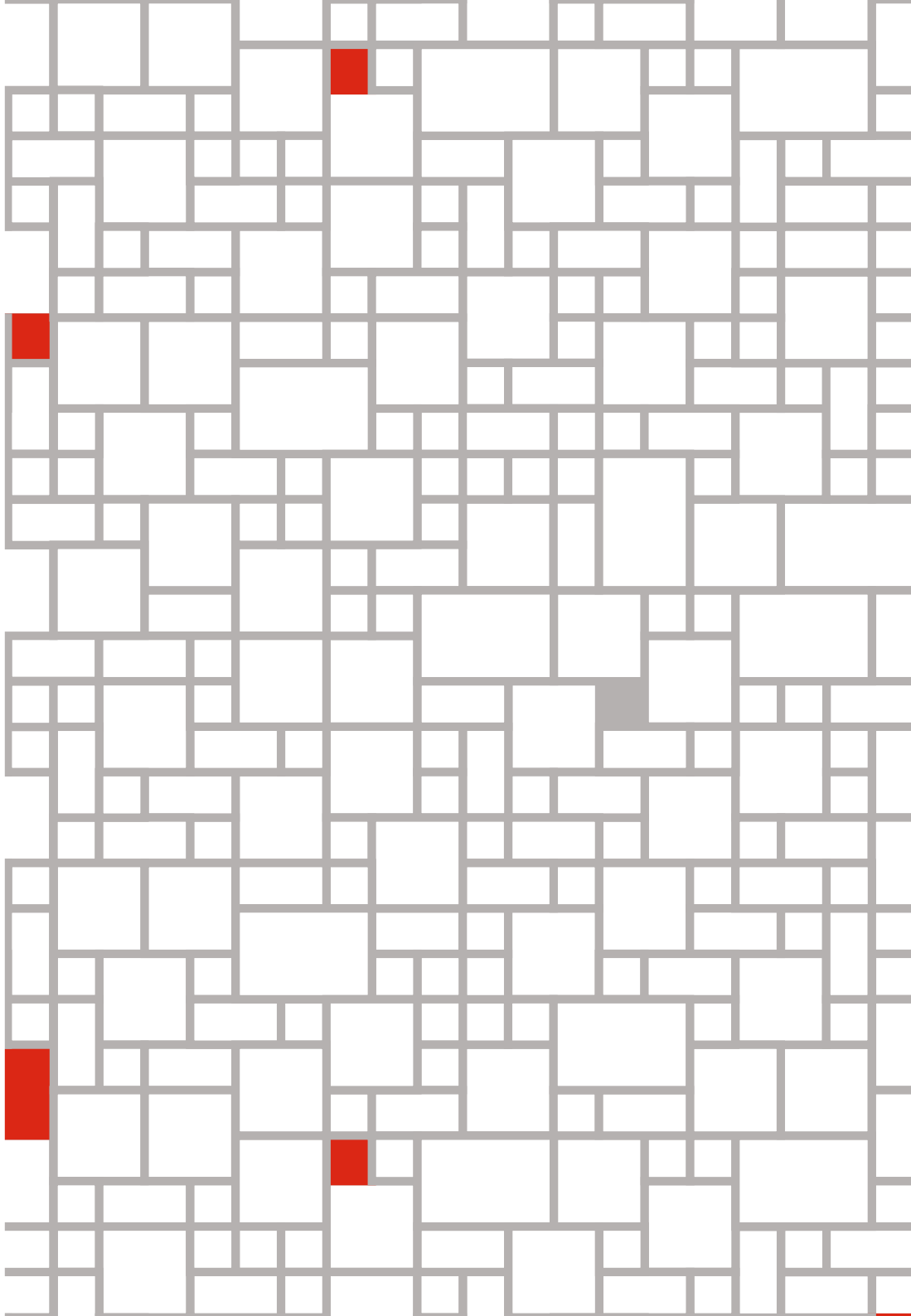
# レジリエンス指数を高めるために

## Digital Trust Insights

－日本企業への示唆－

pwc

www.pwc.com/jp

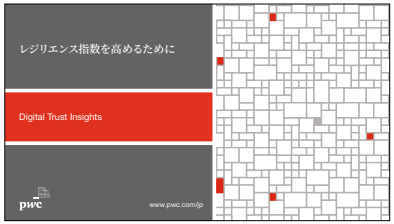


# はじめに

デジタルトランスフォーメーションによるビジネスの変革が進展すると同時に、サイバーセキュリティにかかるリスクも増大の一途をたどっている。このような環境変化の中で、デジタルレジリエンスの構築と高度化が企業にとって重要な経営課題の1つであるという認識は、多くの企業ですでに浸透しつつある。一方で、デジタルレジリエンスを高めるために必要な具体的取り組みについては、いまだ十分な理解があるとは言い難いのが現実である。

PwCは、国や地域、業界を問わずさまざまな企業を支援する中で上記のような現状を知得した。そこで、企業がレジリエンスを高めるための方針に示唆を提供するべく、全世界3,500名以上のビジネスITリーダーに対しDigital Trust Insights調査を行った（2020年2月発刊『レジリエンス指数を高めるために』以下、「グローバル版レポート」）。その結果、レジリエンス戦略の成熟度を測った3つの領域全てにおいて、上位25%に位置するレジリエンス指数の高いグループが存在することが分かった。さらに本調査では、これらデジタルレジリエンス構築に関して先進的な企業（高RQ企業）が、どのような取り組みを進めているのかを明らかにしている。

本レポートは、上記Digital Trust Insights調査を基に日本企業に焦点を当て、日本企業固有の状況や、グローバルとの差異を分析した。そしてそこから浮かび上がる、レジリエンス指数を高めるために日本企業が実施すべき取り組みについての考察を解説するものである。




レジリエンス指数を高めるために グローバル版レポート
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/resiliency-quotient2002.html

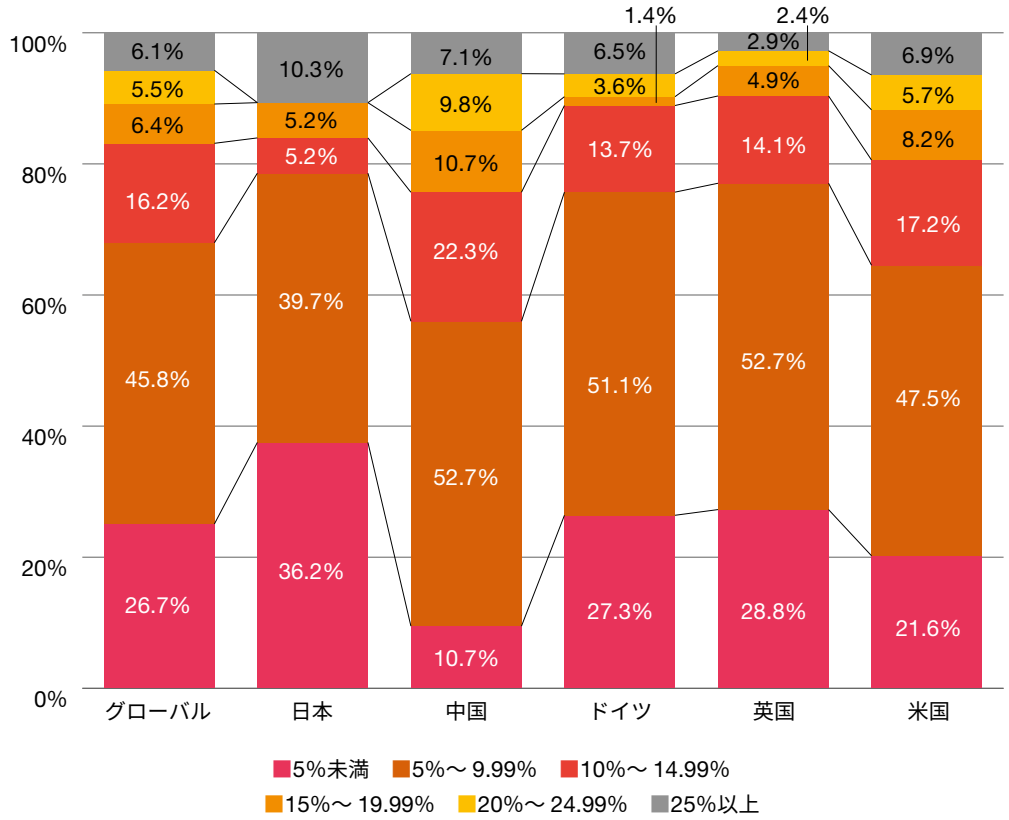
# IT予算に占める投資額の割合から見るサイバーセキュリティへの姿勢

前述のとおり、デジタルトランスフォーメーションによるビジネス変革に伴い、サイバーセキュリティにかかるリスクも増大している。このリスク増大に対処する上では、企業の事業内容なども考慮した、管理面および技術面双方からの対策が必要であり、対策の実装・運用には、専門人材の確保や製品の調達などへの投資が必要不可欠である。したがって、サイバーセキュリティへの投資額は、その企業のセキュリティリスクへの取り組み状況を図る重要な指標の1つとなっている。

各企業のIT予算に占めるサイバーセキュリティへの投資額の割合を調査した結果、日本は世界平均および主要各国と比較してIT予算に占めるサイバーセキュリティへの投資額が5%未満の企業の割合が大きいことが明らかになった（図表1）。この要因として、日本企業では、デジタルトランスフォーメーションに対してサイバーセキュリティ部門が関与する度合いが低いことが挙げられる（2019年12月発行『サイバーセキュリティの先進的企業は、新たな枠組みで事業の成長を促進』を参照）。すなわち、日本企業ではサイバーセキュリティ部門が予算策定に対して影響力を発揮できていない傾向にあることが推察される。

一方で、IT予算に占めるサイバーセキュリティへの投資額が25%を上回る企業の割合についても、日本は世界平均および主要各国と比較して大きいことが明らかになった。つまり、グローバル（世界平均）と比較して、日本では投資額の割合が5%未満の企業と25%を上回る企業の割合が多い。以上から、日本では他国よりも、サイバーセキュリティに対する企業の姿勢の二極化が進んでいると考えられる。

**図表1　2020年のIT予算に占めるサイバーセキュリティへの投資額の割合**

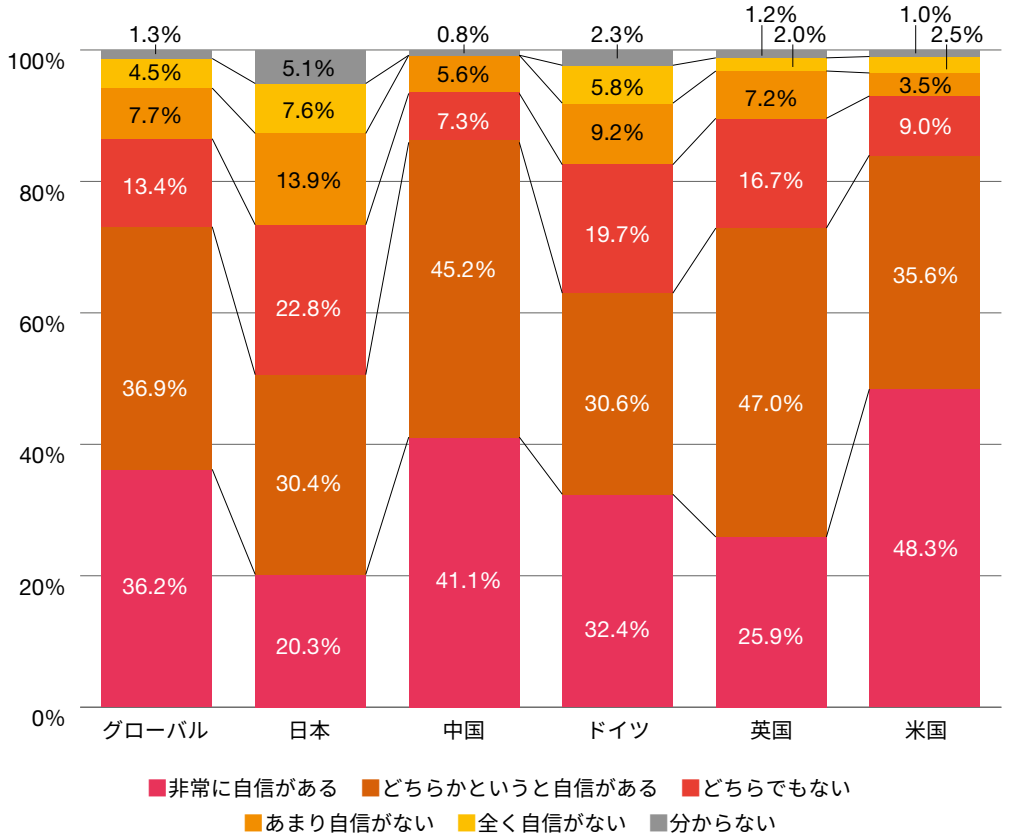


# セキュリティリスクに対するデジタルレジリエンスの実現状況

IoTなどの革新的技術をビジネスに取り込んだデジタルトランスフォーメーションが進む中、セキュリティ侵害に対する防御力だけでなく、侵害を受けた際のレジリエンスが試されるような、新たなリスクが顕在化してきている。このような状況下で、今や企業に求められているのはデジタルトランスフォーメーションを推進することだけではない。それぞれの企業が潜在的なリスクを認知して適切に管理することも求められている。そこでPwCでは、各企業のセキュリティリスクに対するレジリエンスの自信の程度を調査した。

レジリエンスを試されるような新出のリスクの管理について「自信がある」（「非常に自信がある」と「どちらかというと自信がある」の合計）と回答した企業の世界平均は73%に上り、グローバルの企業の多くが新出のリスクを認知しこれを適切に管理できていると自負していることが見て取れた（図表2）。一方で、「自信がある」と回答した日本企業は51%にとどまり、グローバルおよび主要各国の平均値を大きく下回っている。日本企業の多くは、自社が新出のリスクへの対処を十分に行えているかの確証を持っていないことが分かる。もちろん、本調査の対象は「自信」の程度であるため、この結果は各企業のデジタルレジリエンスの水準を直接反映しているものではなく、国や地域、そして各企業の文化などの影響も多分に受けていることが想定される。しかし本調査から、日本企業は、海外を含む他社の事例を参考にしつつ「何をすべきか」を明らかにするとともに、専門家などを交え自社の対策状況を客観的に把握することが必要であると考えられる。

**図表2　セキュリティリスクに対するデジタルレジリエンスの自信の程度**



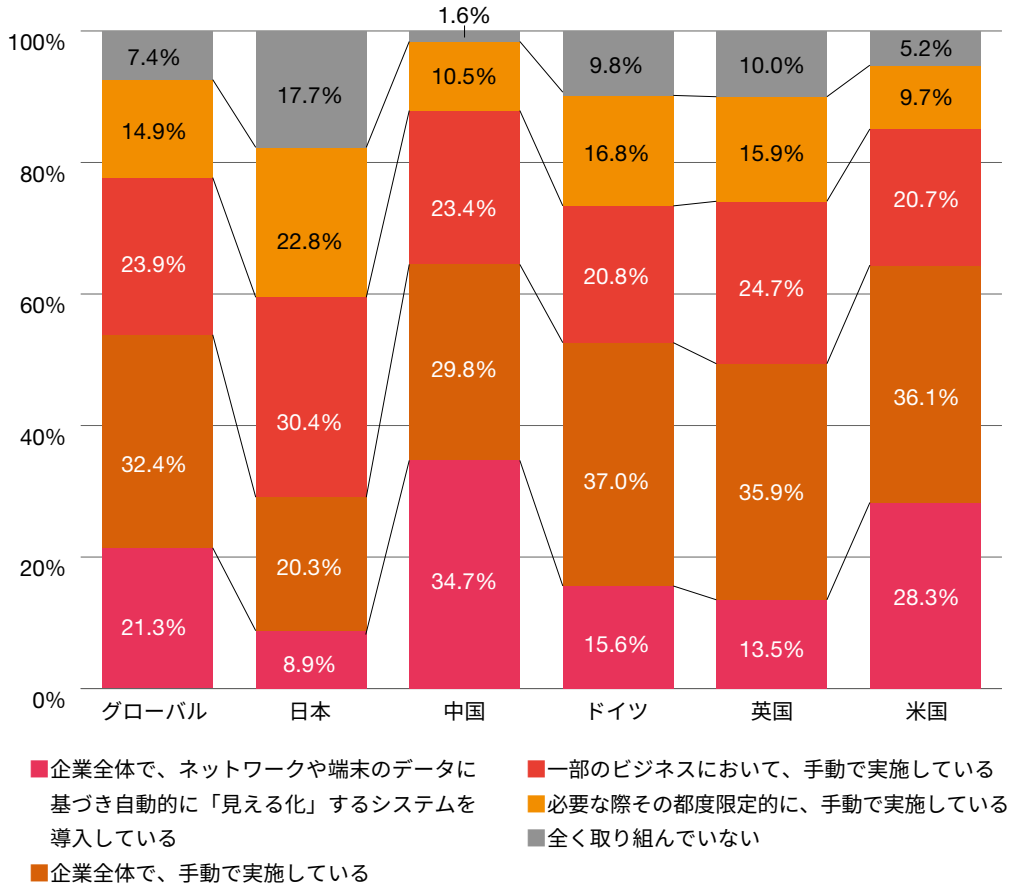
# レジリエンス構築
# 第1ステップ：資産とプロセス、およびその関係性の可視化

グローバル版レポートで示したように、レジリエンス構築における第1ステップは、組織のコアプロセス、資産、相互依存関係を可視化することである。自社の持つ資産がコアビジネスサービスとどのようにつながり、相互に関係しているかを理解していなければ、サイバー攻撃などにより障害が発生した場合に、どのシステムまたは資産を切り離したらよいかを判断できないだろう。実際、高RQ企業の91%が正確な資産のインベントリ（リスト）を作成・維持し、必要に応じて更新していることが分かっており、他の一般的な企業との顕著な相違点の1つに挙げられている。

一方で、大企業の場合、IT資産数は数百万規模、接続数は数億規模になるため、レジリエンス構築におけるこの第1ステップを実現することは容易ではない。この困難を乗り越える助けとなるのが、テクノロジーを活用したインベントリおよびマッピングプロセスの自動化だ。実際、高RQ企業の50%以上が最重要の資産とプロセスのインベントリ作成およびマッピングを自動化しているのに対し、それ以外の組織における割合はわずか10%であることが、本調査で明らかになっている。

この第1ステップの中でも、自社の持つ資産とプロセスの全容を把握する取り組み、すなわちインベントリ作成に関する問いに対し、日本企業とグローバルまたは主要各国の間では回答に顕著な差が見られた（図表3）。まず、「全く取り組んでいない」または「必要な際その都度限定的に、手動で実施している」と回答した日本企業は40.5%に上り、グローバルの22.3%や主要各国の割合に比べ著しく大きくなっている。次に、企業全体で自動化を行っているという回答についても、グローバルの21.3%や主要各国の割合に対し、日本企業は8.9%と著しく低いことが分かる。これらのことから、日本企業では、資産とプロセスのインベントリ作成を全社的に自動化する以前に、資産およびプロセスの全容を把握する取り組みそのものが十分に行われていない傾向にあると考えられる。

**図表3　主要なビジネスプロセスと資産のインベントリ作成状況**

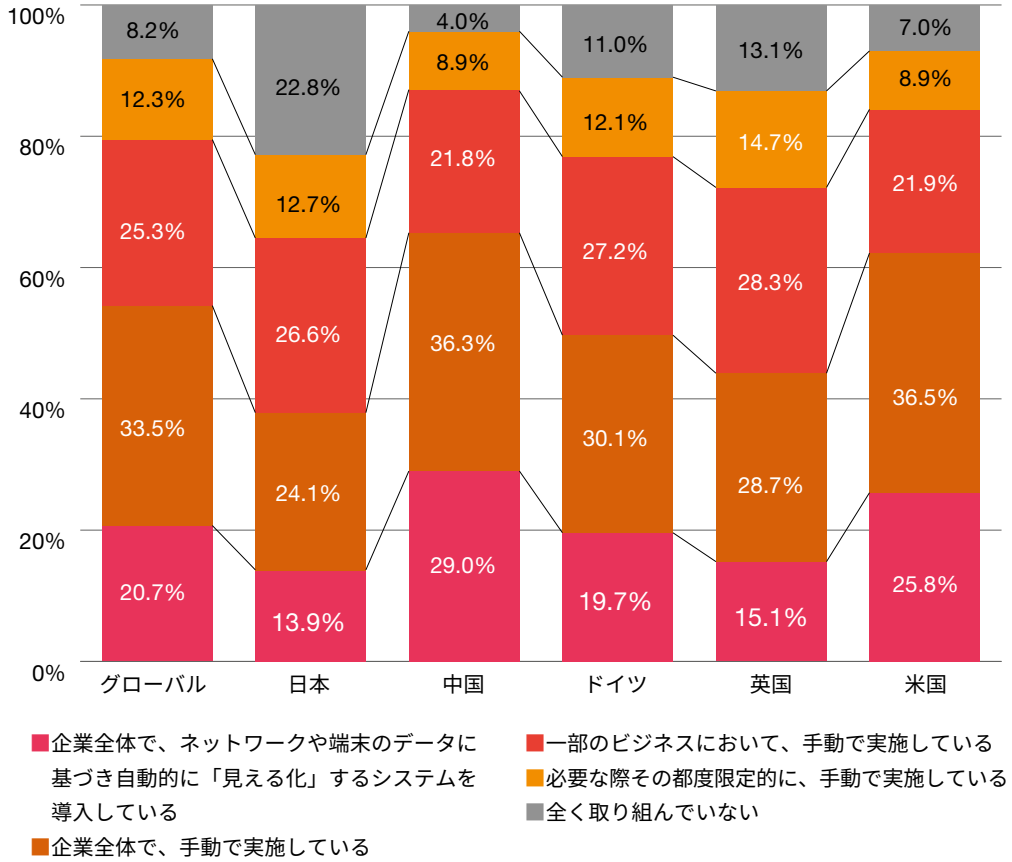


組織のコアプロセス、資産、相互依存関係性を可視化することは、レジリエンス構築の第1ステップである。さらに日本企業においては、まずは自社の持つ資産とプロセスの全容を把握することが、速やかに対処すべき重要な課題の1つであるといえる。

レジリエンス構築の第1ステップにおいては、資産とプロセスの全容を把握するだけでは十分とはいえない。これらの資産やプロセスの相互依存関係を明らかにすることで初めて、有事の際の判断材料として有用なものとなる。資産とプロセスを紐づける取り組みに関する問いにおいても、前項と同様の傾向が見られた（図表4）。すなわち、「全く取り組んでいない」または「必要な際その都度限定的に、手動で実施している」と回答した日本企業の割合（35.5%）は、グローバル（20.5%）や主要各国のそれと比べて大きく、企業全体で自動化を行っていると回答した日本企業の割合（13.9%）は、グローバル（20.7%）や主要各国のそれに比べ小さい結果が得られた。資産とプロセスの全容を把握する取り組みそのものが不十分な日本企業において、それらの紐づけが十分に行われていないことは理解に難くないだろう。

レジリエンス構築の第1ステップについて、日本企業がグローバルまたは主要各国の水準に追いつくためには、今一度自社の取り組みを見直す必要がある。

**図表4　ビジネスプロセスと資産の依存関係のマッピング状況**



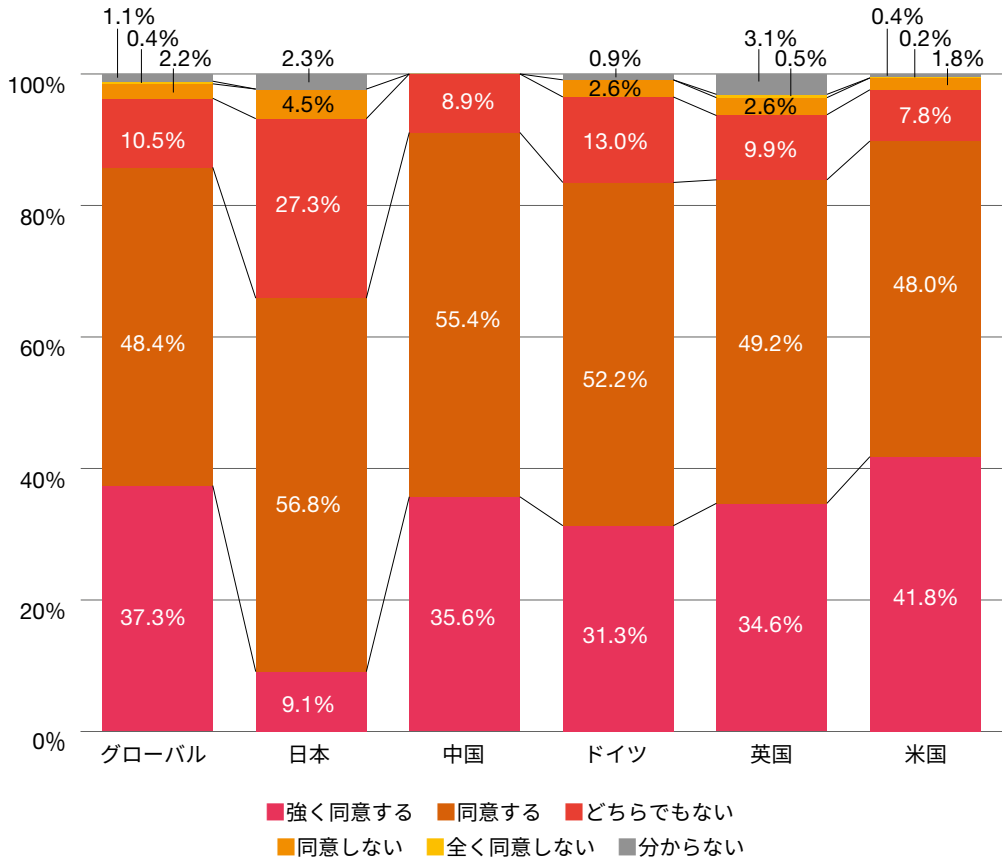
# レジリエンス構築
# 第2ステップ：ビジネスインパクト許容度の定義

レジリエンス構築の第2ステップは、自社のビジネスがどの程度の障害まで許容できるかを見定めることである。そのためにはまず、自社にとって、クライアントに提供する最重要のビジネスサービスは何であるかを定義する必要がある。そして、これらの最重要サービスを守る上で、有事の際に持ちこたえられる時間と拠出できる費用の上限を定義したものが、ここでいう「インパクト許容度」だ。インパクト許容度があらかじめ具体的に定められていることが、有事の際の判断・対応を迅速にし、ひいてはビジネスへの影響を少しでも抑え込むことにつながるのである。

グローバル版レポートで示したように、この取り組みは、高RQ企業と他の一般的な企業の間では実施状況に著しい差が見られた重要な指標の1つである。そして、その実施状況は日本企業とグローバルまたは主要各国の間でも明確な差異が見いだされている（図表5）。「具体的な指標・基準として定められたインパクト許容度が存在するか」という問いに対し、「同意する」または「強く同意する」と回答した日本企業の割合は65.9%にとどまり、グローバルの85.7%や主要各国で同じ回答をした企業の割合に比べ明らかに低い値を示している。これをさらに「強く同意する」に限定すると、グローバルの37.3%をはじめ主要各国がいずれも30%以上をマークしているのに対し、日本企業ではわずか9.1%と、その差はさらに顕著となる。明確な指標・基準が存在しない状況下では、有事の際の判断も場当たり的にならざるを得えないため、対応の遅延や一貫性のなさにつながる可能性が大きくなってしまう。

日本企業がデジタルレジリエンスにおいてグローバルや主要各国の水準に追いつくために、この第2ステップについても急ぎ取り組むべきであると考えられる。

**図表5　自社はビジネスサービスとインパクト許容度のマッピングを行っていると思うか**

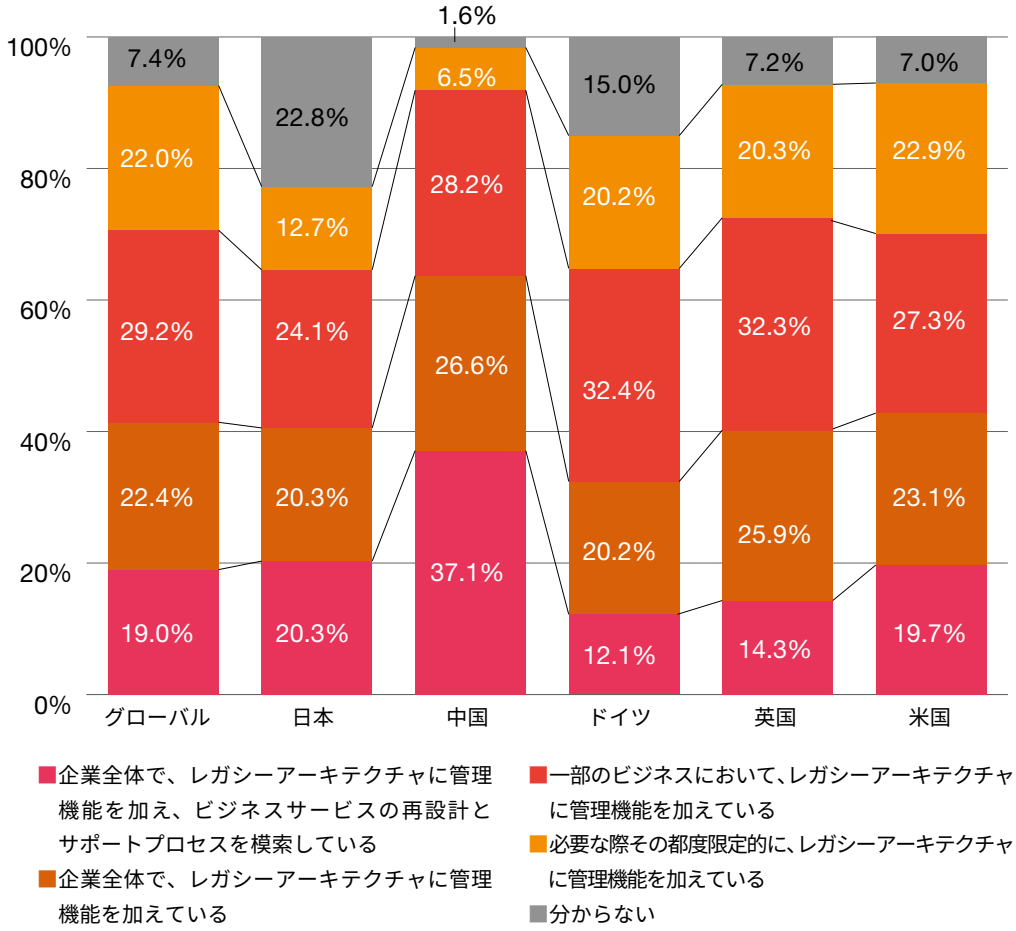


# レジリエンス構築
# 第3ステップ：計画的なデジタルレジリエンス

レジリエンス構築の第3ステップは、「計画的なデジタルレジリエンス」の実装である。有事の際、意思決定者と対応者は連携・協力して、ビジネスとクライアントへのダメージを最小限に抑えつつ速やかにインシデントに対応することが求められる。これを実現するためには、優先度の高いビジネスプロセスと資産のマッピング状況をリアルタイムにレビューするプラットフォームを構築し、的確かつ迅速な意思決定の材料を確保する必要がある。

難度が最も高いこの第3ステップは、グローバル全体でも達成している企業はほとんど存在しないのが現状だ（図表6）。「計画的なデジタルレジリエンスをどの程度実装しているか」という問いに対して、「企業全体で、レガシーアーキテクチャに管理機能を加え、ビジネスサービスの再設計とサポートプロセスを模索している」と回答した企業の割合は、グローバルでは19.0%と低い値を示しており、中国を除く主要国のほとんどでも、これに類する割合を示している。したがって、「計画的なデジタルレジリエンス」の構築は、日本を含めグローバル全体における次なる課題であるといえるだろう。

**図表6　計画的なデジタルレジリエンスの実装状況**



# おわりに

本レポートでは、グローバル版レポートを基に、日本企業に焦点を当て、レジリエンス指数を高めるための取り組みの分析と考察を行った。ここまでで示したように、日本企業がこれら大きく3つのステップに分解される取り組みにおいて、グローバルと同水準に達するためには、これまで以上に注力すべき課題が残されている。特に、第3ステップとして挙げた「計画的なレジリエンス」に関しては、グローバル全体でも依然として十分な取り組みが行われているとは言い難い。現代のように技術革新が進み、それと並行して新たなセキュリティリスクが次々と発生している状況下で何より重要なことは、日々変化する状況に鑑み「何をすべきか」を見直し続けることであるといえる。本レポートが、クライアントの皆さまにとって、グローバルにおける自社の相対的な立ち位置を見極め、次に何をすべきかを見いだすための一助となれば幸いである。

# 関連コンテンツ


**2019年 Vol.3**
「サイバーセキュリティの先進企業は、
新たな枠組みで事業の成長を推進
－ Digital Trust Insight －」


**2019年 Vol.1**
「デジタルトラストへの道」

PwCは、グローバル情報セキュリティ調査（GSISS）として20年間、サイバーリスク環境について解説するリソースとして参照されてきました。近年は「情報セキュリティ」よりもデジタルリスク管理が重視されるようになっています。そこでPwCはGSISSをDigital Trust Insightsと改めた調査を継続して実施しています。

調査結果をまとめた報告書を参照していただく以外に、地域別、業種別、企業規模別などのデータを抽出し、企業のデジタルリスク管理対策に関わるベンチマークデータとして活用していただくことが可能です。


**2019年 Vol.2**
「2019年は地政学的サイバー活動が激化、CEOはレジリエンスが試される」


**2018年 Vol.2**
「データが動かす世界に向けてプライバシーと信頼に新たな命を吹き込む」


**2018年 Vol.1**
「サイバーショックに備え、デジタル社会を強化する」


**2017年 Vol.3**
「IoTの可能性を探る」


**2017年 Vol.2**
「スレットマネジメントの新たな可能性に向けて」


**2017年 Vol.1**
「先進的サイバーセキュリティおよびプライバシーの実現」

# お問い合わせ先

**PwC Japanグループ**
https://www.pwc.com/jp/ja/contact.html

**外村 慶**
PwCコンサルティング合同会社
パートナー

**綾部 泰二**
PwCあらた有限責任監査法人
パートナー

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約8,100人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、社会における信頼を築き、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界157カ国に及ぶグローバルネットワークに276,000人以上のスタッフを有し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細は www.pwc.com をご覧ください。

電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/knowledge/thoughtleadership.html
発刊年月：2020年6月　管理番号：I202005-06