の期待に応えるための継続的な機能改善においても、クラウドを有効活用するようになります。SaaS（Software-as-a-Service）、PaaS（Platform-as-a-Service）、IaaS（Infrastructure-as-a-Service）などのクラウドコンピューティングによって、企業は顧客向けアプリの遠隔管理、新技術の開発・テスト、外部でのデータ保存・管理が可能になります。時には、サードパーティプロバイダーと一緒に実施することも珍しくありません。

Everything-as-a-Serviceモデルには、多くのメリットがあります。テクノロジー資産と関連コストを削減しながら、ITはより柔軟に、マーケットスピード（市場の変化速度）に応じて製品やサービスを進化させることができます。しかし、それと同時にレジリエンスと信頼性に関する疑問も生じます。例えば、クラウドベンダーがサービスを停止したり廃業したりした場合はどうなるのでしょうか。Everything-as-a-Serviceモデルの効果性を担保するために、サードパーティを適切に活用し、先を見越してリスクを管理する強力なポリシーが必要です。

サービスのレジリエンス

アプリの読み込みが遅ければ、顧客はそのアプリを削除します。ウェブサイトに接続できなければ、他のサイトへ行ってしまうでしょう。

スタートアップ企業やテクノロジー企業は顧客体験を巡る競争を加速させていますが、その影響を受け、ブランドに対する顧客の期待値は変化しています。今日の顧客には、いつでも満足が得られるオンデマンドが定着し、欲しい製品やサービスがあれば、即座にアクセスします。製品やサービスが、いつでも、どこでも使えることを当然のように見なしているため、顧客の信頼を得るには、製品やサービスの信頼性が重要な要素となります。

テクノロジー部門は、レジリエントな技術によって、信頼性の高い製品やサービスの提供を支援します。KPMGの調査によると、テクノロジーリーダーの62%が、一貫性のある安定したITパフォーマンスを提供することはビジネス上の重要な課題だとしています[22]。これらのリーダーは、デジタルサービスはアナログ体験と同様に（できればそれ以上に）機能しなければならないと認識しています。

摩擦のない体験

顧客は自分の時間を大切にします。貴重な時間の節約につながったデジタル体験は印象深いものになるでしょう。反対に、認証プロセスが面倒で時間がかかったり、直観的に分かりにくいインターフェースで操作に苦労すると、顧客は離れていきます。このような過去の経験が製品やサービスにおける摩擦のない体験に対する顧客の期待値を形成しています。

IT組織は、テクノロジー開発の主目的に顧客中心で優れた顧客体験の提供を据えることにより、直観的で自然なデジタル体験を提供できるようになります。たとえ自社が製品の市場投入を急いでいる時でも、IT組織は時間を確保してユーザー体験を検討しなければなりません。

デジタル製品やサービスの設計において、顧客中心主義は信頼構築と広範囲な自社製品の利用促進につながります。顧客中心の企業は、そうではない企業に比べ、高い利益率を上げる可能性が38%高くなっている[23]、という調査もあり、労力に値する見返りが得られるはずです。

小売業が自らを一新するにつれて、顧客信頼がすべてになります。

小売業界では、デジタル技術とそこから生まれる新しいビジネスモデルが、顧客に対するサービス提供方法に変革を起こしています。小売業は、かつては伝統的なブリックアンドモルタル店舗が独占していました。続いて、オンラインショッピングが登場しましたが、現在の小売のビジネスモデルは両者のハイブリッドへと進化しており、顧客には購入方法の選択肢が与えられます。また、非従来型の破壊的イノベーターなど、最先端の小売業者は、即日配送、店舗受け取り、個人の好みに合わせたおすすめ機能、対話型モバイルアプリなど、ショッピング体験をさらに向上させる革新的サービスを開始しています。

小売業界にとっては、可能性に満ちた刺激的な時代ですが、リスクもあります。現在、そして将来競争する小売業者にとって、デジタル消費者にリーチするだけでは十分ではありません。次第に高まる顧客の期待に対応し、従来を上回る方法でデジタル消費者にサービスを提供するために、アクセスしやすくパーソナルな摩擦のないサービスをいつでも利用できるようにする必要があります。また、最近の小売業者の倒産事例からも明らかなように、これはかつてないほど大きな賭けになるかもしれません。

[22] Harvey Nash／KPMG 2018年度CIO調査

[23] Harvey Nash／KPMG 2018年度CIO調査

プラットフォーム企業がビジネスの範囲を拡大するには、データセキュリティに重点を置くことが必要です。

信頼獲得の大きな障害の1つは、顧客が、自らが被害に遭うのではと不安に感じることです。顧客が引きつけられるブランドとは、正しい行動を取り、質の高い製品を提供し、個人情報を保護してくれると感じられるブランドです。

過去10年間に、有力なグローバルテクノロジー企業は、顧客が信頼し、使用しても安全だと感じるプラットフォームを構築することによって急成長を遂げ、かつてない程の範囲にサービスを拡大し、影響力を与えることになりました。最近のテクノロジー業界のプライバシー論争が顧客の信頼を裏切る形になっているものの、これらの企業は一般的に、安全な製品を作り、顧客データを保護し、問題が生じた時には迅速な対応と解決策を提供できるよう高い基準を設定しています。

保護: 顧客の保護

保護

— セキュリティとプライバシーの設計
— 資産としてのデータ
— ダイナミックなインシデント対応

安全への欲求は人間本来の欲求であり、デジタルの世界でも変わりません。もし、顧客が不当な扱いを受けた、または危険に晒されたと感じるようなことがあれば、それまでどんなに素晴らしい顧客体験をしていても、即座に忘れ去られてしまうでしょう。企業が顧客と信頼関係を構築し、それを維持するには、顧客の保護が必須要件となります。

まずは、顧客とやりとりするデジタルプラットフォームに安全対策を施し、顧客が提供に同意したデータを脅威から守ることです。

テクノロジー的には、顧客を保護するために次の3点を踏まえておく必要があります。設計段階からセキュリティとプライバシーを優先すること、データを資産として扱うこと、そしてダイナミックなインシデント対応を確立することです。

セキュリティとプライバシーの設計

デジタル顧客に触手を伸ばす企業はすべて「テクノロジー企業」へと変貌を遂げつつあります。この新たに広がったコネクティビティとそれに伴う固有の技術的な複雑さによって、企業は新しい脅威に晒されているものの、対処方法が確立していません。サイバー攻撃者は、価値が高まり続けるデータ資産を狙い、新手で巧妙な手段を探してデジタル資産にアクセスし、曝露しようとしています。最近公開されたデータ侵害の中には、悪意のハッカーによるものではなく、個人情報の非倫理的な使用も見受けられます。このような事例は、情報の窃盗ではなく、大企業が顧客の個人情報の扱いにおいて顧客の信頼を裏切る行為によるものです。このようなことがあると、プライバシーに関して消費者の不安が拡大するため、EU一般データ保護規則（GDPR）やカリフォルニア州消費者プライバシー法制定等、広範囲に及ぶ新たな規制が必要とされることになります。

私たちが生きている時代では、セキュリティとプライバシー保護が、良好な顧客関係を築く上で当然のこととして見なされています。つまり、今日のビジネス環境では、顧客の個人情報を保護するため、デジタル製品とサービスにセキュリティとプライバシー対応を実装することは当然であると受け止める必要があります。このように、企業はテクノロジーの設計方法を変える必要に迫られているのです。

設計段階からセキュリティとプライバシー保護を織り込んでいれば、多様なリスクから最終顧客を守ることが可能で、ブランドへの信頼毀損を防ぐことができます。それはまた、様々なリスク、すなわち、規則違反、ノンコンプライアンス、公的不祥事による財務、法律、事業、評判上の悪影響から企業を守ることにもなります。

さらにこれは、コスト削減の好機でもあります。開発時にセキュリティとプライバシー対策を組み込む方が、事後的に対処するよりはるかに低コストで済むからです。

ある調査によると、ソフトウェア障害の大半はバグ、不具合、セキュリティ上の脆弱性などの予防可能なソフトウェアエラーによるもので、それらによる経済的損失は2017年には1兆7000億ドルに上りました[24]。別の分析によると、大企業は、ウェブサイトやEコマース上でページのアップロードが遅いなどの回避可能なエラーによって簡単に月に数百万ドルもの売上高と顧客を失う場合があります。それらのエラーをさかのぼって修復する費用は月に数万ドルと推定されます[25]。

資産としてのデータ

データは、デジタル世界の新しい価値ある資産であり、組織はデータを貴重な資産として扱う必要があります。顧客との信頼関係を築くには、顧客データの保護が特に重要です。

人口統計情報から行動履歴といった顧客データを、アナリティクスとオートメーションにかけると望外な価値を生み出します。顧客へのサービス提供方法を改善することに寄与する貴重な洞察も得られますが、顧客は自分のデータの使われ方は、ある程度コントロールしたいと考えるため、自分のニーズに適う場合にデータを提供します。言い換えれば、企業からの度重なるデータ要求、単純なサービスのための無用なデータ要求、データの目的外使用、データを安全に取り扱う基本的な手順の欠如、データポリシーの不透明さを感じた場合には、データの提供を警戒するでしょう。GDPRの新しい要件や、顧客データが悪用・換金される事件が公になる中で、企業には、オプトイン／オプトアウトのポリシーと手続き、データの最小化、ユースケースの承認、データのライフサイクルの保護、保有と処分など、正式なデータガバナンス機能を持つことが期待されています。

テクノロジー組織ならば、データガバナンスプログラムを導入し、貴重な顧客データを盗難、損失、誤用から遠ざけることができるでしょう。また、誰がどのようにデータを利用しているかを顧客が常に把握できるようにしておくことも、顧客に対する責務でしょう。

ダイナミックなインシデント対応

現在のビジネス環境はより複雑になり、コネクティビティが拡大しているため、サイバーインシデントは今やいつでも起こりうるものという認識が広まりつつあります。KPMGの年次調査では、取締役会ではサイバーインシデント対応が他のどのテーマよりも重要な議題となっています[26]。

また、顧客は侵害をすべて防止できるわけではないことに理解はあるものの、侵害の検知の失敗や隠蔽は許されません。大手ブランドがサイバーセキュリティの失敗を即座に認めなかったため、消費者の不信感が強まった事例があります。

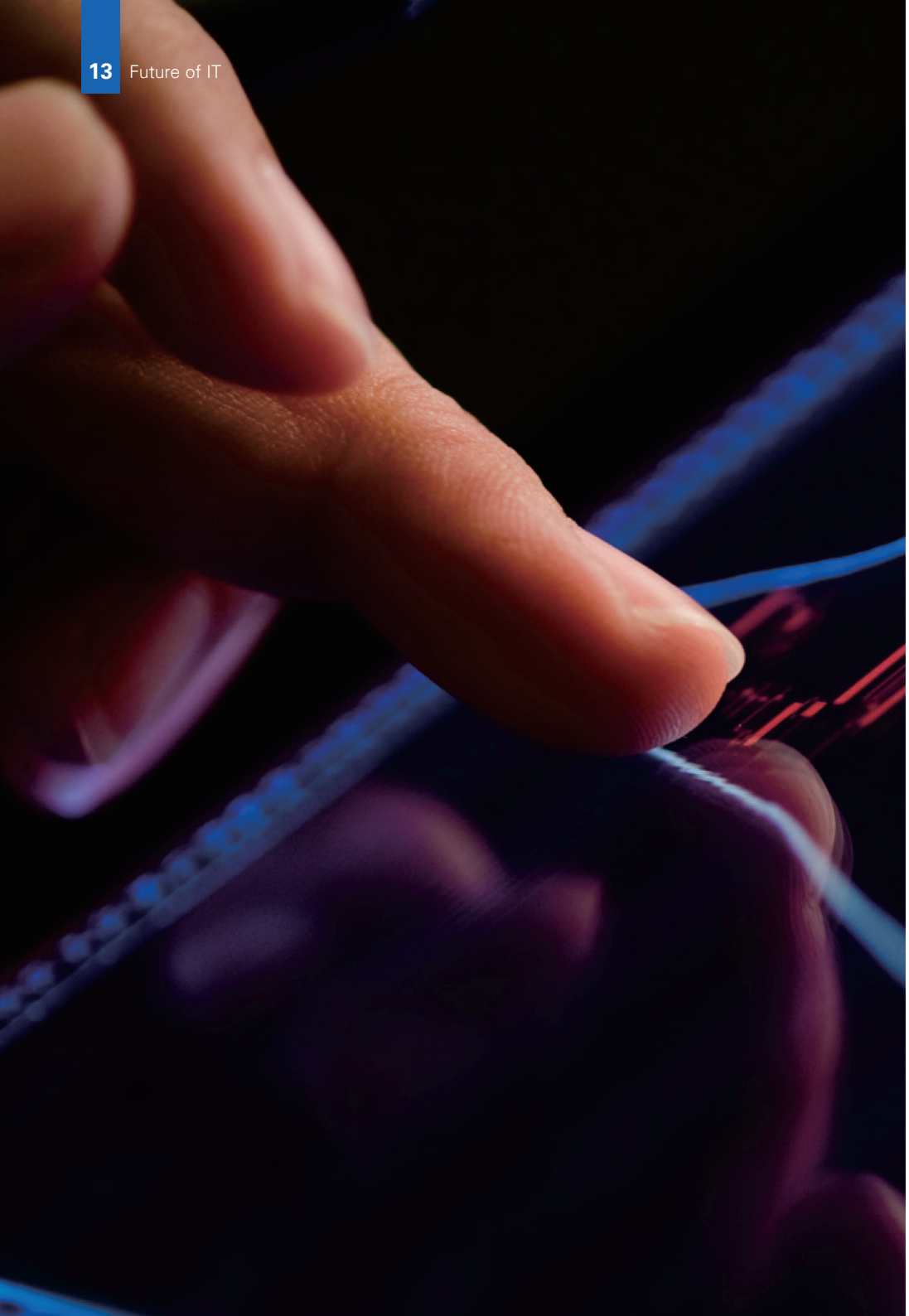
事後対応ではなく事前にインシデント対応に備えておけば、サイバー侵害のダメージを最小限に抑えられます。多層防御を実装し、潜在的脅威に対するテクノロジー環境を強化することが基本になりつつあります。多層防御によって、データやシステムの妨害、盗難、その他の悪意ある行為から保護し、疑わしい活動がネットワークに深く侵入する前に特定して警告することができます。

優れたテクノロジー部門は、サイバーセキュリティの問題によるブランド棄損を避けるため、予測能力にも投資します。脅威を早期発見し、封じ込めの能力を高めるとともに、インシデント対応や救済策の策定労力を軽減して、透明性の高い方法で顧客に伝達することも可能になります。

[24] 2017 Software Fail Watch report（Tricentis.com）

[25] Cost of software errors（Raygun.com）

[26] Harvey Nash／KPMG 2018年度CIO調査



統治: 技術リスクを管理する

統治

— 継続的な資産管理
— デジタルリスクマネジメント
— 統一的なコンプライアンス

製品・サービスが顧客の信頼を勝ち取るために、テクノロジーは非常に大きな役割を果たしています。しかしながら、このテクノロジーは、絶えず新たな要求に対応すべき宿命にあります。テクノロジーが進歩、進化すると新しいリスクが現れ、それに対処する規制が拡大されます。

この変わりやすいデジタルエコシステムを管理するため、デジタルガバナンスが着目されています。デジタルガバナンスとは、共通のビジョンを組織に浸透させ、共通のツールとプラットフォームでデジタル製品とサービスを創造し管理するものであり、官僚主義的に手続きばかり増やして機敏さに欠けるというものではありません。

デジタルガバナンスプログラムには、重要で実践的な手段が3つあります。すなわち、継続的な資産管理、デジタルリスクマネジメント、統一的なコンプライアンスの3つです。デジタルガバナンスプログラムの適切な運用により、官僚的で煩雑な管理からイノベーションを解き放ち、持続的な成長が可能となります。

継続的な資産管理

デジタル時代にはテクノロジー資産の定義が変化しています。以前はほとんどのIT資産が企業のデータセンターの物理装置内に収まっていました。今日のデジタル製品・サービスは、資産によっては、企業内ネットワークの外部に存在する場合もあり、以前とは様相が異なります。

顧客の信頼醸成に必要な能力の大元は、これらの内外の資産を追跡、監視できることです。これが備わっていないと、ビジネスのレジリエンス、サイバー脅威への対応、データプライバシー規制への対応、効率的な業務運用、業績向上等は不確実と言えます。新たにネットワークに参加するデバイスがあればリアルタイムに特定、プロファイリングするとともに、標準的なセキュリティ要件を適用、その後にその新しいデバイスにリソースへのアクセス権を与えることになります。これら一連のことを適切に実行するには、ツールの助けが必要でしょう。

デジタルリスクマネジメント

顧客との信頼関係を維持し、顧客に安心してサービスを利用してもらうためには、当該サービスに内在するテクノロジーリスクを特定し、リスク軽減策を準備しておく必要があります。最も有効な方法は、事業上の優先課題とリスクの特定・軽減策を連携させ、共通の枠組みで取扱うことです。

部門横断的なデジタルリスクマネジメントフレームワークは、企業が常時リスクを測定、管理するための土台として、また、デジタル製品・サービスの継続的な成長の促進剤として有益なものです。

さらに、将来を見通した新技術の適応や、リスクが顕在化しても問題化する以前に対応するためにも役立ちます。

ブロックチェーンやインテリジェントオートメーションのような最先端テクノロジーは、リスクマネジメントに革新を引き起こすでしょう。たとえば、固有のリスクを軽減し、リソースの時間を節約したり、ブロックチェーンによってデジタルトランザクションの信頼性と透明性が保証され、多数のノードで検証された信頼性の高い記録を作成することが可能になります。また、インテリジェントオートメーションによって、高いリスクがあると見込まれる業務プロセスも継続的に監視が可能になります。さらに、データ分析は、リスク予測の一助になります。

統一的なコンプライアンス

テクノロジー組織において、コンプライアンス要件が拡大すると、対応には大きな困難を伴います。要員のストレス、対応コスト、監査疲れといった事態が発生するからです。多くのデジタル製品は、取扱いに注意を要する繊細なデータを収集し利用しているので、コンプライアンス対応には大きな負担が発生します。データ保護に関する新法のGDPRでは、3分の2以上の企業が影響を受けます。規則に違反した企業に最高2000万ユーロ、または年間の全世界売上高の4%に相当する金額の罰金が科されます[27]。その他、顧客データの収集と処理に影響を与えるコンプライアンス要件には、SOC2、HITRUST、ISO27001、PCIなどがあります。

こうした法的要件が強化される状況下では、各コンプライアンス対策を個別に取り組むべきではありません。テクノロジーリーダーは、コンプライアンス対策を1つのプログラムに統合する必要があります。それによって、製品の改善、監査要件の整合、管理の標準化の促進、人員のタッチポイントの制限、不要な情報要求の削減が可能になります。

また、主要なリスク指標とリスク情報が集約されたダッシュボードを準備し、それを監視することで、貴重な情報を各部門や組織に提供できます。

この施策の目標は、コンプライアンス業務を合理化し、自立した管理体制を構築することで、ビジネスチームと製品チームに貴重な時間を取り戻し、ひいては顧客に優れたサービスを提供することにあります。

テクノロジーの進化とともに、テクノロジーのガバナンスも進化しなければなりません。

企業のあらゆる側面に相互接続技術が組み込まれるようになっていくと、プロセスの標準化を進め、コンプライアンス要件を満たす活動を継続的に実施していく必要があります。

先進的な企業は、リスクマネジメント機能と企業ガバナンス機能を進化させることでリスクマネジメントを維持し、先進的技術によるリスクにも適応します。これには、IT資産の配置および監視方法の最新化、リッチデータソースを利用したパフォーマンスフィードバックの循環と新しいリスクの特定、総体的なコンプライアンスプログラムなどが含まれます。

これらの活動は、リスクの軽減に役立つだけでなく、資源の効率化とプロセスの最適化を通じて価値の創出にも貢献します。

[27] Harvey Nash／KPMG 2018年度CIO調査

未来の成功に向けたキーアクション

信頼されるブランドの中心には技術的信頼があります。それを築くのは長い道程ですが、今日から始めることができます。

企業がテクノロジー組織の文化規範を変え、技術的信頼を築いていく上で、重視すべき5つの基本的行動があります。これらの行動を日々の業務に浸透させることが、デジタル時代に企業が競争優位を築くための鍵になります。

今日の行動は、明日の実りある成果のために

1

顧客中心のテクノロジーソリューションを構築し運用すること

ITデリバリーモデルを顧客のニーズに合わせるには、全社的な調整が必要です。プロジェクトベースのIT組織は過去のものです。顧客向けソリューションをサポートするチームを構築し、サービスデリバリーに対する期待を顧客の期待に直接結びつける必要があります。

成果：
フロントオフィス、ミドルオフィス、およびバックオフィス機能が円滑に連携し、組織全体が顧客に集中します。システム間の「遅延時間」は減少し、あらゆる事業分野でデータモデルが利用されます。

2

競争優位を生み、洞察に満ちた決定を下し、優れたリスク管理を行うための破壊的技術に投資すること

現在、人の手によるオペレーションが生産性と効率を抑制し、誤って障害が起きるリスクを高めています。インテリジェントオートメーション、人工知能、機械学習を活用した強力な最先端ツールを利用し、よりスムーズなデータ駆動型オペレーションを促進すべきです。

成果：
脅威の状況はますます複雑さを増す一方です。しかし、先進技術が企業の対応力の底上げをもたらしてくれます。企業全体のあらゆる階層で働く人々が、人工知能と機械学習の情報をもとに、より早く賢明な決定を下すことができます。企業は新たなパフォーマンス指標とリスク指標を設定し、それらに基づきより迅速かつ戦略的に行動できるようになります。スタッフに対し、分析に関する再教育を施すことで、データを利用してトレンドモデルと予測モデルを理解できるようになります。インシデント管理手続きを必要とするイベントは減少し、営業効率が高まり利益が増加します。

3

貴重なデータは、管理できるように常に所在を把握しておくこと

相互接続されたデジタルの世界は、データによって動かされているといっても過言ではありません。そのため、強力なデータガバナンスプログラムによってデータを管理・保護しないと、データから導出されるインサイトを最適化できません。データ管理の瑕疵（誤用や侵害）によってデータ管理の信頼を失うと、企業全体の評判や信頼に影響が及ぶ可能性があります。組織の管理外にあるデータも含め、データのライフサイクルをコントロールすることが必要です。

成果：
データは「黙っていない」ものです。データを適切な管理下に置き、完全に透明性をもって利用していることを示せば、安全に利用していることを顧客に証明できます。また、データのライフサイクルに関する管理と可視性が向上するため、規制要件対応とコンプライアンス要件対応の効率性が向上します。さらに、データの価値評価の精度が上がり、分析に基づく貴重なインサイトが得られます。

4

***トラスト・バイ・デザイン* の導入で機敏にリスクを管理すること**

ダイナミックなリスク管理の重要性がプロジェクトのライフサイクル全般を通して、明確に認識されています。ダイレクト・トゥ・コンシューマー（Direct to Consumer, D2C）テクノロジーとアジャイルデリバリー手法により、デジタルソリューションはかつてないほど迅速に顧客のもとに届くようになっています。セキュリティとプライバシーの管理といったテーマは、もはやチェックポイントではありません。デジタル製品・サービスの設計では、製品の中核に信頼されるテクノロジーの基本原則を織り込むこととなっています。そのためには、製品チームに明確なガイドラインとアクセラレータ、十分な資源とトレーニングモデルを提供し、ライフサイクルを通じて技術リスクを測定、軽減する必要があります。

成果：
従来の開発後半にリスク対策を施す方法に対し、顧客と摩擦（不十分な認証方法、直観的にわかりにくいデータ制御、既知のソフトウェアの脆弱性など）が発生する可能性が減少します。販売後は、技術的なトラブルによるインシデントが減少し、顧客は自分のデータを信頼して預けるようになります。

5

現状の技術に満足しないこと

顧客体験は急速に進化しており、現在の基準で「十分」なものも、急速に新技術に取って代わられます。強力なテクノロジーガバナンスを導入することで、技術的信頼の成果を進化させ続けることができます。ガバナンスを負担のかかる官僚的形式主義と捉えるべきではなく、むしろ戦略的リーダーシップ機能と捉え、リスクマネジメントに関する洞察に満ちた視点を提供してくれるコラボレーションと一貫性の促進要因と考えるべきです。

成果：
人工知能や機械学習を利用した最先端のツールを迅速に採用することにより、企業は成果を達成できるだけでなく、本質的に安全な製品やサービス開発のサポートも期待できます。製品と、その実現技術が市場の需要のペースを決め、顧客の期待どおりか、それ以上のものを提供します。テクノロジーのトレンドを前もって予測できるようになり、企業全体でイノベーションが自然と育成されるようになります。

KPMGによる支援

KPMGは、長年にわたり、信頼されるビジネスアドバイザーであるべく務めてきました。グローバル企業が顧客の信頼を勝ち取るためのテクノロジーの設計や実装のサポートなど、企業が技術的信頼の主要要素を理解し構築することで、ロイヤルティの高い顧客ベースを獲得・構築できるよう、幅広いサービスを提供します。

顧客信頼に関するアセスメント

顧客信頼に関する行動基準の調査、技術的信頼に関する実態と成熟度調査を支援します。これにより、企業に内包された技術面のリスク・脅威が明確化されます。また、業界の期待値とKPMGの専門家の経験を基に、デジタル技術に対する信頼性向上のためのロードマップを作成します。

技術的信頼の創出

顧客の信頼を中心とした新しいガバナンスモデルとオペレーティングモデルを構築し、技術的信頼プログラムを導入または改善し、顧客体験と継続的なデジタルトランスフォーメーションへの取組みに合った技術要件を定義できるよう支援します。

信頼のトランスフォーメーション

重大インシデント後の信頼回復、および次世代の顧客体験に対応可能な企業文化の改革を支援します。信頼に基づく行動原則の確立により、テクノロジーとイノベーションへの取組みを、顧客信頼確保に向たけソリューションへと変えることができます。

信頼できるデータによるインサイト

データを中心とするデジタルカスタマーソリューションの中で価値を生かせるようサポートします。データは優れたインサイトと意思決定に有用です。現代のデジタルカスタマーは、新しい機会と同時に、これまで経験したことがないほど深いレベルのデータへのアクセスを許可してくれます。KPMGのテクノロジーソリューションは、豊富なデータソース、価値駆動型のユースケース、パフォーマンス指標やリスク指標を特定し、より優れたオートメーションの実現と、より洞察に満ちた経営判断が行えるよう支援します。

著者紹介

Martin Sokalski

KPMGインターナショナル
エマージング・テクノロジー・リスク・サービス担当
グローバルリーダー

KPMG米国
プリンシパル

KPMGのエマージング・テクノロジー・リスク・ネットワークのグローバルリーダー。19年以上にわたってイノベーションと先端技術で実現する新しい（そして信頼できる）デジタル運用モデルとガバナンスモデルの設計を支援するアドバイザリー業務を提供。主に技術主導型のイノベーションとトランスフォーメーション、リスクマネジメント、セキュリティ、ガバナンス、コンプライアンス、内部統制についてクライアントに助言してきた実績を持つ。

Mike Krajecki

KPMG米国
エマージング・テクノロジー・リスク・サービス
デジタルリスク・ソリューション担当
ディレクター

KPMG米国のエマージング・テクノロジー・リスク・サービス事業のディレクター。10年以上にわたって、 KPMGのIoTリスクおよびガバナンス・サービスの開発を主導するなど、組織が破壊的技術のリスクとリターンのバランスを取れるように支援を提供。コネクテッドデバイス、自動運転車、モバイルアプリ、ブロックチェーン技術、クラウドプラットフォーム、インテリジェントオートメーションなどのデジタル製品・サービスに関連して信頼を構築し、リスクを管理できるよう企業をサポートしてきた幅広い実績を持つ。

関連文献

本書は、今後5年間にマーケットリーダーがIT分野で取り組むことになる6つの重要な要素を考察したKPMGの「Future of IT（ITの未来）」シリーズの一部です。Future of ITをさらに詳しく知りたい方、またシリーズの他のレポートをお読みになりたい方は、 **home.kpmg/jp/Future-IT**にアクセスしてください。

お問い合わせ先

KPMGコンサルティング株式会社

T : 03-3548-5111

E : kc@jp.kpmg.com

home.kpmg/jp/kc

本冊子は、KPMGインターナショナルが2019年3月に発行した「Building technical trust 」を翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

Designed by CREATE | CRT106359