



PwC's View

Vol. 64 September 2026

特集

転換期を迎える暗号資産市場

—— 2026年金商法改正とブロックチェーンガバナンス



PwC's View Vol.64

特集

転換期を迎える暗号資産市場 —— 2026年金商法改正とブロックチェーンガバナンス

●	ブロックチェーンは企業の信頼をどう変えるのか —— 暗号資産時代のガバナンスとリスクマネジメント	6
●	暗号資産に係る2026年金商法等改正の概要	8
●	金融商品取引法におけるブロックチェーンに関する開示要件と想定される対応事項	18
●	暗号資産取引規制におけるブロックチェーンに対する攻撃の位置付けと想定される対応事項	21
●	ブロックチェーンビジネスにおいて求められるサイバーレジリエンスの構築	24
●	AI・ブロックチェーン時代のデータトラスト —— 暗号資産関連ビジネスに求められるガバナンスと説明責任	29
特別企画	● 内部監査におけるAI活用と監査品質管理を考える	34
連載	インダストリーインサイト (25) ● 小売事業における多店舗展開ビジネスのDX戦略の考察と ガバナンス・内部統制への影響	39
法務	● AIエージェント利用者に求められるAIガバナンス —— 「AI利活用における民事 責任の解釈適用に関する手引き」から読み解く法的リスク低減の視点	45
海外	● ポーランド再考：欧州事業の可視化と統制を支える運営基盤へ	48
ご案内	PwC調査レポートピックアップ	54
	Viewpoint	56
	書籍紹介	58
	海外PwC日本語対応コンタクト一覧	59

※法人名、役職、インタビューの内容などは掲載当時のものです。

特集

転換期を迎える暗号資産市場

—— 2026年金商法改正とブロックチェーンガバナンス

暗号資産市場の拡大や金融商品取引法などの制度見直しを背景に、ブロックチェーンを活用したビジネスへの関心が再び高まっています。暗号資産は投資対象としての存在感を増すとともに、決済・資産保全を支える金融インフラとしての役割も広がっています。ブロックチェーンは、社会や企業活動の信頼性、透明性、効率性を高めると期待されていますが、規制対応、情報開示、内部統制、サイバーセキュリティ、データガバナンスを一体的に設計し、ステークホルダーへの説明責任を果たせる態勢づくりが必要です。

本特集では、暗号資産とブロックチェーンを「投資のための資本」にとどまらず、「信頼のための資本」という視点から捉え直します。そのうえで、制度・市場・技術の変化を踏まえ、企業が持続的な競争力に結び付けるための実務上の論点を探ります。

最初の論考では、暗号資産・ブロックチェーンビジネスの広がりを概観し、技術だけでは生み出せない「信頼」を下支えするガバナンス、内部統制、セキュリティ、情報開示の意義を整理します。

2つ目の論考では、暗号資産に係る2026年の金融商品取引法等改正を取り上げます。暗号資産に関する規律の金融商品取引法への移行を軸に、情報公表制度、暗号資産交換業者への規制の強化など、事業者が備えるべき実務を読み解きます。

3つ目の論考では、特定暗号資産の発行者および金融商品取引業者に求められる情報開示に焦点を当てます。

4つ目の論考では、51%攻撃、チェーン再編成、コンセンサス形成の妨害、スマートコントラクトなどへの攻撃を題材に、暗号資産取引規制上の位置付けを明らかにします。

5つ目の論考では、改正金融商品取引法とフロンティアAIの進展を踏まえ、暗号資産事業者にとってのサイバーレジリエンスについて掘り下げます。委託先管理、開発・運用プロセス、不正送金の防止、スマートコントラクト・DeFi、外部評価と脅威情報の活用などを扱います。

6つ目の論考では、「データトラスト」をテーマに、データ証跡を横断的に管理する重要性を論じます。さらに、適切なAI利用に関する説明責任を通じて、信頼を事業継続と成長の基盤へ転換する道筋を示します。

ブロックチェーンは企業の信頼をどう変えるのか

—— 暗号資産時代のガバナンスとリスクマネジメント

PwC Japan有限責任監査法人
リスク・アシュアランス部
パートナー 須田 真由



はじめに

金融商品取引法など各種法規制の見直しと暗号資産市場の拡大を背景に、暗号資産・トークンを含むブロックチェーンビジネスに対する関心は改めて高まりを見せています。

また、各業界で進展するブロックチェーンを活用したビジネスイノベーションは極めて多様かつ複雑であり、それに伴って生じる課題の解決には、ガバナンスやコンプライアンスに関する高度な専門性が求められます。

そのような中で、PwC Japanグループでは、企業とともに課題を解決へ導き、社会における信頼を構築していく支援が行えるよう、これまで個別に提供してきたサービスを体系的に拡充・標準化し、監査・規制対応や、社内ガバナンスに関連した一連のルール・組織体制の構築、ビジネスにおいて必要なガバナンスの整備、会計処理における助言業務にまで支援の対象を広げています。

本稿では、暗号資産の技術的基盤であるブロックチェーンの特徴と、暗号資産ビジネスにおけるセキュリティリスクと「信頼」の重要性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 Japan有限責任監査法人および所属部門の正式見解ではないことをお断りしておきます。

1 投資対象として転換期を迎える暗号資産

暗号資産およびブロックチェーンビジネスを取り巻く背景について概観します。

仮想通貨として始まり、現在では暗号資産と呼ばれるこの新たな資産は、2026年の法改正により、従来の資金決済法から金融商品取引法に基づく規制の対象となることが決まりました。これにより、暗号資産は制度上も決済・送金的手段ではなく、投資対象としての性格を有する資産として位置付けられることになりました。もっとも、暗号資産に対する社会の見方が大きく変わったわけではありません。2025年12月10日に公表された金融審議会「暗号資産制度に関するワーキング・グループ」報告では、暗号資産の投資対象化に伴う規制強化が打ち出されましたが、その中では「暗号資産へ資金を投入することについて、投資ではなく投機という言葉を用いるべきではないかとの意見があった」との記述がありました。そこには、暗号資産がなお価格変動の大きい投機の商品として受け止められている現実が表れています。

2 信頼を支える基盤としてのブロックチェーン

暗号資産の技術的基盤であるブロックチェーンの価値は、このような見方だけで捉えられるべきではありません。ブロックチェーンは、取引や権利、証明に関する記録を複数の主体で共有し、検証し、改ざんされにくい形で保持する技術基盤です。その意義は、暗号資産の発行や移転を支えることにとどまらず、企業間あるいは社会全体における信頼、透明性、効率を高める仕組みとなり得る点にあります。ブロックチェーンが信頼を高める仕組みとなり得るのは、従来、信頼の担保のために必要とされて

きた確認や照合作業といった中間プロセスを効率化・再構築する可能性を有しているためです。

取引や権利移転の記録が、関与主体や更新履歴を含めて迅速に検証され、共有されるならば、従来は紙の証憑や個別の照会に依拠していた確認手続を、より効率的で透明性の高い形に置き換えることができます。

一例として、医師資格の確認を考えてみましょう。従来、医師資格を証明するには、医師免許証や医師資格証カードを提示する必要がありました。仮に厚生労働省が医師資格に関する証明情報をブロックチェーン上で管理・提供するようになれば、医師は就職先などに対して、自らの資格情報を迅速かつ確実に示すことができます。その結果、紙の証憑提出や個別照会に依存した確認手続は大きく簡素化され、時間とコストの削減につながるでしょう。紙の証明に比べれば、偽造や改ざんのリスクも抑えやすくなります。

3 技術だけでは生み出せない「信頼」

他方で、その信頼は技術だけで自然に生まれるものではありません。企業がこれを社内外の業務や事業に生かしていくためには、適切な規制の順守に加え、ガバナンス、内部統制、セキュリティ、情報開示といった取り組みが不可欠です。その背景には、ブロックチェーンがハッシュ関数、電子署名、コンセンサスアルゴリズム等の技術により高い改ざん耐性や透明性を備えている一方で、秘密鍵やウォレットの管理、外部委託先管理、クラウド利用、頻繁なシステム変更、KYC／AML（顧客確認／マネー・ローンダリング防止）、取引監視等に関連する多面的なリスクを内包しているという特性があります。

4 セキュリティを経営アジェンダとして捉える

暗号資産関連のインシデント対応一つをとっても、単一の技術的脆弱性だけでなく、ソーシャルエンジニアリング、内部統制の不備、秘密鍵管理の不備、委託先との責任分界の不明確性といった複数の要因が重なって発生する傾向があります。したがって、ブロックチェーンビジネスにおけるセキュリティ対策は、システム部門に閉じた技術課題ではなく、事業部門、リスク管理部門、コンプライアンス部門、システム部門および経営層が一体となって取り組むべき経営アジェンダとして位置付ける必要があります。ここで重要となるのは、セキュリティを個別の防

御策の集合として捉えるのではなく、リスクを識別・評価し、適切に牽制・是正し、外部に対して説明可能な状態を確保するためのガバナンスとして捉えることです。特に暗号資産ビジネスでは、顧客資産の保護、規制対応、システムの安定稼働、データの完全性、委託先管理が相互に関連しており、いずれか一つの不備でも、企業における市場からの信頼失墜につながる可能性があります。

5 「信頼のための資本」を競争優位へ

このように、ブロックチェーンは、新たな金融サービスやデジタル資産ビジネスとして、新たな市場開拓や事業展開、多様なステークホルダーとの連携を可能とします。既存のビジネスモデルやシステムの置き換えとしてのツールの一種ではなく、AIをはじめとする先端技術との融合を通じて、新たなビジネスモデルや社会基盤の構築を可能にするデジタルトランスフォーメーション（DX）の基盤技術となり得るのです。

本特集では、暗号資産とブロックチェーンを、従来の「投資のための資本」という視点だけでなく、「信頼のための資本」という観点から捉え直します。そのうえで、この信頼を持続可能な競争優位へと転換するために、企業に求められるガバナンスとリスクマネジメントの在り方について考察していきます。

須田 真由（すだ まさよし）

PwC Japan 有限責任監査法人 リスク・アシュアランス部 パートナー
製造業、情報通信業および金融業（資金決済・暗号資産）を中心とした、IT領域において財務諸表監査、ならびに国内上場企業の内部統制監査を担当。また、米国証券取引委員会（SEC）登録日本企業、外資系企業の米国企業改革法に基づく内部統制監査業務にも従事。アドバイザリー業務としては、財務報告に係るIT統制の構築および評価支援やフィンテックに関連するITガバナンス構築支援業務をリード。ブロックチェーン技術のセキュリティおよびガバナンスに関する講演も多数実施。
メールアドレス：masayoshi.suda@pwc.com

暗号資産に係る2026年金商法等改正の概要

PwC弁護士法人
弁護士 松下 祐



PwC弁護士法人
弁護士 山中 雄太



はじめに

2026年4月10日、「金融商品取引法及び資金決済に関する法律の一部を改正する法律案」が閣議決定のうえ第221回国会に提出され^{※1}、2026年7月15日、「金融商品取引法及び資金決済に関する法律の一部を改正する法律」（以下、「本改正法」）が成立しました。

本改正法は2025年12月に取りまとめられた金融審議会「暗号資産制度に関するワーキンググループ」報告（以下、「WG報告」）^{※2}等を受けて、その提言のうち金融商品に関する制度のさらなる拡充を図るものです。本改正法においては、日本の金融・資本市場の変化に対応しつつ、成長資金の供給を拡大するとともに、市場の公正性・透明性および投資者保護を確保するため、「暗号資産に係る規制の見直し」、「企業のサステナビリティ情報の開示・保証」、「スタートアップへの資金供給の促進」、「不正取引規制の見直し」等に関する制度を整備する改正がなされました。

本稿では、本改正法における改正内容のうち、「暗号資産に係る規制の見直し」に関して、特に金融商品取引法（以下、「金商法」）の改正法（以下、本改正法による改正後の金商法を「改正金商法」）および資金決済に関する法律（以下、「資金決済法」）の改正法（以下、本改正法による改正後の資金決済法を「改正資金決済法」）に焦点を当てて解説します。

なお、文中の意見は筆者の私見であり、PwC弁護士法人および所属部門の正式見解ではないことをお断りしておきます。

1 暗号資産に係る規制の見直しの概要

日本においては、暗号資産はその決済手段としての側面に着目し、2016年に改正された資金決済法によって規制されてきました。しかし国内のアンケート調査によると、投資経験者の暗号資産保有率は、FX取引や社債等よりも高く、利用者の取引動機のほとんどは暗号資産の長期的な値上がりを期待したものとされており、暗号資産が投資対象として定着していることがうかがえます。また、国内の暗号資産の取引に係る口座開設数は1,400万件を超えていますが、口座保有者のうち、約7割が年収700万円未満となっており、個人の利用者における暗号資産の保有も身近になっているといえます。

また、暗号資産を分散投資の機会と捉え、国内の機関投資家における投資意欲の高まりが見られるとの調査結果も示されているところです。さらに、国内のみならず、国際的にも米国等で暗号資産ETF（上場投資信託）が上場され、近年、機関投資家からの資金流入が増加しています。

このような、暗号資産の投資対象化の進展を背景として、暗号資産を巡っては図表1のような喫緊の課題が生じています。

※1 <https://www.fsa.go.jp/common/diet/221/02/01.pdf>

※2 https://www.fsa.go.jp/singi/singi_kinyu/tosin/20251210.html

図表1：暗号資産を巡る課題

喫緊の課題	課題の具体的内容
適正な取引の確保・無登録業者への対応の必要性	暗号資産の投資目的保有が進展することにより、無登録の暗号資産業者による投資勧誘や詐欺的行為が多発し、金融庁等への相談件数が増加している。
投資アドバイス等に係る不適切行為への対応の必要性	暗号資産取引に関する投資セミナーや、オンラインサロンが出現し、詐欺的な行為が疑われる事例も発生しており、早急な対応が求められている。
情報提供の充実の必要性	暗号資産発行時のホワイトペーパー（説明資料）等の記載内容が不明確であったり、記載内容と実際のコードに差があったりする例が多く、現状の自主規制によっては適切な情報の開示ができない状況にあった。
適切なセキュリティの確保の必要性	暗号資産交換業者へのサイバー攻撃等により、暗号資産が流出する事案が継続して発生しており、顧客資産の安全確保を一層徹底する必要がある指摘されていた。
価格形成・取引の公正性の確保の必要性	インサイダー取引規制に関するIOSCO（証券監督者国際機構）の勧告や欧州等での法制化等、市場濫用・詐欺対策の国際的な規制強化が進んでいる一方、本改正法成立前の制度では十分な手当がなされていなかった。

出所：PwC作成

図表1に挙げている課題は、従前のWG報告においても議論が重ねられてきたものです。本改正法では、WG報告が示した方向性に沿って、暗号資産取引に係る規制を、(1) 資金決済法から金商法に移管し、有価証券とは異なる金融商品として金商法に位置付けることで、利用者保護の充実に加え、(2) 下記の4点について、新たに規制を設ける旨の改正がなされました。

- ① 無登録業者等への対応の強化
- ② 情報公表規制の整備（以下、「情報提供規制」）
- ③ 暗号資産交換業者への規制の強化（以下、「業規制」）
- ④ インサイダー取引規制の創設を含む不公正取引規制の強化

以下では、(1) および (2) の各改正内容の概要について、具体的に解説します。

2 資金決済法から金商法への移管

(1) 改正の全体像

本改正法では、暗号資産取引に係る規制を資金決済法から金商法へと移管するにあたり、暗号資産に係る規定を資金決済法から削除し、金商法において従来の規定を拡充した規定が新設されています。

これにより、本改正法のうち改正資金決済法において暗号資産に係る規定が削除され、従前の「暗号資産交換業」は改正金商法において、「暗号資産取引業」として改正金商法上の金融商品取引業の一形態として規定されています（改正金商法28条5項等）。

また、「電子決済手段・暗号資産サービス仲介業」は2025年の資金決済法の改正で追加されましたが、本改

正法において暗号資産取引の仲介行為に係る規定のみを、別途、改正金商法の金融商品仲介業の一形態として、新たに規定しています（改正金商法2条1項2号、66条以下参照）。なお、電子決済手段取引の仲介に係る規制については、従来どおり改正資金決済法で規定されています。

(2) 暗号資産の種類による切り出し

本改正法では、「暗号資産」を有価証券とは異なる金融商品の一類型として新たに規定しています。

なお、本改正法においては本改正前の資金決済法2条14項で定義されている「暗号資産」の定義内容を維持しつつも、暗号資産のうち、その発行者を観念できる暗号資産を別個に切り出し、「特定暗号資産」として定めています。

「特定暗号資産」とは、「暗号資産であって、特定の者のみが当該暗号資産を発行する権限を有するもの（これに類するものとして内閣府令で定めるものを含む。）」をいいます（改正金商法2条50項）。暗号資産のうち、「特定の者のみが当該暗号資産を発行する権限を有する」暗号資産として、例えば、暗号資産取引業者が発行者の依頼に基づいてIEO（Initial Exchange Offering）により販売する暗号資産が考えられます。また、暗号資産のうち、「これに類するものとして内閣府令で定めるもの」として、パーミッション型ブロックチェーンによる暗号資産や、ERC-20等の基盤となるトークン規格に基づいて発行される暗号資産が含まれることが想定されますが、詳細については今後公表される予定の内閣府令の内容を注視する必要があります。

なお、これら暗号資産の定義に係る改正内容は、WG報告で示された、「現行の資金決済法における『暗号資産』の定義を維持する」という方向性、および「『暗号資産』

は一般に何らかの法的な権利を表章するものではなく、収益の配当や残余財産の分配等が行われないことから、有価証券とは別の規制対象として位置付けるべき」といった方向性と合致するものであり、本改正前の資金決済法における暗号資産の範囲に関する解釈は維持されるものと推察されます^{※3}。

3 情報提供規制

改正金商法において、暗号資産に係る情報の公表制度として、以下の4点が規定されています。

- (1) 暗号資産の発行者が負担する暗号資産の発行時および発行後における継続的な情報公表義務
- (2) 暗号資産取引業者が負担する暗号資産に関する情報提供義務
- (3) 特定暗号資産発行者が負担する監査証明取得義務
- (4) 虚偽記載等についてのエンフォースメント強化

(1) 発行者に対する情報公表義務

①暗号資産の類型等による規制

改正金商法では、従来の「暗号資産」という枠組みに加えて、上記のとおり、「特定暗号資産」という定義が新設されました。これに伴い、改正金商法では、暗号資産の類型により、情報公表義務を区別しています。

また、改正金商法においては公表対象となる情報についても区分を設けており、「特定暗号資産情報」と「暗号資産情報」を区別しています。

さらに、公表義務者についても、「特定暗号資産発行者」と「暗号資産取引業者」とを分けて整理しています。

②特定暗号資産の発行者に対する発行時の情報公表義務

特定暗号資産を発行し、または発行しようとする者（以下、「特定暗号資産発行者」）は、あらかじめ一定の情報（後述の「特定暗号資産情報」）を内閣府令に定めるとこ

ろにより公表しなければ、当該特定暗号資産の募集・売出しをすることができません（改正金商法27条の39第1項本文）。

「特定暗号資産の募集・売出し」とは、新たに発行される特定暗号資産の「有償の提供の申込み若しくはその有償の取得の申込みの勧誘」または既発行の特定暗号資産の「売付けの申込み若しくはその買付けの申込みの勧誘」のうち、改正金商法2条52項各号のいずれかに該当するものをいいます。具体的には、以下の行為が「募集・売出し」に該当します。

- 多数の者を相手方として行う場合として政令で定める場合。
- 上記の政令で定める場合に該当しない場合であって、後述のプロ私募にも少人数私募にも該当しない場合。

したがって、「特定暗号資産の募集・売出し」に該当しない場合としては、例えば、①暗号資産の無償付与の勧誘、②マイニング（暗号資産の承認作業）等の報酬として行う暗号資産の付与に関する勧誘、③適格機関投資家のみを相手方として行う一定の勧誘（プロ私募）、④少人数を相手方として行う一定の勧誘（少人数私募）などが挙げられます。これらに該当する場合、「特定暗号資産の募集・売出し」には当たらず、特定暗号資産発行者に発行時の情報公表義務は発生しません。

情報公表義務の対象となるのは「特定暗号資産情報」です。その内容は、以下のとおりです。

- 当該特定暗号資産に関して投資者に明らかにされるべき基本的な情報として内閣府令で定める情報
- 当該特定暗号資産に係る特定暗号資産取得勧誘等に関する事項として内閣府令で定める事項に関する情報
- 当該特定暗号資産の特定暗号資産発行者の商号、当該特定暗号資産に係る業務の内容および経理の状況その他の公益または投資者保護のため必要かつ適当なものとして内閣府令で定める事項に関する情報

「特定暗号資産情報」の内容の詳細は内閣府令により定められますが、WG報告を踏まえると、例えば、**図表2**の内容が含まれると予想されます。

※3 資金決済法上、「代価のために不特定の者に対して使用することができ」という要件については、暗号資産とNFT（Non-Fungible Token）を区別するという解釈が示されていたが、改正金商法においても当該文言が維持されていることから、暗号資産とNFTの区別に関する従来の解釈を変更するとの指針が公表されない場合には、そのような解釈が維持されるものと推察されます（金融庁「事務ガイドライン第三分冊：金融会社関係「16. 暗号資産交換業者関係」」1-1-1①（注）や、金融庁「事務ガイドライン第三分冊：金融会社関係「16. 暗号資産交換業者関係」の一部改正（案）の公表に対するパブリックコメントの結果等について（コメントの概要及びコメントに対する金融庁の考え方）」（2023年3月24日）No.2、16、21等参照）。

<https://www.fsa.go.jp/news/r4/sonota/20230324-2/20230324-2.html>

図表2：特定暗号資産情報の具体例

特定暗号資産情報	具体例
特定暗号資産に関して、投資者に明らかにされるべき基本的な情報として内閣府令で定める情報	● 暗号資産の性質・機能や供給量 ● 基盤技術 ● 付随する権利義務 ● 内在する流動性リスク等 ● 中央集権的管理者（発行者）に関する情報（当該者の情報、調達資金の使途に関する情報、対象事業に関する情報、暗号資産の保有状況）
特定暗号資産に係る特定暗号資産取得勧誘等に関する事項として、内閣府令で定める事項に関する情報	
特定暗号資産の特定暗号資産発行者の商号、当該特定暗号資産に係る業務の内容および経理の状況その他の公益または投資者保護のため必要かつ適当なものとして、内閣府令で定める事項に関する情報	

出所：PwC作成

③継続的な情報公表義務

特定暗号資産発行者は、特定暗号資産の募集・売出し後も、以下の継続的な情報公表義務を負います。

（ア）特定暗号資産定期情報の公表

特定暗号資産の募集・売出しを行った特定暗号資産発行者は、各事業年度終了後、原則として3カ月以内に、当該事業年度に係る特定暗号資産定期情報を公表しなければなりません（改正金商法27条の50第1項本文）。

（イ）特定暗号資産臨時情報の公表

特定暗号資産定期情報を公表しなければならない特定暗号資産発行者は、当該特定暗号資産について公益または投資者保護のため必要かつ適当なものとして内閣府令で定める場合に該当することとなったときは、遅滞なく、その内容に関する情報を公表しなければなりません（改正金商法27条の51）。ただし、特定暗号資産発行者が暗号資産の分権化等の事由により発行者による情報公表が不要であるとして内閣総理大臣の承認を受けた場合、継続的な情報公表義務は免除されることになっています（改正金商法27条の50第1項但書）。

（2）暗号資産取引業者に対する情報公表義務

①特定暗号資産に関する情報公表義務

特定暗号資産の募集・売出しの取扱いを行おうとする暗号資産取引業者は、あらかじめ、特定暗号資産情報を内閣府令に定めるところにより自らも公表しなければ、当該募集・売出しの取扱いを行うことができません（改正金商法27条の39第4項）。例えば、IEOにおいて、特定暗号資産発行者が公表した情報を暗号資産取引業者においても提供する場面が想定されます。

②暗号資産情報に関する情報公表義務

特定暗号資産情報が公表されていない暗号資産（例えば、特定暗号資産に該当しない暗号資産）や国内で募集・売出しが行われていない特定暗号資産を新たに取り扱おうとする暗号資産取引業者は、あらかじめ、当該暗号資産に関して投資者に明らかにされるべき基本的な情報として内閣府令で定める情報（暗号資産情報）を公表しなければなりません（改正金商法27条の60第1項本文）。

暗号資産情報として公表が求められる情報の内容は内閣府令によりますが、WG報告を踏まえると、暗号資産の性質・機能や供給量、基盤技術等が予想されます。

③暗号資産臨時情報の公表義務

暗号資産取引業者は、暗号資産情報の公表後、当該暗号資産について公益または投資者保護のため必要かつ適当なものとして内閣府令で定める場合に該当することとなったことを知ったときは、遅滞なく、その内容に関する情報（暗号資産臨時情報）を公表する義務を負います（改正金商法27条の61本文）。

（3）特定暗号資産発行者の監査証明取得義務

特定暗号資産発行者は、特定暗号資産の募集・売出しに関して公表する特定暗号資産情報のうち、貸借対照表、損益計算書その他の財務計算に関する情報で内閣府令で定めるものについて、当該特定暗号資産発行者と特別の利害関係のない公認会計士または監査法人の監査証明を受けなければなりません（改正金商法27条の59第1項本文）。ただし、当該募集・売出しに当たり投資家が払い込む額が少額であるものとして政令で定める要件を満たす場合、監査証明の取得義務は免除されます（改正金商法27条の59第1項但書）。

(4) 虚偽記載等に対するエンフォースメント強化

有価証券における開示制度の場合と同様に、特定暗号資産発行者により公表される情報の虚偽記載等については、特定暗号資産発行者およびその関係者に対し、一定の民事責任が課されます（改正金商法27条の41から48）。例えば、虚偽の特定暗号資産情報の公表について、特定暗号資産発行者は、特定暗号資産の募集・売出しに応じて当該特定暗号資産を取得・買付けを行った投資家に対して損害賠償責任を負います（改正金商法27条の42）。この賠償責任は、発行者が、自らに過失がなかったことを立証しても免れることはできず（無過失責任）、損害額については推定規定が置かれています（改正金商法27条の43）。また、このような虚偽記載が行われた場合、特定暗号資産発行者の取締役や監査法人などの関係者にも、一定の民事責任（立証責任が転換された過失責任）が課されます（改正金商法27条の45）。

特定暗号資産以外の暗号資産情報の虚偽等については、これを取り扱う暗号資産取引業者に対し、一定の民事責任（過失責任）が課されます（改正金商法27条の66および67）。

特定暗号資産に関する虚偽記載につき、10年以下の拘禁刑もしくは1,000万円以下の罰金またはこれらの併科が規定されています（改正金商法197条1項4号の3）。

また、虚偽記載等については、証券取引等監視委員会の犯則調査の対象に追加されるほか（改正金商法210条1項）、課徴金制度の対象とされています（改正金商法172条の13～19）。

4 業規制

WG報告では、暗号資産には、セキュリティトークン（有価証券をトークン化したもの）と同様の流通性があることを踏まえ、暗号資産交換業者には、基本的に第一種金融商品取引業に適用される規制と同様の規制を適用することが示されていました。

改正金商法では、上記のようなWG報告の内容を踏まえ、暗号資産交換業者（改正金商法においては「暗号資産取引業者」に変更されています）への業規制の強化等の改正が行われました。具体的には、以下の点が規定されています。

① 暗号資産を投資対象とする投資運用および投資助言行為について、それぞれ業規制の対象に含めるなど業

規制の対象を拡大すること

- ② 暗号資産取引業には第一種金融商品取引業に相当する規制を適用すること
- ③ 暗号資産の管理を行うための重要なシステムの提供者（暗号資産管理関係業務提供者）に対する業規制を導入すること
- ④ 暗号資産取引に係る仲介業を金融商品仲介業の対象に追加すること
- ⑤ 無登録業者対応を強化すること

(1) 業規制の対象範囲の拡大

改正金商法では、業規制の対象範囲を広げ、①暗号資産の借入れ、②暗号資産現物を投資対象とする投資運用行為や投資助言行為を業として行う場合にも投資運用業および投資助言・代理業の登録が必要とされました（改正金商法2条8項11号、12号、14号および15号、28条3項、同条4項、29条）。

また、利用者から暗号資産の借入れを行う業務は、暗号資産取引業の対象となります（改正金商法2条8項25号、28条5項）

(2) 第一種金融商品取引業に相当する規制の適用

上述のとおり、暗号資産取引業者には、基本的に第一種金融商品取引業に相当する規制が適用されることとなりました。主な業規制とその内容は図表3のとおりです。

(3) 暗号資産管理関係業務に対する業規制

金融商品取引業者（暗号資産の管理を業として行う者に限る）に対し顧客の暗号資産の管理に必要な情報システムを継続的に利用させる等の業務（以下、「暗号資産管理関係業務」）について、業規制が新設されました。

「暗号資産管理関係業務」とは、次の業務をいいます。なお、これらの具体的内容は、今後の内閣府令の内容によります。

- ① 金融商品取引業者（暗号資産の管理を業として行う者に限る）に対して、顧客の暗号資産の管理に必要な情報システム（内閣府令で定めるものに限る）を継続的に利用させる業務
- ② 当該金融商品取引業者の委託を受けて当該情報システムの保守または管理（内閣府令で定めるものに限る）を行う業務
- ③ 当該金融商品取引業者の委託を受けて顧客の暗号資

図表3：暗号資産取引業者に適用される規制

業規制	課題の具体的内容
兼業規制	暗号資産取引業を行う金融商品取引業者は、金融商品取引業のほか、付随業務と（事前）届出業務を行うことができる（改正金商法35条の2の2第1項、改正金商法35条の2の2第3項、改正金商法35条の2の2第4項）。
業務管理体制	金融商品取引業者は、暗号資産取引業を含む金融商品取引業を適確に遂行するための業務管理体制を整備しなければならない（改正金商法35条の3第2項）。改正金商法に基づき整備すべきことになる業務管理体制の内容は内閣府令で定められる予定だが、WG報告によれば、例えば以下の体制の整備が求められると予想される。 ● 取り扱う暗号資産の審査体制 ● 顧客適合性確保のための確認体制 ● 売買審査体制
公益または投資者保護の基準に適合しない暗号資産の取扱い禁止	金融商品取引業者は、公益または投資者の保護を確保するために必要な基準として内閣府令で定める基準に適合しない暗号資産の取扱いが禁止されることになった（改正金商法43条の7）。詳細は内閣府令で定められる予定。
外部委託先の管理義務	金融商品取引業者は、他の者が提供する暗号資産売買等業務に必要な情報システムを継続的に利用する場合、内閣府令で定めるところにより、当該情報システムを提供する者の選定に係る基準および手続の整備、当該者に対する指導その他の暗号資産売買等業務の適正かつ確実な遂行を確保するために必要な措置を講じなければならない（改正金商法43条の13第1項）。
責任準備金	暗号資産取引業を行う金融商品取引業者は、暗号資産の売買その他の取引の取引量に応じ、内閣府令で定めるところにより、金融商品取引責任準備金の積立てが義務付けられる（改正金商法46条の5）。コールドウォレット等で管理する暗号資産についても流出リスクがあることを踏まえ、不正流出事案が生じた場合の補償原資に充てられる責任準備金の積立てが義務付けられることになった。具体的な積立率については、管理する暗号資産の残高に応じ、セキュリティ水準も勘案しながら定められる予定。
自己資本規制	暗号資産取引業を行う金融商品取引業者には、自己資本規制比率の算出等が法令上義務付けられることとなります（改正金商法46条の6）。具体的な比率は、今後策定される予定の内閣府令の内容を注視する必要がある。
外務員制度	金融商品取引業者は、勧誘員、販売員、外交員その他いかなる名称を有する者であるかを問わず、その役員または使用人のうち、その金融商品取引業者等のために、①暗号資産の売買、②暗号資産の売買の媒介、取次または代理、③特定暗号資産の引受け、④特定暗号資産取得勧誘等の取扱い、⑤暗号資産の売買またはその媒介、取次もしくは代理の申込の勧誘を行う者について、外務員登録を行わなければならない（改正金商法64条1項）。
暗号資産等管理業務に係る規制	顧客の金銭の預託を受けるまたは暗号資産を管理する暗号資産等管理業務を行う金融商品取引業者は、顧客に対し善良な管理者の注意をもって当該業務を行わなければならない。また、暗号資産等管理業務を行うにあたっては、内閣府令で定めるところにより、顧客の暗号資産を適正に管理するための方法によらなければならない（改正金商法43条の10、43条の11）。

出所：PwC作成

産の管理に係る業務のうち内閣府令で定めるものを行う業務

暗号資産管理関係業務に係る主な規制の概要は以下のとおりです。

● 参入規制

暗号資産管理関係業務を行う者は、あらかじめ当局に対し、届出をしなければなりません（改正金商法66条の94）。当該届出を行った暗号資産管理関係業務を行う者が「暗号資産管理関係業務提供者」（改正金商法2条55項）となります。

● 善管注意義務

暗号資産管理関係業務提供者は、暗号資産管理関係業務の提供を受ける金融商品取引業者に対し、善管注意義務を負います（改正金商法66条の96）。

● 業務管理体制の整備

暗号資産管理関係業務提供者は、①暗号資産管理関係業務を適確に遂行するための業務管理体制を整備し、②情報の漏洩等の防止その他の安全管理のために必要な措置を講じなければなりません（改正金商法66条の97）。

● 暗号資産管理関係業務提供者以外の者から暗号資産管理関係業務の提供を受けることの禁止

金融商品取引業者（暗号資産の管理を業として行う者に限る）は、暗号資産管理関係業務提供者以外の者から暗号資産管理関係業務の提供を受けてはなりません（改正金商法43条の12第1項）。また、暗号資産管理関係業務提供者から暗号資産管理関係業務の提供を受ける場合には、内閣府令で定めるところにより、暗号資産管理関係業務提供者の選定に係る基準および手続の整備、当該暗号資産管理関係業務提供者に

対する指導その他の顧客の暗号資産の管理に係る業務の適正かつ確実な遂行を確保するために必要な措置を講じなければなりません（改正金商法43条の12第2項）。

(4) 暗号資産取引に係る仲介業を金融商品仲介業の対象に追加

暗号資産取引に係る仲介業が金融商品仲介業の対象に追加されました（改正金商法2条11項2号、66条以下）。

(5) 無登録業者対応の強化

無登録で暗号資産取引業を行う者に対する罰則として、資金決済法における3年以下の拘禁刑もしくは300万円以下の罰金またはその併科から、10年以下の拘禁刑もしくは1,000万円以下の罰金またはその併科に引き上げられました（改正金商法197条1項4号の3）。

また、裁判所による緊急差止命令の対象に暗号資産関連の無登録業が追加され、証券取引等監視委員会の申立て権限が付与されました（改正金商法192条1項、194条の7第4項2号）。

さらに、証券取引等監視委員会が無登録業者に対し犯則調査権限を行使することが可能となりました（改正金商法210条1項）。

金商法に違反する無登録業者による売付けについては、原則として、無効となります（改正金商法171条の15第1項）。

5 暗号資産取引に係る不公正取引規制の見直し

本改正前の金商法では暗号資産についても、上場有価証券等と同様に、偽計・相場操縦行為等の禁止規制が整備されていましたが、インサイダー取引を直接規制する規定は設けられていませんでした。

しかし、インサイダー取引規制に関するIOSCO（証券監督者国際機構）の勧告等の国際的な情勢を踏まえ、取引の公正を確保する観点から、本改正法においては暗号資産のインサイダー取引規制が新設されました（改正金商法171条の7～10）。

具体的には、上場有価証券等のインサイダー取引規制の枠組みをベースとして、(i)対象暗号資産について、(ii)「重要事実」に接近できる、(iii)特別の立場にある者（インサイダー）が、当該事実の公表前に、売買等を行うことを禁止する旨が規定されています。これらの改正内容は、

WG報告において指摘された不公正取引規制の強化という方向性に沿うものです。

(1) 規制対象とされる暗号資産

インサイダー取引規制の規制対象となる暗号資産は、国内の暗号資産取引業者で取り扱われる暗号資産および取扱いの開始が暗号資産取引業者の業務執行決定機関において決定された暗号資産に限定されます（本改正法と同時に金融庁が公表した2026年4月付「金融商品取引法及び資金決済に関する法律の一部を改正する法律案説明資料」^{※4}（以下、「説明資料」）5頁および改正金商法171条の7～9参照）。

そのため、国内または国外における無登録業者で取り扱われている暗号資産等は、基本的にはインサイダー取引規制の対象外となります。

(2) インサイダー取引規制の規制対象とされる「重要事実」

本改正法において規制対象とされる「重要事実」は、①特定暗号資産発行者に関する重要事実、②暗号資産取引業者に関する重要事実、③大量売買者に関する重要事実の3つの類型に大別されます（改正金商法171条の7第2項、171条の8第2項、171条の9第2項）。各重要事実は具体的に、以下のとおり規定されています。

① 特定暗号資産発行者に関する重要事実

- 発行者の業務執行機関が一定の事項（特定暗号資産の技術的仕様の変更、新たに発行される特定暗号資産の申込みの勧誘、関連サービス提供の開始・休止または終了、業務上の提携またはその解消、技術的仕様の保守に係る業務の廃止、合併を除く発行者の解散等）を行うことについての決定をしたこと、または当該機関が当該決定のうち公表されたものに係る事項を行わないことを決定したこと（改正金商法171条の7第2項1号）
- 発行者に関する一定の事項（災害または業務遂行の過程で生じた障害・特定暗号資産の取扱いの開始・廃止の決定またはオプションの上場の承認・廃止の原因となる事実、提携先サービスの開始・休止または終了の決定等）の発生（同項2号）
- 上記のほか、特定暗号資産またはこれに係る業務に

※4 <https://www.fsa.go.jp/common/diet/221/02/03.pdf>

関する重要な事実であって、投資者の投資判断に著しい影響を及ぼすもの（同項3号）

②暗号資産取引業者に関する重要事実

- 暗号資産取引業者による一定の事項（暗号資産の暗号資産売買業務における取扱いの開始または終了、暗号資産取引業者の解散等）を行うことについての決定をしたこと、または当該機関が当該決定のうち公表されたものに係る事項を行わないことを決定したこと（改正金商法171条の8第2項1号）
- 暗号資産取引業者に関する一定の事項（顧客暗号資産の不正な移転、業務に関する障害、関連するサービスの提供の開始・休止または終了の決定等）の発生（同項2号）
- 上記のほか、暗号資産取引業者による暗号資産の取扱いまたは当該取扱いに係る暗号資産に関する重要な事実であって投資者の判断に著しい影響を及ぼすもの（同項3号）

③大量売買者に関する重要事実

- 暗号資産の大量売付け^{※5}もしくは大量買付けの実施またはその中止に関する事実

(3) 規制対象者

改正金商法においては、前記（2）の重要事実の類型に

応じて、それぞれ以下の者が所定の方法により重要事実を知るに至った場合は、インサイダー取引規制の対象者とされることが規定されています。

①特定暗号資産の発行者に関する重要事実における規制対象となり得る関係者

改正金商法171条の7第1項は、特定暗号資産発行者関係者であって、特定暗号資産等に関する重要事実を知った者は、当該重要事実の公表^{※6}がされた後でなければ売買等^{※7}を行ってはならないと定めています。また、特定暗号資産発行者関係者は所定の方法により知った場合にのみインサイダー取引規制の対象となります。概要は図表4のとおりです。

②暗号資産取引業者に関する重要事実における規制対象となり得る関係者および大量売買者に関する重要事実における規制対象となり得る関係者

改正金商法は暗号資産取引業者関係者（改正金商法171条の8第1項）および大量売買者関係者（改正金商法171条の9第1項）をインサイダー取引規制の対象者として規定しています。

なお、各規制対象者の範囲については、上記表で示した特定暗号資産発行者関係者と概ね同様の規定が定められています。

また、上記の関係者から重要事実の伝達を受けた者

図表4：特定暗号資産発行者関係者がインサイダー取引規制の対象となるケース

号	特定暗号資産発行者関係者	重要事実を所定の方法により知ったもの
1号	特定暗号資産発行者（親会社を含む）の役員等（法人以外の場合は代理人・使用人）	その者の職務に関し知ったとき
2号	特定暗号資産発行者の会社法433条1項に定める権利を有する株主または社員（株主または社員が法人であるときは役員等を含む）	当該権利の行使に関し知ったとき
3号	特定暗号資産発行者に対する法令に基づく権限を有する者であって、当該権限の行使に関し重要事実を知った者	当該権限の行使に関し知ったとき
4号	特定暗号資産発行者と契約を締結している者または締結の交渉をしている者（法人の場合は役員等を含む）であって、当該特定暗号資産発行者の役員等以外の者（法人以外の者である場合には代理人または使用人）	当該契約の締結もしくはその交渉または履行に関し知ったとき
5号	第2号または第4号に掲げる者が法人である場合の当該法人の役員等（その者が役員等である当該法人のほかの役員等がそれぞれ第2号または第4号に定めるところにより当該特定暗号資産発行者に係る特定暗号資産等に関する重要事実を知った場合におけるその者に限る）	その者の職務に関し知ったとき

出所：PwC作成

※5 「大量売付け」および「大量買付け」とは、暗号資産等の売付けおよび買付けのうち、「暗号資産等の価格等に対して重要な影響を与えるおそれがあるものとして政令で定めるもの」を意味しますが、説明資料5頁を参照すると、「政令では発行済み暗号資産の20%以上の売買等を定める予定」とされています。

※6 「公表がされた」とは、「第1項に規定する特定暗号資産等に関する重要事実について、当該暗号資産発行者により多数の者の知り得る状態に置く措置として政令で定める措置がとられたこと又は当該特定暗号資産等に関する重要事実が記載され、若しくは記録されている当該特定暗号資産発行者の特定暗号資産情報等若しくは訂正特定暗号資産情報等が公表されたことをいう」と改正金商法171条の7第4項で定められています。

※7 「売買等」とは、改正金商法171条の7第1項柱書において、「売買その他の有償の提供若しくは譲渡若しくは取得若しくは譲受け、合併若しくは分割による承継又はデリバティブ取引」をいうと規定されています。

図表5：暗号資産のインサイダー取引の適用除外類型

	インサイダー取引規制の適用除外（例）
1	対象暗号資産の提供または譲渡を受けることができる権利を有する者が当該権利を行使することにより、対象暗号資産の取得または譲受けを受ける場合
2	対象暗号資産に係るオプションを取得している者が、当該オプションを行使することにより対象暗号資産等に係る売買等をする場合
3	法令上の義務に基づき対象暗号資産等に係る売買等をする場合
4	改正金商法159条3項または171条の5第3項の政令で定めるところにより対象暗号資産等に係る売買等をする場合
5	重要事実を知っている者との間において、金融商品取引業者の暗号資産売買業務または取引所金融市場等によらないで売買等をする場合
6	合併等により承継させ、または承継する場合
7	いわゆる「知る前契約」の履行（重要事実を知る前に締結された売買等に関する契約の履行等）
8	いわゆる「知る前計画」の実行（合併等の契約に係る取締役会決議が重要事実を知る前にされた場合における当該合併等による暗号資産の承継等）
9	対象暗号資産の技術的仕様に基づいて一定の役務を提供することにより当該対象特定暗号資産の提供または取得する場合その他これに準ずる特別の事情に基づく対象暗号資産等に係る売買等であることが明らかな売買等をする場合（内閣府令で定める場合に限る）
10	（大量売買者の関係者による取引のみ）一定の情報受領者による取引（改正金商法171条の9第5項第6号参照）

出所：PwC作成

等の一定の者^{※8}もインサイダー取引規制の対象者とされます（改正金商法171条の7第3項、171条の8第3項、171条の9第3項）。

(4) 適用除外

改正金商法171条の7第5項、171条の8第5項、171条の9第5項は、図表5のとおり暗号資産のインサイダー取引についても上場有価証券等のインサイダー取引規制と類似した適用除外類型を定めています。

(5) 情報伝達・取引推奨行為の禁止

このほか、改正金商法171条の10各号は、暗号資産のインサイダー取引規制についても上場有価証券のインサイダー取引規制と同様に、関係者による情報伝達・取引推奨行為を禁止しています。

(6) 罰則

改正金商法では、暗号資産に係るインサイダー取引規制に違反した場合においても、上場有価証券等と同様に、5年以下の拘禁刑もしくは500万円以下の罰金または併科とする旨が定められています（改正金商法197条の2第1項16号～19号）。

(7) その他の不公正取引行為の禁止

改正金商法では、上記インサイダー取引規制に加えて、有価証券に係る不公正取引規制その他有価証券の取引等に係る規制のうち、規制趣旨が暗号資産にも妥当すると

考えられる規制を、併せて整備しています。

① 安定操作取引の禁止

改正金商法171条の5第3項は、何人も政令で定めるところに違反して、暗号資産等の相場をくぎ付けし、固定し、または安定させる目的をもって、一連の暗号資産売買等またはその申込み、委託等もしくは受託等、または一連の有価証券売買等またはその申込み、委託等もしくは受託等を行うことを禁止しています。

② 対価受領開示義務^{※9}

改正金商法171条の12は、暗号資産の発行者や金融商品取引業者等から対価を受けて暗号資産の取引判断に関する意見をインターネット等で表示する場合には、対価を受ける旨の表示をすることを義務付けています。なお、広告料を受け取る者が、当該広告料を対価として広告を表示するような場合については、この限りではないものと定められています（改正金商法171条の12但書）。

6 おわりに

本改正法は、暗号資産を、決済手段としての性質のみならず、投資対象としての性質を踏まえて金商法上の規制枠組みに位置付け直すものです。暗号資産取引業者に第一種金融商品取引業に相当する規制を適用し、発行者および暗号資産取引業者に情報公表義務を課すとともに、暗号資産管理関係業務提供者への規制やインサイダー取

※8 第一次情報受領者等をいいます。

※9 いわゆる「ステルスマーケティング規制」等を指します。

引規制を含む不公正取引規制を整備する点で、国内市場における利用者保護、取引の公正性・透明性および市場インフラの信頼性を高める重要な制度整備^{※10}といえます。

もっとも、本改正法は主として国内の暗号資産取引業者による取扱い、国内利用者への勧誘・取引および国内市場における価格形成の公正性確保を念頭に置くものであり、グローバルに展開される暗号資産取引および関連ビジネスの全体を直接カバーするものではありません。暗号資産は関係者が国境を越えて分散し得るため、国内規制の適用範囲、クロスボーダー取引への影響、海外事業者との役割分担等については、事業モデルごとに検討する必要があります。

実務上は、自社の事業、取扱銘柄および提供サービスが新たな情報提供規制、業規制または不公正取引規制の対象となるかを早期に整理し、開示、審査、顧客管理、売買管理、外部委託先管理等の体制を見直すことが重要です。特に、既存の暗号資産交換業者は、経過措置により施行日から6カ月間は改正金商法上の登録を受けずに業

務を継続することができ、同期間内に登録申請を行った場合には、登録、登録拒否または業務廃止処分まで、最長2年間、業務継続が可能とされています（本改正法附則8条1項および2項）。ただし、猶予期間中も改正金商法上の行為規制・監督規制がみなし適用されるため（本改正法附則8条3項）、施行日までに業務管理体制やインサイダー取引防止体制等を整備しておく必要があります。また、施行後2週間以内の届出義務（本改正法附則10条）や、既存取扱銘柄に関する暗号資産情報の施行後3カ月以内の公表義務等（本改正法附則8条5項）にも留意が必要です。

改正金商法の詳細は、今後の政令・内閣府令、自主規制規則、監督指針その他の実務上のガイダンスに委ねられる部分が多く残されています。また、暗号資産市場は技術、取引形態、国際的な規制動向に応じて急速に変化しており、今後も継続的な制度見直しが行われる可能性があります。そのため、暗号資産取引に関与する事業者においては、下位法令および当局・自主規制機関の実務運用を注視しつつ、必要に応じて専門家の助言を得ながら、自社の事業モデルに即した対応を計画的に進めることが求められます。

※10 なお、本改正法に関しては、衆議院および参議院において、暗号資産取引業者の適合性原則遵守の実効性の確保、無登録業者による詐欺的被害からの国民の財産の保護、不公正取引規制および無登録業者に対する対応措置の実効性確保などの附帯決議がなされています。

松下 祐（まつした ゆう）

PwC弁護士法人 弁護士

2017年弁護士登録。国内外を問わず、暗号資産や証券分野に関する金融規制対応・金融取引等の案件を取り扱う。国内法律事務所にて渉外法務、金融規制対応・金融取引、M&A、人事・労務を中心に幅広い業務を経験した後、PwC弁護士法人に入所。

メールアドレス：yu.matsushita@pwc.com

山中 雄太（やまなか ゆうた）

PwC弁護士法人 弁護士

2025年弁護士登録。一般企業法務をはじめ、各種金融規制対応やファンドビジネス、国内外の投資案件に携わる。金融系国内法律事務所にて勤務後、PwC弁護士法人に入所。

メールアドレス：yuta.yamanaka@pwc.com

金融商品取引法におけるブロックチェーンに関する開示要件と想定される対応事項

PwC Japan有限責任監査法人
ガバナンス・リスク・コンプライアンス・
アドバイザリー部
パートナー 竹内 秀輝



PwC Japan有限責任監査法人
ガバナンス・リスク・コンプライアンス・
アドバイザリー部
マネージャー 安嶋 建



はじめに

本特集の「暗号資産に係る2026年金商法等改正法の成立」（前記事）で解説したとおり、2026年金融商品取引法改正により、暗号資産に関する情報公表制度が新たに整備されました。本稿では、その中でもブロックチェーンに関係する開示要件および想定対応事項に焦点を当てて整理します。

なお、文中の意見は筆者の私見であり、PwC Japan有限責任監査法人および所属部門の正式見解ではないことをお断りしておきます。

1 特定暗号資産の発行者による開示

(1) 特定暗号資産情報の公表

今般の法改正においては、「暗号資産であって、特定の者のみが当該暗号資産を発行する権限を有するもの」を「特定暗号資産」として位置付け^{※1}、その発行者に対して、情報公表義務を課しています。開示制度の概要は既に前記事で示しているため、本稿では、開示内容のうちブロックチェーンに関連する項目に着目します。

現状、ブロックチェーンに関する文言が直接置かれているわけではありません。また、今後、内閣府令等において詳細が規定される可能性もありますが、そこにおいても当該文言が盛り込まれることが確定しているわけではありません。もっとも、諸外国における実務の進展や投資家保護という規制の趣旨を踏まえれば^{※2}、特定暗号資産の募集・売出しに際して発行者から投資家に明らかにされるべき基本的情報の中には、少なくとも実務上、投資家の利害に影響を及ぼす可能性があるものとして、以下のような事項が含まれると想定されます。

- 当該暗号資産の技術的仕様の概要
- 発行・移転・保管の仕組み
- 基盤となる分散型台帳または電子情報処理組織の特性
- 技術上の制約や前提条件
- 保有者に影響し得るシステム上の重要事項

これらが必要となる理由は、暗号資産の発行・移転・保

※1 金融商品取引法2条50項。

※2 これ以降の記載も同様の考慮に基づいています。

管の安全性や継続性、将来的な仕様変更リスク等に影響し得るため、投資判断上重要な情報になり得るからです。

(2) 定期情報の公表

特定暗号資産発行者には、事業年度ごとに定期情報を公表する義務も課されています^{※3}。これは、募集・売出し時点に限らず、発行後も継続的な情報提供を求めるものです。

そして、ブロックチェーン関連では次のような事項が実務上重要になると考えられます。

- 技術保守・開発体制の状況
- システム運営体制の変更の有無
- 技術基盤の安定性に関する重要情報
- 委託先や保守運営主体への依存状況
- 継続的なサービス提供に関する重要なリスク

(3) 臨時情報の公表

ブロックチェーン関連の開示という観点で、今回の改正で最も実務的に重要と考えられるものとして、投資判断に重要な影響を及ぼす事由が生じた場合における臨時情報の公表義務も規定されています^{※4}が、ブロックチェーン関連では、技術仕様変更や重大障害等に係る以下のような情報が臨時開示の対象となる可能性があります。

- 技術的仕様の変更
- 技術的仕様に関連するサービスの提供開始・休止・終了
- 技術的仕様の保守に係る業務の廃止
- その他、投資判断に重要な影響を及ぼす技術上・運営上の重要事実

(4) 開示情報の訂正および虚偽情報の公表停止

以上のほか、発行者による開示情報について訂正すべき事項がある場合には、適時に訂正することが求められています^{※5}。また、重要事項について虚偽があることを認識した場合には、虚偽情報を解消するための情報が公表されるまでの間、当該虚偽情報の公表を停止しなければならないとされています^{※6}。

そして、開示情報の訂正が問題となる典型例として、以下が想定されます。

- 技術仕様の重要部分の不記載
- 実際には存在する重大な制約の不開示
- 保守態勢に関する過度に楽観的な説明
- サービス継続性に関する誤解を招く表現
- 仕様変更の影響についての不適切な説明

2

暗号資産取引業を行う金融商品取引業者による開示

(1) 暗号資産情報の公表

暗号資産取引業者についても、取り扱う暗号資産に関する情報公表が求められることになります。これは、流通段階においても投資家に必要な情報を確保するための制度といえます。

これに該当するものとして、暗号資産取引業を行う金融商品取引業者がある銘柄の暗号資産について新たに売買等の業務を行おうとする場合に、あらかじめ当該暗号資産に関する基本的情報を公表する義務^{※7}が挙げられます。ここで実務上、公表が求められる情報については、特定暗号資産発行者の場合と基本的に同様と想定されます。

(2) その他の対応

暗号資産交換業を行う金融商品取引業者には、当初公表した暗号資産情報に加え、必要に応じて臨時情報^{※8}や訂正情報^{※9}を公表するとともに、情報を継続的に公表する義務も課されています^{※10}。また、重要事項について虚偽があることを認識した場合には、虚偽情報を解消するための情報が公表されるまでの間、当該虚偽情報の公表を停止しなければならないとされています^{※11}。

そして、実務上重要になると想定されるものとして、重大な障害やセキュリティインシデントに関する事項が挙げられます。

3

発行者および金融商品取引業者において想定される対応事項

(1) 技術情報を開示情報として管理する態勢の整備

従来、ブロックチェーン関連の情報は主に技術部門内

※3 金融商品取引法27条の54。

※4 金融商品取引法27条の51。

※5 金融商品取引法27条の52。

※6 金融商品取引法27条の54第3項。

※7 金融商品取引法27条の60。

※8 金融商品取引法27条の61。

※9 金融商品取引法27条の62。

※10 金融商品取引法27条の63。

※11 金融商品取引法27条の54第3項。

で管理される傾向があったと考えられます。しかし、今般の法改正により、技術仕様やその変更が法定開示事項に含まれる可能性があるため、技術情報を開示統制の枠組みに組み込む必要があります。実務上有益な取り組みとして、以下のものが想定されます。

- 技術的仕様の社内定義の明確化
- 「重要な仕様変更」の判定基準整備
- 技術部門から法務・開示部門への報告ルート整備
- 開示要否判定会議体の設置
- 臨時開示トリガーの一覧化

(2) 訂正対応を見据えたレビュー体制の構築

技術的な説明は誤解を生みやすいため、開示文書については、技術、法務、コンプライアンスの各部門、さらには必要に応じて内部統制・内部監査部門を交えたレビュー

体制を構築しておくことが重要といえます。

4 おわりに

金融商品取引法の改正により、特定暗号資産の発行者および金融商品取引業者の双方に対して、体系的な情報開示義務が整備されました。ブロックチェーンに関しては、技術一般の説明義務というよりも、暗号資産の技術的仕様、その変更、関連サービスの開始・休止・終了、保守体制の変更等について、投資判断に重要な情報として適切に開示することが求められる点が重要といえます。

したがって、今後の実務では、技術部門と開示・法務・コンプライアンス部門との連携を前提とした開示統制の構築が不可欠になると想定されます。特に、仕様変更や障害情報を適時に捕捉し、法定開示に結び付ける態勢整備が規制対応の中心的な課題になると考えられます。

竹内 秀輝（たけうち ひでき）

PwC Japan有限責任監査法人 ガバナンス・リスク・コンプライアンス・アドバイザリー部 パートナー

監査法人で保険会社に対する監査業務および各種アドバイザリー業務を幅広く経験した後、2011年から2014年にかけて、金融庁監督局保険課および総務企画局総務課国際室で勤務。金融庁在籍期間中は、保険監督者国際機構（IAIS）のメンバーとして国際保険規制に関する検討に携わった他、国内外の監督カレッジへの参画を通じたクロスボーダーでの監督にも従事。現在、規制およびコンプライアンス領域のアドバイザリー業務を金融機関等に提供するほか、テクノロジー活用によるコンプライアンス業務変革関連サービスを主導している。

メールアドレス：hideki.h.takeuchi@pwc.com

安嶋 建（あじま たつる）

PwC Japan有限責任監査法人 ガバナンス・リスク・コンプライアンス・アドバイザリー部 マネージャー

金融系シンクタンク、大学（教員）、ITベンダー系戦略コンサルティングファーム、監査法人系コンサルティングファームを経て、2022年9月に入所。現在は主として金融機関向け規制対応支援業務を担当。博士（法学）Ph.D. in Law.

メールアドレス：tatsuru.ajima@pwc.com

暗号資産取引規制におけるブロックチェーンに対する攻撃の位置付けと想定される対応事項

PwC Japan有限責任監査法人
ガバナンス・リスク・コンプライアンス・
アドバイザリー部
パートナー 竹内 秀輝



PwC Japan有限責任監査法人
ガバナンス・リスク・コンプライアンス・
アドバイザリー部
マネージャー 安嶋 建



はじめに

ブロックチェーンは暗号資産の技術的基盤として用いられており、ブロックチェーンに対する攻撃は暗号資産の価格形成や暗号資産取引の公正性を害する行為として、暗号資産市場に重大な影響を与える可能性があります。

2017年に暗号資産に関する規制が資金決済法に追加されて以降、ブロックチェーンに対する攻撃は暗号資産交換業者等が管理する利用者資産の安全性や業務の適正性を脅かすものと位置付けられ、主として暗号資産交換業者（暗号資産取引所および暗号資産販売所）におけるリスク管理の対象として扱われてきました^{※1}。

その後、2026年7月23日には「金融商品取引法及び資金決済に関する法律の一部を改正する法律」が公布され^{※2}、暗号資産の取引に適用される規制内容は資金決済法から金融商品取引法に移管されることになりました。また、併せて、従来「暗号資産交換業」^{※3}と位置付けられてきた、暗号資産の売買または他の暗号資産との交換等の業務は特定暗号資産の引受け等の業務とともに「暗号資産取引業」^{※4}へと位置付けが変わり、これを行う事業者は「暗号資産交換業者」^{※5}から「金融商品取引業者」^{※6}へと位

置付けが変更され、より広範な規制が適用されることとなりました。

さらに、暗号資産に係る不公正取引規制の導入は、ブロックチェーンに対する攻撃が不公正取引の問題にもなり得ることを示しています。このような状況において、暗号資産取引業を行う金融商品取引業者が犯罪と評価され得る行為に対して適切な対応を行わないことは、規制上求められる態勢整備上の問題のみならず、レピュテーションの深刻な悪化にもつながりかねません。

本稿では、日本において今般導入された暗号資産に係る不公正取引規制を前提として、ブロックチェーンに対する攻撃の法規制上の扱いを整理するとともに、PwCによる支援の経験を踏まえて暗号資産取引業を行う金融商品取引業者において求められる実務対応を示します。

なお、文中の意見は筆者の私見であり、PwC Japan有限責任監査法人および所属部門の正式見解ではないことをお断りしておきます。

1 ブロックチェーンが攻撃される背景

本稿で想定している「ブロックチェーンに対する攻撃」とは、暗号資産の記録、承認、移転の基盤となる分散型台帳またはその周辺インフラに対して、不正または不当な影響を与える行為を指します。

これに該当する行為の例として以下のものが挙げられます。

※1 資金決済法63条の10参照。

※2 以下に示す金融商品取引法上の規定内容および条文番号は、本法による改正後のものです。なお、改正後の金融商品取引法の規定については以下を参照。
<https://www.sangiin.go.jp/japanese/joho1/kousei/gian/221/meisai/m221080221057.htm>

※3 資金決済法2条15項。

※4 金融商品取引法28条5項、同法2条8項18号から25号まで。

※5 資金決済法2条16項、同法63条の2。

※6 金融商品取引法2条9号、同法29条。

- **51% 攻撃**：攻撃者がブロックチェーンのコンセンサス形成能力（例：計算能力やステーク量）の過半数を支配し、取引の承認・拒否やチェーンの書き換えを行う攻撃
- **二重支払を目的とするチェーン再編成の誘発**：攻撃者が秘密裏に別のチェーンを構築し、後から正規チェーンに置き換えることで、既に使用した暗号資産を再び利用可能にする攻撃
- **コンセンサス形成の妨害**：ネットワークの正常な運営を妨げることを目的として、ノード間の合意形成プロセスを阻害し、取引の確定やブロック生成を遅延・停止させる攻撃
- **ノード間通信の阻害**：ネットワークの正常な運営を妨げることを目的として、ノード同士の通信を妨害・遮断し、ネットワークの同期や取引・ブロック情報の伝播を妨げる攻撃
- **大量トランザクション送信によるネットワーク混雑の誘発**：大量の取引を送信してネットワーク資源を消費させ、取引処理の遅延や手数料の高騰を引き起こす攻撃
- **スマートコントラクト、ブリッジ、オラクル等への攻撃**：コードの脆弱性や外部データ連携機能を悪用し、資産の不正取得、価格操作、誤作動を引き起こす攻撃

2 ブロックチェーンに対する攻撃の法規制上の位置付け

(1) ブロックチェーンに対する攻撃の評価

不公正取引と評価されるブロックチェーンに対する攻撃について、暗号資産取引業を行う金融商品取引業者が適切な対応を行わない場合、レピュテーションの深刻な悪化が懸念されます。もっとも、ブロックチェーンに対する攻撃は、それ自体が一律に独立した不公正取引の類型として明示されているわけではありません。したがって、その規制上の評価は、攻撃の態様、目的、価格形成への影響、関連売買の有無等を踏まえ、関連する金融商品取引法上の概念に照らして判断されることになる想定されます。

なお、2026年9月時点においては改正後の金融商品取引法の不公正取引関連の規定は施行されておらず、裁判所による判例や監督官庁による公定解釈も示されていないことから、以下では規制上の文言に照らした一般論を示すにとどめます。

(2) 金融商品取引法上の各禁止行為への該当性

金融商品取引法上の禁止行為として、「暗号等資産の売買〔略〕その他の取引又はデリバティブ取引等〔略〕について、不正の手段、計画又は技巧をすること」（金融商品取引法171条の3第1項）が示されています。このうち「不正の手段」はブロックチェーンに対する攻撃に関連する余地があると考えられます。「不正の手段」という文言からはどのような行為が禁止されているかが必ずしも明確に読み取れるわけではないものの、同様の禁止規定^{※7}が設けられている有価証券の取引に関する判例においては、『不正の手段』とは、有価証券の取引に限定して、それに関し、社会通念上不正と認められる一切の手段をいう^{※8}として、もっぱら社会通念によって禁止行為への該当の有無が判断されています。仮に同様の判断が暗号資産に関する不公正取引規制においても下されるのであれば、社会通念上、ブロックチェーンに対する攻撃が暗号資産の取引に関して不正と認められる手段と評価される限り、本規定による禁止の対象と評価され得ると考えられます。

このほか、ブロックチェーンに対する攻撃が、それを取り巻く事情によって、「偽計」（金融商品取引法171条の4）等の各種概念に該当するか否かについては、今後の判断の蓄積が期待されます。

3 暗号資産取引業を行う金融商品取引業者に求められる実務対応

(1) 管理態勢の整備

ブロックチェーンに対する攻撃に起因するリスクに対処するためには、まず管理態勢の整備が求められます。

求められる対応の例として、①ブロックチェーンに対する攻撃に起因する不公正取引の発生リスクをリスク管理規程に明記すること、②システムリスク管理部門と市場監視部門との情報連携プロセスを明確化すること、③重大事案に係るエスカレーションルールを整備すること、④経営レベルでの報告・意思決定体制を明確化することが挙げられます。

(2) 取扱暗号資産の審査・評価

暗号資産は、その技術的なセキュリティ構造やネットワークの規模が多様であり、ブロックチェーンに対する攻

※7 金融商品取引法157条1項及びその前身となった証券取引法58条1号。

※8 最判昭和40年5月25日集判155号831頁。

撃のリスクは暗号資産の銘柄ごとに大きく異なることから、取扱暗号資産について適切な審査・評価を行うことも重要です。

求められる対応として、①新規取扱審査項目にブロックチェーンに対する攻撃への耐性を含めること、②既存取扱銘柄について定期的な再評価を実施すること、③海外での攻撃事例、取引停止事例、チェーン再編成履歴等を継続的に把握すること、④銘柄ごとに危機発生時の対応方針および施策を定めることが挙げられます。

(3) 市場監視およびオンチェーン監視の高度化

市場監視およびオンチェーン監視の高度化を図ることも有効です。

求められる対応の例として、①市場アラート（例：価格急変、出来高急増、スプレッド拡大）やオンチェーンアラート（例：承認遅延、ブロック停止、チェーン再編成、

大口移転）を設定すること、②市場データとオンチェーンデータの相関分析を実施すること、③疑義の生じた口座と外部ウォレットの関係把握に向けた分析手法を整備することが挙げられます。

4 おわりに

暗号資産市場における攻撃類型は多様であり、現時点では過去事例の蓄積も十分とはいえません。事業者においては、ブロックチェーンに対する攻撃をサイバーセキュリティ上の問題としてのみ取り扱うのではなく、総合的なリスク管理の対象と位置付けた上で対応を進めることが重要です。今後、暗号資産市場における実務の高度化が進む中で、こうした統合的な管理態勢の整備は、事業の継続や市場の信頼性の確保の観点から一層重要になるものと考えられます。

竹内 秀輝（たけうち ひでき）

PwC Japan 有限責任監査法人 ガバナンス・リスク・コンプライアンス・アドバイザリー部 パートナー

監査法人で保険会社に対する監査業務および各種アドバイザリー業務を幅広く経験した後、2011年から2014年にかけて、金融庁監督局保険課および総務企画局総務課国際室で勤務。金融庁在籍期間中は、保険監督者国際機構（IAIS）のメンバーとして国際保険規制に関する検討に携わった他、国内外の監督カレッジへの参画を通じたクロスボーダーでの監督にも従事。現在、規制およびコンプライアンス領域のアドバイザリー業務を金融機関等に提供するほか、テクノロジー活用によるコンプライアンス業務変革関連サービスを主導している。

メールアドレス：hideki.h.takeuchi@pwc.com

安嶋 建（あじま たつる）

PwC Japan 有限責任監査法人 ガバナンス・リスク・コンプライアンス・アドバイザリー部 マネージャー

金融系シンクタンク、大学（教員）、ITベンダー系戦略コンサルティングファーム、監査法人系コンサルティングファームを経て、2022年9月に入所。現在は主として金融機関向け規制対応支援業務を担当。博士（法学）Ph.D. in Law.

メールアドレス：tatsuru.ajima@pwc.com

ブロックチェーンビジネスにおいて求められる サイバーレジリエンスの構築

PwC Japan有限責任監査法人
リスク・アシュアランス部
パートナー 須田 真由



PwC Japan有限責任監査法人
リスク・アシュアランス部
マネージャー 望月 夕衣



はじめに

暗号資産をはじめとするブロックチェーン関連サービスは、投資・決済・資産保全を支える金融インフラとしての存在感を高めています。一方で、暗号資産はインターネット上で移転可能な財産的価値であり、攻撃が成功した場合には短時間での資産流出に直結し得るという特性があります。近年では、署名鍵の盗難にとどまらず、ソーシャルエンジニアリング、外部委託先への侵入、サプライチェーンを介した攻撃など、ブロックチェーン関連事業者を取り巻く脅威は一層高度化・複雑化しています。

加えて、生成AIをはじめとするフロンティアAIの進展は、攻撃者の能力を押し上げる可能性があります。脆弱性探索、攻撃経路の特定、フィッシングの高度化、マルウェア開発支援などが低コスト化・高速化することで、従来以上に迅速かつ実効性のあるサイバーリスク管理が求められます。

本稿では、改正金融商品取引法、フロンティアAIへの対応、経営陣の関与、リスクベースアプローチ、暗号資産業界特有の留意点の5つの観点から、ブロックチェーン関連事業者求められるサイバーレジリエンスの再構築について考察します。

なお、文中の意見は筆者の私見であり、PwC Japan有限責任監査法人および所属部門の正式見解ではないことをお断りしておきます。

1 拡大する暗号資産関連のビジネス領域とリスク

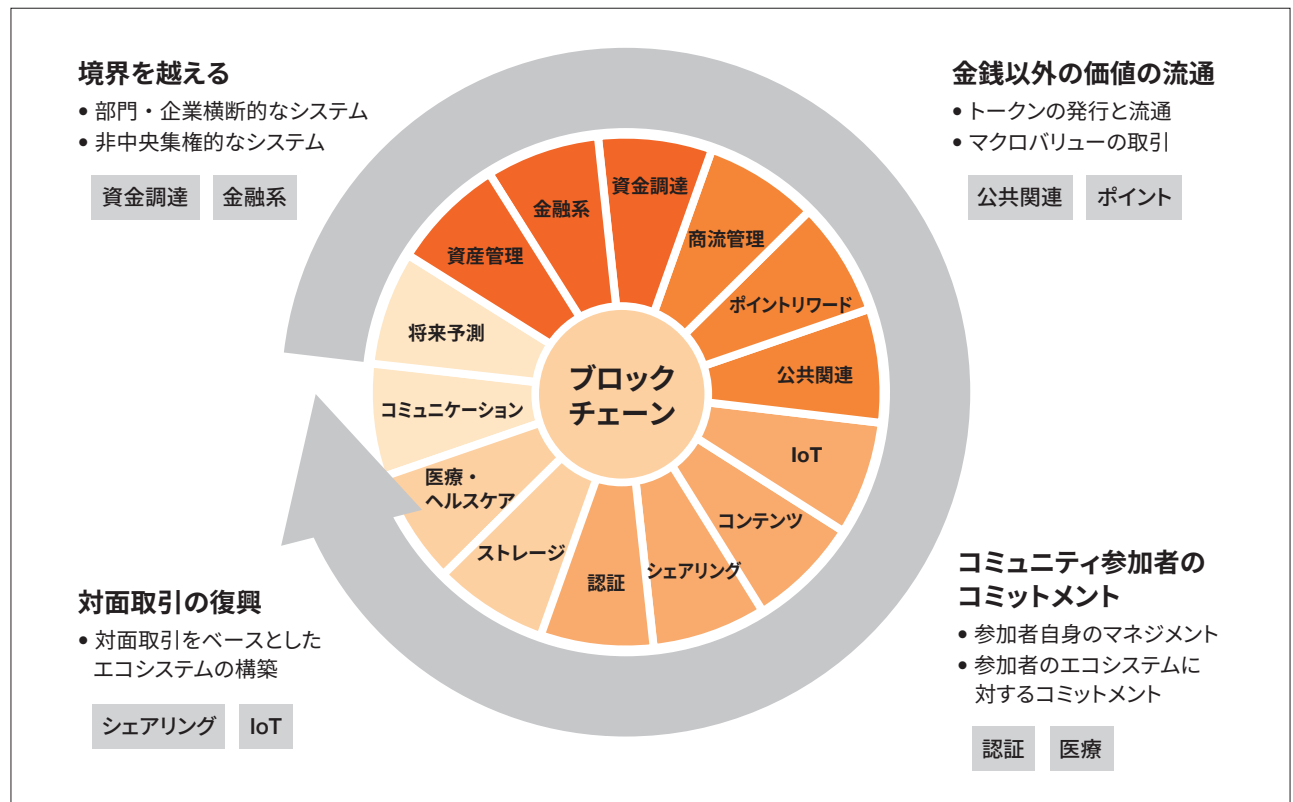
暗号資産をはじめとするブロックチェーン関連サービスは、ブロックチェーン技術を基盤とする新たな金融サービスとして発展してきました。近年では、暗号資産そのものに加え、トークン化、カストディ、DeFi（分散型金融）、ステーブルコイン、決済、投資商品など、関連するビジネス領域が広がっています（図表1）。こうした市場の拡大は、利用者の利便性や金融イノベーションの可能性を高める一方で、事業者には利用者資産の保護、市場の信頼確保、事業継続の観点から、より高度なリスク管理が求められることを意味します。

特に、暗号資産の移転には不可逆性があるため、ひとたび不正送金が発生すると、金融機関における一般的な不正送金以上に事後的な回復が困難となるおそれがあります。そのため、暗号資産事業者におけるサイバーセキュリティは、単なるIT管理やシステム部門の課題ではなく、利用者保護、規制対応、経営戦略、企業価値に直結する経営課題として位置付ける必要があります。サイバー対策を、規制対応のためにチェックリスト的に文字通り対応するのではなく、経営として優先順位を付けて設計・運用すべきサイバーレジリエンスの課題として捉えるべきです。

2 規制対応を超えて問われる、暗号資産ビジネスの統制力

2026年7月に改正金融商品取引法（改正金商法）が成立しました。改正金商法への対応として、暗号資産関連サービス事業者は、業務管理態勢、内部管理態勢、コンプライアンス、リスク管理、サイバーセキュリティを一体として設計することがより重要となります。

図表1：ブロックチェーンの活用領域



出所：PwC作成

特に暗号資産関連サービス事業者は、中央集権的な運用主体と分散型基盤の双方のリスクを併せ持ちます。ブロックチェーンは透明性や耐改ざん性を備える一方で、実際のサービス提供では、取引所、カストディアン、ウォレット、フロントエンド、クラウド、API、外部委託先といったオフチェーン要素に大きく依存しています。

したがって、改正金商法対応においては、オンチェーンのコードやプロトコルだけでなく、オフチェーンの運用統制、外部依存関係、アクセス管理、署名プロセス、ガバナンス、インシデント対応、利用者保護を含めた包括的な統制基盤としてサイバー対策を設計する必要があります。

また、規制対応を進めるにあたっては、サイバーセキュリティを「個別規制への適合項目」として扱うだけでは不十分です。重要なのは、利用者資産の保護、重要業務の継続、重大インシデント時の意思決定、外部委託先を含むサプライチェーン管理といった経営上の論点と結び付け、実効性のある管理態勢として具体化することです。

3 フロンティアAIが変える、サイバー攻撃の速度と精度

生成AIをはじめとするフロンティアAIの進展により、

攻撃者は従来よりも低いコストで高度な攻撃能力を獲得できるようになっています。脆弱性探索の自動化、攻撃経路の特定、フィッシングメールの高度化、なりすまし、マルウェア開発支援、標的型攻撃の大規模化など、脅威環境は急速に変化しています。

暗号資産業界では、この影響が特に大きいと考えられます。攻撃が成功した場合、短時間で直接的な資産流出につながる可能性があるためです。特に、署名鍵、ウォレット、アクセス制御、CI/CD（ソフトウェア変更の自動化）、クラウドIAM/KMS（権限管理／鍵管理）、署名サービス等の運用インフラは、攻撃者にとって高い投資対効果を持つ標的となり得ます。

また、攻撃者は「侵入する」だけでなく、認証情報、セッショントークン、フェデレーションアクセスを悪用して「ログインする」傾向を強めています。人間のアイデンティティだけでなく、サービスアカウント、APIキー、CI/CDパイプライン、クラウド権限、署名権限といった非人間アイデンティティを含めた管理が不可欠です。

フロンティアAI時代のサイバー対策では、従来型の境界防御だけではなく、侵害を前提とした検知・封じ込め・復旧能力が重要になります。加えて、AIを悪用した攻撃

の高速化に対応するためには、ログ監視、アラート対応、脅威インテリジェンス、演習、レッドチーム、外部評価などを組み合わせ、組織として継続的に防御能力を検証することが求められます。

4 サイバーリスクを経営のトップアジェンダに引き上げる

改正金商法対応とフロンティアAIへの対応は、いずれも暗号資産関連サービス事業者におけるサイバー対策の重要性を高めています。サイバーインシデントが発生した場合、利用者資産、事業継続、市場の信頼に直ちに影響が及ぶ可能性があるため、サイバーリスクはIT部門だけの管理課題ではなく、経営として優先的に管理すべきトップリスクのひとつとして位置付ける必要があります。

前述したように、暗号資産の移転には不可逆性があるため、ひとたび不正送金が発生すると、事後的な回復が困難となるおそれがあります。そのため、経営陣は重要資産、重要業務、重要委託先、重大インシデントシナリオを把握したうえで、予防、検知、停止、復旧を含む多層的な管理態勢を整備する必要があります。

また、経営陣の関与は、単に方針を承認することだけにとどまりません。リスクアパタイト、投資優先順位、KRI（重要リスク指標）、報告ライン、インシデント時の意思決定プロセスを明確にし、第1線、第2線、第3線が連携してサイバーリスクを継続的に管理する態勢を整えることが重要です。

特に暗号資産関連サービス事業者では、専門性の高い技術領域と、経営判断を要するリスク領域が密接に結び付いています。たとえば、ウォレット構成、署名方式、クラウド権限、委託先の運用、スマートコントラクトのアップグレード権限、緊急停止手続きなどは、技術的な論点であると同時に、利用者資産の保全や事業継続に直結する経営判断でもあります。

5 ガイドラインを出発点に、実効性あるリスク管理へ

現在、当局や関係機関から各種ガイドラインや指針が公表されています。これらは、金融機関に求められる管理態勢を整理するうえで役に立ちます。一方で、暗号資産関連サービス事業者が留意すべきなのは、ガイドラインをチェックリストとして機械的に充足するだけでは、実効的なセキュリティ態勢につながるとは限らないという点です。

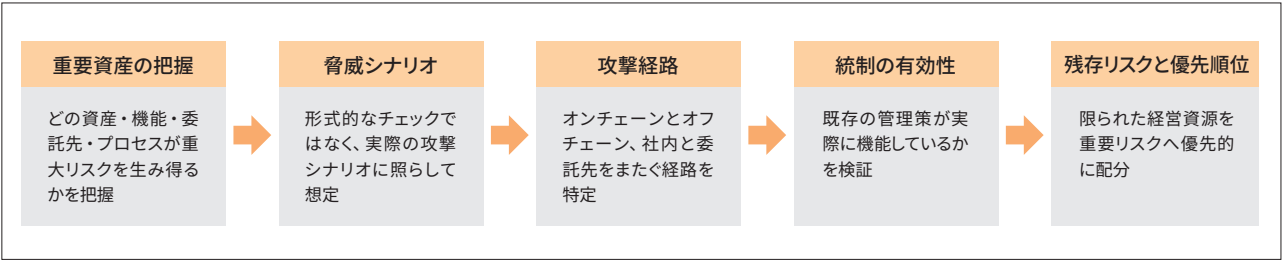
既存のガイドラインには、暗号資産関連サービス事業者における主要な脆弱性に対応する項目も含まれています。しかし、実際の管理策は、自社のシステム構成、委託関係、ウォレット・鍵管理方式、DeFiや外部サービスの利用状況に応じて具体化し、必要に応じて深掘りすることが求められます。

たとえば、同じ「アクセス管理」であっても、一般的な社内システムのID管理と、出庫承認、署名権限、MPC（マルチパーティ計算）運用、クラウドKMS、スマートコントラクトのアップグレード権限、CI/CD環境への本番反映権限では、リスクの性質も管理すべき統制も異なります。

ガイドラインは到達点ではなく出発点です。重要なのは、ガイドラインの各項目を文字通りに充足することそのものではありません。自社にとって、どの資産、機能、委託先、プロセスが重大なリスクを生み得るのかを把握し、限られた経営資源を重要リスクに優先配分することです。

そのためには、重要資産・重要業務を起点に、脅威シナリオ、攻撃経路、統制の有効性、残存リスクと優先順位を明確化する必要があります（図表2）。特に暗号資産関連サービス事業者では、オンチェーンとオフチェーン、技術と運用、社内と委託先が複雑に結び付くため、形式的なチェックよりも、実際の攻撃シナリオに照らしたリスク評価が重要になります。

図表2：重要資産・重要業務を起点としたリスク評価の流れ



出所：PwC作成

6 暗号資産固有の攻撃シナリオにどう備えるか

暗号資産業界では、一般的な金融機関と共通するサイバーリスクに加え、業界特有のリスクを踏まえた対策が必要です。特に、**図表3**に挙げた領域については、自社の事業モデルやシステム構成に即して優先的に確認することが重要です。

(1) 委託先は「外部」ではなくリスクの一部として管理する

暗号資産関連サービス事業者は、出庫、署名、鍵管理、ウォレット運用、CI/CD、クラウド基盤、監視、KYC/AML（顧客確認／マネー・ローンダリング防止）など、多数の重要業務を外部サービスに依存しています。そのため、委託先管理では、契約上のセキュリティ条項を確認するだけでは十分ではありません。

委託先のシステム構造、管理体制、アクセス権限、再委託関係、ログ監視、インシデント対応、プログラム変更管理、特権ID管理、要員管理、復旧能力を確認し、自社のリスク管理上不足する部分を補完することが重要です。

また、委託先の侵害が自社サービスや利用者資産に波及することを前提に、追加承認、利用上限、異常検知、自動停止、代替手段、緊急時連絡体制などをあらかじめ整備する必要があります。

(2) 正規の開発・運用プロセスが攻撃経路になり得る

暗号資産サービスでは、UI、API、CI/CD、スマートコントラクト、署名前トランザクション生成ロジック、本番環境プログラムが攻撃対象となり得ます。そのため、開発環境と本番環境の分離、コードレビュー、変更承認、署名

付きビルド、SBOM（ソフトウェア部品表）管理、脆弱性管理、リリース前検証、CI/CD権限管理、緊急変更の統制、開発者端末の保護を一体として設計する必要があります。

特に、正規の署名者が悪意あるトランザクションを承認してしまうリスクを踏まえると、署名前の内容検証、送金先アドレスの検証、異常な出庫パターンの検知、追加承認、自動停止、利用上限の設定が重要です。

(3) 不正送金を「起こさせない・止める」仕組みを設計する

暗号資産の不正送金は、発生後の回復が困難です。そのため、事前の防止と即時検知が重要となります。ホットウォレットとコールドウォレットの分離、出庫上限、複数者承認、MPCやHSM（ハードウェア・セキュリティ・モジュール）の適切な利用、承認者の職務分離、送金先アドレスのホワイトリスト管理、異常検知、オンチェーン分析、トランザクションモニタリング、緊急停止手続、インシデント時の連絡・封じ込め手順を整備することが求められます。

また、出庫プロセスでは、技術的統制だけでなく、オペレーション統制も重要です。画面表示、エラーメッセージ、例外処理、承認手順、担当者教育、複数名確認など、人的ミスや不審事象の見落としを防ぐ設計が必要です。

(4) スマートコントラクトとDeFiのリスクを運用レベルで捉える

DeFiやスマートコントラクトを利用する場合、従来型のシステム管理だけではリスクを十分に捉えきれません。スマートコントラクトの脆弱性、アップグレード権限、管理者権限、フラッシュローン攻撃、流動性リスク、ガバナ

図表3：暗号資産固有の攻撃シナリオへの5つの備え

1	2	3	4	5
委託先管理	開発・運用プロセス	不正送金の防止と停止	スマートコントラクト・DeFi	外部評価と脅威情報
委託先を「外部」ではなくリスクの一部として管理。再委託・特権ID・復旧能力まで確認し、自動停止や代替手段を事前整備。	UI・API・CI/CD・本番環境が攻撃経路になり得る。環境分離、変更承認、権限管理、署名前の内容検証を一体で設計。	ホット／コールド分離、出庫上限、複数者承認、MPC・HSM、ホワイトリスト、異常検知、緊急停止手続。	スマートコントラクトの脆弱性、ブリッジ等の固有リスクを評価。外部監査は範囲と時点を継続確認。	TLPT、レッドチーム、机上演習、第三者評価を組み合わせ、結果を経営報告・投資判断・改善計画へつなげる。

出所：PwC作成

ンス攻撃、プロトコル連携リスク、ブリッジリスクなど、暗号資産特有のリスクを評価する必要があります。

その際、外部監査を実施していることだけで安心するのではなく、監査範囲、監査時点、除外範囲、是正状況、運用変更後の再評価、依存プロトコルの変化などを継続的に確認することが重要です。

(5) 外部評価と脅威情報で、自社の実力を継続的に検証する

攻撃手法が高度化する中では、自社による点検だけでなく、外部評価や脅威インテリジェンスの活用が重要です。脅威ベースのパネトレーションテスト、レッドチーム演習、机上演習、インシデント対応訓練、第三者評価、クラウド設定診断、スマートコントラクト監査、ブロックチェーン分析、脅威情報共有機関からの情報収集を組み合わせることで、組織の実効的な防御・検知・対応能力を確認できます。

また、評価結果は単なる報告書として扱うのではなく、経営報告、改善計画、投資判断、KRI、訓練シナリオ、委託先管理の見直しにつなげることが重要です。

7 おわりに

改正金商法への対応とフロンティアAIの進展は、暗号資産関連サービス事業者に対して、サイバーリスクをトップリスクとして捉え、経営陣が強く関与することの重要性を示しています。

そのうえで求められるのは、ガイドラインへの形式的な適合にとどまらない対応です。自社のビジネスモデル、システム構成、委託関係、ウォレット・鍵管理方式、DeFiや外部サービスの利用状況を踏まえ、リスクベースで対策を具体化し、継続的に見直していくことが不可欠です。

特に暗号資産業界では、委託先管理、開発・運用プロセス、不正送金防止、スマートコントラクト・DeFi、外部評価と脅威情報の活用といった固有の論点を踏まえて、実効的なサイバー対策を設計する必要があります。

サイバーセキュリティは、もはや規制対応のためのコストではありません。暗号資産関連サービス事業者が社会的信頼を獲得し、金融インフラとして持続的に成長するための競争力そのものとして位置付けられるべきです。

須田 真由 (すだ まさよし)

PwC Japan 有限責任監査法人 リスク・アシュアランス部 パートナー
製造業、情報通信業および金融業（資金決済・暗号資産）を中心とした、IT領域において財務諸表監査、ならびに国内上場企業の内部統制監査を担当。また、米国証券取引委員会（SEC）登録日本企業、外資系企業の米国企業改革法に基づく内部統制監査業務にも従事。アドバイザー業務としては、財務報告に係るIT統制の構築および評価支援やフィンテックに関連するITガバナンス構築支援業務をリード。ブロックチェーン技術のセキュリティおよびガバナンスに関する講演も多数実施。

メールアドレス：masayoshi.suda@pwc.com

望月 夕衣 (もちづき ゆい)

PwC Japan 有限責任監査法人 リスク・アシュアランス部 マネージャー
証券会社での個人向け営業、金融機関向けシステム会社での開発・導入・管理フロー構築、外資系コンサルティングファームでのシステム監査やITガバナンス構築経験を経て2019年5月より現職。金融機関向けサイバーセキュリティ評価（NIST CSF、FFIEC CAT、CRI Profile、当局監督指針に基づく態勢評価、シナリオベースでのサイバー脅威に対する態勢評価〔技術的観点を含む〕など）やクラウドセキュリティ評価の経験を有する。その他、フィンテックに関連する内部監査支援、セキュリティ体制構築支援、法令対応支援等の各種支援提供実績を有する。また、各種金融機関を中心とする監査において、J-SOXのIT全般統制やIT業務処理統制等のITシステムを対象とする領域を担当。

メールアドレス：yui.mochizuki@pwc.com

AI・ブロックチェーン時代のデータトラスト

——暗号資産関連ビジネスに求められるガバナンスと説明責任

PwC Japan有限責任監査法人
リスク・アシュアランス部
パートナー 須田 真由



PwC Japan有限責任監査法人
リスク・アシュアランス部
マネージャー 望月 夕衣



はじめに

ブロックチェーンの登場以降、暗号資産やNFT（非代替性トークン）の社会実装が進んでいます。さらに、決済、証券化、ID管理、サプライチェーン、トレーサビリティなど、幅広い領域へ活用範囲を広げています。また、生成AIをはじめとするAI技術の進展により、ブロックチェーン上の取引データ（オンチェーンデータ）やオフチェーンデータを、業務判断、リスク管理、顧客対応、内部統制に活用する動きも現実味を帯びてきました。

その一方で、ブロックチェーンが持つ改ざん耐性や追跡可能性は、ビジネス全体の信頼性を自動的に保証するものではありません。記録されたデータが改ざんされにくいとしても、入力されたデータが正確であるか、適切な同意や利用条件に基づいているか、法令・規約に沿ってAIに利用できるかは、別途検証する必要があります。誤ったデータが記録された場合は、その誤りが改ざん困難な形で残り続けるというリスクもあります。

AI・ブロックチェーン時代に問われるのは、技術を導入しているという事実そのものではなく、金銭・商品・権利・同意・利用条件といったデータの流れを、事業者がどのように管理し、どのような証拠に基づいて外部に説明できるかです。本稿では、このような信頼性に関わる概念を「データトラスト」と捉え、暗号資産関連ビジネスにおけるAIガバナンスのあり方を、データガバナンス、統制の自動化、説明責任の観点から整理します。

なお、本稿では、ブロックチェーン固有のセキュリティ、ウォレット・鍵管理、外部委託先管理、内部

統制に関する論点を、データトラストを支える実務上の要素として扱います。個別の技術対策を網羅するのではなく、市場・利用者・規制当局から信頼を獲得するための経営基盤としてデータトラストをどのように実装するかに焦点を当てます。

なお、文中の意見は筆者の私見であり、PwC Japan有限責任監査法人および所属部門の正式見解ではないことをお断りしておきます。

1 データトラストが重要となる背景

ブロックチェーンは、暗号資産やNFTに代表される価値移転の基盤として注目されてきました。その後、資金調達、決済、商流管理、公共サービス、認証、医療、IoT、コンテンツ、シェアリング、コミュニティ運営など、活用領域は着実に広がっています。すなわち、ブロックチェーンは、金銭の移転に限らず、権利、参加、同意、証明といった多様なデータを流通させる社会基盤になりつつあります。

その際、重要となるのがデータそのものの信頼性です。ブロックチェーンは、記録されたデータの改ざんを困難にし、取引履歴を追跡しやすくします。しかし、入力データの正確性、利用条件との整合性、同意の有無、鮮度、来歴までは自動的に保証しません。ブロックチェーンは記録後の改ざん防止に強みを発揮する一方で、事業者は記録前後の業務プロセスやデータ利用の妥当性を別途担保しなければなりません。

暗号資産交換業者、NFT発行・管理事業者、ブロックチェーンを用いたトレーサビリティ事業者にとっては、利用者や市場に対し、「この取引データは信頼できる」「この

NFTの発行・移転プロセスは適切である」「このデータは利用規約や法令に沿ってAIに投入されている」と説明できることが競争力となります。AIを活用する場合には、オンチェーンデータ、オフチェーンデータ、顧客データ、委託先データ、外部データが組み合わせられるため、データの来歴、利用条件、品質、アクセス権限、証跡を一体として管理する必要性がさらに高まります。

したがって、AI・ブロックチェーン時代における信頼は、技術の性質に依存して自然に生じるものではありません。事業者がデータの流れを説明可能な形で管理し、必要に応じて外部に示せる状態を整えることが、事業継続と成長の前提となります。

2 データトラストを支えるデータガバナンス

データトラストを支える基盤は、データを「正しく・速く・信頼して」利用できる状態に整えることです。データが散在し、定義が曖昧で、品質が確認できず、アクセス権限や利用条件が管理されていない場合、どれほど高度なAIやブロックチェーンを導入しても、信頼できるサービスや意思決定にはつながりません。

データガバナンスは、単にデータ管理のルールを整備する取り組みではありません。企業のビジョンやビジネスニーズを起点に、ガバナンス体制、業務プロセス、ITイン

フラを一体として整備し、データを意思決定やサービス提供に活用できる状態にするための経営基盤です。言い換えれば、データガバナンスは、AI時代における意思決定の質と速度を左右する仕組みです。

AI Readyなデータ基盤を構築するには、少なくとも5つの要素を統合的に整備する必要があります（図表1）。第1に、AI倫理、アクセス権限、ビジネスKPIとの連携を含むデータガバナンスです。第2に、リアルタイム監視、異常検知、データクリーニングなどにより信頼性を継続的に担保するデータ品質です。第3に、API連携、クラウドネイティブな設計、データレイクハウスなど、事業成長に追隨できるデータアーキテクチャです。

第4に、ビジネス要件を共通言語として定義し、組織横断でデータを理解できる状態をつくるデータモデリングです。第5に、データの来歴、意味、利用条件、AIトレーニングデータとしての適格性を可視化するメタデータ管理です。これらを個別施策としてではなく、事業戦略と統制をつなぐ一体的な仕組みとして設計することが、データトラストの土台となります。

3 ブロックチェーンの価値を活かすための統制設計

ブロックチェーンの価値は、記録の改ざん耐性や追跡可能性にとどまりません。部門・企業を横断するシステ

図表1：データマネジメントの5つの柱



出所：PwC作成

ム、非中央集権的なエコシステム、トークンの発行と流通、参加者のコミットメント、ID管理、証明、商流管理など、多様なステークホルダーが同じ基盤を参照しながら価値をやり取りできる点にあります。

一方で、ブロックチェーンの技術的特性を過信すべきではありません。ブロックチェーンのタイプによって、関係者の範囲や責任分界は大きく異なります。誰でも参加できるパブリックチェーンでは、個社でガバナンスを整備できる範囲に限界があります。複数の企業・組織が共同で運営するコンソーシアムチェーンでは、参加者間で一定の管理水準を共有する必要があります。プライベートチェーンでは個社の統制が重要になりますが、分散性や耐改ざん性の強みが十分に発揮されない場合もあります。

さらに、業務システムに係るリスクも看過できません。取引管理システム、ウォレット管理システム、鍵管理システム、データを取得・加工する仕組みに不備があれば、オンチェーン上の記録が形式的に正しくても、入力データの誤り、不正な署名、権限管理の不備、委託先の障害や不正を通じて、利用者保護や事業継続に重大な影響が生じます。ブロックチェーンの価値を活かすには、オンチェーンとオフチェーンを分断せず、データ全体の信頼性を設計する必要があります。

4 データトラストの実践に向けたアプローチ

データトラストを実践するには、まず、自社のビジネスにおいて重要なデータがどこで生成され、どのシステムで処理され、誰に利用され、どのような意思決定や外部説明に使われているかを可視化することが重要です。暗号資産関連ビジネスでは、オンチェーンデータとオフチェーンデータ、顧客情報、ウォレット・鍵管理情報、委託先から取得するデータ、価格情報、取引履歴、会計データが相互に関連します。これらを個別の管理対象としてではなく、一連のデータライフサイクルとして把握する必要があります。

次に、データライフサイクルの各段階において、どのようなリスクが存在し、どのような統制が必要になるかを整理します。例えば、データ生成時には入力データの正確性や同意取得状況、加工時にはデータ品質や変換ロジック、転送時にはアクセス権限や暗号化、AI利用時には利用目的との整合性や出力結果の検証が論点となります。これらの論点を、規程やマニュアルに記載するだけでなく、業務フロー、システム設定、ログ、承認記録、例外処

理記録と対応付けて管理することが実務上有効です。

また、データトラストの実装では、事後的に問題を発見するだけでは不十分です。データの取り込み、加工、転送、利活用の各段階で、継続的に確認できるモニタリングの仕組みを整えることが望めます。具体的には、データの来歴、同意、正確性、完全性、鮮度、改ざん対応、利用条件との整合性を確認し、例外が発生した場合には、データ利用の一時停止、再確認、隔離、再処理、関係部門へのエスカレーションにつなげることが考えられます。

さらに、3線モデルを踏まえて役割を明確化することも重要です。第1線の業務・IT部門は、データの利用目的、同意、分類、アクセス権限、保存期間などを業務ルールとして整理します。第2線のリスク管理・コンプライアンス部門は、規制要件、社内ポリシー、AIガイドライン、セキュリティ基準との整合性を確認し、統制の設計・運用状況を監督します。第3線の内部監査部門は、設定されたルール、実行ログ、承認記録、例外処理履歴を基に、統制が設計どおりに機能しているかを評価します。このように、データトラストは特定のツール導入ではなく、データ、業務、システム、統制、証跡を連動させる実務設計として捉えることが重要です。

5 AI活用を見据えた適切なデータ利用の説明力

AI活用においては、データには必ず利用条件があるという前提に立たなければなりません。ある顧客データは統計分析には利用できても、個別マーケティングには利用できないかもしれません。ある取引データはAML（マネー・ローンダリング防止）目的には利用できても、商品提案を行うAIには投入できないかもしれません。こうした利用条件をタグとして管理し、目的と合致するデータのみをAIへ投入することが重要です。

暗号資産関連ビジネスでは、顧客データ、取引データ、ウォレットアドレス、オンチェーン分析結果、外部データベンダーから取得する情報、SNSなどの非構造化データが、AI分析やリスク評価に利用され得ます。これらについて、同意取得状況、利用規約、法令上の制限、利用目的、保存期間、第三者提供の可否、AI学習への利用可否を管理しなければ、AIの出力が有用であっても、その利用自体を外部に説明できない状態になりかねません。

そのため、AIガバナンスの実装では、規程や原則を掲げるだけでなく、データの利用条件をメタデータとして管理し、AIへの投入、外部連携、分析環境への転送時に自

動的に照合・遮断できる仕組みに落とし込む必要があります。データパイプラインの設定値や動作ログを評価し、適切なデータ利用を証拠に基づいて説明できる状態を整えることで、法令・規約・同意に沿ったAI活用を外部に示すことができます。

この点は、AIを用いたAML/CFT（テロ資金供与対策）、不正検知、顧客対応、商品提案、取引モニタリング、内部統制評価のいずれにも共通します。AIは説明責任を代替するものではありません。むしろ、AIを利用するほど、どのデータを、どの目的で、どのような統制の下で利用し、どのようなログとレビューに基づいて判断したのかを説明する責任は増すことになります。

また、権限管理、ウォレット・鍵管理、外部委託先管理、サイバーセキュリティは、データトラストを支える不可欠な統制要素です。秘密鍵の流出は資産に対する支配の喪失を意味し、取引管理システムの不備は誤ったオンチェーン記録につながります。外部委託先との役割分担や監査権限が不明確であれば、自社のデータや統制の状況を十

分に説明できません。これらの論点は、AIガバナンスの周縁的な論点ではなく、データトラストを実効的に支える基礎的な管理領域と位置付けるべきです。

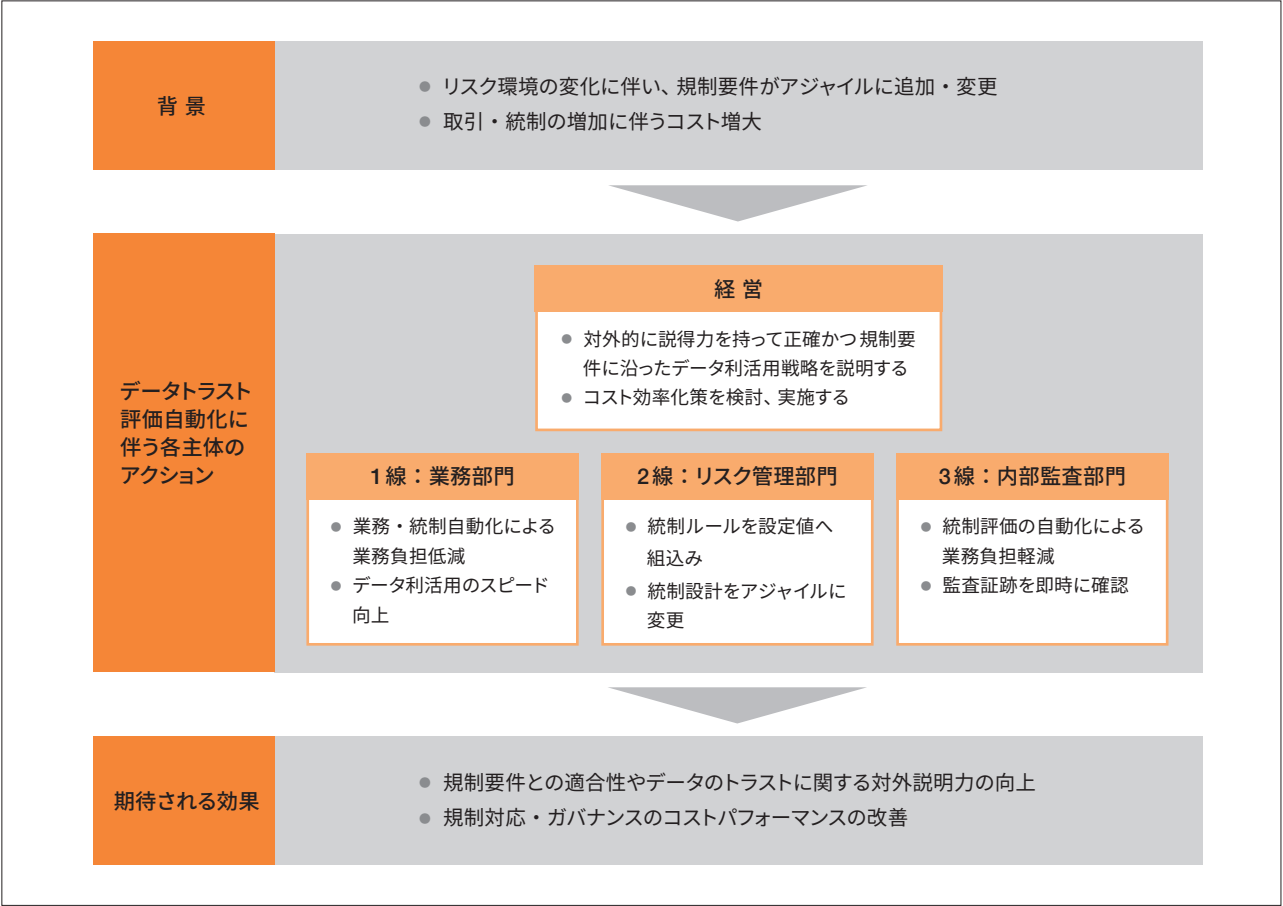
6

おわりに

データトラストは、規制対応やリスク管理のためだけの概念ではありません。暗号資産事業者やブロックチェーンビジネス事業者にとって、データトラストは、市場や利用者から信頼を得て、持続的にサービスを成長させるための競争力の源泉となります。ブロックチェーン上に記録されるデータ、ブロックチェーン外で生成・加工・利用されるデータ、AIに投入されるデータ。それら全体の信頼性を設計・管理し、説明できる企業は、規制環境の変化にも柔軟に対応しやすくなります。

そのためには、制度設計、技術実装、ユースケースに応じたアジャイルなガバナンス設計、アシュアランスに関する専門知見を組み合わせる必要があります。どのような

図表2：AI・ブロックチェーン時代におけるデータトラストの重要性



出所：PwC作成

リスクを想定し、どのような統制を設計し、どのような証拠に基づいて外部に説明するのか。この一連の仕組みを、ビジネス、技術、規制、保証の観点から統合して設計することが重要になります（図表2）。

AI・ブロックチェーン時代において、信頼は技術だけで獲得できるものではありません。事業者が、自社のデータ

の生成・保護・活用プロセスを把握し、利用条件に即したAI活用を行い、例外やリスクをタイムリーかつ客観的に検知し、必要に応じて制御し、その結果を外部に説明できることが求められます。暗号資産関連ビジネスにおけるAIガバナンスは、このデータトラストを実装するための経営基盤として捉えるべきです。

須田 真由（すだ まさよし）

PwC Japan 有限責任監査法人 リスク・アシュアランス部 パートナー
製造業、情報通信業および金融業（資金決済・暗号資産）を中心とした、IT領域において財務諸表監査、ならびに国内上場企業の内部統制監査を担当。また、米国証券取引委員会（SEC）登録日本企業、外資系企業の米国企業改革法に基づく内部統制監査業務にも従事。アドバイザー業務としては、財務報告に係るIT統制の構築および評価支援やフィンテックに関連するITガバナンス構築支援業務をリード。ブロックチェーン技術のセキュリティおよびガバナンスに関する講演も多数実施。

メールアドレス：masayoshi.suda@pwc.com

望月 夕衣（もちづき ゆい）

PwC Japan 有限責任監査法人 リスク・アシュアランス部 マネージャー
証券会社での個人向け営業、金融機関向けシステム会社での開発・導入・管理フロー構築、外資系コンサルティングファームでのシステム監査やITガバナンス構築経験を経て2019年5月より現職。金融機関向けサイバーセキュリティ評価（NIST CSF、FFIEC CAT、CRI Profile、当局監督指針に基づく態勢評価、シナリオベースでのサイバー脅威に対する態勢評価（技術的観点を含む）など）やクラウドセキュリティ評価の経験を有する。その他、フィンテックに関連する内部監査支援、セキュリティ体制構築支援、法令対応支援等の各種支援提供実績を有する。また、各種金融機関を中心とする監査において、J-SOXのIT全般統制やIT業務処理統制等のITシステムを対象とする領域を担当。

メールアドレス：yui.mochizuki@pwc.com

内部監査におけるAI活用と監査品質管理を考える

PwC Japan有限責任監査法人
ガバナンス・リスク・コンプライアンス
アドバイザリー部
パートナー 辻田 弘志



はじめに

生成AIをはじめとするAI技術は、内部監査の実務において、資料の要約、リスクシナリオの抽出、監査手続の検討、調書作成の補助など、幅広い場面で活用され始めています。

AIの活用は、単なる作業効率化にとどまらず、監査対象の網羅性を高め、分析の深度を増し、よりタイムリーな監査報告の実現、ひいては組織体全体に対する保証提供の実現につながる可能性を持っています。また、監査人の暗黙知を形式知化することによる監査品質の均質化も視野に入ります。そのため、内部監査部門はAIを避けるのではなく、適切な管理の下で積極的に活用する姿勢が求められます。

一方で、AIの出力は常に正確であるとは限りません。AIが誤った情報をもっともらしく生成したり、利用者がその回答を過度に信頼したりすることもあります。したがって、AI活用は「便利なツールの導入」ではなく、監査品質に影響を与える「監査プロセス、品質管理プロセスの変更・強化」として捉える必要があります。内部監査におけるAI管理は利用を過度に制限することではなく、監査リスクを適切に把握し品質を確保しながら活用を促進することにあります。

本稿では全社的なAIガバナンスの下でのAIツールの企画・開発・提供・保守・改廃などのライフサイクル管理や共通ルール（倫理的利用、情報の機密性管理等）を前提とし、監査上、留意すべきリスクと必要な統制について解説します。

なお、本稿の意見に関する部分は筆者の私見であり、PwC Japan有限責任監査法人および所属部の

正式見解ではないことを申し添えます。

1 AI活用を監査リスクの観点から捉える必要性

内部監査において、監査結果の誤りや重要なリスクの見落としは、経営判断や組織の信頼性に影響を及ぼします。AIを利用する場合、この監査リスクの考え方を意識する必要があります。従来は、「監査に誤りがあるてはならない」という考え方が強く、誤謬が発生した場合の対応や許容水準が明文化されていないことも少なくありません。AIの活用を契機として、どのような誤りを許容せず、どのような場面では人による確認でリスクを低減するのかを定義することが重要です。

内部監査部門として受け入れ可能なリスク水準（監査におけるリスクアペタイト）を考慮し、AIに委ねてよい作業と人が判断を担うべき領域を区別する必要があります。

特に重要な不備の評価、監査意見の形成、経営への提言についてはAIの出力をそのまま採用するのではなく、監査人が職業的懐疑心をもって検証し最終判断を行うことが不可欠です。

2 AI活用に伴うリスク

AI活用に伴うリスクは、大きく3つに整理できます。

1つ目は、「AIによるアウトプットのリスク」です。AIが生成する文章、分析結果、リスク評価、監査手続案には、誤情報、論理の飛躍、前提条件の欠落が含まれる可能性があります。根拠資料が限定的な場合や、専門的判断を要する場合には、AIの回答が一見整っていても、監査での利用に十分でないことがあります。また、監査リスクの

観点から、利用するAIが被監査部署と共有・共用されている場合、そのAIに共通する特性や限界によってリスクを見落とす可能性（監査部署が同一AIによって単に再実施をしているだけなど、監査の客観性の欠落やAIにおけるモデルリスクの内包）がないかも考慮してAI利用を検討する必要があります。AIによるアウトプットのリスクは、インプットデータ、AIへの指示、AI技術要因（パフォーマンス）の3つの観点から整理できます。

2つ目は、「監査人による誤用のリスク」です。監査人がAIの出力内容や前提を十分に理解せず、調書や報告書に反映してしまう場合、誤りが監査成果物に混入します。例えば、限定された範囲から導かれたアウトプットを全体に対するものと捉え、本来必要な追加手続きを省略してしまうなどが想定されます。また、AIの回答を過度に信頼する自動化バイアスにより、本来であれば疑問を持つべき事項を見逃す可能性もあります。AIの利用により、監査人の判断が強化される場合もあれば、反対に思考停止を招き、職業的懐疑心を弱める場合もあることを認識する必要があります。監査人による誤用のリスクはアウトプット自体の誤った解釈と監査手続の適用誤りの2つの観点で整理されます。

3つ目は、「監査基準や監査手法からの乖離のリスク」です。AIは内部監査人に求められる独立性・客観性、職業的懐疑心、証拠評価の考え方を自律的に担保できるものではありません。AIが提示した手続や結論が形式的には妥当に見えても、内部監査基準、監査計画、監査目的、組織のリスク特性と整合しない場合があります。そのため、AIの利用方法と利用結果が、監査基準に準拠し、かつ内部監査部門が採用する監査手法と整合しているかを確認する仕組みが必要です。例えば、サンプリングによらず、AIで全数網羅的に検証している場合でも、十分な深度をもって検証できていない場合は、いわゆる「検査」としては十分でも「監査」として見た場合に監査基準や監査手法で求められる要求事項を満たしていない可能性があります。この乖離リスクは監査人に起因する要因もありますが、そもそもAIを前提とした監査基準や監査手続になっていないところに本質的な課題があると考えます。

3 リスクベースの管理

AI利用はリスクベースで管理し、利用場面に応じて管理水準を変えることが望まれます。その際に次の4つの観点からリスク識別と、リスクに応じた管理を行うことが有

効と考えます。

第1の観点は、内部監査のコア活動に利用するのか、アドミニストラティブな業務に利用するのかです。リスク評価、監査計画立案、監査手続の実施、監査報告書の内容作成など、監査の意見形成、監査結果の伝達に直接関係するコア活動への利用は、監査品質への影響が大きいいため慎重な管理が必要です。一方、会議メモの整形、日程調整、一般的な文章校正など、監査判断への影響が限定的なアドミニストラティブな利用は、比較的低い管理水準で足りる場合があります。

第2の観点は、監査の重要性、すなわち監査リスクの許容水準です。システム統合レビューのように内部監査の検証結果が重要な経営の意思決定に使われるもの、業務改善計画の実施状況の十分性のように当局への報告に活用されるもの、外部への開示文書について内部監査が事前レビューを行うものは、許容可能な監査リスクが低くなります。このような監査ではAI利用に対して、より厳格なレビュー、承認・記録を求める必要があります。

第3の観点は、AIへの依存度です。AIの出力が監査意見の形成、発見事項の評価、報告書の表現、経営層等への監査結果伝達内容にどの程度影響するかを確認します。AIを単なる論点整理や参考情報として使う場合とAIの分析結果を監査上の判断や報告内容に大きく反映する場合とでは、必要な統制の水準は異なります。依存度が高いほど、人による反証、根拠資料との突合、上席者レビューを強化する必要があります。

第4の観点は、複雑性、すなわち管理可能性やAIの固有リスク（特に技術面）です。

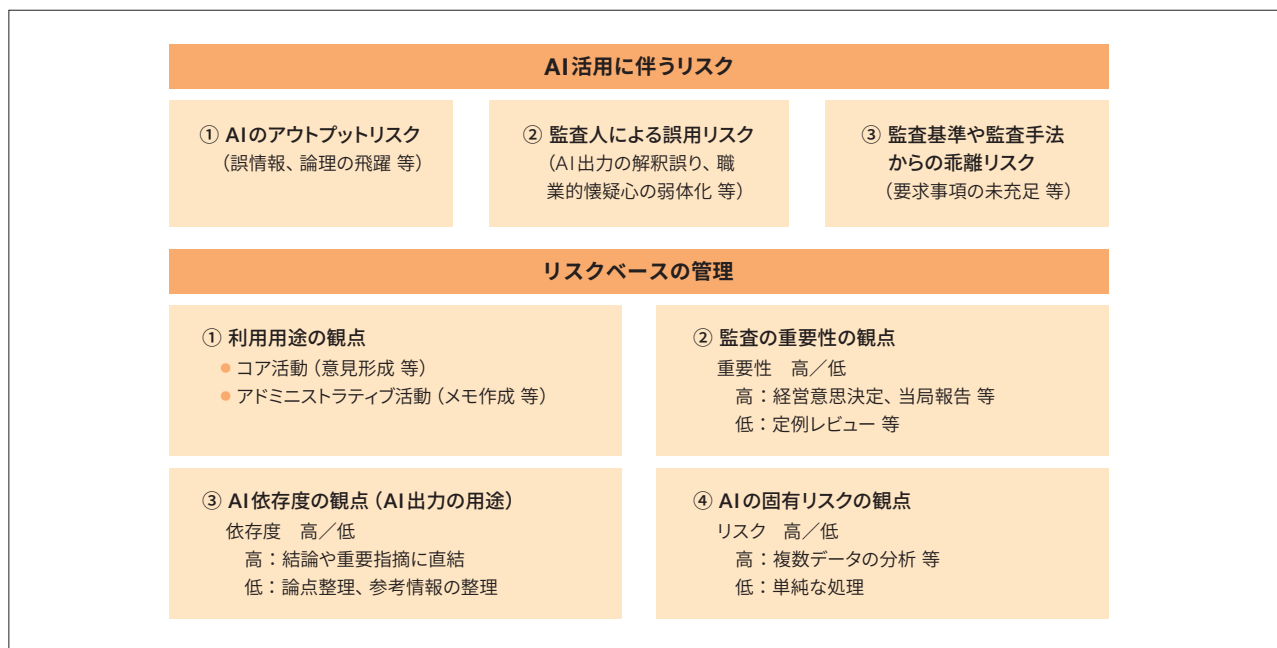
AIの利用方法が複雑である場合、処理過程が見えにくくなり、再現性や管理可能性（検証可能性）が低くなります。複数のデータソースを組み合わせる場合や長いプロンプトを用いる場合、AIエージェントが自律的に処理を行う場合には、結果の検証が難しくなります。場合によってはAI活用以外の方法も含めて検討し、利用する場合にはログ管理、検証手続、停止条件を明確に定め、管理・検証可能性を確保する必要があります。

図表1では、内部監査におけるAI活用に伴うリスクとリスクベースの管理の要点を整理しています。

4 AIは結論ではなく判断材料である

内部監査におけるAI活用の基本原則は、AIの出力を「結論」ではなく「判断材料」として位置づけることです。

図表1：内部監査におけるAI活用に伴うリスクとリスクベースの管理



出所：PwC作成

AI利用の結果責任は、一義的には監査に責任を負う監査人にあります。

AIは、論点の整理、仮説の提示、関連リスクの洗い出し、文章の叩き台の作成には有用ですが、その出力は監査上の結論を代替するものではありません。最終的な監査判断、発見事項の重要性評価、提言の妥当性判断（特に優先順位づけ）は、監査人がAIに投入・出力された情報以外の要素も含め全体を俯瞰して行う必要があります。

この原則を実効的にするためには、Human in the Loopを形式的な確認にとどめないことが重要です。監査人は、AIの出力に対して、根拠は何か、反対の見方はないか、監査基準や監査手法と整合しているか、組織の実態を適切に反映しているかを検討する必要があります。必要に応じて、AIに反証仮説を提示させる、前提条件を明示させる、異なる観点から再評価させるなど、批判的な検討を促す利用方法も有効です。

そして、AIを活用しても人が実施した場合と同等以上の品質（監査品質管理上求められる水準）を確保することが前提です。

これらを前提としAIを用いることで、監査人はリスクの本質、真因分析、改善提言、組織文化・コンダクトリスクの把握等に、より多くの時間と注意を振り向けることができます。

この点に、AI時代における内部監査人の職業専門職としての価値（特に職業的懐疑心）があると言えます。

5 再現性の確保

監査品質を確保するうえで、AI利用の再現性と文書化は重要です。監査調書には、AIをどの業務で使用したのか、使用したツールやモデル、入力した主なプロンプト、参照したデータ、AI出力のうち採用した内容、監査人が加えた修正、最終判断の根拠を記録する必要があります。これにより、第三者が監査判断の過程を追跡できる状態を確保します。

ただし、AIとのやり取りを全て調書等に記録することは現実的ではありません。重要なのは監査上の結論に影響した利用について、判断過程・根拠を説明できる記録を残すことです。低リスク利用では利用目的と確認結果を簡潔に記録し、高リスク利用ではプロンプト、出力、検証内容、レビュー結果をより詳細に保存するなど、リスクに応じた文書化水準を設けることが望まれます。

また、再現性の確保はAI利用に対する説明責任を果たすための基盤にもなります。

6 品質保証・改善プログラム（QAIP）

AI活用は、内部監査部門の品質保証・改善プログラム（以下、QAIP）の対象として位置づける必要があります。AIを利用した監査業務について、監査計画、実施、調書

化、報告、フォローアップの各段階で、品質が適切に確保されているかを評価することが求められます。特に、高リスク領域でAIを利用した場合には、レビューの深度、承認手続、記録の十分性を確認する必要があります。

内部監査マニュアルや内部監査AI利用ガイドラインには、AI利用の基本方針、禁止事項、リスク評価方法、リスク別管理要件、文書化基準、レビュー手続、教育研修内容を反映します。ただし、AI技術や利用環境は急速に変化するため、マニュアル本体に細かな運用ルールを全て固定化すると、実態との乖離が生じるおそれがあります。そのため、マニュアル本体には原則と責任分担を定め、詳細な利用手順や具体例は内部監査AI利用ガイドラインとして機動的に更新する方法が有効です。

さらに、AI管理台帳を整備して内部監査部門での利用可能AIを定義し、どの監査で、どのような目的で、どの程度AIを利用したかを把握することも重要です。利用実態を可視化することで、リスクの高い利用領域、教育が必要な領域、ルールの改善点を把握できます。QAIPは、

AI利用を監視するだけでなく、より良い活用を促進する機能として運用することが望まれます。

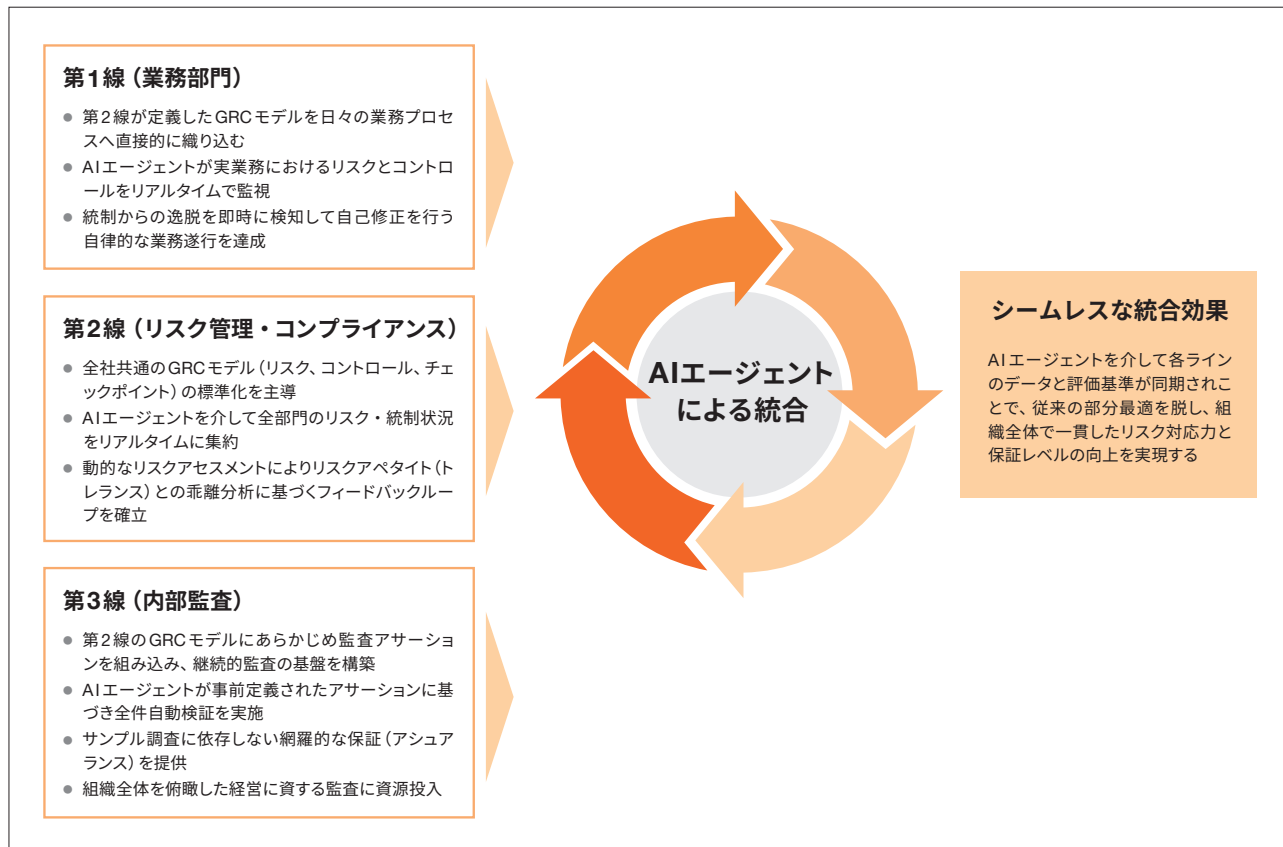
7 AIエージェント時代を見据えた監査基準の詳細化

今後は、AIが単に回答を生成するだけでなく、複数のシステムに接続し、情報収集、分析、文書作成、タスク実行を自律的に行うAIエージェントの利用が進む可能性があります。AIエージェントはタイムリーアシュアランス、さらにはリアルタイムアシュアランスを実現するための強力なツール、インフラになる可能性を秘めています。

さらに、第1線から第3線まで連携することで、監査活動で検証するアサーションの観点をあらかじめ監視プロセスに組み込むことでアシュアランスマップによる組織全体でのGRC（ガバナンス・リスク管理・コンプライアンス）の最適化実現（Aligned Assurance Model^{※1}）につながる可能性もあります（図表2）。

この場合、従来の「監査人が都度AIに指示し、結果を

図表2：AIエージェント時代の3ラインモデル（Aligned Assurance Model）イメージ



出所：PwC作成

※1 Aligned Assurance：3つのライン間でリスクタクソノミー・基準などを整合させ、リスク・コントロールに係るモニタリング・保証活動の重複を排除し、連携させるモデル。Coordinated Assurance、Combined Assuranceともいう。

確認する」では、人が中断要因となりエージェント化する意味がなくなります。AIがどの範囲までアクセスできるのか、どの操作を実行できるのか、どの段階で人のレビュー・承認を必要とするのかを明確に定める必要があります。

また、AIエージェント時代には、監査基準や監査手法の曖昧性を見直すことが重要になります。これまでは、監査基準に一定の抽象性や解釈の余地があっても、経験のある監査人が状況を踏まえて補完し、職業的懐疑心や組織への理解に基づいて判断してきました。しかし、AIに監査プロセスの一部を担わせる場合、曖昧な基準のままでは、AIがどの判断をどの根拠で行うべきかが不明確になり、監査基準や監査手法からの乖離を招くおそれがあります。

そのため、内部監査部門は、AIが参照可能な形で、監査基準、判断基準、エスカレーション条件、レビュー要件をより詳細に定義する必要があります。例えば、どのような証拠があれば十分と判断するのか、どの例外事項を重要と評価するのか、どの段階で人の承認を必須とするのかを明文化します。これは人の判断を不要にするためではなく、人が担うべき専門的判断を明確にし、AIに委ねる領域との境界を定めることになります。

内部監査におけるAI活用は、効率化と品質向上の両面で大きな可能性を秘めています。しかし、その効果を十分に引き出すためには、AIの出力を無条件に信頼するのではなく、監査リスク、職業的懐疑心、再現性、説明責任の観点から適切に管理する必要があります。内部監査部門は、AIを監査人の作業を代替し、その判断を補強する手段として位置づけ、リスクベースの管理、Human in the Loop（その先にはHuman on the Loop）、文書化、QAIPとの連動（さらに言うとQAIPのAIエージェントへの自律機能としての組み込み）、監査基準の詳細化を組み合わせる必要があります。

さらなる進展が見込まれるAI時代ですが、内部監査の信頼性と専門性を維持しながら、組織体に対する保証提供と助言を次のレベル（これをPwCでは「信頼されるアドバイザー（Trusted Advisor）」と呼びます）に高めることが期待されます。

【参考文献】

- Generative and Agentic AI Guidance, Financial Reporting Council, 2026
- Internal Audit in the Age of Generative AI, IIA Netherlands, 2026

辻田 弘志（つじた ひろし）

PwC Japan 有限責任監査法人 ガバナンス・リスク・コンプライアンスアドバイザー部 パートナー

大手金融機関を経て入社。大手金融グループ、一般事業法人に対し、内部監査、リスクマネジメント、コンプライアンスに係るアドバイザリーサービスを提供。近年は非財務リスク管理の一環として3つのラインモデル、オペレーショナルレジリエンス、コンダクトリスク管理の高度化、リスクカルチャーの組織内浸透に力を入れている。

メールアドレス：hiroshi.tsujita@pwc.com

インダストリーインサイト(25)

小売事業における多店舗展開ビジネスのDX戦略の考察とガバナンス・内部統制への影響

PwC Japan有限責任監査法人
パートナー **島袋 信一**
PwC Japan有限責任監査法人
ディレクター **坂巻 拓二**

PwC Japan有限責任監査法人
シニアマネージャー **松永 大輔**
PwC Japan有限責任監査法人
マネージャー **勝山 雄也**

PwC Japan有限責任監査法人
マネージャー **玉井 希**

はじめに

AIをはじめとする最新テクノロジーの進化と普及は、経済や産業に大きな影響を与えるファクターとなっています。また、企業にとっては、変化が激しい経営環境において、テクノロジーの変化の波に対してどのように適応していくかが重要な課題となっています。とりわけ、多店舗展開を行う企業では、店舗数の多さや現場環境の違いに加え、基幹システムが多岐にわたるなど、DXを推進する際の影響が広範囲に及ぶことが想定されます。

本稿では、小売事業における多店舗展開ビジネスのDX戦略について考察し、ガバナンス・内部統制への影響について解説します。

なお、文中の意見は筆者らの私見であり、PwC Japan有限責任監査法人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 経営者層が抱えている経営課題

PwCが2025年9月から11月にかけて、世界95カ国・地域の4,454名のCEO（うち日本は139名）を対象に実施した「第29回世界CEO意識調査」（以下、本調査）では、CEOの課題意識として、テクノロジーの変化に対応したビジネス変革が目立っています。

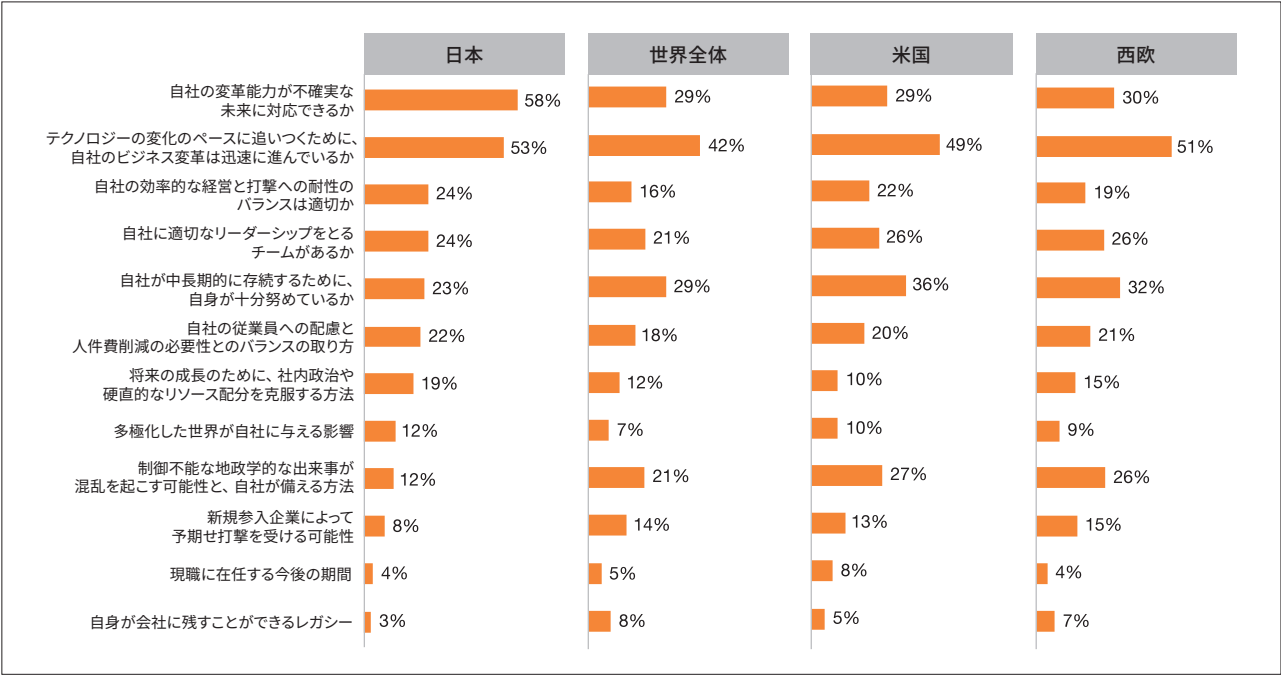
本調査によると、「テクノロジーの変化のペースに追いつくために、自社のビジネス変革は迅速に進んでいるか」について課題意識を持っていると回答した割合は、世界全体で42%、日本では53%となっています（**図表1**）。

この調査結果から、経営者は、AIなどの最新テクノロジーの活用に関して課題を認識していることがわかります。特に多店舗展開ビジネスを行っている企業では、店舗数の拡大に伴い地域・店舗ごとの顧客特性や消費行動が多様化しています。こうした状況においては、店舗ごとの現場ニーズに応えることと、本社機能による統制を構築・運用することの両立が求められます。

また、DXを推進するためには、増大する初期投資コストへの対応、旧来の現場文化や複雑に連携している各種レガシーシステムからの脱却、DX・IT人材の育成など、さまざまな課題に対応していく必要があります。

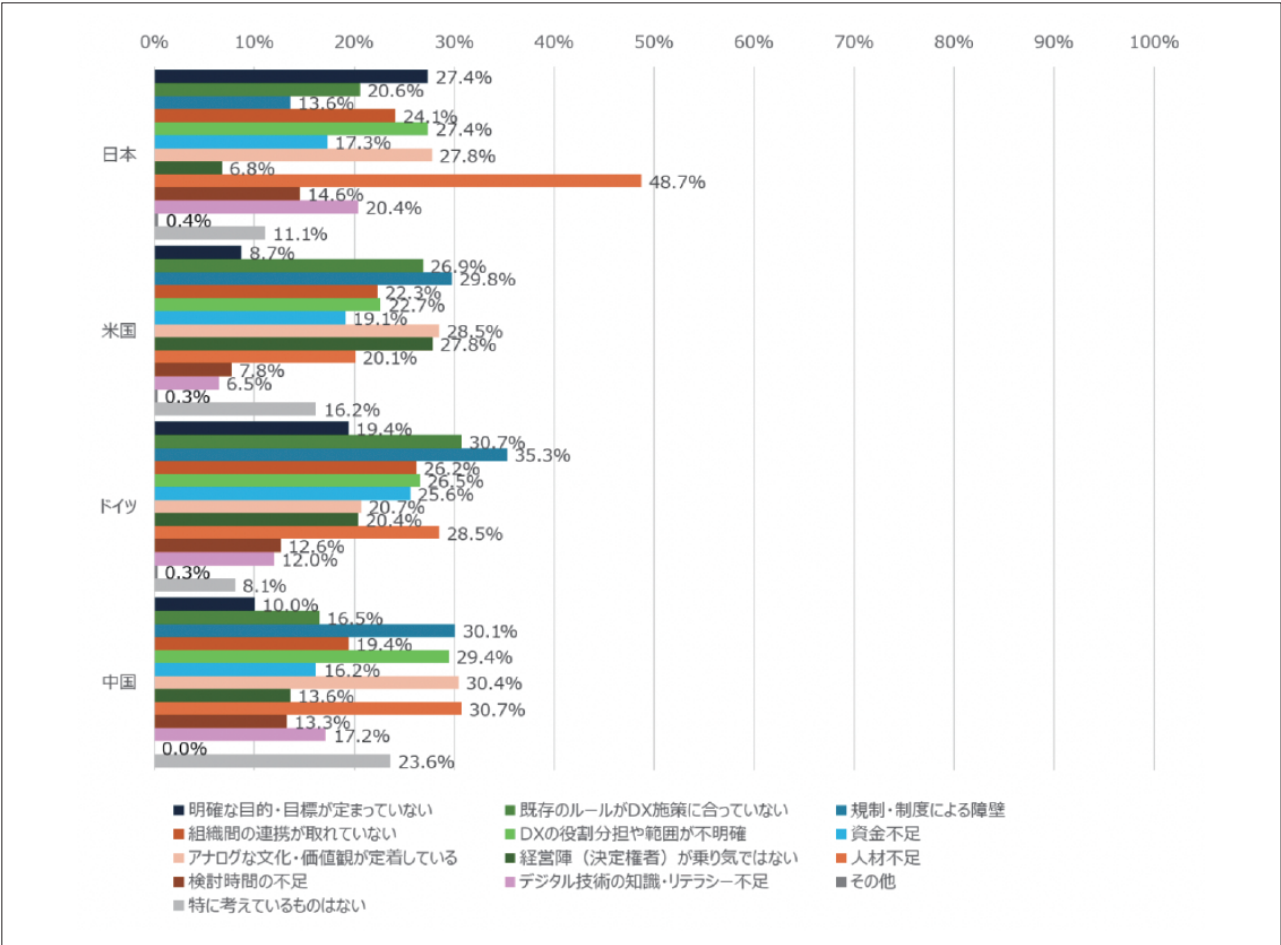
実際に、総務省情報流通行政局情報通信政策課情報通信経済室が2025年に公表した「国内外における最新の情報通信技術の研究開発及びデジタル活用の動向に関する調査研究の請負成果報告書」においても、デジタル化に関して認識している課題や障壁について調査結果が示されています（**図表2**）。

図表1：CEOの課題意識に対する質問（懸念していることを3つまで選択）



出所：PwC作成「第29回世界CEO意識調査（日本分析版）」

図表2：デジタル化に関して認識している課題や障壁（国別）



出所：総務省情報流通行政局情報通信政策課情報通信経済室「国内外における最新の情報通信技術の研究開発及びデジタル活用の動向に関する調査研究の請負成果報告書（2025年3月）」 https://www.soumu.go.jp/johotsusintokei/linkdata/r07_02_houkoku.pdf

こうした状況を踏まえると、経営者にはまず、DX推進によって期待される効果を正確に把握したうえで、推進にあたっての課題を特定し、必要な施策を検討することが求められます。また、企業全体としてDXを進めるためには、迅速な意思決定と実行、組織の変革促進、現場の巻き込みなどが必要となるため、トップダウン型の変革とボトムアップ型の変革の両方をバランスよく組み合わせながらDXを推進することが重要と考えられます。

2 DXで期待される効果

DXには、業務効率化を目的とした側面（図表3）と、デジタル技術を前提にビジネスモデル・業務プロセス・組織文化・人材の在り方を抜本的に変革し、企業価値を向上させることを目的とした側面（図表4）があると考えられています。図表3及び図表4の「期待される効果」からもわかるように、業務効率化は導入効果が見えやすい一方で、価値創出による効果は、業務効率化と比較して因果関係の把握や定量化が容易ではありません。

そのため、DX推進は主として業務効率化を目的として活用されていることが多いと考えられます。

3 国内におけるDX推進の事例と海外との比較

本節では、多店舗展開ビジネスにおける国内のDX推進事例と海外との比較について考察します。

（1）事例紹介

国内における主な事例

【事例①】AIによる需要予測・発注最適化

販売実績や天候、イベント情報などを基に需要を予測し、発注量や仕込み量、シフト配置を最適化することで、欠品・廃棄の削減と業務効率化を実現しています。また、食品ロスやエネルギー消費の削減にもつながり、サステナビリティの観点からも重要な取り組みとなっています。

【事例②】ロボット×AIによる店舗オペレーションの省人化・自動化

人手不足への対応を目的として、ロボットやAIを活用した店舗運営の自動化が進んでいます。コンビニエンスストアでは欠品確認や商品補充、外食チェーンでは配膳や食器回収などへの活用が広がっています。こうした取り組みにより、スタッフは接客や調理などの業務により注

図表3：業務効率化による効果

活用領域・導入例	期待される効果
業務自動化 RPAなどによる定型業務の自動化	- 作業時間の削減 - 人為的ミスの低減 - 高付加価値業務への時間創出
働き方・コミュニケーション リモートワーク、オンライン会議などの活用	- 柔軟な働き方の実現 - 多様な人材の採用・定着への寄与 - ナレッジ共有・属人化解消の促進
データ可視化・活用 顧客データ、生産・在庫データなどのリアルタイム可視化	- 意思決定の高度化・迅速化 - データドリブンな判断への転換 - 需要予測・価格戦略・在庫最適化の精度向上 - 機会損失・過剰在庫の削減

出所：PwC作成

図表4：価値創出による効果

価値創出領域・導入例	期待される効果
顧客体験の高度化 EC、アプリ、デジタルマーケティングなどによる顧客接点のオンライン化	- 顧客行動の把握 - パーソナライズされた提案 - 顧客満足度・ロイヤルティの向上
新たな収益モデル サブスクリプション型、プラットフォーム型ビジネスへの展開	- 収益源の多様化 - 継続的な顧客接点の確保 - データ活用による追加サービス創出
製品・サービスの高付加価値化 AIやデジタル技術を組み込んだ既存製品・サービスの高度化	- 既存製品・サービスへの付加価値付与 - 差別化要素の強化 - 顧客単価・利用頻度の向上

出所：PwC作成

力できるようになり、省人化とサービス品質向上の両立が期待されています。

【事例③】セルフオーダー／セルフレジ・AI接客など顧客接点のDX

セルフオーダーやセルフレジの普及に加え、AIによる商品提案やドライブスルーでの自動注文受付など、接客業務の効率化が進められています。

海外における主な事例

【事例①】外販（SaaS化・店舗技術外販）

自社で培った業務ノウハウやDX技術をSaaSとして外部企業へ提供し、新たな収益源とするモデルであり、「事業会社＋テック企業」として収益の多角化を進めています。

【事例②】メディア化（広告在庫化）

店舗、アプリ、ECサイト、配送網などの顧客接点を広告媒体として活用し、広告収入を得るモデルであり、購買データを活用したターゲティングや効果測定により、高付加価値の広告サービスを提供しています。

【事例③】プラットフォーム化（マーケットプレイス・コミュニティ）

自社のブランドや顧客基盤を土台として、外部事業者やユーザーが参加できる仕組みを構築し、手数料や広告収入を得るモデルであり、ネットワーク効果を生かしながら収益源の拡大と多様化を図っています。

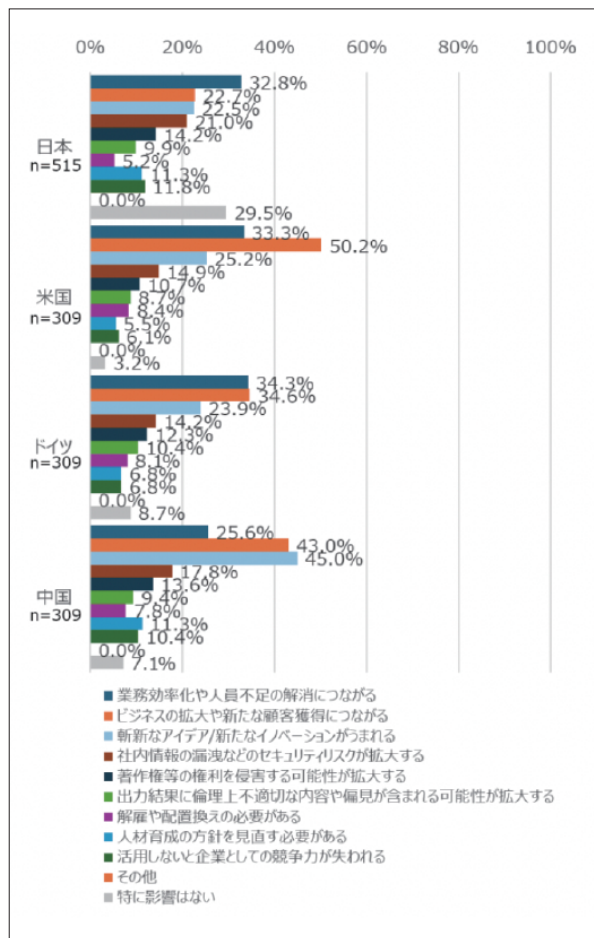
(2) 海外企業との比較

総務省情報流通行政局情報通信政策課情報通信経済室が2025年に公表した「国内外における最新の情報通信技術の研究開発及びデジタル活用の動向に関する調査研究請負成果報告書」によると、DXを支える重要なデジタル技術の1つであるAIの活用について、日本企業では業務効率化や人手不足への対応に軸足を置く傾向がある一方、海外では新たな売上や顧客価値の向上につなげる取り組みが進んでいます。

AIの活用期待される効果として、日本企業では「業務効率化」や「人手不足の解消」を挙げる割合が高い一方、「新たな商品・サービスの創出」や「売上拡大」といった価値創出に関する項目を挙げる割合は、米国、中国、ドイツと比較して低い傾向にあります（図表5）。

前述の海外事例に共通するのは、AIを需要予測や店舗運営の効率化にとどめず、自社が保有するデータ、顧客接点、運営ノウハウを、外部提供や広告事業、プラット

図表5：生成AIの活用推進による自社への影響（国別）



出所：総務省情報流通行政局情報通信政策課情報通信経済室「国内外における最新の情報通信技術の研究開発及びデジタル活用の動向に関する調査研究の請負成果報告書（2025年3月）」 https://www.soumu.go.jp/johotsusintokei/linndata/r07_02_houkoku.pdf

フォーム運営などの新たな収益機会へ転換している点です。

日本企業においても、まずは効率化による生産性向上やデータ基盤の整備を進めつつ、その成果をいかに事業資産化し、価値創出につなげるかを検討することが重要です。DXの競争軸は「効率化」から「価値創出」へと広がりつつあり、その実現に向けた戦略の構築が求められます。

4 DX推進により変化するガバナンス・内部統制

DX推進は、業務効率化や価値創出だけでなく、企業のガバナンスや内部統制にも影響を及ぼします。多店舗展開ビジネスでは、店舗運営や本部機能の自動化が進むことで、従来の「人による確認・牽制」を中心とした統制から、「システム、データ、AIを前提とした統制」への転換

が求められます。

この変化は、単に業務の担い手が人からシステムへ移るということではありません。自動化された処理やAIによる判断をどのように監督し、設定の誤り、データの不備、サイバー攻撃、ブラックボックス化といった新たなリスクをどのように管理するかが、経営上の重要な論点になります。

(1) DX推進による人材の役割変化

DX推進により、店舗・本部の双方で定型業務の自動化が進んでいます。その結果、人材には、従来のオペレーション業務を遂行する役割に加え、顧客体験の向上、データ分析、システムやAIの利用状況の監督といった、より高度な役割が求められます。

店舗では、セルフオーダーやセルフレジ、配膳ロボットなどの導入により、一部の作業は自動化されています。一方で、顧客との関係構築や例外対応、サービス品質の維持・向上など、人が担うべき領域の重要性は引き続き高いと言えます。本部においても、RPAやAIによる業務自動化が進むことで、管理業務そのものよりも、データに基づく判断や自動化された業務のモニタリングを担う人材の重要性が高まります。

このように、人材の役割変化は人的資源管理の問題にとどまらず、誰がシステムやAIを監督し、異常を検知し、必要な判断を行うのかという内部統制上の責任設計にも関係します。したがって、DX推進においては、デジタル人材の確保・育成とあわせて、役割分担、権限、レビュー体制を明確にすることが重要です。

(2) 店舗オペレーションにおける内部統制の変化

多店舗展開ビジネスの店舗では、セルフレジ、モバイルオーダー、需要予測システム、在庫管理システムなどの導入により、オペレーションの一部が自動化されています。これにより、入力ミスや確認漏れといったヒューマンエラーが低減する一方、システム設定の誤り、アクセス権限の不備、データ連携の不整合、システム障害時の対応といった新たなリスクが生じます。

例えば、セルフレジでは価格マスタ、税率設定、割引設定が誤っている場合、誤った金額で会計処理が行われる可能性があります。モバイルオーダーでは、注文・決済・POSの各データが正確かつ網羅的に連携されているかが重要になります。需要予測AIでは、予測結果に基づく発注・在庫調整が財務数値や店舗運営に影響を与えるため、

入力データの品質や例外時のレビューが重要になります。

そのため、店舗における内部統制は、従来の「人の作業を確認する統制」に加えて、システム設定、マスタ変更、データ連携、障害対応、例外処理を対象とする統制へと広がります。店舗の自動化が進むほど、本部が店舗データをリアルタイムに把握し、異常値や例外処理をモニタリングする仕組みも重要になります。

(3) 本部機能における内部統制の変化

本部においても、経理、購買、人事、在庫管理、業績管理などの領域でRPAやAI、データ分析ツールの活用が進んでいます。これにより、手作業による集計や照合は減少する一方で、自動化された処理が想定どおりに動作しているかを継続的に確認することが重要になります。

例えば、経理業務で仕訳作成や請求書処理を自動化する場合、入力データの正確性、処理ロジックの妥当性、例外取引の抽出・レビュー、設定変更の承認といった統制が必要になります。また、異常検知ツールを利用する場合でも、検知基準の妥当性や、検知された例外に対する対応状況を確認する必要があります。

さらに、本部では各店舗から収集された大量のデータを用いて需要予測、価格戦略、在庫最適化、業績管理を行う場面が増えています。こうした業務では、データの正確性・網羅性・適時性が意思決定や財務報告の前提となるため、データガバナンスやマスタ管理、システム間連携に関する統制の重要性が高まります。

加えて、店舗システムや本部システムへの依存度が高まるほど、サイバー攻撃やシステム停止が事業継続に与える影響も大きくなります。多店舗展開ビジネスでは、システム停止が店舗営業、売上計上、在庫管理、決済処理に直結するため、サイバーセキュリティや事業継続計画を内部統制の一部として位置付けることが重要です。

(4) DX時代に求められる内部統制の高度化

DX推進により業務が自動化されたとしても、内部統制が不要になるわけではありません。むしろ、統制の対象が人の作業からシステム、データ、AIに広がることで、内部統制の設計・運用はより高度化が求められます(図表6)。

特にAIやRPAを統制活動に組み込む場合には、処理ロジックがブラックボックス化しやすい点に留意が必要です。自動化された処理を過信するのではなく、重要な判断や例外処理については人によるレビューやモニタリングを組み合わせ、システムが想定どおりに機能している

図表6：内部統制において重要となるポイント（従来／DX推進後）

従来の統制の主眼	DX推進後に重要となる統制
人による作業・承認の確認	システム設定、マスタ変更、アクセス権限の管理
手作業での照合・チェック	自動化処理のロジック、例外検知、レビュー結果の確認
経験や勘に基づく判断	データ品質、データガバナンス、分析結果の妥当性確認
店舗ごとの現場管理	本部によるリアルタイムモニタリング、異常値管理
ヒューマンエラーへの対応	システム障害、サイバーリスク、AIのブラックボックス化への対応

出所：PwC作成

ことを継続的に確認する必要があります。

多店舗展開ビジネスでDXを企業価値の創出につなげるには、攻めのデジタル投資と、それを支えるガバナンス・内部統制の整備を一体として進めることが重要です。店舗・本部・IT部門・経営層が連携し、データ、システム、AIを適切に管理する枠組みを構築することが、DX時代の持続的な成長を支える基盤になると考えられます。

5 おわりに

本稿で見てきたように、日本企業、なかでも多店舗展開ビジネスにおけるDX推進は、業務効率化については一

定の成果を上げつつも、企業価値の創出へと結び付いている例はまだまだ限定的です。

経営者は、DXを起点に顧客接点やサプライチェーン全体の設計を見直し、新たな体験価値・収益モデルを生み出す「攻めのDX」へと舵を切ることが求められます。

同時に、DX活用の拡大に伴い、ガバナンスや内部統制の在り方についても再設計が不可欠になります。AIモデルの妥当性やバイアス、データ利活用に伴うプライバシー・セキュリティリスク、サイバー攻撃によるオペレーション停止といった新たなリスクに対し、経営・現場・IT・専門人材が一体となって統合的に管理する枠組みを構築することが求められます。

島袋 信一（しまぶくろ しんいち）

PwC Japan有限責任監査法人 パートナー
2003年に入所後、小売、製造、サービス業を中心に監査業務やIFRSアドバイザリー業務に従事。2011年から3年半PwC英国ロンドン事務所へ出向し、監査・財務会計アドバイザリー業務に従事。現在、PwC Japan有限責任監査法人の流通・消費財インダストリーリーダーを務めている。公認会計士。
メールアドレス：shinichi.shimabukuro@pwc.com



坂巻 拓二（さかまき たくじ）

PwC Japan有限責任監査法人 ディレクター
大手電機メーカーにてシステムエンジニアとして勤務後、2008年に入所。主に小売、製造、サービス業の財務諸表監査および内部統制監査に従事。2020年から2022年まではリスク・アシュアランス部に異動し、主にシステム監査やデジタルフォレンジックに関する業務に関与。公認会計士。
メールアドレス：takuji.sakamaki@pwc.com



松永 大輔（まつなが だいすけ）

PwC Japan有限責任監査法人 シニアマネージャー
2014年に入所後、外食・小売業を中心に、消費財、再生可能エネルギーなど幅広い業界を対象とした会計監査業務に従事。2020年から2023年8月までPwCタイの日本企業部へ赴任。会計監査、内部統制監査などの監査業務のサポートから、移転価格文書の作成支援を含む税務、会社設立や労働法などの法務、財務アドバイザリー業務まで、日系企業向けに多岐にわたる支援を提供。公認会計士。
メールアドレス：daisuke.matsunaga@pwc.com



勝山 雄也（かつやま ゆうや）

PwC Japan有限責任監査法人 マネージャー
2014年に入所後、半導体・電子部品商社、製造装置メーカー、アパレル、小売業等多様な業種の日本の上場企業に対する会計監査業務、内部統制監査業務。公認会計士。
メールアドレス：yuya.katsuyama@pwc.com



玉井 希（たまい のぞむ）

PwC Japan有限責任監査法人 マネージャー
大手電子部品メーカーにて海外営業、米国駐在を経験後、2016年に入所。入所後は、製造、卸売、小売、外食等幅広い業界の監査業務に従事。公認会計士。
メールアドレス：nozomu.tamai@pwc.com



AIエージェント利用者に求められるAIガバナンス

——「AI利活用における民事責任の解釈適用に関する手引き」から読み解く法的リスク低減の視点

PwC弁護士法人
パートナー代表 **北村 導人**
PwC弁護士法人
パートナー **山田 裕貴**

PwC弁護士法人
弁護士 **黒瀧 海詩**
PwC弁護士法人
弁護士 **高松 礼奈**

PwCコンサルティング合同会社
トラストコンサルティング事業部
パートナー **橋本 哲哉**

はじめに

近時、複雑な業務プロセスの自動化・効率化を目的として、AIエージェントなどの高度なAIシステムの活用が進みつつあります。AIエージェントは、総務省および経済産業省が公表する「AI事業者ガイドライン（第1.2版）」^{※1}（以下、「AI事業者ガイドライン」）本編11ページにて、「特定の目標を達成するために、環境を感知し自律的に行動するAIシステム」と定義されているとおり、人間による個別の入力や指示を前提とせず、環境を感知し、一定の範囲で自律的に処理を進める点に特徴があります。こうしたAIのうち、人がその判断に依拠しながら用いることが予定されているもの（依拠／代替型AI）については、人の判断や行動を前提としてきた従来の不法行為責任^{※2}判断の枠組みでは捉えられないリスクをどのようにコントロールするかが重要な課題となります。

この課題に対する基礎的な考え方を提示するものとして、経済産業省は、2026年4月9日、「AI利活用における民事責任の解釈適用に関する手引き〔第1.0版〕」^{※3}（以下、「本手引き」）を公表しました。本手引きは、AIを用いたサービスやシステムが事故に寄与した基本的な想定事例を題材に、主として不法

行為法などの観点から、AI利活用の場面における解釈適用上の論点および考え方を整理し、現行法がどのように適用され得るかの方向性を示すものです。本手引きでは、AIエージェント利用者が、不法行為に基づく損害賠償責任リスクを低減するために講じるべき措置について一定の示唆が提示されており、AIエージェントの利活用を検討中の事業者であれば把握しておくべき資料と言えます。

本稿では、本手引きを踏まえ、依拠／代替型AIに該当するAIエージェントを利用する事業者の責任判断の枠組み、そして、不法行為責任リスクを低減するためのAIガバナンス構築のポイントを概説します。

なお、文中の意見は筆者らの私見であり、PwC弁護士法人およびPwCコンサルティング合同会社ならびに所属部門の正式見解ではないことをお断りします。

1 依拠／代替型AIに該当するAIエージェント

本手引きは、AIの利活用に関する各当事者の責任判断にあたり、AIの利用形態を以下の2類型に整理して検討する手法を提示しています。

- **補助／支援型AI**：AI利用者の判断の補助ないし支援としてのみ用いられ、最終的に人の判断や行動を介在させることが予定されている類型
- **依拠／代替型AI**：人の判断や行動の全部または一部を代替する前提で提供され、AIの判断に依拠しながら用いることが予定されている類型

※1 総務省のウェブサイト「AI事業者ガイドライン」掲載ページ（https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html）および経済産業省のウェブサイト「AI事業者ガイドライン」（https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20260331_report.html）参照。

※2 故意または過失によって他人の権利または法律上保護される利益を侵害した場合、それによって生じた被害者の損害について、賠償する法的責任（不法行為に基づく損害賠償責任）が生じます（民法第709条）。

※3 経済産業省のウェブサイト「AI利活用における民事責任の解釈適用に関する手引き」を公表しました」（<https://www.meti.go.jp/press/2026/04/2026040901/20260409001.html>）参照。

AIエージェントであればただちに依拠／代替型AIに該当するというものではなく、依拠／代替型AIに該当するかは、人による判断や行動を介在させるだけでは実現困難な効用が見込まれること（必要性）と、AIが一定の精度や安全性を備えていること（精度および安全性）の2つの要件で判断するとされています。

例えば、カスタマーサポート業務を自律対応するAIエージェントが、休日・深夜帯の柔軟な対応など、人手のみでは実現しがたい効果をもたらす場合には、「必要性」の要件を満たし得ると考えられます。そして、当該AIエージェントが、同種業務に従事する通常人の作業水準と比較して同等以上の精度や安全性を備えている場合には、「精度および安全性」の要件も満たし^{※4}、依拠／代替型AIに該当し得ると考えられます。

2 依拠／代替型AIエージェントの利用者の責任判断構造とAIガバナンス

(1) 依拠／代替型AI利用者の責任判断の枠組み

依拠／代替型AIでは、最終的な人の判断や行動の適切性が論点となる補助／支援型AIとは異なり、①AI利用者がAIシステムを組み入れた業務プロセスを適切に「構築」し、②AIの望ましくない出力が権利侵害や損害を生じさせる可能性を低減するため合理的に可能な「運用」を行っていたかが、過失^{※5}判断の対象になるとされています。そして、これらの観点においてAI利用者が適切な措置を講じていた場合には、AIが個別の場面で不適切な出力をしたとしても、その全てを検証して是正するまでの結果回避義務は負わないとされています。

① AIシステムを組み入れた業務プロセスの「構築」に関する注意義務

対象業務がAIによる自動化に適しているか、その業務に求められる水準の精度・安全性を備えたAIシステムを用いているかなどが問題となるとされています。また、AIのリスクを踏まえて適切な利用体制やガバナンスの構築を行っているかも重要な要素とされています。例えば、特定条件下で精度が低下する場合などには、業務プロセス

全体として望ましい精度・安全性を確保するために必要な人の関与を介在させることなどが注意義務の内容となり得ると考えられます。

② 構築した業務プロセスの「運用」に関する注意義務

AIの望ましくない出力により権利侵害が生ずる可能性を低減するため、AI利用者がシステムの運用において合理的な措置を講じていたかが問題となるとされています。例えば、AIは継続学習やアップデートにより事後的に精度などが変化し得るため、運用過程で精度が低下し、依拠／代替型AIとしての運用に適しない状態となっていないかを確認することのほか、誤出力のフィードバックおよびこれを踏まえたアーキテクチャの改善や、当該出力がAIによるものであり、誤りを含む可能性がある旨の表示などが注意義務の内容となり得ると考えられます。

(2) AI事業者ガイドラインなどを踏まえたAIガバナンス構築の重要性

AIシステムを組み入れた業務プロセスの「構築」と「運用」において、具体的にどのような措置を講じるべきかについて、本手引きは、AI事業者ガイドラインが示す、AIの利活用に伴うリスクをコントロールするためのガバナンスの内容を参考にして、合理的に可能な措置を講じることが考えられるとしています。例えば、2025年度に行われたAI事業者ガイドラインの「別添5.AI利用者向け」の更新の際には、AI利用者が留意すべき事項に関する具体的なアプローチとして、以下の措置などが追記されました。

● ログの定期的な確認

- ▶ システム利用状況や異常操作を把握するため、ログを定期的にレビューする
- ▶ 異常な操作を検知した場合に即時報告する体制を整備する

これは、AIエージェントが自律性を持って行動するため、定期的な操作履歴の確認や報告が重要であることを踏まえたものです^{※6}。こうした措置を参考にリスクに応じたAIガバナンスを構築することは、依拠／代替型AIエージェントを利用するうえで、不法行為責任リスクを低減

※4 消費者の重要な利益に関わる説明などを行う場面では、消費者保護の観点から高度の注意義務が認められやすく、依拠／代替型AIに求められる水準も高まるとされている点に留意が必要です。

※5 前記注2のとおり、不法行為に基づく損害賠償責任の発生には少なくとも「過失」が必要ですが、「過失」は、法的な注意義務（損害の発生を予見し得たこと（予見可能性）を前提とした、損害の発生を回避する規範的な義務（結果回避義務））の違反があった場合に認められます。

※6 総務省・経済産業省「AI事業者ガイドラインの令和7年度更新内容」（令和8年3月12日AIネットワーク社会推進会議（第32回）・AIガバナンス検討会（第30回）合同会議（https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02tsu-shin06_04000138.html）【資料2】）参照。

する対応として重要と考えられます。

一方で、本手引きでは、AI事業者ガイドラインについて、そこに記載された事項を全て遵守することが求められるものではなく、また、各場面に即して求められる措置が網羅的に記述されているわけではないとされている点にも留意が必要です。以下は筆者らの私見ですが、依拠／代替型AIエージェントの利用者に課せられる注意義務は、個々の状況に応じて不法行為法の観点から定まるものであることに加え、不法行為責任リスクが顕在化するの訴訟などの紛争に至った段階です。そのため、不法行為責任リスクを低減するうえでは、AIガバナンスの構築に際し、AI事業者ガイドラインのみに依拠することは十分と言いがたいように思われます。裁判例^{※7}を含む不法行為法の知見や立証・和解などの訴訟・紛争実務の知見も踏まえ、どのような措置をどこまで講ずるかを個別具体的に検討することが肝要と考えます。

※7 本手引きでは、AIの自律性やブラックボックス性を踏まえた、既存の民事責任ルールの解釈適用について裁判例の蓄積はないとされている一方で、依拠／代替型AIを利用する際の責任判断の枠組みについては、預金払戻しシステムに係る裁判例を踏まえて検討されています。このように、直接の裁判例がなくとも、当該事案と一部共通点を有する裁判例を参照することは、個々の状況に応じたAIガバナンスの構築にあたって有効なアプローチとなり得ると考えられます。

北村 導人 (きたむら みちと)

PwC弁護士法人 パートナー

2000年弁護士登録、1996年公認会計士登録。大手法律事務所を経て、2016年にPwC弁護士法人にパートナーとして入所、2020年より同法人パートナー代表。企業法務、サステナビリティ（ビジネスと人権を含む）、税務などの分野を専門とし、AIと人権（差別、プライバシー、自己決定権など）の観点からAIガバナンス領域も扱う。

メールアドレス：michito.kitamura@pwc.com



山田 裕貴 (やまだ ひろき)

PwC弁護士法人 パートナー

2008年弁護士登録、2016年米国ニューヨーク州弁護士登録。大手法律事務所を経て、2017年にPwC弁護士法人に入所、2022年より同法人パートナー。個人データ・プライバシー保護対応、パブリックセクター案件、M&A その他各種企業法務の案件を取り扱う。

メールアドレス：hiroki.yamada@pwc.com



黒瀧 海詩 (くろたき かいし)

PwC弁護士法人 弁護士

2019年弁護士登録。大手法律事務所、国内法律事務所を経て2024年にPwC弁護士法人に入所。情報法、知財、ヘルスケア分野に注力しており、AI導入に関するものも含め、個人データ・プライバシー保護対応や特許・著作権・営業秘密といった知財取引などの案件を扱う。



3 おわりに

以上のとおり、依拠／代替型AIエージェントの利用にあたり、不法行為責任リスクを効果的に低減するためには、本手引きが指摘するAI事業者ガイドラインの知見に加え、不法行為法の知見や訴訟・紛争実務の知見も踏まえてAIガバナンスを構築することが必要と考えられます。

AIエージェントの利活用を、リスクを理由に控えるのではなく、リスクを適切にコントロールしつつベネフィットを最大化するための仕組みを早期に設計し、改善を重ねていくことが、今後の重要な競争力になると考えます。

PwC Japanグループでは、PwC弁護士法人（第一東京弁護士会所属）やPwCコンサルティング合同会社をはじめとしたメンバーファームが協働することで、こうした法的知見・弁護士実務知見と、AI活用状況の現状把握、リスク評価、ポリシー・ガイドラインの策定、AIガバナンス実施体制の構築、モニタリングプロセスの策定といったコンサルティングサービスを組み合わせ、法的リスクにも対応したAIガバナンス構築を一貫して支援することが可能です。

高松 礼奈 (たかまつ れな)

PwC弁護士法人 弁護士

2020年弁護士登録。国内法律事務所を経て、2021年にPwC弁護士法人に入所。個人データ・プライバシー保護対応、知的財産、M&A その他各種企業法務の案件を取り扱うほか、AI・リーガルテック分野にも注力する。



橋本 哲哉 (はしもと てつや)

PwCコンサルティング合同会社 トラストコンサルティング事業部 パートナー

外資系ITベンダーを経て、2015年にPwCコンサルティング合同会社に入社。2022年よりAIガバナンス領域のリードを担う。官公庁を含む多業種において豊富なAIガバナンスプロジェクトの経験を有する。サイバーセキュリティや事業継続、デジタル関連規制対応などの幅広い案件を取り扱う。

メールアドレス：tetsuya.hashimoto@pwc.com



ポーランド再考：欧州事業の可視化と統制を支える運営基盤へ

PwC Advisory sp. z o.o. sp.k.
アドバイザー部門
マネージャー **ロルスキ 真美**



はじめに

日系企業の欧州事業において今後問われるのは、「どの国に進出するか」だけではありません。各国に分散した機能を、どこで、どのように標準化し、どのような統制の下で運営するかが、経営上の重要な論点となっています。さらに、AI活用が加速する中、その効果を引き出すためには、業務プロセスやデータの可視化・共通化と、適切なガバナンスがこれまで以上に重要になっています。欧州事業の管理・運営基盤といえば西欧の主要市場を想起しがちですが、こうした業務基盤の整備とAI活用による高度化という観点からも、ポーランドは再評価に値します。ポーランドは、欧州連合（EU）加盟国としての制度整合性、グローバル・ビジネス・サービス（以下、「GBS」）の集積、人材の厚み、複数国向け業務の運営経験を背景に、単なる製造・低コスト拠点から、欧州事業を支える運営基盤へと進化しています。本稿では、日系企業が直面する欧州オペレーションの課題を起点に、ポーランドのGBSおよびManaged Services（マネージドサービス、以下、「MS」）のデリバリー基盤としての意義を考察します。

なお、文中の意見に係る記載は筆者の私見であり、PwC ポーランド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 日系企業が直面する欧州オペレーションの複雑化

日系企業の欧州事業は、国ごとの個別最適を積み上げる形で発展してきたケースが少なくありません。各国に小規模な経理、税務、人事、法務機能を置き、ローカル人材や外部アドバイザーに依存しながら拠点運営を行うモデルです。進出初期には機動的に機能しますが、拠点数や業務量が増えるにつれて、いくつかの課題が顕在化します。

第1に、業務の属人化です。欧州では、会計、税務、規制要件が国ごとに異なるため、実務が特定のローカル人材や外部専門家に依存しやすくなります。その結果、「キーパーソンが退職すると業務が回らない」というリスクが生じます。

第2に、本社からの可視性不足です。各国でレポート形式や業務プロセスが異なると、欧州全体で何が起こっているのかを把握しにくくなります。業務品質や対応スピードのばらつきも生じやすく、内部統制や経営管理の観点から課題となります。

第3に、規制対応の高度化です。CSRD（企業サステナビリティ報告指令）、Pillar 2（グローバル・ミニマム課税）、CBAM（炭素国境調整措置）など、EUレベルでの規制対応は年々高度化しています。業種や事業内容によってはDORA（デジタル・オペレーショナル・レジリエンス法）やNIS2指令（EUが策定したサイバーセキュリティ規制）などへの対応も視野に入ります。サステナビリティ、税務、サイバーセキュリティ、事業継続性に関する要請は、各国単位で個別に対応するだけでは十分ではなく、データ、プロセス、責任体制を欧州横断で整備する必要があります。

さらに、人材とコストの両面で、各国拠点が個別に管理

機能を維持する難しさも増しています。ジェトロ（日本貿易振興機構）の調査では、欧州に進出する日系企業にとって「労働コストの高さ」は欧州全体で最大の経営課題となっており、「労働コスト上昇率の高さ」は特に中東欧で高い傾向が示されています。ポーランドでも同項目を課題とする回答は7割を超えています¹。各国に小規模な管理機能を分散配置し続けるモデルは、今後さらに維持が難しくなる可能性があります。

例えば、欧州15カ国以上に拠点を持つ日系企業では、財務・税務・給与・レポーティングの運用が国ごとに異なり、本社からリスクや改善の優先度が見えにくくなることがあります。また、少人数の現地ファイナンス体制では、決算、内部統制、監査対応などの負荷が一部の担当者に集中しやすくなります。

もっとも、日系企業の欧州事業では、単純な一律標準化には限界があります。事業ごとに商流、収益構造、在庫管理、規制対応が異なるためです。重要なのは、すべてを同じ形に揃えることではありません。共通化すべき領域と、事業特性や各国の要件を踏まえて個別性を残す領域を見極め、欧州全体として可視化・統制可能な運営モデルを設計することです。

2 ポーランドをどう再定義するか

こうした課題を踏まえると、ポーランドに対する見方も変わります。ポーランドは、製造拠点や販売市場としてだけでなく、欧州事業の運営を支える基盤として捉える必要があります。

ポーランドを語るうえで、「レジリエンス」は欠かせない視点です。同国は、歴史的に大きな政治・経済体制の転換を経験しながら、制度を再構築し、市場経済への移行、EUへの加盟、外資系企業の受け入れを進めてきました。この適応力は、不確実性の高い欧州環境の中で、ポーランドが事業運営の基盤として評価される理由の1つです。

現在、ポーランドは人口約3,800万人を擁する中東欧最大級の市場であり、EU、NATO、OECDの加盟国として制度基盤も整っています。世界銀行の分類では高所得国に位置付けられており、もはや単なる低コストの新興国とは言えません²。EU加盟国であることは、事業運営上も重要な意味を持ちます。GDPR（一般データ保護規則）、VAT（付加価値税）、CSRDなど欧州共通ルールの枠組みの中で業務を設計しやすく、複数国にまたがるプロセスの共通化や統制設計と親和性があります³。

ジェトロの調査によると、ポーランドに進出する日系企業の過半数が、今後1～2年の間に事業を「拡大する予定」と回答しており、その割合は欧州全体平均および中東欧平均を上回っています⁴。また、2026年の営業利益見通しについても、約半数が2025年と比較して「改善する」と回答しています⁵。こうしたデータは、ポーランドが単なる生産拠点ではなく、欧州事業の中で継続的に位置付けを高めていることを示唆しています。

しかし、本稿でより注目したいのは、ポーランドに形成されたGBS・ビジネスサービス産業の集積です。ポーランドのビジネスサービス業界を代表する団体であるABSL（Association of Business Service Leaders）のレポートによれば、ポーランド国内には2,000を超えるビジネスサービス拠点があり、約50万人規模の就業者を有しています⁶。また、同セクターはポーランドのGDPや商業サービス輸出においても一定の存在感を示しています⁷。

これらの拠点は、財務会計、人事、税務、データ分析、IT、リスク管理など、企業運営に不可欠な業務を担っています。ABSLによれば、ミドルオフィス業務や専門性の高い業務の比率も高く、従来型の定型処理中心のBPOにとどまらない機能が広がっています⁸。これは、ポーランドが単なる業務処理拠点ではなく、欧州事業の運営を支える実務基盤へと進化していることの表れです。

投資インセンティブを活用できる可能性も、拠点設計における検討要素の1つです。ポーランドでは、Polish Investment Zone (PSI) による法人税の優遇措置、政府補助金、R&D Tax Relief（研究開発税制）、IP Boxなどの制度が整備されています。近年は、従来型の製造投資や雇用創出に加え、高付加価値のビジネスサービス機能や、高度人材・デジタル技術を活用する投資も重視される傾向にあります。投資インセンティブの適用可否や支援内容は、投資規模、立地、雇用計画、業務内容等によって異なるため、最新の制度要件を確認することが欠かせません⁹。

図表1では、拠点数、就業者数、GDP・輸出への貢献などから、ポーランドのビジネスサービス／GBSエコシステムの規模を示します。

中東欧には複数の有力な候補地がありますが、ポーランドは市場規模、GBS集積、欧州広域へのデリバリー実績の組み合わせという点で、バランスの取れた拠点です。必ずしも最も低コストの選択肢ではありません。しかし、欧州主要国との時差、EU制度との整合性、人材の厚み、複数国向けの運営経験を踏まえると、コスト・品質・統制

図表1：ポーランドにおけるビジネスサービス／GBSエコシステムの規模

指標	数値・内容	示唆
ビジネスサービス企業数	1,303社	多様な企業によるサービス集積
ビジネスサービスセンター数	2,179センター	欧州有数のデリバリー基盤
就業者数	約50万人	大規模な専門人材プール
GDPへの推定寄与	6.1%	ポーランド経済における存在感
商業サービス輸出に占める推定比率	36.9%	海外向けサービス提供基盤
ミドルオフィス業務比率	63.4%	単純処理にとどまらない業務領域
専門性の高い業務比率	58.2%	高付加価値業務への進化

出所：ABSL, Sektor usług biznesowych w Polsce 2026 (p.42) 他をもとにPwC作成

のバランスを取りやすい拠点と言えます。

3

マネージドサービス：外部委託ではなく、運営設計の選択肢

欧州オペレーションの複雑化に対する選択肢として、近年あらためて注目されているのがMS（マネージドサービス）です。

MSとは、単に業務を外部に委託することではありません。専門人材、テクノロジー、AI、SLA（サービスレベル合意）、KPI（重要業績評価指標）、ガバナンス体制を組み合わせ、各国・各事業で分断された業務プロセスを可視化し、共通化できる領域を揃えながら、必要なローカル要件を適切に管理する運営モデルです。つまり、業務を「外に出す」ことではなく、欧州全体として、どの機能を、どこで、どのような統制の下で運営するかを設計することに本質があります。

日系企業にとって重要なのは、自社が担うべき判断機能と、外部の専門性を活用すべき実行機能を切り分けることです。例えば、事業方針の決定、重要事項に関する意思決定、リスク評価、例外対応の承認といった経営・統制機能は社内に残す必要があります。一方で、共通化が可能な業務プロセス、複数国にまたがるレポーティング、規制対応のためのデータ収集・管理、業務プロセスの運営管理などは、外部の専門人材やテクノロジーを活用しながら運営することが考えられます。その際、統制を手放すのではなく、統制を維持しながら実行力を高めることがポイントになります。

欧州事業の運営モデルには、企業の成熟度や目的に応じて複数の選択肢があります。各国に管理機能を分散配置するモデル、自社でGBSを構築・運営するモデルに加え、外部パートナーを活用する形として、外部支援型キャプティブ（Assisted Captive）、MS、ビルド・オペレート・

トランスファー（BOT）なども考えられます。いずれかのモデルが一律に優れているわけではありません。自社で保持すべき統制機能を明確にしたうえで、どこに外部の専門性、スケール、継続的な改善の仕組みを取り込むかを設計することが求められます。

MSは、単なるコスト削減策ではありません。ただし、業務の標準化、集約化、自動化、グローバルデリバリーモデルの活用、継続改善を組み合わせることで、結果として運営効率やコスト競争力の向上につながるケースもあります。個別ケースによりますが、一定の条件下では、5年間の累計で最大45%程度のコスト最適化効果が見込まれるケースもあります。もっとも、効果は対象業務、移行範囲、既存体制、テクノロジー活用の度合いによって異なるため、初期費用や契約条件だけでなく、中長期の累積効果を含めて検証することが重要です¹⁰。

また、業務基盤を可視化・標準化することは、将来の選択肢を広げることにもつながります。一部業務の再内製化、地域体制の見直し、テクノロジー活用を見据え、外部化を恒久的な「片道切符」とするのではなく、柔軟な運営モデルの一部として位置付けることが大切です。

近年では、AIやエージェント型AIなどの先端技術を、単独のツールとして導入するのではなく、運用プロセスに組み込み、日々の業務の中で活用する設計も進みつつあります。例えば、レポート作成の補助、異常値の検知、データ分析、問い合わせ対応、ナレッジ検索などの領域では、AIを活用することで業務の質やスピードを高められる可能性があります。一方で、最終判断やガバナンスは人が担うべき領域であり、AIはそれを補完するものとして位置付ける必要があります。MSの特徴は、こうしたAIやテクノロジーを、業務プロセス、SLA／KPI管理、品質管理、継続改善の仕組みと一体で運用できる点にあります。

さらに、MSの価値は日々の業務処理にとどまりません。運用プロセスやデータから得られるインサイトを、経営判断に資する情報として活用できるという特徴もあります。例えば、地域・事業ごとの収益性やコスト構造の差異、例外処理や非効率の集中を可視化することで、欧州全体を見渡した事業戦略や経営判断を支えるデータ基盤を構築できます。

図表2では、各国分散モデル、自社主導モデル、外部専門性活用モデルを、本社からの可視性、統制・ガバナンス、人材・専門性、コスト競争力、AI・テクノロジー活用、将来的な内製化といった観点から整理しています。重要なのは、どのモデルが一律に優れているのではなく、自社の事業規模やガバナンス要件に応じて、どの機能を内製化し、どの機能を共通化・外部活用するかを設計することです。

一方で、日系企業がMSを検討する際に、「品質は維持できるのか」「移行時に混乱しないか」「本社の統制が弱まらないか」「知見が社内に残らないのではないか」といった懸念が生じることがあります。これらの論点に対しては、運営設計の段階であらかじめ対応しておく必要があります。

具体的には、対象業務の範囲、社内に残す判断機能、外部に委ねる実行機能を明確にしたうえで、移行計画、SLA、KPI、エスカレーションルート、ガバナンス会議、BCP（事業継続計画）、品質レビュー、本社向けレポートニングなどを設計します。さらに、業務手順や判断基準を文書化し、定期的に見直すことで、属人的な知見を組織知へと転換していくことも重要です。

したがって、MSは、適切に設計されれば、社内機能を空洞化させるものではありません。むしろ、各国に分散していた業務プロセスや知見を可視化し、共通化できる領域を整理しながら、本社が統制可能な運営基盤へと再構築するための手段になり得ます。

4 なぜポーランド／グダンスクなのか

では、MSや欧州横断オペレーションのデリバリー拠点として、なぜポーランドが有力な候補となるのでしょうか。

第1に、人材と業務経験の厚みがあります。ポーランドには、ファイナンス、税務、IT、データ分析、リスク管理などの領域で、多国籍企業向け業務を支えてきた人材が蓄積されています。ABSLのデータでも、ワルシャワ、クラクフ、ヴロツワフなどの主要都市や、グダンスクを含むトリシティ地域には、ビジネス、IT、工学、言語系分野の人材が広く分布しています¹⁾。英語に加え、欧州主要言語に対応できる人材も多く、複数国向けの業務運営を支える基盤があります。

第2に、欧州域内のデリバリー拠点としての近接性があります。ポーランドは必ずしも最も低コストの選択肢ではありませんが、欧州主要国との時差が小さく、EU制度との整合性もあります。西欧に自社GBSを置く場合と比べても、コスト、専門人材、スケールのバランスを取りやすい点が特徴です。

第3に、既存のGBS・ビジネスサービス集積があります。ABSLの欧州比較でも、ポーランドはEU内有数のビ

図表2：日系企業の欧州事業における運営モデルの選択肢

比較軸	各国分散モデル	自社主導モデル	外部専門性活用モデル
代表的な形態	各国拠点ごとに管理機能を保有	欧州統括、自社GBS	外部支援型キャプティブ、マネージドサービス、ビルド・オペレート・トランスファー（BOT）
基本構造	各国が個別に経理・税務・人事等を運営	自社で業務を集約・標準化	外部専門性、テクノロジー、デリバリー基盤を活用
本社からの可視性	国ごとにばらつきやすい	設計次第で高めやすい	KPI・SLA・レポート設計により高めやすい
統制・ガバナンス	拠点間で差異が生じやすい	自社主導で統制しやすいが運営負荷あり	ガバナンス会議、エスカレーション、品質管理を組み込みやすい
人材・専門性	各国で個別確保が必要	集約人材の採用・維持が必要	専門人材やテクノロジーを活用可能
コスト競争力	重複コストが残りやすい	初期投資・固定費が発生	標準化・自動化・継続改善により中長期でコスト競争力を高める余地
AI・テクノロジー活用	拠点ごとにばらつきやすい	自社投資能力に依存	運用プロセスにAIや分析機能を組み込みやすい
将来的な内製化	既に内製だが分散	内製維持	BOTや段階的移管により内製化の選択肢を持てる
適するケース	各国主体の運営を重視する場合	十分な規模・投資余力がある場合	可視化・統制・専門性・スケールを高めたい場合

出所：PwC作成

ジネスサービスセンター雇用を有する国として示されています¹²。

その中でも、グダンスクを含むトリシティ地域は、テクノロジー、ファイナンス、ビジネスサービス人材の集積が進む拠点の1つです。港湾都市としての国際性、北欧・西欧・中東欧への接続性、複数国向けサービスの経験は、欧州横断業務のデリバリー拠点としての適性を高めています¹³。

PwCのグローバルネットワークにおいても、グダンスクはEMEA（欧州、中東およびアフリカ）向けMSを支えるデリバリー拠点の1つです。ただし、MSを有効に機能させるには、デリバリー拠点の専門性だけでは十分ではありません。日本本社、欧州統括会社、現地拠点、デリバリーチームの間で期待値を調整し、意思決定と実務をつなぐ役割が鍵となります。

この点で、日本語によるコミュニケーションを含む橋渡し機能は、日系企業にとって大きな意味を持ちます。PwCのJapan Business Network（JBN）は、日系企業への支援に特化したグローバルネットワークであり、日本

側の問題意識と欧州現地の実務をつなぐ役割を担っています。こうしたネットワークを通じて両者を接続できれば、MSは単なる業務移管ではなく、欧州運営モデルを再設計するための実務的な選択肢となります。

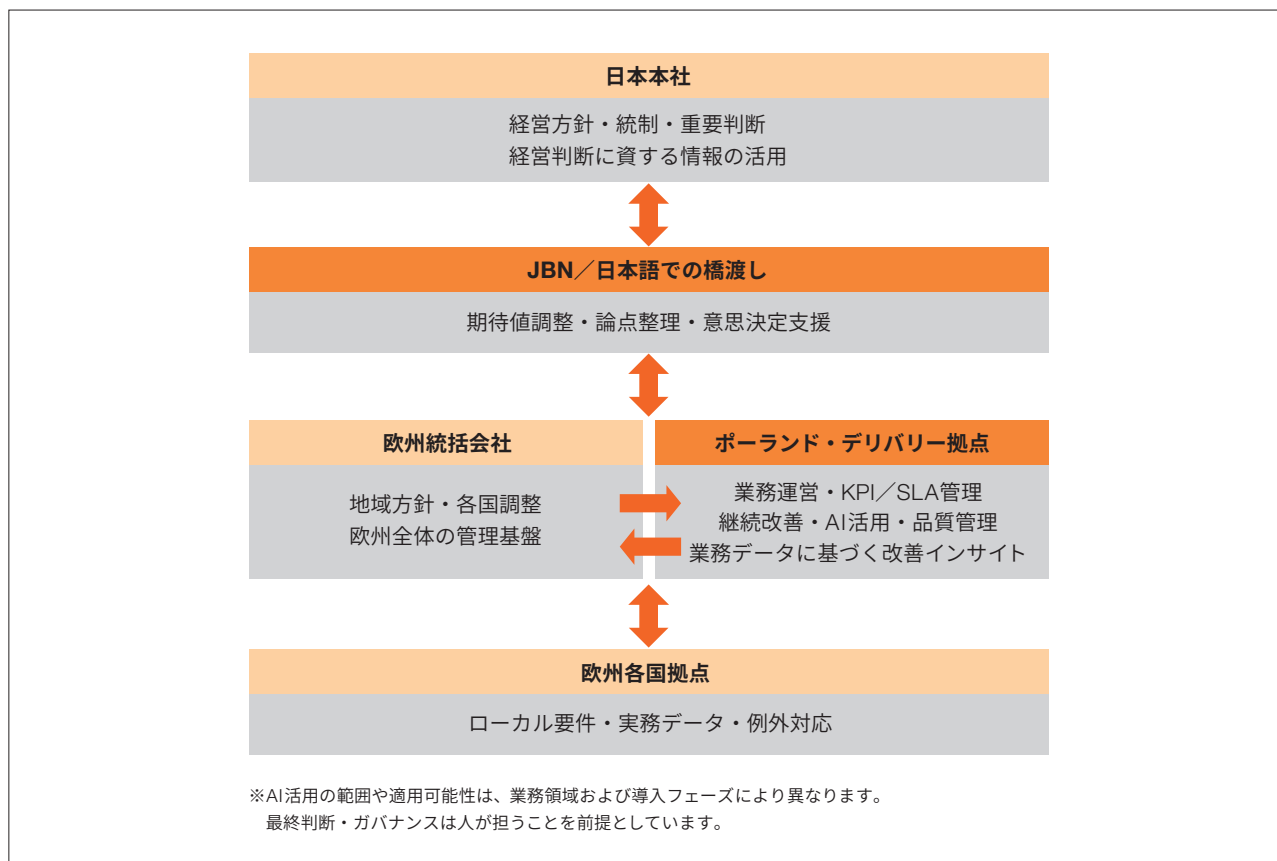
図表3では、日本本社、欧州統括会社、欧州各国拠点、ポーランドのデリバリー拠点、JBN／日本語での橋渡し機能の関係を示しています。ポイントは、デリバリー機能に加え、ガバナンスと業務可視化を支える連携の仕組みです。

5 おわりに

ポーランドを再考することは、単に新たな投資先を探すことではありません。欧州各国に分散した業務を、どのように可視化し、どの機能をどこで運営し、どのように日本本社から統制するかという欧州事業の運営モデルを見直すことでもあります。

日系企業にとって、欧州事業の複雑性は今後も高まると考えられます。人材不足、属人化、規制対応、データ整

図表3：日系企業の欧州運営を支えるMS連携モデル



出所：PwC作成

備、各国拠点の運営のばらつきは、個別拠点の努力だけでは解決しにくい課題です。求められているのは、各単位での個別最適ではなく、欧州全体を俯瞰し、共通化すべき領域と各国要件を残す領域を見極める運営モデルです。

ポーランドは、制度の安定性、レジリエンス、人材基盤、GBS集積、欧州広域へのデリバリー経験を備えた拠点として、その問いに対する1つの現実的な選択肢となり得ます。賃金上昇、人材獲得競争、地政学的近接性といった課題はありますが、それらも含めて、どの機能をどこで、どのようなガバナンスの下で運営するかという設計課題として捉えることが重要です。

自社の欧州事業において、どの業務が各国に分散し、どの業務が属人化し、どの情報が本社から見えにくくなっているのか。こうした現状を棚卸しすることが、次の運営モデルを構想する第一歩になります。

今後、各企業の欧州事業ポートフォリオにおいて、ポーランドはどのように位置付けられるでしょうか。単に「進出先として魅力的か」だけではなく、「欧州事業の可視化と統制を支える運営基盤として、どのように活用できるか」という観点からも、改めてポーランドについて検討する価値があるのではないのでしょうか。

【脚注・出典】

- 1 ジェトロ「2025年度 海外進出日系企業実態調査 | 欧州編 ー高コストや地政学リスクに向き合う日系企業、サステナビリティ規制緩和には期待ー」(2025年12月)、p.44。欧州全体で「労働コストの高さ」が56.7%、「労働コスト上昇率の高さ」が41.3%、ポーランドでは「労働コスト上昇率の高さ」が70.4%。
- 2 World Bank, Country and Lending Groups; Statistics Poland (GUS); OECD, Poland country profile; 外務省「ポーランド共和国 基礎データ」。
- 3 European Commission, GDPR, VAT, Corporate Sustainability Reporting Directive (CSRD), Carbon Border Adjustment Mechanism (CBAM); Digital Operational Resilience Act (DORA), NIS2 Directive 関連公式情報。
- 4 ジェトロ「2025年度 海外進出日系企業実態調査 | 欧州編 ー高コストや地政学リスクに向き合う日系企業、サステナビリティ規制緩和には期待ー」(2025年12月)、p.13。今後1〜2年の事業展開の方向性について、欧州全体では「拡大」が48.9%、ポーランドでは55.6%。
- 5 ジェトロ「2025年度 海外進出日系企業実態調査 | 欧州編 ー高コストや地政学リスクに向き合う日系企業、サステナビリティ規制緩和には期待ー」(2025年12月)、p.11。ポーランド進出日系企業の2026年営業利益見通しにおける「改善」は50.0%。
- 6 ABSL, Sektor usług biznesowych w Polsce 2026, p.42。2026年第1四半期末時点で、ポーランドのビジネスサービス部門は1,303社、2,179センター、500,500人の雇用。
- 7 ABSL, Sektor usług biznesowych w Polsce 2026, p.42。同セクターのポーランドGDPに占める推定比率6.1%、商業サービス輸出に占める推定比率36.9%。
- 8 ABSL, Sektor usług biznesowych w Polsce 2026, p.42。ミドルオフィス業務比率63.4%。専門性の高い業務比率58.2%。
- 9 Polish Investment and Trade Agency (PAIH)、Polish Investment Zone (PSI)、Government Grants、R&D Tax Relief、IP Box等に関する公式情報。制度内容、適用条件、支援期間は投資内容や地域等により異なる。
- 10 コスト最適化に関する記述は、匿名化した参考ケーススタディを踏まえて一般化したもの。5年間累計で最大45%程度という数値は特定ケースに基づく参考値であり、実際の効果は、対象業務、移行範囲、既存体制、テクノロジー活用の度合い等により異なる。
- 11 ABSL, Sektor usług biznesowych w Polsce 2026, p.136。主要都市・地域別の言語、ビジネス・管理、ICT、工学系等の卒業生データ。
- 12 ABSL, Sektor usług biznesowych w Polsce 2026, p.35。EU各国等におけるビジネスサービスセンター雇用比較。
- 13 ABSL, Sektor usług biznesowych w Polsce 2026, pp.77, 79。トリシティ地域におけるSSC/GBSおよびBPOの雇用データ。

ロルスキ 真美 (ろるすき まみ)

PwC Advisory sp. z o.o. sp.k. アドバイザリー部門 マネージャー
米国公認会計士。米国・カナダの大手監査法人を経て、2023年にPwCポーランド入社。IFRS・US GAAPに基づくクロスボーダー監査やPCAOB監査をはじめ、監査・アドバイザリー業務に従事し、北米・欧州の日系企業および多国籍企業を支援。現在はJapan Business Network (JBN) の一員として、日本と欧州の間の橋渡しに携わり、Managed Servicesを活用した業務運営モデルの高度化、ガバナンス強化、オペレーション変革を支援している。

メール：mami.rolski@pwc.com

PwC調査レポートピックアップ

PwC Japan有限責任監査法人 企画管理本部
ディレクター 三橋 敏

AIパフォーマンス調査



本レポートは、PwCが世界の上場企業1,217社の経営幹部を対象に実施した調査を基に、AIの活用によって大きな成果を上げる企業とそうでない企業の違いを分析したものである。最大の結論は、「AIを使う量」ではなく、「AI適合性 (AI Fitness)」の高さが成果を決定するという点にある。

AI適合性とは、「重要課題にAIを適用し、適切な基盤を整備し、それを全社に展開する能力」を指す。具体的には、戦略、投資、人材、データ・テクノロジー、ガバナンス・リスク、イノベーションという6つの基盤要素に加え、AI活用の範囲や高度化、業界融合への対応を含めた9つの要素で構成される。

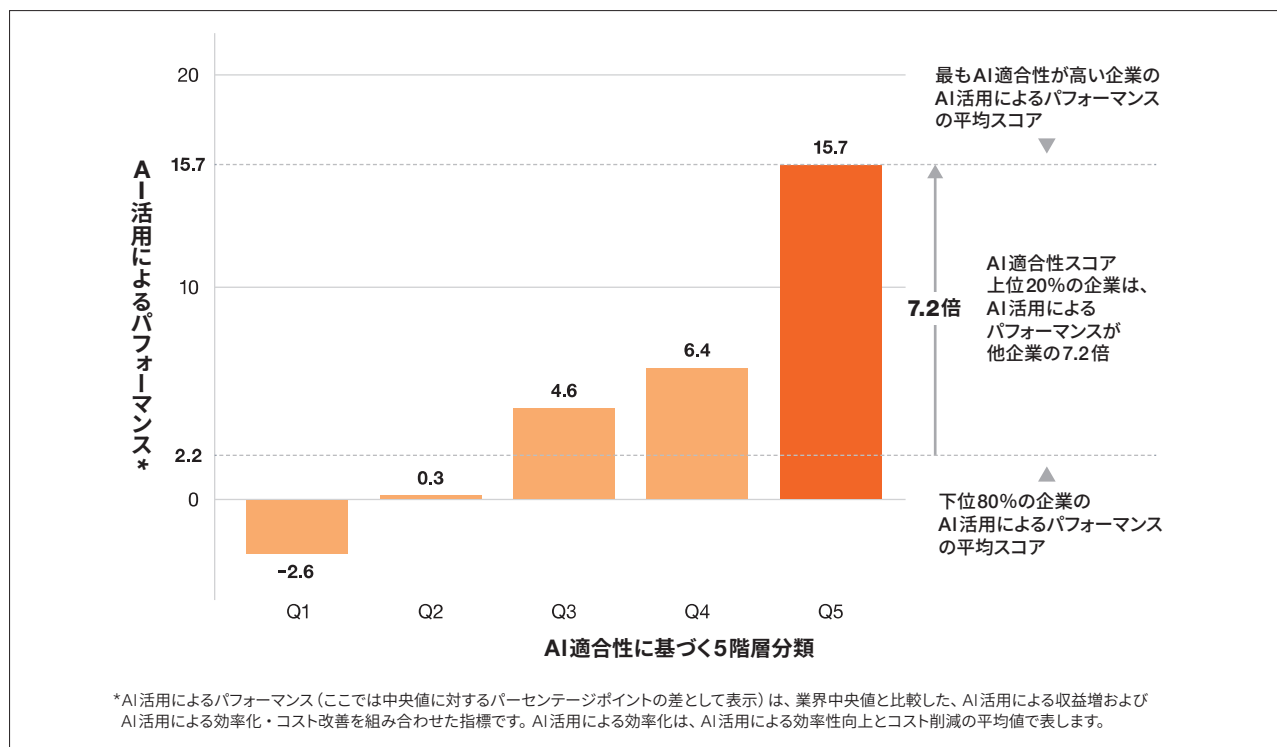
調査では、AI適合性が最も高い上位20%の企業は、AI活用による財務パフォーマンスが、下位80%の企業平均の7.2倍に達していた(図表1)。しかも、調査対象企業全体のAI成果の74%を、この上位20%が生み出している。

多くの企業がAIの実証実験や個別導入を進めているものの、明確な収益向上やコスト削減につなげられている企業は限られている。

日本企業の現状を見ると、AI適合性指数は10点満点中4.8であり、中央値の5.5を下回る。中国の6.9、韓国の5.4、米国の5.2と比較しても遅れが見られる。もっとも日本企業のAI導入率自体は欧米と大差なく、課題は導入そのものではなく、導入効果を財務成果に結び付ける能力にある。実際、AI活用で得られた効果を財務的に還元できていると回答した割合は約40%にとどまっている。

成果を上げる企業には共通点がある。社長直轄による推進体制やCAIO (Chief AI Officer) の配置、明確なユースケース設定、AI活用を前提とした業務プロセスとデータ整備など、全社的な推進体制を構築している点である。重要なのは個別のAIツール導入ではなく、再現可能な仕組みづくりである。

図表1：AI適合性が最も高い企業は、AI活用によるパフォーマンス（業界調整済み）が7.2倍



出所：PwC「AIパフォーマンス調査」

AI時代のB2Bビジネスと、人に求められる力



本レポートは、生成AIの普及によってBtoBビジネスの購買・営業活動がどのように変化するかを整理し、その中で企業や営業人材に何が求められるのかを論じている。最大のメッセージは、「AIを使うかどうか」ではなく、「AIを前提とした購買・営業構造の変化に適応できるか」が競争力を左右するという点である。

従来のBtoB購買は、「認知→比較→検討→決裁→発注」という直線的なファネルを前提としていた。しかし今後は、顧客側のAIエージェントが課題発見、要件定義、候補比較、リスク評価などを同時並行で処理するため、購買プロセスそのものが圧縮される。さらに、買い手側AIと売り手側AIが交渉する世界では、人間が主体だった購買活動が、AI主体へ移行する可能性が示されている。

顧客側の変化としては、5つの特徴が挙げられる。第1に、課題は人が気づく前にAIが検知する。第2に、AIが常時市場情報を収集・評価する「コンティニュアスマーケットプレイス」が形成される。第3に、要件整理や選択肢比較など意思決定の下準備をAIが完了させる。第4に、契約や発注などの実行部分もAIが担うようになり、企業

にはガバナンスや責任分界の設計が不可欠となる。第5に、顧客側のAIがROIを継続的に監視するため、営業には契約獲得後の成果創出と定着支援がより強く求められる。

一方、営業側にも大きな変化が生じる。営業は歴史的に「人柄と関係性の時代」から「情報量と経験値の時代」、さらに「顧客課題への示唆を提供する時代」へと進化してきた。しかし生成AIによって情報収集や提案作成が容易になることで、「情報量の厚み」や一般的な提案力は差別化要因ではなくなる。マーケティング、インサイドセールス、フィールドセールス、カスタマーサクセスという従来の分業も再編され、営業は顧客の意思決定を支援し、合意形成を設計する役割へと変わる。

このようなB2Bビジネスの変化に伴い、AI前提社会において人が担う役割は大きく再定義される（図表2）。顧客ごとの複雑な状況や文脈を捉え、解決策に結び付ける「柔軟な課題接続力」や「顧客インサイトを見抜く力」が重要になる。

図表2：AIに代替されづらい能力

競争フェーズ	求められる力	AI代替性
参加条件	筋肉質（情報量・整備力）	高い（AIが底上げ）
差別化条件	課題接続力	一部代替されるが人の判断が残る
最終選択条件	多様性に寄り添う力	代替困難

出所：PwC作成

Viewpoint

会計・監査に関するPwCの総合情報サイト



Viewpointとは、これまでのInformに置き換わる、会計・監査に関する情報を提供するPwCのグローバルのデジタル・プラットフォームです。Viewpointは、IFRS関連情報が中心ですが、US GAAP（米国会計基準）、日本基準についても取り上げています。Viewpointには、日本サイト（日本語）だけでなく、GlobalサイトやUSサイトもあります。

Viewpointの特徴のご紹介

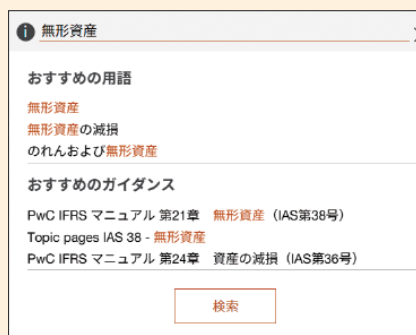
- **リアルタイムなアップデートとパーソナライズ**
ユーザーが登録した好みを中心にコンテンツが整理されますが、Viewpointを使えば使うほど、ユーザーに最適な情報をタイムリーに提供します。

- **直感的な検索機能（予測変換）**
よく検索される用語に基づいて、おすすめの用語やガイダンスが表示され、必要な情報にすばやくアクセスできます。

- **PwCの専門家によって編集されたコンテンツページ**
コンテンツページを閲覧しているときに、サイドパネル上で関連リンクを見ることができます。また、ユーザーが最初にアクセスするページにホットピックを集め、関連するニュースや解説資料をワンストップで探すことができます。

- **メニューナビゲーション**
クリック数を最低限に抑えて、人気コンテンツにアクセスできます。

▼直感的な検索機能（予測変換）



▼PwCの専門家によって編集されたコンテンツページ



いつでも、どこでも、Viewpointは
あなたに最適な情報をお届けします。

外出先で

Viewpointは、モバイルやタブレット、PCで検索履歴などを共有し、シームレスに連携します。また、タイムリーに更新された情報に容易にアクセスできます。

オフィスや自宅で

直感的なインターフェースとナビゲーションにより、必要な情報を容易に見つけることができます。検索に役立つ予測検索機能は、必要なときに必要なものを見つけるのに役立ちます。

チーム内で

SNSなどでのコンテンツ共有機能を使って、チームのメンバー同士で瞬時にPwCのインサイトを共有し、スピード感をもって、重要なトピックを把握することができます。

Viewpointのコンテンツ

Viewpointには、次の3つのコンテンツがあります。

無料コンテンツ

IFRSの速報や速報解説など、どなたでもご覧いただけるコンテンツです。

無料登録会員コンテンツ (Viewpointサイト上で登録可能)

IFRSおよび日本基準の比較、IFRSに基づく連結財務諸表のひな型など、PwCのナレッジを集約したコンテンツです。

有料会員コンテンツ

IFRS基準書やPwC IFRSマニュアル、詳細解説などIFRSに関する詳細なガイダンスです。

Viewpointの特徴のひとつであるパーソナライズを有効に使うため、まずは無料登録会員の登録からはじめましょう。

<https://viewpoint.pwc.com/jp/ja.html>

● ニュースレターご登録

Viewpoint日本サイトでは、更新情報や便利な機能のご紹介など、E-Mailで無料にてお届けするニュースレターを月1回無料で配信しています。是非ご登録ください。

ニュースレター 新規登録（「会計・監査ニュースレター」を選択）

<https://www.resource.jp.pwc.com/newsletter>

コンタクト

PwC Japan 有限責任監査法人 Viewpoint事務局
E-mail: jp_asr_viewpoint-mbx@pwc.com



実務解説 SSBJ基準の適用と開示例

サステナビリティ基準委員会（SSBJ）から公表された4つのサステナビリティ開示基準（適用基準、一般基準、気候基準、温対法基準）は、2027年3月期から段階的に適用が義務付けられます。本書は、PwC Japan有限責任監査法人のサステナビリティ開示に関する知見と経験を踏まえ、SSBJ基準の定めを実務でどのように適用すべきかを解説するものです。

解説にあたっては、PwCのサステナビリティ・レポート・ガイドに示された見解に基づく「Point Of View」、特定の事象についてより具体的に解説する「ケーススタディ」、本書の内容を理解する上での補足的な情報をまとめた「Short Break」といった項目も設けました。また、PwCが公表している開示例から日本企業の実務に役立つものを選定して紹介しています。

さらに、SSBJ基準の他にも目的や対象の異なるさまざまな基準・フレームワークが存在することから、サステナビリティ関連の主な基準、規則、フレームワークについても概説しました。

PwC Japan有限責任監査法人編、中央経済社
A5判 436ページ、5,000円＋税、2026年9月発行



サステナビリティ保証の実務対応 〈改訂版〉

2023年6月、国際サステナビリティ基準審議会（ISSB）のIFRS S1号およびIFRS S2号が最終化されました。欧州では企業サステナビリティ報告指令（CSRD）および欧州サステナビリティ報告基準（ESRS）の制度整備や見直しが進められ、一定規模以上の欧州拠点を持つ日本企業にも影響を及ぼしています。

一方、日本では、2025年3月にサステナビリティ基準委員会（SSBJ）の開示基準が公表され、情報開示の実務は新たな段階に入りました。関連する法定開示も段階的に導入され、企業には迅速な対応が求められます。

加えて、国際サステナビリティ保証基準（ISSA）5000や、日本公認会計士協会のサステナビリティ保証業務実務指針5000が公表され、保証実務の基盤整備も進展しています。第三者保証の取得には、企業内の内部統制とガバナンスの強化が不可欠であり、組織体制や人材の確保など、早期の備えが必要です。

本書では、国内外のサステナビリティ第三者保証の最新情報を踏まえ、サステナビリティ報告と保証の実務対応を解説します。今回の改訂では、SSBJ基準および保証業務実務指針5000を踏まえた記述を追加し、業種別課題を拡充しました。各章末には、実務上よく課題となるテーマをFAQとして収録しています。

PwC Japan有限責任監査法人編、中央経済社
A5判 444ページ、4,600円＋税、2026年9月発行

海外PwC日本語対応コンタクト一覧

PwCは、全世界137の国と地域、36万人以上のスタッフによるグローバルネットワークを生かし、クライアントの皆さまを支援しています。ここでは各エリアの代表者をご紹介します。

	担当国・地域	写真	担当者名		電話番号	メールアドレス
アジア太平洋	中国統括		吉田 将文	Masafumi Yoshida	+86-150-0027-0756 +852-9537-9560	masafumi.g.yoshida@hk.pwc.com
	中国本土		吉川 正大	Masahiro Yoshikawa	+86-150-2686-7130	masahiro.m.yoshikawa@cn.pwc.com
	香港地区		高城 勝	Masaru Takashiro	+852-5335-1004	masaru.takashiro@hk.pwc.com
	台湾		奥田 健士	Kenji Okuda	+886-2-2729-6115	kenji.okuda@pwc.com
	韓国		原山 道崇	Michitaka Harayama	+82-10-6404-5245	michitaka.h.harayama@pwc.com
	シンガポール・ミャンマー		宮尾 祥平	Shohei Miyao	+65-8125-0594	shohei.m.miyao@pwc.com
	マレーシア		杉山 雄一	Yuichi Sugiyama	+60-3-2173-1191	yuichi.sugiyama@pwc.com
	タイ・カンボジア・ラオス		武部 純	Jun Takebe	+66-2-844-1000	jun.takebe@pwc.com
	ベトナム		今井 慎平	Shimpei Imai	+84-90-175-5377	shimpei.imai@pwc.com
	インドネシア		菅原 竜二	Ryuji Sugawara	+62-21-5212901	ryuji.sugawara@pwc.com
	フィリピン		東城 健太郎	Kentarō Tojo	+63-2-8459-2065	kentarō.tojo@pwc.com
	オーストラリア・ニュージーランド		諏訪 航	Wataru Suwa	+61-418-854-962	wataru.a.suwa@au.pwc.com
欧州・ アフリカ	インド・バングラデシュ・ネパール		土井 俊悟	Shungo Doi	+91-73030-88022	shungo.d.doi@pwc.com
	英国		小浜 淳子	Junko Kohama	+44-7841-803-661	junko.kohama@pwc.com
	フランス		猪又 和奈	Kazuna Inomata	+33-1-5657-4140	kazuna.inomata@avocats.pwc.com
	ドイツ		大矢 亮輔	Ryosuke Ohya	+49-1515-5907131	ryosuke.o.ohya@pwc.com
			藤井 隆行	Takayuki Fujii	+49-171-495-5987	takayuki.b.fujii@pwc.com
	オランダ		中村 聡一郎	Soichiro Nakamura	+31-6-18528154	soichiro.n.nakamura@pwc.com
	イタリア		前田 裕	Yu Maeda	+39-346-507-3014	yu.maeda@pwc.com
	ルクセンブルク		森本 薫	Kaoru Morimoto	+352-621-33-5157	kaoru.m.morimoto@pwc.lu
	ベルギー		横山 嘉伸	Yoshinobu Yokoyama	+32-473-910230	yoshinobu.yokoyama@pwc.com
	中東欧諸国*		山崎 俊幸	Toshiyuki Yamasaki	+420-733-611-628	toshiyuki.x.yamasaki@pwc.com
米州	ポーランド		ロルスキ 真美	Mami Rolski	+48-571-779-608	mami.rolski@pwc.com
	カナダ		北村 朝子	Asako Kitamura	+1-604-806-7101	asako.kitamura-redman@pwc.com
	米国 (M&A)		菊池 一彰	Kazuaki Kikuchi	+1-646-361-1917	kazuaki.x.kikuchi@pwc.com
	米国 (Tax)		清宮 陽二	Yoji Kiyomiya	+1-917-697-6448	yoji.kiyomiya@pwc.com
	米国 (Assurance)		川谷 智史	Satoshi Kawatani	+81-70-2284-3024	satoshi.s.kawatani@pwc.com
	メキシコ		加藤 幸博	Yukihiro Kato	+52-55-5263-6000	yukihiro.k.kato@pwc.com

※チェコ、ハンガリー、ルーマニア、ウクライナ、リトアニアほか (2026年8月1日現在)

日本企業の海外事業支援の詳細はWebをご覧ください。
<https://www.pwc.com/jp/ja/services/globalization.html>





本誌に関するご意見・ご要望ならびに送付先変更などのご連絡は、下記までお願いいたします。

jp_llc_pwcs-view@pwc.com

PwC Japan 有限責任監査法人

〒100-0004 東京都千代田区大手町1-1-1 大手町パークビルディング

Tel : 03-6212-6800 Fax : 03-6212-6801

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。各法人は独立して事業を行い、相互に連携をとりながら、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、法務のサービスをクライアントに提供しています。

© 2026 PricewaterhouseCoopers Japan LLC. All rights reserved.

PwC Japan Group represents the member firms of the PwC global network in Japan and their subsidiaries (including PricewaterhouseCoopers Japan LLC, PwC Consulting LLC, PwC Advisory LLC, PwC Tax Japan, PwC Legal Japan). Each firm of PwC Japan Group operates as an independent corporate entity and collaborates with each other in providing its clients with auditing and assurance, consulting, deal advisory, tax and legal services.

