デジタル変革を支える情報の信頼性の確立

―持続的成長を支えるリスク管理と統制強化―

pwc

www.pwc.com/jp

目次

1 はじめに

近年、AIやクラウドをはじめとする情報技術（IT）の急速な進化により、企業のIT環境は劇的に変化している。経済活動そのものがITを前提として展開されており、業務のデジタル化が加速している。これに伴い、企業は業務効率化や規制対応といった具体的な課題への対応に加え、ITの活用を見据えた経営戦略の見直しが求められている。

こうした変化の中で、企業にとって情報の信頼性（正確性、完全性、一貫性、可用性、機密性）の確保が一層重要となっている。情報に誤りや不整合が存在すると、業務の効率化や迅速な意思決定が妨げられるだけでなく、顧客や取引先との信頼関係にも悪影響を及ぼす可能性がある。さらに、情報漏えいにより機密性が損なわれると、企業の競争力や法令遵守に重大な影響を与える可能性がある。

このようなリスクを回避し、企業の成長や競争力を支えるためには、信頼性の高い情報を常に維持し、提供し続ける体制を構築することが不可欠である。

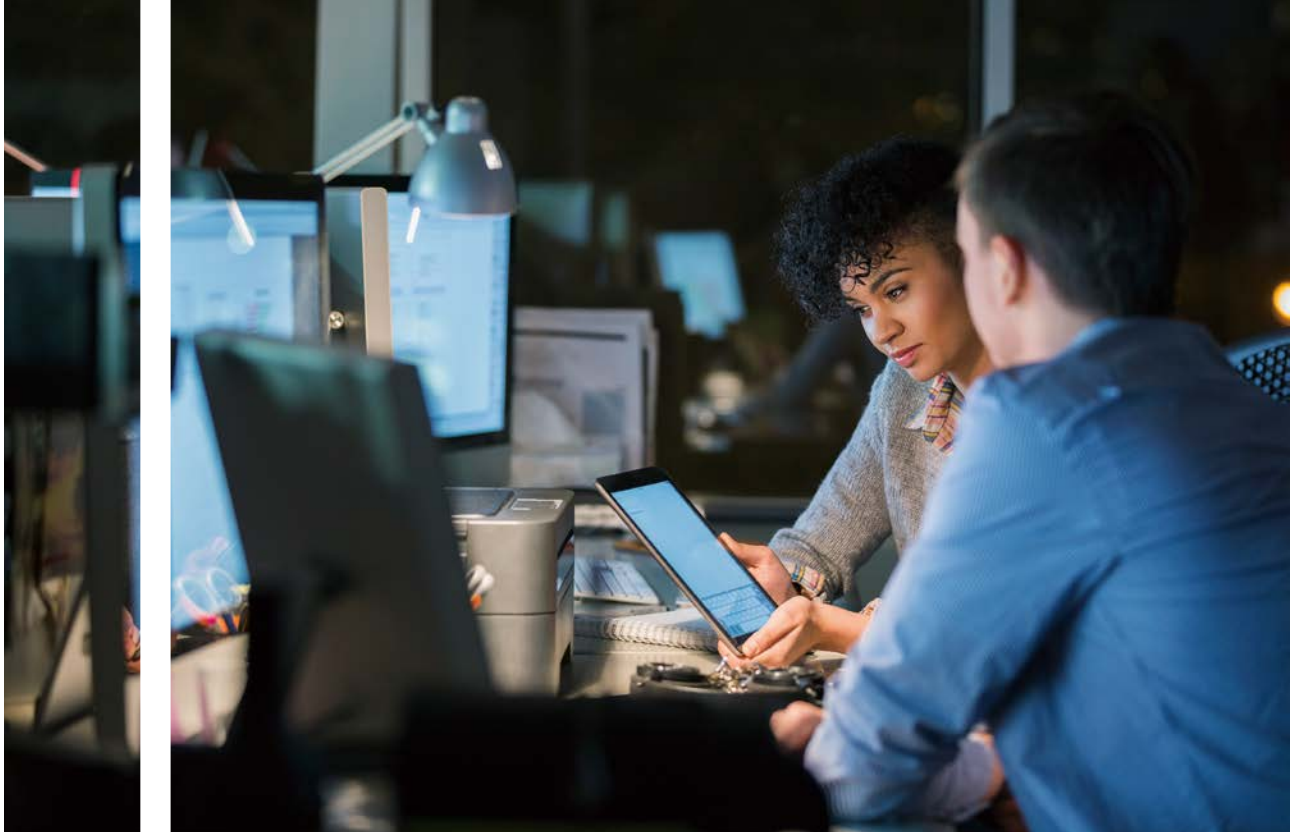
情報の信頼性は、情報セキュリティの3要素（機密性・完全性・可用性）と類似しているが、その目的に違いが存在する。情報セキュリティでは「情報を脅威から守ること」に重点を置くのに対し、情報の信頼性は「情報の整合性と一貫した運用」を重視する。

例えば、セキュリティの観点では機密情報の漏えい防止が重要視されるが、情報の信頼性の観点では、意思決定や業務効率化、さらには顧客に対する信頼性の高いサービス提供を目的として、正確な情報を維持・提供することが求められる。

情報の信頼性を確保するために、企業はITガバナンスの枠組みを活用し、ITのリスク管理や統制を強化する必要がある。

ITガバナンスは、企業戦略とIT戦略を統合し、リスクを適切に管理するための基本的な枠組みを提供する。ITリスク管理は、その枠組みの中で情報システムに関連するリスクを特定・評価し、適切な対策を講じる役割を担う。これにより、企業は潜在的なリスクに迅速に対応し、業務の継続性を確保できる。IT統制は、情報システムが適切に運用されることを保証し、業務プロセスの透明性や信頼性を維持するための仕組みを提供する。ITのガバナンスとリスク管理、統制を連携させることで、企業はリスクを最小限に抑え、効率的に信頼性を確保できるようになる。

本レポートでは、急速に変化するIT環境における主要なITリスクを考察し、求められる対応策を体系的に整理していく。



2 IT環境の変化への対応

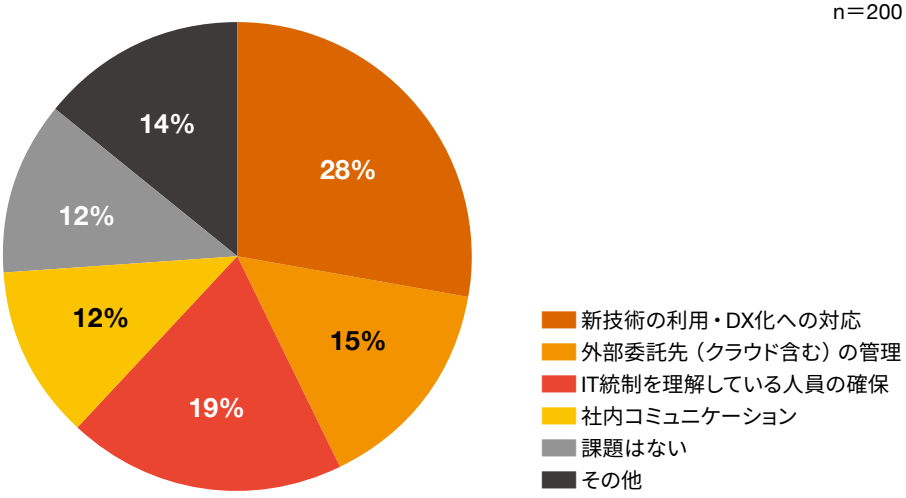
本章では、企業が直面するIT環境の変化に伴うITリスクへの対応策について考察する。

PwCは2025年1月、Web調査にて200社を対象に「IT環境の変化に伴うITリスクに関する課題」に関するアンケート調査を実施した。その結果、新技術の利用・デジタルトランスフォーメーション（以下、DX）化への対応、クラウドサービス利用拡大に伴う外部委託先の管理が主要な課題であることが明らかとなった（図表1）。また、人員の確保や社内コミュニケーションの改善も課題として挙げられた。こうした課題は、IT環境の変化によりその内容や対応策が変化しており、約3割の企業が問題を認識し、対応を検討している。

このような課題認識のもと、ITのガバナンスおよびリスク管理の観点から、企業に求められる対応策についてさらに考察していく。

図表1：IT環境の変化に伴うIT統制に関する課題

n＝200



出所：PwC作成

2.1 DX推進に向けた対応

新技術を活用したDXの推進により、ビジネスモデルや業務プロセスの抜本的な変革に着手する企業が増えている。例えば、AIを活用した需要予測や不正検知、RPAを活用した定型業務の自動化が進んでおり、業務の効率化や精度向上を実現している。なお、DXの取り組みには、業種ごとに差がある。製造業ではIoTとAIを組み合わせたスマートファクトリー化が進んでおり、小売業ではECの強化や需要予測にAIを活用する動きが活発化している。金融業では、AIによるリスク分析や自動審査などが普及しつつあり、業務の自動化と高度化が同時に進んでいる。データ活用の高度化が進む中で、企業は膨大なデータを生成・処理することになり、その結果、データの正確性や整合性の維持が課題となっている。

新技術の導入に先立ち、適切なリスク評価を行いデータ管理のルールを明確化することが重要である。その上で、入力・処理・出力の各プロセスにおいてデータの整合性を確保し、適切なアクセス制御を行うことで、生成される情報の改ざんや誤りを防ぐことが可能となる。

また、DX化のために、既存の業務や社内体制の見直しが不可欠となり、それと同時に従業員の適応やスキル向上も課題となっている。DXを実現するためには、単なる技術の導入だけでなく、組織全体としての文化や運用体制の変革が必要とされる。

さらに、ITの発展により情報資産の価値が高まったことに伴い、サイバー攻撃のリスクも増大している。特に、ランサムウェア攻撃による情報資産の暗号化や破壊、フィッシング詐欺による資産の流出が深刻化しており、情報資産を保護するためのセキュリティ対策も不可欠である。企業は、こうしたサイバー攻撃のリスクに対応しながら、DX推進とのバランスを維持しなければならない。

2.2 外部委託先（クラウド含む）の管理

外部委託先の管理として、クラウドサービスの利用に伴う課題について考察する。

クラウドサービスの普及により、企業は物理的なサーバーを自社で保有せずにITサービスを利用できるようになった。これにより、コスト削減や業務の柔軟性が向上した。

一方で、データの保管場所が不明確になるリスクや、外部のクラウドサービス提供企業への依存が増加するリスクが考えられる。特に、クラウド環境においては、データの管理責任が企業単体ではなく外部委託先にも及ぶため、クラウドプロバイダーのセキュリティ対策やデータ保護の水準が、ITガバナンスの有効性に直接影響を及ぼす。

そのため、企業はITガバナンスの枠組みの中でクラウド利用に伴うリスクを適切に評価・管理し、継続的にモニタリングする体制を整えることが求められる。

具体的には、SLA（サービスレベルアグリーメント）の明確化、定期的な委託業務の監査、自社によるデータのバックアップ管理、委託先の選定基準にISMAP[1]サービスリストを利用することが考えられる。

1 ISMAP：政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program）

2.3 IT統制を理解している人材の確保

企業がITリスク管理を強化し、適切なITガバナンスを確立するためには、IT統制の専門知識を持つ人材の確保が不可欠である。

しかし、IT統制の実務や業務プロセスの設計・運用に精通し、関連する法規制やITガバナンスの要件を理解した人材は限られており、多くの企業で人員不足が課題となっている。

このような状況下で、IT統制を効果的に機能させるために人的リソースの強化が必要で、内部の教育・研修の充実や外部専門家との連携が重要性を増している。

例えば、内部統制のフレームワーク（例：COSOやCOBIT[2]）やITリスク管理の手法を取り入れた研修を社内で実施することで、IT統制への対応力を強化できる。また、外部コンサルタントの活用や、専門機関が提供する外部研修を受講することで、サイバーセキュリティやデータガバナンスに関する実践的な知識などの習得が可能となる。

企業はこれらの人的リソース強化の取り組みを通じて、ITガバナンスの強化、ITリスク管理の高度化、そしてIT統制の実効性向上を図ることが求められる。

2.4 社内コミュニケーション

IT環境の変化に伴い、企業は迅速な意思決定や適切な情報共有が求められるようになっている。ITの利用拡大によって、情報の信頼性を確保するための適切な統制が必要だが、リスク管理の重要性が現場レベルまで十分に浸透していない場合、統制が意図したとおりに機能せず、リスク対応の遅れにつながるおそれがある。

この課題に対応するためには、ITガバナンスの枠組みとして明確に役割分担された組織体制の構築が必要である。具体的には「3つのディフェンスライン」モデルに基づいた組織体制を構築し、業務部門（第1の防衛線）、リスク管理・コンプライアンス部門（第2の防衛線）、内部監査部門（第3の防衛線）がそれぞれ役割を果たしながら相互連携することで、IT統制の実効性を確保できる。特に、ITリスクに関する情報を適切に収集・共有し、迅速かつ適切な対応を可能とするために、これらの部門間の連携を強化することが求められる。

また、部門横断的なワーキンググループを設置し、定期的な会議を通じてITリスクに関する情報を共有することで、リスクを事前に特定し、統制上の対応策を適切に講じることが可能となる。さらに、IT統制に関するガイドラインを明文化し、経営層から現場レベルまでへの周知を徹底することで、リスク管理の枠組みを維持し、ガバナンスの強化につなげることができる。加えて、定期的な教育・研修を実施することも従業員のITリスク管理意識を向上させ、組織全体で統制環境を強化するのに有効である。

2.5 課題の定期的な見直しと統制の継続的な強化

すでに十分なIT統制を確立し、IT環境の変化に適応しながら継続的な改善を進めている企業も存在する。例えば、リスク管理のフレームワークを整備し、定期的な監査や評価を実施している企業では、大きな問題が発生しにくいと考えられる。

一方で、潜在的なリスクの評価や監視体制が十分に機能しておらず、課題を識別できていないケースも想定される。技術革新や法改正に伴い新たな課題が発生するため、定期的な見直しを行い、統制の継続的な強化を図ることが求められる。

2 COSO：Committee of sponsoring organizations of the treadway commission、
COBIT：Control objective for information and related technology

3 IT統制強化のポイント

前章では、IT環境の変化に伴う新たなリスクへの対応を考察した。本章では、内部統制のフレームワークとして広く採用されているCOSOのフレームワークの要素を用いて、体系的に論点を整理していく。

3.1 統制環境（Control Environment）：IT環境の変化に適応できる組織構造を構築する

統制環境は、企業のIT統制の基盤となるため、IT環境の変化に伴い、経営層がデジタルリスクを適切に認識し、ITガバナンスの強化に積極的に取り組むことが求められる。

また、DX推進にあたり、公的機関が発信するガイドラインや基準の情報を収集・共有する仕組みを整えることも重要である。例えば、金融庁が公表する「金融機関のITガバナンスに関する対話のための論点・プラクティスの整理」（第2版）や、経済産業省の「デジタルガバナンス・コード」などの情報を適切に活用し、最新の動向を把握した上での意識決定が求められる。

【具体的な取り組み例】

- 経営層の関与：DXの推進や新技術の導入において、経営層がリーダーシップを発揮し、IT統制の重要性を強調する。
- 役割と責任の明確化：IT統制に関する責任を明確にし、業務部門・IT部門・リスク管理部門の役割を整理する。
- IT統制に関する倫理規範・方針の策定：情報セキュリティポリシーやITガバナンス指針を整備し、全社的に徹底する。
- IT統制を理解する人材の確保と育成計画:社内の教育・研修制度を強化するとともに、外部人材の活用や育成計画を策定する。

3.2 情報と伝達（Information & Communication）：IT環境の変化を踏まえた情報共有の促進と統制の透明性確保

情報と伝達は、ITガバナンスにおける重要な要素であり、企業全体のリスク管理や効率的な運営を支える基盤である。特にIT利用に伴うリスクに関する認識の向上と、部門間での円滑な情報共有が不可欠となっている。企業全体で統制の意識を浸透させ、リスクへの早期対応と予防策の強化を図るためには、部門横断的なコミュニケーションが重要な役割を果たす。このような組織的なコミュニケーションの強化により、情報の伝達が迅速かつ適切に行われ、企業のITガバナンスとリスク管理体制の強化に寄与する。

情報セキュリティ教育と情報伝達

IT環境の変化に伴い、従業員に対する情報セキュリティ教育や意識向上の重要性が高まっている。これに加え、内部統制のルールを全社的に共有し、適切な情報伝達を行うことが求められる。具体的には、教育プログラムを設計し、従業員が必要な知識を習得できる仕組みを整備することが望ましい。また、eラーニングの活用や、社内ポータルサイトに統制関連の情報を集約し、従業員が必要な情報に随時アクセスできる環境を構築することも有効である。

インシデントへの迅速な対応

インシデントが発生した際の迅速な対応も重要である。万が一、インシデントが発生した場合、初動対応の遅れが被害の拡大を招くおそれがあるため、事前に対応フローを明確にし、関係部門間の連携を強化する必要がある。

【具体的な取り組み例】

- 部門横断的な情報共有の強化：定期的なワーキンググループの設置や、研修や説明会を実施する。
- ガイドラインの整備と従業員教育：新技術導入時のIT統制基準を明文化し、従業員に周知することで、現場レベルでの統制意識を向上させる。
- インシデント対応体制の整備：インシデント発生時の対応フローを明確にし、関係部門間の迅速な連携を可能にする。

3.3 リスク評価（Risk Assessment）：IT環境の変化に伴うリスクを特定・評価し、適切な対応策を講じる

クラウドサービスやAIの活用が進むことで、データの信頼性の確保、外部委託先の管理、サイバー攻撃リスクの高まりといった課題が顕在化している。これらのリスクを適切に管理するためには、IT統制の枠組みの中で体系的なリスク評価プロセスを整備し、継続的なリスク評価と対応策の策定を行うことが求められる。

リスク評価のプロセスは、以下のステップで構成される。

1. リスクの特定：新たなIT技術や業務プロセスに関連するリスクの洗い出し。
2. リスクの分析：発生確率と影響度を評価し、リスクの重大性を分類する。
3. リスクの評価：許容可能なリスク水準を定め、対応が必要なリスクを特定する。

リスク評価の手法としては、リスクの影響度と発生確率を分類する定性的リスク評価や、金銭的な影響を数値化する定量的リスク評価がある。さらに、NISTリスクマネジメントフレームワーク（NIST RMF）、ISO 27005（情報セキュリティリスク管理）などのフレームワークを活用することで、より実践的なリスク評価を行うことが可能となる。

【具体的な取り組み例】

- 新技術の活用によるリスクの特定：新技術の活用により発生しうるリスクを評価する。
- 外部委託リスクの管理：第三者リスクマネジメント（TPRM: Third-Party Risk Management）を強化し、ガイドラインを活用してリスクを評価する。
- 法規制の変化への適応：新たな法規制が企業のIT環境に与える影響・リスクを評価し、IT統制との整合性を確保する。

3.4 統制活動（Control Activities）：IT環境の変化に対応するため、リスクに応じた適切な統制手続を構築・実行する

企業は、識別されたリスクに基づき、情報の信頼性を担保するための内部統制を構築し、実行する必要がある。統制活動はリスク管理の一環として、リスクを適切に軽減するための手段であり、統制の実行を通じてリスクを管理し、その実行過程を改善することで、より強固なリスク管理を築いていくことができる。

例えば、アクセス権の管理では、不正アクセスを防止し、データ整合性を維持するために、権限の適切な付与と不要な権限の削除が行われ、定期的な見直しが求められる。また、システム変更管理という点では、変更が業務やシステムに与える影響を最小限に抑え、業務の継続性とシステムの安定性を確保するための手続が重要となる。

さらに、企業の内部統制における各種プロセスや手続の自動化は、手動作業や人的エラーを減少させ、手続の透明性と効果性を向上させる。自動化により、リスク管理の迅速な実行が可能となり、企業はより柔軟かつタイムリーに対応できる環境の整備が可能である。

【具体的な取り組み例】

- アクセス管理：ゼロトラストアーキテクチャの採用や、多要素認証（MFA）の導入により、不正アクセスを防止する。
- データ整合性の確保: AIやビッグデータを活用する際、データの正確性や整合性を担保するための統制手続を構築する。
- IT統制の自動化：RPAやAIを活用し、ログ監査、アクセス管理、異常検知などのプロセスを自動化して、効率性を向上させる。
- 変更管理の徹底：システム導入や改修時の変更管理プロセスを確立し、業務部門、IT部門、リスク管理部門の連携を強化する。

3.5 監視活動（Monitoring Activities）：リスク・統制活動を継続的に評価し、改善を図る

企業が直面する新たなリスクへの対応力を高めるために、定期的な評価と継続的な改善を通じてリスク管理の強化が図られるべきである。監視活動は、統制の実効性を確認し、リスク管理を強化するための基盤であり、企業全体での対応が求められる。ITガバナンスの観点から、2.4で述べた3つのディフェンスライン（第1・第2・第3の防衛線）に基づいた明確な役割分担と管理体制の構築が必要である。

また、AIや機械学習を活用した高度なログ分析により、監視精度の向上が可能となる。これにより、従来の監視活動では見逃されがちな微細な異常も早期に発見でき、リスク対応力が強化される。さらに、AIの活用により、人的リソースの負担を軽減し、より効率的なリスク管理が実現できる。

【具体的な取り組み例】

- （第1の防衛線）リスクモニタリングと初期対応：日常的なシステム監視とログ監視を通じて、リスクの早期発見と迅速な対応を行う。
- （第2の防衛線）リスク評価と対策の実施：定期的なリスク評価の実施と、それに基づくリスク軽減策を講じる。
- （第3の防衛線）内部監査の実施：監視活動やリスク評価の実効性を定期的に評価し、その結果に基づいた改善策を提案する。
- （共通）ITを利用した監視活動の最適化：AIやRPA、機械学習などの技術を活用し、監視活動の精度と効率を向上させる。

4 おわりに

急速に変化するIT環境における企業のITのガバナンス、リスク管理、統制について、どのような取り組みが必要であるかを考察してきた。

現代の企業は、ITの進化に適応する中で、情報の信頼性を確保することが求められている。これを実現するためには、ITのガバナンス、リスク管理、統制に関する活動の強化が必要である。

特に不可欠なのは、ITリスク管理体制の強化や部門横断的な協力の推進といった施策を企業全体に浸透させることだ。IT部門だけでなく業務部門との連携が重要であり、これにより企業全体のガバナンス体制が強化され、統制が実効的に機能する。

これらの施策を通じて企業全体のガバナンスとリスク管理を強化すれば、最終的に変化し続けるIT環境に適応した持続的成長を実現できるようになるはずだ。今後、企業がこれらを戦略的に進めることで、単なるリスク対応にとどまらず、競争優位性の確立と長期的な成長を支える基盤の構築にもつなげられるだろう。

お問い合わせ先

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

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 Japan有限責任監査法人、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、監査およびブローダーアシュアランスサービス、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12,700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構築し、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149カ国に及ぶグローバルネットワークに370,000人以上のスタッフを擁し、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。

発刊年月：2025年5月　　管理番号：I202502-02