# デジタル領域におけるレジリエンス

PwCコンサルティング合同会社
執行役員、パートナー　**山本 直樹**

## はじめに

本稿で取り上げる「レジリエンス」は、古くて新しいテーマです。わが国は地震大国とも呼ばれ、以前から多くの企業が自然災害を想定した事業継続計画（BCP）を策定して、不測の事態に備えてきました。また、世界規模のパンデミックである新型コロナウイルス感染症（COVID-19）が起きた際には、従業員がオフィスに出社する形態から在宅勤務に切り替えるなどの対応によって柔軟に対処してきました。

現在、COVID-19は収束しつつあり、重要性が高まっているのは「デジタル領域におけるレジリエンス」です。コロナ禍において、企業はアナログな業務プロセスの限界を痛感し、大胆にデジタルトランスフォーメーション（DX）を進めました。コンシューマー向けサービスも非接触化が進み、ネット上で取引が完結できるように進化してきました。実際、街中で現金を使う機会も激減しています。

ところが昨今では、システム障害やデジタルサービス停止といった報道が多く見られます。大規模なシステム更改における移行の失敗、生産現場に対するサイバー攻撃、アクセス集中による一時的なシステムダウン、中には単一企業における障害だけではなく世界同時多発的な大規模障害に発展することもあります。細かく見ていくと原因はさまざまですが、デジタル化が進み、ICT環境への依存度が高まった現代のビジネス環境においては、ひとたびそのICTシステムが停止してしまうと、顧客向けのサービスや社内の業務プロセスも停止し、ひいては社会基盤が機能不全に陥ることを意味します。経済活動や私たちの生活に対する影響の大きさは計り知れません。

そこで本稿では、デジタル領域においてオペレーショナルレジリエンスを高めるためのアプローチについて解説します。

なお、文中の意見は筆者の私見であり、PwCコンサルティング合同会社および所属部門の正式見解ではないことをお断りします。

## 1 世界はデジタルにつながっている

企業のオペレーションは、単体の企業の中で閉じて成立するものばかりではなく、多くのケースにおいて、いくつもの組織にまたがって運用されています。製造業のサプライチェーンやシステム開発における外部委託などは、企業間連携の代表的な例だと言えます。

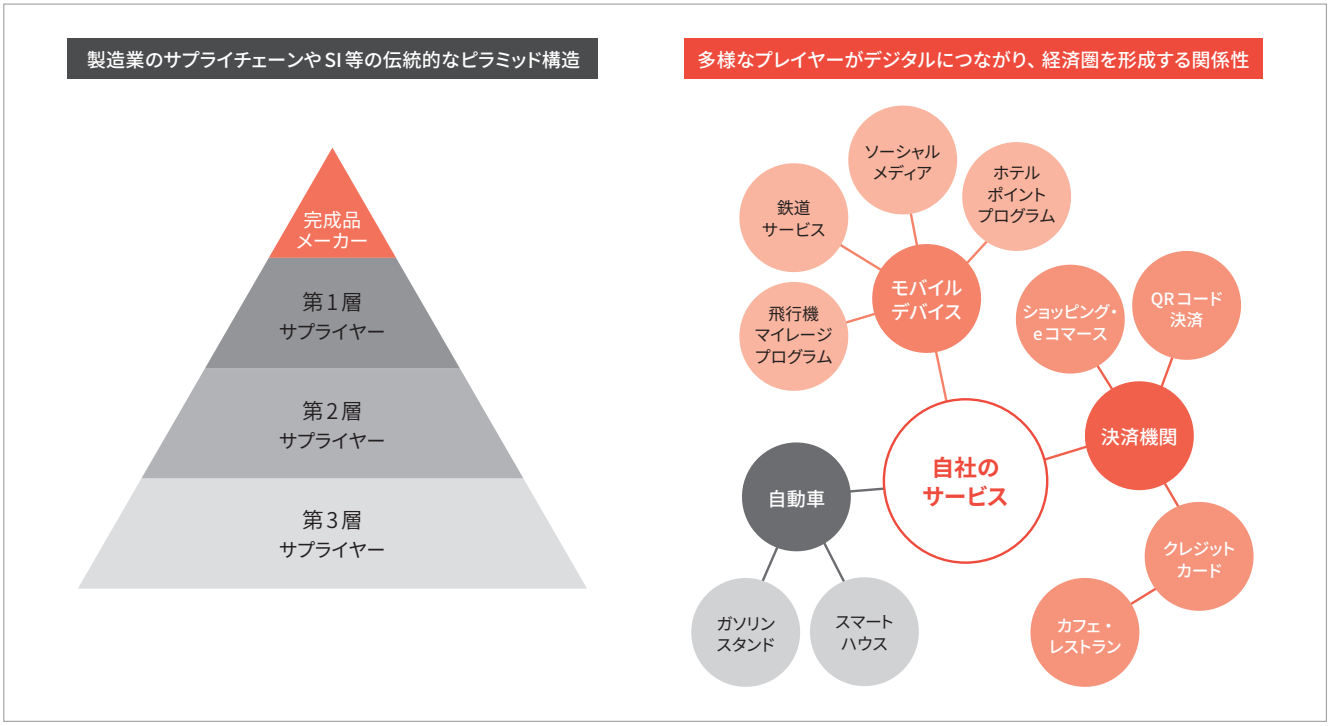
一方、これらの伝統的な連携のあり方に加えて、最近では、「ポイント経済圏」に代表されるデジタルサービスの相互連携も盛んになってきました。ホテルやレストラン、乗り物のチケット等を予約する際、全てスマートフォンのアプリで完結できます。これらのサービスでは、SNSアカウントをログインIDとして設定するケースも多く見られ、共通のIDを通じて各種サービスがつながっていきます。決済方法については少し前まではクレジットカードが主流でしたが、最近では、QRコード等の電子決済サービスを選択することも可能になりました。各社のサービスでは独自のポイントを付与したり、他社のポイントや電子決済で利用可能な通貨同等の価値に交換することも可能になっています。

企業は、魅力的な他社サービスと提携して利用者の利便性を高めることで、競争力の高い経済圏を構成し、優良顧客を囲い込もうとしています。BaaS（Banking as a Service）の手法を使った異業種企業による銀行サービス参入も相次いでおり、デジタル領域の企業間連携は今後ますます活発になることが予想されます。

## 2 ガバナンスが効きにくい複雑な関係性

コンシューマー向けビジネスを展開する企業にとって、ポイント経済圏のようなデジタルな企業間連携を構成することは、顧客の購買活動等に関するデータ分析を容易にし、業績

図表1：伝統的なサプライチェーンとデジタル経済圏における関係性の違い




出所：PwC作成

向上に直結するアプローチとして大きな期待が持てます。しかし、このような企業間の関係性にも難点があります。ガバナンスが効きにくく、障害によるサービス停止時の責任の所在が曖昧になりやすいことです。

伝統的な企業間連携の形である、製造業のサプライチェーンやシステムインテグレーションでは、商流のベクトルが上から下へと一方向に流れ、ピラミッドの頂点に位置する企業が取引上優位な立場にあるため、一次請け先、二次請け先に対して順次ガバナンスを効かせることができます（**図表1**）。

それに対して、デジタルな経済圏においては、機能上ハブになるアプリがあったとしても、特定の企業が経済圏全体を取りまとめて管理しているとは限らず、複数の企業が複雑な関係性でつながっていたり、提携先企業が途中で変わったりすることもあります。そのため、ピラミッド型のサプライチェーンに比べると、極めてガバナンスが働きにくいという特徴があります。このように微妙なパワーバランスの中では、万が一、システム障害やサイバー攻撃等のインシデントが発生したときに、サービス提供企業の担当者であってもサービスの全体像が見えません。ブラックボックス化している部分から障害の原因を究明しなければならず、サービスの復旧までに多くの時間を要してしまう可能性が高いのです。

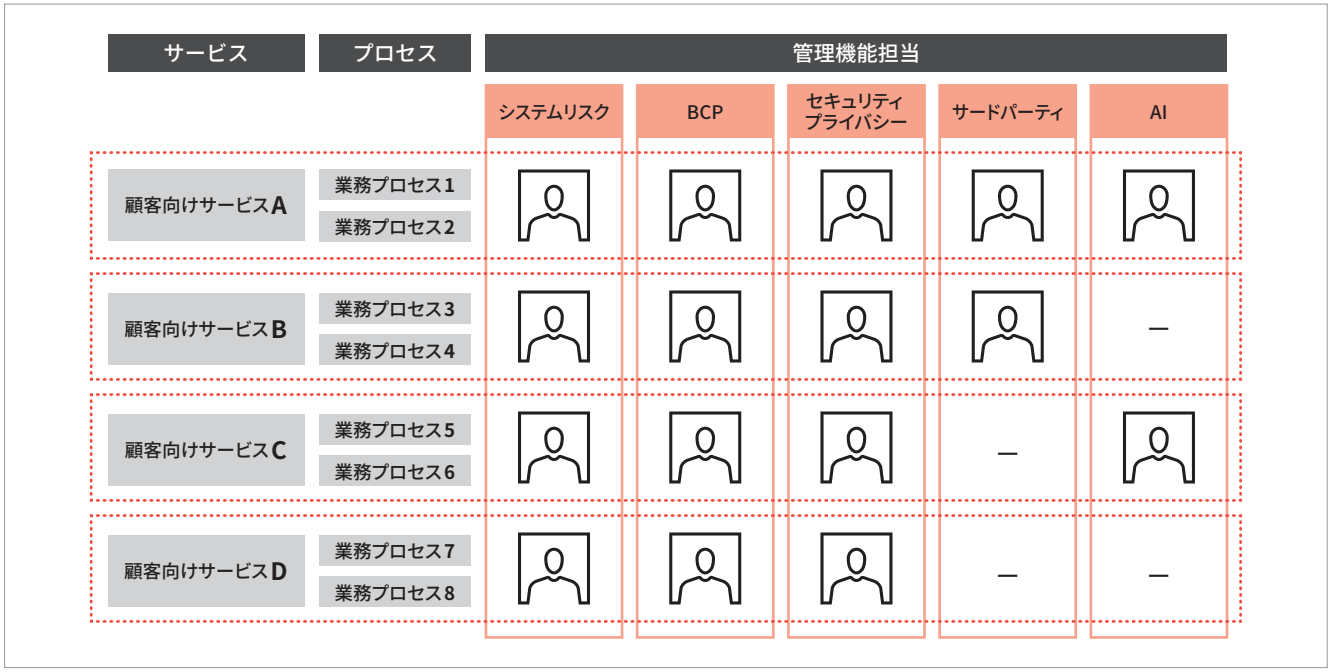
この傾向は、今後、AIが普及することでますます強まります。AI分野への大型投資計画を発表する企業も増えてきました。このような企業の経営者たちは、AIの能力に秘められた大いなる可能性を感じると同時に、AIを使わないことこそが最大のリスク（企業として生き残れないという危機感）であると悟っているようです。

近年、AIに関する規制の動きが世界的に加速しています。2024年5月、欧州では欧州理事会が「AI規制法（Artificial Intelligence Act）」を採択し、日本政府は「AI事業者ガイドライン案」を発表しました。どちらもAIシステムの開発者やAIシステムを活用する事業者に対して、倫理的な側面や技術的な側面における規制が課されることになります。一部の企業は、すでに自社のAIガバナンスを確立しようと自主規制ルールを明文化する取り組みを始めています。このような新規技術の取り扱いは難易度が格段に高まり、企業に問われるデジタル領域の責任はそれ以上に大きなものとなるでしょう。

## 3 デジタル領域におけるレジリエンスの高め方

最後に、デジタル時代においてオペレーショナルレジリエンスを高めるためのアプローチを解説していきます。

図表2：デジタル・オペレーショナル・レジリエンス管理体制再構築のイメージ




出所：PwC作成

### (1) 自社を取り巻くデジタル環境の可視化

何事においても適切に管理するためには、対象となる範囲を明確にし、実態を把握しなければなりません。自社だけでなく、業務提携するパートナー企業、システム開発・運用等の委託先等、全ての関係組織を洗い出します。サードパーティリスク管理（Third-party Risk Management：TPRM）のプログラムが確立されている組織でも、管理対象が委託先に限定されているケースは珍しくありません。その場合、業務提携先等も含めて、サードパーティの範囲をより広く定義し直す必要があるでしょう。

組織単位で範囲を明確にした後は、データセンター、ネットワーク、ハードウェア、アプリケーション、データ等の資産を洗い出し、IT資産台帳やネットワーク構成図、データフロー図のような形に可視化します。これについても自社が保有する資産だけでなく、依存関係にあるビジネスパートナーの資産や契約する外部のクラウド環境等についても可視化の対象とします。社内のクラウドガバナンスが弱い組織においては、ユーザー部門が独自に外部サービスと契約して、いわゆる「野良クラウド」や「シャドーIT」が横行しているかもしれません。単にポリシーを定めるだけでなく、申請・承認プロセスを厳格化したり、社内環境からの外部接続を監視するなどの対応で、ガバナンスを強化することが求められます。このようにビジネスの実態に合わせて管理対象を明確にすることが、デジタル領域のレジリエンスを高める第一歩となります。

### (2) 管理体制の構築

次に取り組むべき課題は、レジリエンス強化のための管理体制を見直し、整備することです。銀行等の金融機関は、これまで他の業界に比べるとレジリエンス強化により真剣に取り組んできたと言えるでしょう。それでも、システムリスク管理、事業継続管理（BCM、ディザスタリカバリー）、サイバーセキュリティ管理、個人情報保護、委託先管理等の部署をその時々の時代の要請に応じて都度整備してきたことで、部署間の連携が不十分だったり、機能が重複するという傾向が見られます。レジリエンス管理部署のあるべき姿については、あらゆる企業に当てはまる模範解答があるわけではありません。したがって、企業の現状やビジネスの方針等によって、企業ごとにあるべき姿を設計する必要があります。

改善のアプローチとしては、既存部署の役割を整理し直して最適化したり、顧客向けサービス単位で、関連する業務プロセスと必要な機能をマッピングしたりすることなどが考えられます（**図表2**）。また、多くの企業ではレジリエンス人材の確保および育成も重要な課題になるでしょう。

### (3) レジリエンスを構成する機能の強化

対象範囲を明確にし、管理体制を整備した後は、具体的な対策を講じます。ここから先は企業によって必要な対策が異なります。自社の実態が分からない場合は、監査法人やコンサルティング会社による第三者評価を受けて、強化すべきポ

イントやその優先順位を明確にすることも効果的です。強化策としては、次のようなものが考えられます。

- サードパーティとの契約やSLA（Service Level Agreement）等の見直し、障害発生時の連絡体制・プロセスの見直し
- 定期的にサードパーティを評価するプログラムの構築
- システム停止を引き起こす想定シナリオの明確化および原因究明・復旧プロセスの確立
- ハードウェアレベルの冗長構成化、クラウドマイグレーション
- システム移行に関わるゲートレビュー基準の明確化・プロセスの厳格化
- サイバーセキュリティの強化（ネットワークトランザクションやシステム上の挙動の監視等）
- 障害発生を想定した対外的コミュニケーション基準やフローの確立

このような対策は、ポイント経済圏のようなデジタルな関係性の企業間だけでなく、伝統的なピラミッド構造を持つ製造業のサプライチェーン等においても同様に重要です。

### (4) デジタルレジリエンスの検証

上記 (1)～(3) の対策を講じた後には、その効果を検証することが重要です。システム障害やサイバー攻撃を想定したBCPの机上訓練を実施している企業はありますが、経済圏を構成する企業が集まって本格的な合同BCP演習を実施したというケースはまだそれほど多くありません。しかし、現代の企業活動や社会生活は既にデジタル環境の上で成り立っており、今後さらにその依存度が増していくことを考えると、その重要性は明白です。万が一、長期間のサービス停止等が発生すれば、売上や株価に影響が出たり、社会的な信用を失うことにもつながりかねません。企業の経営者は、AIを含めたデジタル領域のレジリエンスを最重要課題として捉え、真剣に取り組んでいかなければなりません。

**山本 直樹**（やまもと なおき）

PwCコンサルティング合同会社　執行役員、パートナー
2008年入社。サイバーセキュリティ＆プライバシーリーダー等を務めた後、2019～2021年にPwC香港・中国（上海事務所）に出向して現地日系企業の支援を担当。帰任後の現在は、トラストコンサルティング事業部のパートナー。リスクマネジメント、レジリエンス、サイバーセキュリティ等の領域で多くの経験を持つ。著書に『サイバー攻撃に勝つ経営――先進企業に見るCISOの挑戦』（日経BP）など。公認情報システム監査人（CISA）、公認内部監査人（CIA）。
メールアドレス：naoki.n.yamamoto@pwc.com