

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類型によって、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まれます。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跡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。

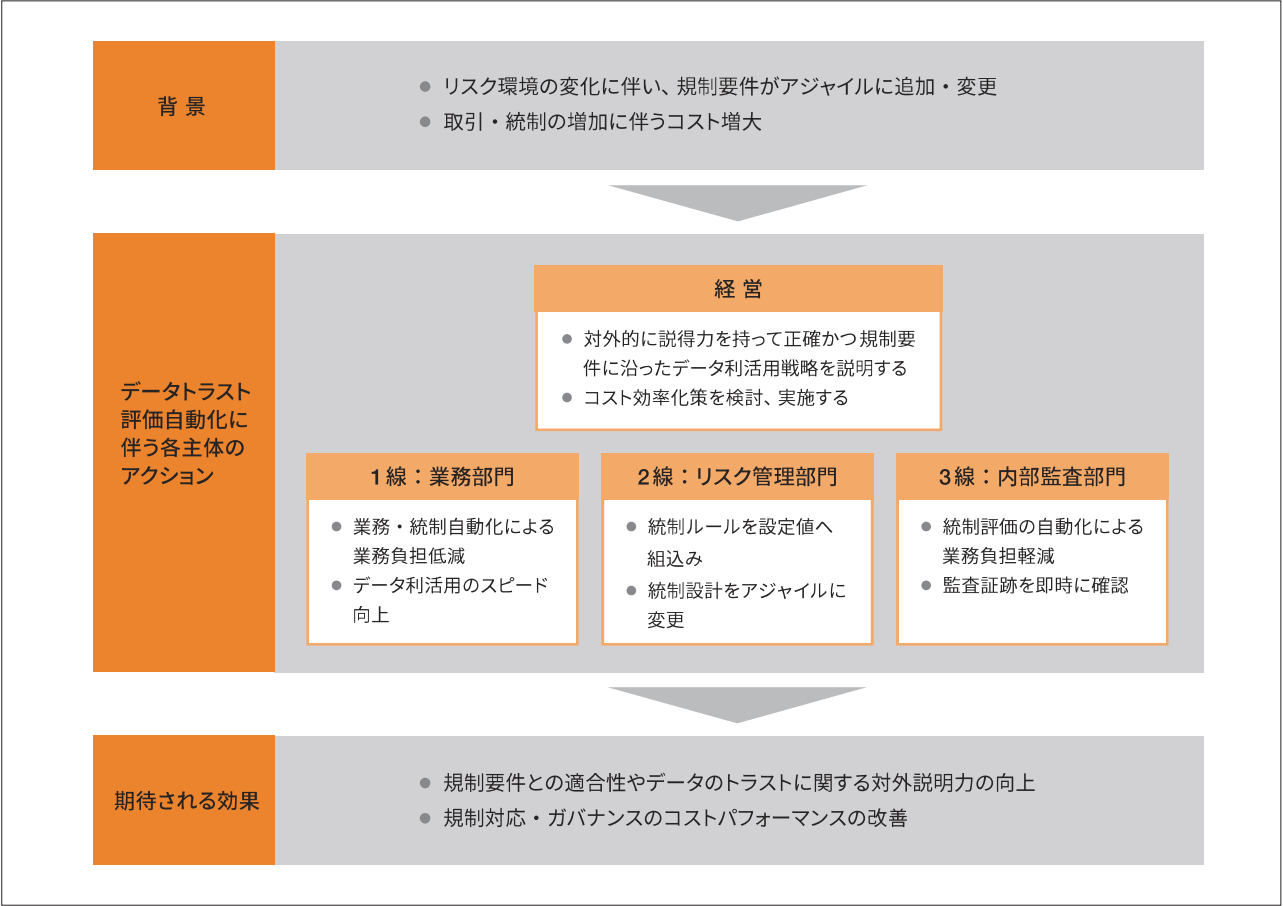
6

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