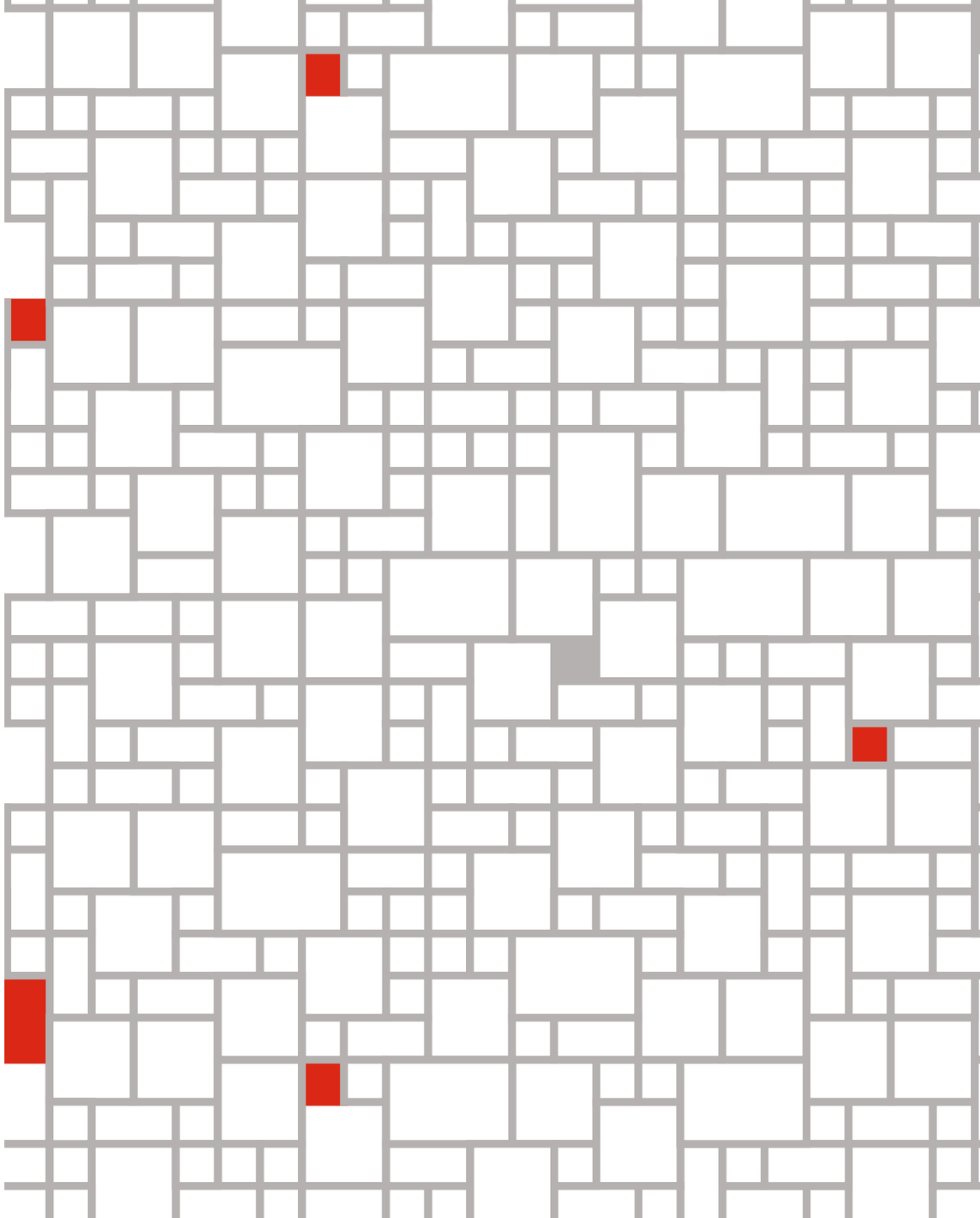
レジリエンス指数を高めるために

Digital Trust Insights

pwc

www.pwc.com/jp



目次

ビジネスを守るために必要な考え方の変化

デジタル接続が増加する中、一流企業が実施している円滑・安全な業務継続に向けたさまざまな取り組み

現代において、「もう十分」なことはない。これは、世界各地の3,500社以上の企業を対象にした、レジリエンス戦略に関するPwCが実施したDigital Trust Insights調査結果からも明らかである。サイバー攻撃による障害から企業を守り、回復していくためには何が重要なのか――企業のスタンスは現在、大きく変化しつつある。ヒントとなるのは、戦略性に優れた企業ほど、レジリエンス計画の刷新にもより積極的であること、活動に終わりはないこと、そうした企業は次のような水準を目指している、という点である。

- 最重要資産およびプロセスのリアルタイム可視化
- 全社規模の計画と対応
- ビジネスサービスおよびプロセスの継続的再設計

PwCによる最新の Digital Trust Insights のグローバル調査によると、全世界3,500名以上のビジネス・ITリーダーの半数以上が、当たり前になりつつあるビジネス上の慣行が「サイバー攻撃に対する脆弱性を大幅に高めている」と答えている。そして、これらの慣行は、企業のレジリエンスに対する計画の更新や戦略の刷新を促すことにつながっているのである。

PwC: Digital Trust Insights

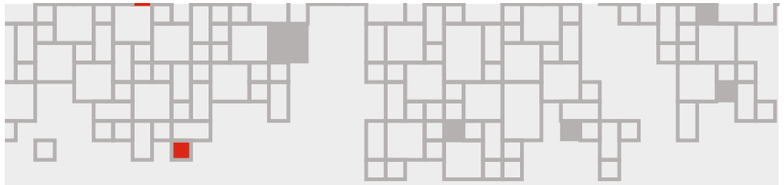
レジリエンス指数の高い企業とはどのような企業か

見えていないものを守ることはできない。チームメンバーが半分では修復もできない。
そして、学びなくして改善も望めない。

レジリエンスを高めるために組織は何を行っているか。どの程度の水準を目標とするべきか。これらについて調べるため、PwCは三つの領域におけるレジリエンス戦略の成熟度調査を行った。その結果、全ての領域で上位25%に位置する、レジリエンス指数の高いグループ（高RQグループ）が存在することが分かった。

この高RQグループに属する企業の59%が、新たな「非常に重大な」脅威に直面して戦略を刷新してきたと回答しており、それ以外のグループにおける割合（39%）を上回っている。また、サイバーレジリエンスが試される新たなリスクに対しても、「うまく乗り越えられる」と答えた高RQグループの割合は73%と、より自信を持っていることが分かった（それ以外のグループは24%）。

要するに、高RQグループに分類される企業は、旧来の、そして近視眼的な災害復旧／事業継続モデルから「計画的なレジリエンス」へと既に考えを転換しているのである。より対応幅の広いこの手法には、優先順位が高いプロセスのリアルタイムな可視化が含まれている。これによって、意思決定者と対応者は、事業への損害を最小限に抑えつつ、協力してインシデントに対応できるようになる。



54%以上の企業が、以下の慣行により、自社の脆弱性が大幅に高まっていると回答：

- 事業のIoT化促進および消費者との関係深化
- サードパーティークラウドプロバイダーを用いた資産やアプリケーションの増加
- 自分たちの業界を対象にサイバーを用いる民族・国家の増加
- 請負業者へのアウトソーシング増加
- 複数テクノロジーの組み合わせ活用の増加

出所：PwCのDigital Trust Insights調査、2019年9月実施
対象総数 3,532

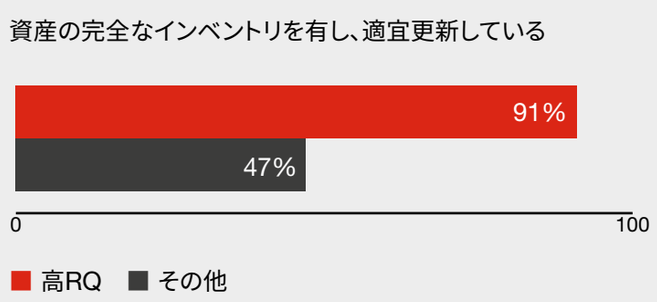
レジリエンス構築の3ステップ

1 組織のコアプロセス、資産、相互依存関係性を可視化

データ資産やプロセスがコアビジネスサービスとつながり、相互に関係しているか理解できなければ、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分からない。高RQグループとそれ以外のグループとの最も顕著な相違点は、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・維持しており、必要に応じて更新しているという点である。それ以外のグループにおける割合は47%にとどまっている。

このような、資産を網羅するインベントリを作成するだけでも重要な知見が得られる。例えば、ある企業は、最重要な資産・システム数は50で、一つの領域にまとまっており、サイバーインシデントから十分に保護されていると考えていた。しかし、ソフトウェアを使用してネットワークを徹底調査したところ、システム間で二次的・三次的つながりがあることが判明し、その結果、最重要システム数は想定の9倍、450まで増加した。これら450のシステムは「隠れた」状態だったために、障害に対する組織の脆弱性をより高める要因となっていたのである。

こうしたインベントリは、サードパーティーとの関係まで範囲を広げる必要がある。企業にとって慎重を要する接続は、実際には外部で行われるケースもあるためだ。最近の主要な顧客データ侵害のケースでは、ハッカーは顧客サービス関連の管理用に複数の小売業者が使用していたチャットサービスベンダーを侵害している。



出所：PwCのDigital Trust Insights調査、2019年9月実施
対象総数 3,532

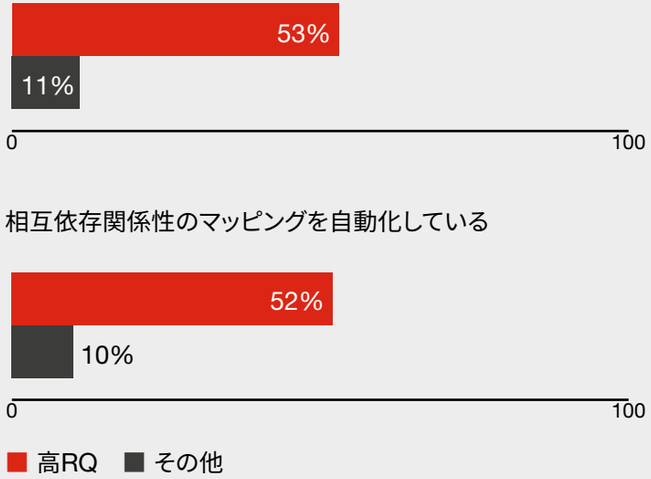
レジリエンス構築の3ステップ

大企業の場合、IT資産は数百万規模、接続数は数億規模になる。しかし、現在は最重要の資産とプロセスを詳細にマッピングするテクノロジーが存在する。高RQ組織の50%以上がインベントリおよびマッピングプロセスを自動化しているが、それ以外の組織での割合はわずか10%であった。

レジリエンスに向けた、この第1ステップは容易ではない。5月に実施した『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推進 - Digital Trust Insights - 』調査でも、IT専門家（あるいはサイバー対策先駆者さえ）、「米国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」指針における「Identify（特定）」機能（保護が必要な資産とプロセスを特定する能力）に関して、自分たちの力は「成熟には程遠い」と考えていることが分かった。

高RQグループに追いつくために：

- 状況変化に応じて更新可能な、資産の正確なインベントリを維持する方法を開発する
- インベントリおよびマッピングプロセスを自動化して、ネットワークおよびデータエンドポイント全体にわたり、継続的かつ正確な可視化を実現する



出所：PwCのDigital Trust Insights調査、2019年9月実施
対象総数 3,532

レジリエンス構築の3ステップ

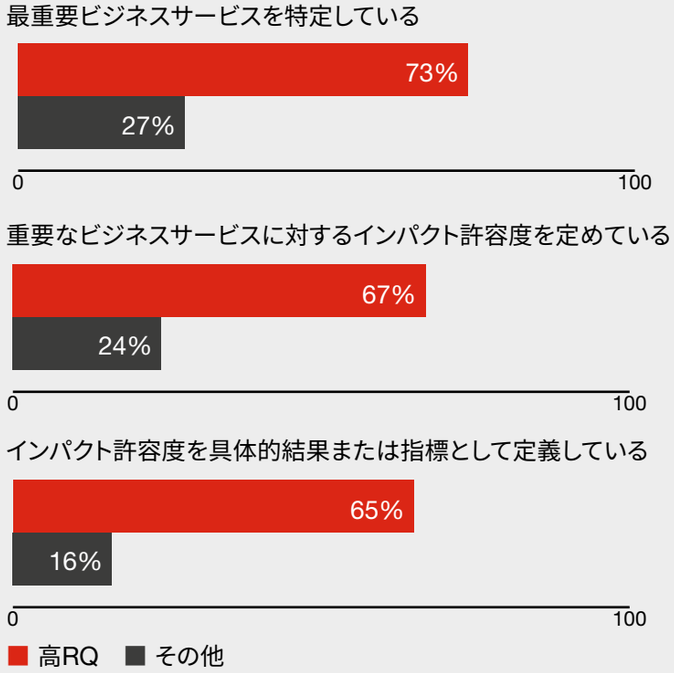
2 組織がどの程度の障害まで許容できるか見定め、テストする

組織は、どの程度の障害までならクライアントへのサービス提供能力を損なわずにいられるか。

この問いに答えるためには、まず自分たちの会社にとって「最重要ビジネスサービス」は何かを定義する必要がある。これは重要なタスクである。高RQグループの73%が、自社の最重要ビジネスサービスを特定しているのに対して、それ以外のグループでは27%という数字なのも驚くことではない。

次に組織がすべきことは、有事に対して持ちこたえられる時間と拠出できる費用の上限、すなわち「インパクト許容度」を定めることである。高RQグループの3分の2の企業が、最重要ビジネスサービスに関するインパクト許容度を定めているのに対して、それ以外のグループでこれを定めているのはわずか24%だ。

高RQグループでは、インパクト許容度を具体的な指標に表しているケースが多く見られる。例えば、ランサムウェア被害企業は、攻撃を受けた後に貴重な時間を割いて許容度を決めている余裕などない。事前に定めた、障害の質、深刻度、時間に関する上限設定および身代金支払いの判断に役立つその他のリスク検討事項を用いなければならないのである。



出所：PwCのDigital Trust Insights調査、2019年9月実施
対象総数 3,532

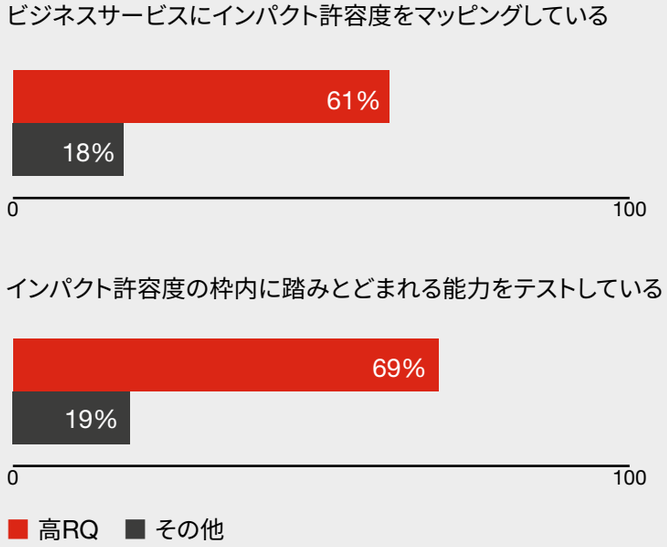
レジリエンス構築の3ステップ

レジリエンスの高い企業は、インパクト許容度内に踏みとどまり続ける力のテストも行っている。このテストは、自ら考案したシナリオやラウンドテーブルディスカッションを通じた「机上」演習から開始する。これによって、チームは障害時の重要なコミュニケーションの予行演習を行うことができるだけでなく、ガバナンスその他のプロセスの穴を見つけるのに役立つ。一部の企業は、机上レベルを超えて、シミュレーション環境にシステムをミラーリングし、そこでシステム間の相互依存関係や接続性をテストしている。

そして最後にもうひとつ、高RQグループとそれ以外のグループを分ける要素がある。それは、高RQグループの61%が、最重要サービスだけでなく、ビジネスサービスに対するインパクト許容度のマッピングも行っている、という点である。それ以外のグループでこれを実践しているのは18%のみであった。こうした活動は、障害によってビジネスパートナーに契約上の罰金を支払うことになった場合に特に重要である。

高RQグループに追いつくために：

- 自社の最重要ビジネスサービスを特定し、中断時のインパクト許容度を定めておく
- インパクト許容度を具体的指標または結果の形で定義しておく
- インパクト許容度のテストを行う
- ビジネスサービスに対するインパクト許容度のマッピングを行う



出所：PwCのDigital Trust Insights調査、2019年9月実施
対象総数 3,532

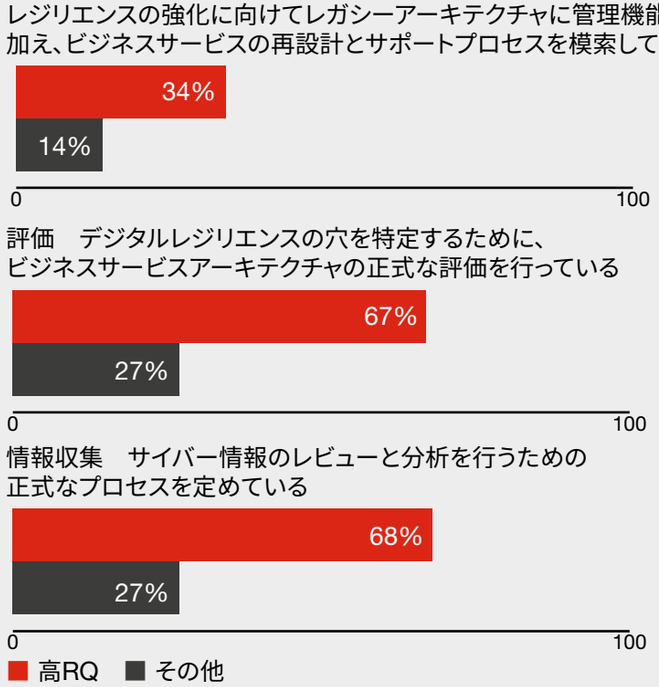
レジリエンス構築の3ステップ

3 計画的なデジタルレジリエンスの構築：次なるフロンティア

レジリエンスに必要な歩みにおける「第3ステップ」は、難易度も最も高くなる。そのため、高RQグループに属していても、完了している企業はほとんど存在しない。組織に対して、全社規模で「計画的なデジタルレジリエンス」を実施しているかどうかを尋ねたところ、「はい」と答えたのは高RQグループのわずか34%であった。それ以外のグループについては、さらに14%まで落ち込んだ。

第3ステップは三つの要素からなる：

- コアとなる資産のパフォーマンスとITとの依存関係について、全社規模で常時監視できるしくみを構築する。ビジネスサービスへのデータ資産とプロセスのマッピングという困難な取り組みを成し遂げた後、もう一段階、全てをまとめて常に最新のビューで見られるような形にすることで、今後の更新時に時間を節約できる。つまり、数カ月要する作業を数分で完了できるようになるのである。
- 情報の流れを監視し、理解し、協力して対応するチームを構築する。過去に脅威情報に関して協力したことのない、または復旧・回復活動を組織的に行った経験のない社員を招集せざるを得ない場合もある。現在あなたの企業がさらされている状況は、影響を受ける全ての領域の可視性とコミュニケーションなしに乗り越えることはできない。



出所：PwCのDigital Trust Insights調査、2019年9月実施
対象総数 3,532

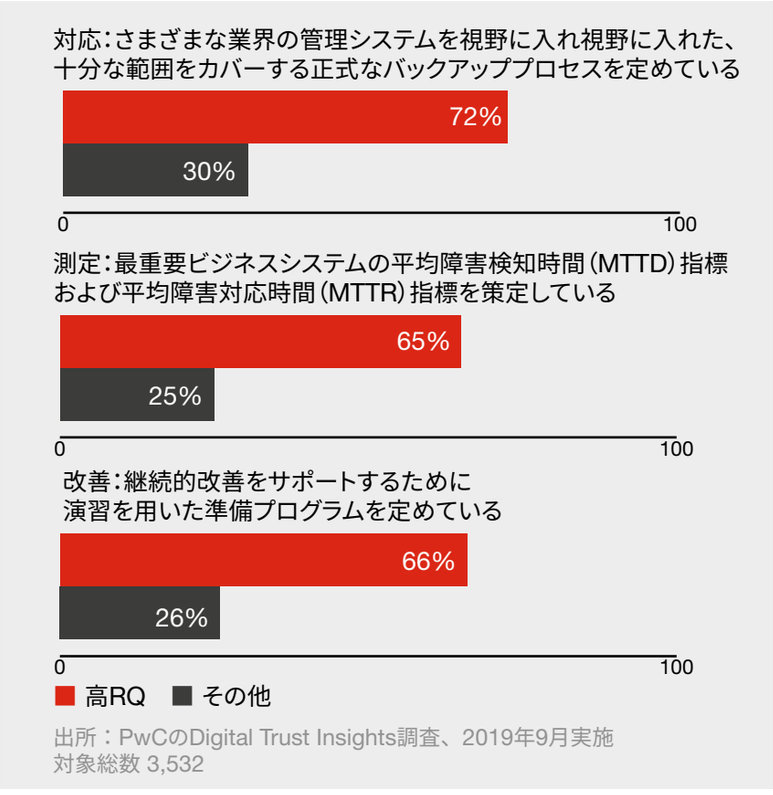
レジリエンス構築の3ステップ

- プラットフォームを使用し、障害から学び、ビジネスサービスとサポートプロセスを継続的に再設計する。そうすると、これまで見えていなかったものや、解読しづらかったことが浮き彫りになる。例えば、ある資産を保持することで危機にさらされる機会は増えるがビジネスに付加価値をもたらすことはないと分かった場合、そうした資産に固執する必要は本当にあるだろうか。システムを回復できない場合、サービスを復旧するための、他の回復方法はあるだろうか（例えば、停電が起きた際、銀行は別の決済処理システムに決済情報を送信することで、顧客の便益を守れる）。または、あなたの会社が別の企業と合併を進めており、ベンダーネットワークやリスク、プロセスが拡大・複雑化する場合、セキュリティにどのような変更が必要になるだろうか。計画的なレジリエンスとはすなわち、事業環境とともに進化することなのである。

PwCは、最重要ビジネスサービスおよび関連するIT資産とプロセスの現況を常に得るための自動化やアナリティクスおよび視覚化がもたらす進化と恩恵を見てきた。これらのテクノロジーを採用することで、組織のレジリエンス機能が継続的に向上する。

高RQグループの次なるフロンティア：計画的なレジリエンス

優先順位の高いプロセスのリアルタイムビューを実現するプラットフォーム構築により、意思決定者と対応者は、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、協力してインシデントに対応できるようになる。



出所：PwCのDigital Trust Insights調査、2019年9月実施
対象総数 3,532

組織が「計画的なレジリエンス」に移行するには何が必要か

例えば、既に高RQグループに属する金融サービス企業にとって、規制が移行の引き金となるかもしれない。同分野の多くの企業がまず思い浮かべるのは、イングランド銀行が実施している、障害が支払いにどのような影響をもたらすかを試すパイロットストレステストだろう。サイバー障害が顧客に及ぼす波及効果に焦点を当てたこのテストは、レジリエンス強化に向けた計画策定の促進につながっている。

規制上の課題や急激な危機が発生しない限り、計画的なレジリエンスに向けた歩みを開始する動機を見いだすのは難しいかもしれない。しかし、取締役やCEOが次のような問いを投げかけることが、「始めなくてはいけない」と思うきっかけになるかもしれない――「大損失を招く甚大な障害や一大ニュースになるようなインシデントが起きたとき、この会社は大丈夫だろうか」

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
kei.tonomura@pwc.com

綾部 泰二
PwCあらた有限責任監査法人
パートナー
taiji.t.ayabe@pwc.com

John W. Oleniczak
Principal, PwC US
john.oleniczak@pwc.com

Joseph Nocera
Principal, Cybersecurity and Privacy, PwC US
joseph.nocera@pwc.com

Shawn Connors
Principal, Cybersecurity and Privacy, PwC US
shawn.joseph.connors@pwc.com

Chris Morris
Principal, Cybersecurity and Privacy, PwC US
christopher.morris@pwc.com

Grant Waterfall
EMEA Cybersecurity and Privacy Leader, PwC United Kingdom
grant.r.waterfall@pwc.com

Paul O'Rourke
Asia Pacific Cybersecurity and Privacy Leader, PwC US
paul.orourke@pwc.com

www.pwc.com/jp

本報告書は、PwCメンバーファームが2019年9月に発行した『Digital Trust Insights - Raising the Resilience Quotient』を翻訳したものです。
翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
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
オリジナル（英語版）はこちらからダウンロードできます。www.pwc.com/us/en/services/consulting/cybersecurity/raising-resiliency-quotient.html
日本語版発刊年月：2020年2月　　管理番号：I201911-1