会計・監査への影響は？

1からわかる 暗号資産・ブロックチェーン

第❹回・終

ブロックチェーンを利用したビジネスに関する保証業務

安達知可良　EY 新日本有限責任監査法人　Blockchain center

《はじめに》

ブロックチェーンを暗号資産と同義と認識される方も少なくないだろう。代表的暗号資産であるビットコインの基盤技術として公表された論文（いわゆるサトシナカモト論文）により世間に知られることになったため，そのように想像されることは自然なことである。しかし，実は貿易金融，サプライチェーン間のデータ管理，トレーサビリティ管理等，ビジネスの場面において実証実験が進められている。

ブロックチェーンがビジネスシーンで利用される理由の1つとして，改ざんが困難な状態でデータを関係者間で共有できる特徴を持つことがあげられる。たとえば，国際間で多くの事業者が関与する貿易取引では，多様な書類（信用状，船荷証券，保険証券等）のやり取りが発生する。この煩雑な手続にブロックチェーンを活用することで，複数の関係者間で即時に情報共有が可能となり，かつデータ改ざん対策にもなる。

会社の情報システム，特に財務諸表の作成に関連する情報システムの運営を第三者（受託会社）に委託している場合，その会社（委託会社）の監査人（委託会社監査人）は受託会社の内部統制を含む提供業務を理解する必要がある。複数の会社に業務提供する受託会社の中には，自社の監査人（受託会社監査人）から保証報告書の提供を受け，委託会社に配布している場合もある。ブロックチェーンを利用したビジネスでは，複数の会社が利用者として関与するケースが多いことから，保証報告書を委託会社に配付する受託会社が少なくないと想定される。

本稿では，ブロックチェーンを利用したビジネスに係る保証業務について論じていく。その前提知識として，ブロックチェーンの技術的側面についても触れなければならないが，頁数の制約を鑑み技術要素を深掘りしすぎることは避けて最低限の範囲の紹介にとどめることとしたい。なお本稿における意見は私見が多く含まれており，必ずしも所属組織の正式見解ではないことを申し添える。

Ⅰ　ビジネスで利用されるブロックチェーン

1　ブロックチェーンの類型

従来型のシステムのようなサーバーにデータを一元管理する中央管理型のシステムと異なり，ブロックチェーンでは対等の関係である複数のコンピューターが，ネットワーク上で同期をと

〔図表1〕ノード参加制限の観点でのブロックチェーンの分類

分 類	主な特徴	運営主体の存在	取引の合意形成方法
パブリック型ブロックチェーン	誰でもノードとして参加可能 参加者の信頼性は求めない（トラストレス）	なし	参加者全員での合意形成
コンソーシアム型ブロックチェーン	ノードへ参加する組織を限定 参加者の信頼性が重要	限られた複数の参加者による運営	限られた複数の参加者による合意形成
プライベート型ブロックチェーン	運営組織以外の参加を認めない	運営組織（１社）	運営組織（１社）が取引確定

りながらデータを持ち合う。これがP2Pネットワークという形態であり，これに参加するノードと呼ばれるコンピューターは，取引データの保持やデータの正当性検証等，ブロックチェーンネットワークの運営の一部を担うことになる。

ブロックチェーンの設計次第では，ノードの参加に制限をかけることができる（**図表１**参照）。パブリック型ブロックチェーンは，不特定多数の者がノードとして参加して取引の正当性を検証している。従来型のシステムでは，信頼できる中央管理者の存在がデータの信頼の拠り所となっていたところ，パブリック型ブロックチェーンでは各ノードに信頼関係がなくても，テクノロジーや仕組みにより，正当な取引を関係者間で合意できるようになっている。

一方，コンソーシアム型とプライベート型のブロックチェーン（両者をあわせて，以下「非パブリック型ブロックチェーン」という。）の場合，ノードの参加者を制限し，彼らが運営主体となる点がパブリック型ブロックチェーンとの大きな違いとなる。データを共有する者を限定できるためビジネスで利用する際に採用されることが多い。この場合のデータの信頼性は，利用されている環境はもちろんのこと，運営主体の内部統制にも影響を受けることになる。

２　ブロックチェーンに係る保証報告書

ブロックチェーンの運営主体，つまり受託会社は，自社の内部統制の有効性に係る証拠の提出を委託会社から求められることも考えられる。多数の会社が利用する非パブリック型ブロックチェーンの場合，受託会社は自社の監査人（受託会社監査人）から提供される保証報告書を委託会社に配布することが効率的であると判断するかもしれない。受託会社監査人が財務諸表に係る重要な虚偽表示リスクの評価に係る保証報告書を発行する際，日本公認会計士協会（The Japanese Institute of Certified Public Announcements，以下「JICPA」という。）の保証業務実務指針3402「受託業務に係る内部統制の保証報告書に関する実務指針」（以下「保証実3402」という。）が指針となる。またJICPAは，非パブリック型ブロックチェーンを活用したビジネスの運営主体とする際の補助的な適用指針を示した保証業務実務指針3701「非パブリック型のブロックチェーンを活用した受託業務に係る内部統制の保証報告書に関する実務指針」（以下「保証実3701」という。）を2021年４月23日に公表した。

保証実3701が示す適用指針では，主に次の２点に焦点が当たっているといえる。以下ではこの２点に係る，受託会社監査人における主要な論点について見ていくことにする。

〔図表２〕ブロックチェーンの主要な基盤技術

P2Pネットワーク	▶クライアント／サーバー型とは異なり，「ノード」と呼ばれる各端末が対等の関係で直接通信する ▶単一障害点がない
ハッシュ関数	▶平文を一定の長さのデータ（ハッシュ値）に変換する技術 ▶１文字でも変わると異なる結果となる ▶ハッシュ値から平文への逆算はほぼ不可能
暗号技術	▶ブロックチェーンでは公開鍵暗号方式（秘密鍵と公開鍵の組合せ）を採用 ▶鍵を組み合わせ，暗号化とともに電子署名にも利用される

- ブロックチェーンを利用したビジネス特有のシステムの理解と証拠の入手に係る留意事項
- コンソーシアム型ブロックチェーンにおける受託会社の特定に係る留意事項

Ⅱ ブロックチェーンを利用したビジネス特有のシステムの理解と証拠の入手に係る留意事項

保証実3701ではブロックチェーンを利用しているシステムにおいて，受託会社監査人が通常理解すべき事項に係る留意点があげられている。紙面の都合もあるので本稿では主要な点に絞り紹介する。

１　ブロックチェーンで利用される基礎技術の理解

ブロックチェーンで利用される基礎技術は，そのためにできた新たな技術というものではなく，すでに広く使われているものの組合せであり，ある種「練れた」技術である。代表的なものとして図表２のものがあげられる。すでに触れたP2P ネットワークを除いた２点について以下で説明する。

⑴　ハッシュ関数

ブロックチェーンには，そのブロックチェーンが生成されてから現時点までのすべての取引データが記録されている。ブロックチェーンネットワークに参加するノードにより検証が行われた取引データは，一定期間でひとまとまりの「ブロック」に含まれ記録される。

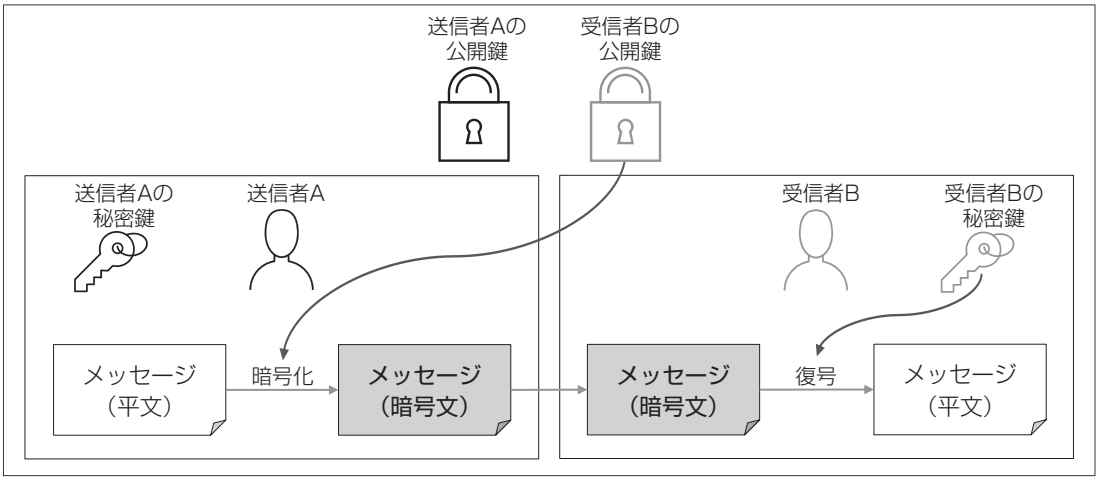
ブロックのヘッダーに，当該ブロックに内包された取引データをダイジェスト化したデータと，当該ブロックの直前に出来上がっていたブロックをダイジェスト化したデータを格納する。こうして直前のブロックとのつながりができるところから「ブロックチェーン」と呼ばれている（図表３参照）。

ダイジェスト化したデータをハッシュ値という。これは，指定されたデータを規則性のない固定長の文字列に変換するハッシュ関数により生成される。ハッシュ値は元データへの復元や，同じハッシュ値が得られる異なるデータの発見等が極めて困難であり，「一方向性」の特徴を持っている。元の値を求める方法は，ランダムの値をハッシュ関数に入れて当たりを求めるほかはない。

ブロックチェーン上の取引データを変更すると，当該ブロックのハッシュ値が全く異なる値に変更されるうえ，次のブロックにある，直前のブロックのハッシュ値との不一致も生じてしまう。そこで次のブロックにある直前のブロックのハッシュ値を書き換える必要性が生じるが，これを次のブロックが生成される短時間で実施することは困難であるうえ，すべてのノードから変更の合意を得ることも困難である（合意を得る方法については後述するコンセンサスアルゴリズムを参照）。ハッシュ関数はデータの改ざんを困難にしているといえる。

〔図表３〕ブロックの連関性に関するイメージ

〔図表４〕公開鍵暗号方式を利用した電文送信のフロー



⑵ 暗号技術

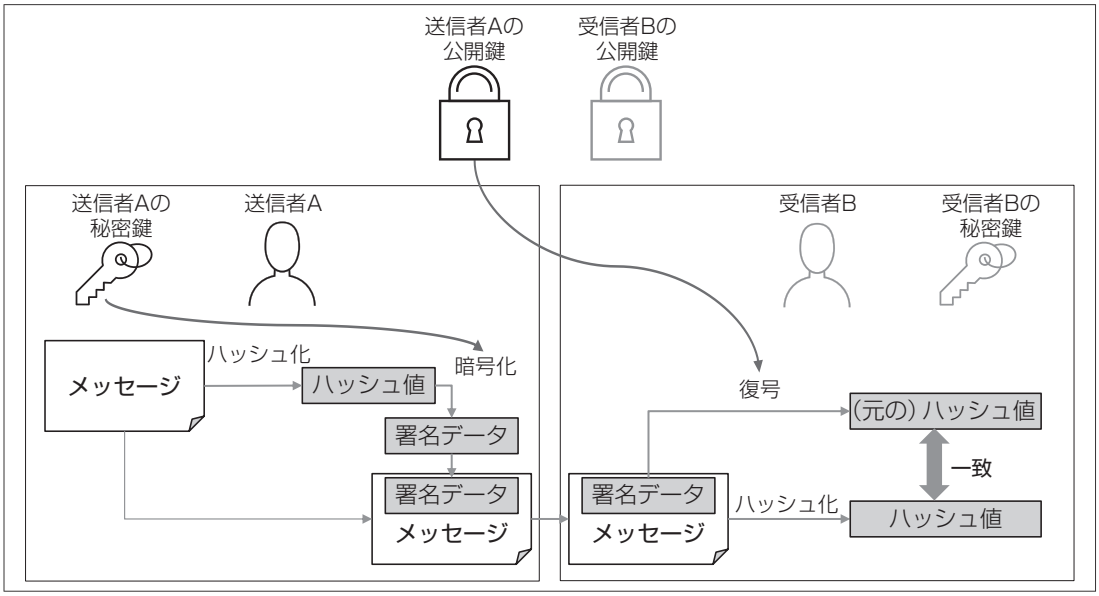
ブロックチェーンでは，秘密鍵と公開鍵のペアを利用する公開鍵暗号方式が使われている。公開鍵は文字どおり第三者に公開されており誰でも利用することができ，一方の秘密鍵は自分以外には公開しない運用を前提としている。公開鍵で暗号化したものは，ペアである秘密鍵のみが復号できる仕組みとなっている。メッセージ送信者が受信者の公開鍵で暗号化したメッセージは，その公開鍵のペアである秘密鍵を保持する者（通常は受信者）のみが復号できる，といったことが可能になる（図表４参照）。

公開鍵暗号方式は，秘密鍵で暗号化したものについてはペアとなる公開鍵でのみ復号できるという性質も持ちあわせている。この特性を利用したものが電子署名である。

送信者は自身が保持する秘密鍵で，「署名の元となるデータ」を暗号化して作成した「署名データ」をメッセージに付して送信する。秘密鍵は本人以外が持ち得ないものであることを前提とすれば，この署名データが送信者の公開鍵で復号できることをもって，送信者がそのペアとなる秘密鍵の持ち主であると受信者は判断できる。

なお，この「署名の元となるデータ」はメッセージのハッシュ値を使う。受信者は，署名データの復号結果と，受信したメッセージのハッシュ値が一致するか否かを比較することで，メ

〔図表５〕公開鍵暗号方式を利用したデジタル署名のフロー



ッセージの改ざん可能性を検証することもできる（図表５参照）。

⑶ 技術の危殆化に関する検討

利用している基礎技術は，現状の技術レベルが所与のものであることをもって有効であるが，一方で基盤技術が危殆（きたい）化する可能性について留意が必要である。たとえば，暗号技術やハッシュ関数は，効率的な暗号鍵の解読法の考案や，圧倒的計算能力を持つ機器（量子コンピューター等）の登場等により，現在前提としているシステムでは安全性が担保できなくなるリスクが考えられる。受託会社監査人としては，技術トレンドについて常に把握しておくことが重要となる。

２ コンセンサスアルゴリズムとノードの役割に関する理解

⑴ コンセンサスアルゴリズム

ブロックチェーンに取引データを記録する際の，データの真正性を担保するためのルールをコンセンサスアルゴリズムという。これはブロックチェーンネットワークに参加するノードが，どの取引データが正当なもので，どれを共有するかについて参加者の合意を得るためのプロセスである。コンセンサスアルゴリズムにはいくつか種類があり，どのアルゴリズムが採用されているか理解することは重要である。非パブリック型ブロックチェーンでは，Practical Byzantine Fault Tolerance（PBFT）がコンセンサスアルゴリズムとして採用されることが多い。保証実3701でも PBFT を利用するブロックチェーンを想定したものとなっているため，以下では PBFT について触れていく。

⑵ PBFT におけるノード種別と評価における留意事項

PBFT では参加するノードの役割を分担させることができる。ブロックチェーンプラットフォームにより役割や呼称は異なるものの，保証実3701で整理している３つのノード種別（図表６参照）を前提に検討することがわかりやすい。

⑶ ノード対象範囲に関する留意事項

コンセンサスアルゴリズムでは，データの検

〔図表６〕PBFT に参加するノード種別

ノード種別	主な機能	記述書に含めるかどうかの留意点
リーダーノード	▶発生したトランザクションデータを受け取り，承認ノードに転送する ▶承認ノードの一部がリーダーノードとなる	▶ブロックチェーンにデータを供給する重要な役割であり，通常は記述書に含める
承認ノード	▶リーダーノードから転送された取引データを，コンセンサスアルゴリズムに従い検証，承認する ▶承認されたデータを保有する	▶データの検証，承認の重要な役割を果たすため，通常は記述書に含める ▶委託会社が承認ノードを所有，管理している場合，委託会社の相補的な内部統制を理解すべきである
非承認ノード	▶データの検証，承認には関与しない ▶データの監視，閲覧などのデータを利活用目的であることが多い	▶記述書の対象外にすることが多い ▶保有しているデータの管理に係る内部統制を評価することを目的として記述書の対象に含めることも考えられる

証・承認等を主体的に行う**承認ノード**が重要な役割を果たすため，通常は「受託会社のシステムに関する記述書（以下「記述書」という。）」に含まれることになる。一方，**非承認ノード**はデータの検証・承認には関与しないため，記述書の対象外とすることが多いものと考えられる。受託会社監査人は，受託会社における参加ノードの実態と記述書におけるノードの範囲について十分に理解する必要がある。

コンセンサスアルゴリズムに参加できるノードの数や種類を設計できる非パブリック型ブロックチェーンにおいて，運営主体の一部の参加者が有利となるようなバランスを欠いた設計の場合，サービス利用者の信頼を損ねることになる。受託会社監査人は，当該ブロックチェーンを維持するために必要となるノード構成やその他の条件等を含め，受託会社のシステムを理解することが重要となる。

また，ブロックチェーンでは，全ノードが一斉にデータの同期をとるわけではなく，ノード間で更新の時差が生じ，各ノードで保有しているデータの異なるタイミングが生じうる。そのため，各ノードのデータ同期タイミングや監査証拠を入手するノードの性質について理解しておくことは，運用評価手続での証拠の入手を計画する際に役立つ。

３　秘密鍵とウォレットの管理に関する理解

⑴　秘密鍵とウォレット

ブロックチェーンの世界では秘密鍵を所持することが本人を証明する手段となる。これは逆にいえば，秘密鍵が盗まれてしまうと自身の権利を主張できないばかりでなく，搾取した者が「なりすまし」を犯すリスクがある。したがって，ブロックチェーンのアクセス管理という観点において秘密鍵管理は重要な役割を担っている。

秘密鍵は通常**ウォレット**で管理される。ウォレットにはいくつか種類がある（**図表７**参照）が，ここでは代表的なものを紹介する。

USB メモリ等の専用の物理媒体にて電子的に秘密鍵を管理するハードウェアウォレットと呼ばれる。このタイプは通常ネットワークから切り離して管理しているため，**コールドウォレット**と分類される。

一方，ネットワークに接続された環境で管理されるものは**ホットウォレット**と分類される。自身の PC にインストールするウォレット管理ソフトであるデスクトップウォレット，スマートフォンアプリであるモバイルウォレット等が含まれる。

また，ウェブ形式で事業者がサービス提供するウェブウォレットと呼ばれるものもある。オンライン上からウェブサイトにアクセスするだ

〔図表7〕秘密鍵の管理方法の観点ウォレットの種類

ウォレットの種類	ホット／コールド	秘密鍵の保管場所	主な特徴
ペーパーウォレット	コールド／ウォレット	紙に記載	▶ネットワークから完全に分離されているが，残高確認等の際，ネットワークに接続されている他の媒体を利用する必要がある ▶紛失のリスクがある
ハードウェアウォレット	コールドウォレット	専用の物理媒体（USB メモリ等）	▶ネットワークから完全に分離されているが，残高確認等の際，ネットワークに接続されている他の媒体を利用する必要がある ▶紛失のリスクがある
デスクトップウォレット	ホットウォレット※1	自身のローカル PC	▶ウォレット機能を有するソフトウェアを自身の PC にインストールして利用する
モバイルウォレット	ホットウォレット	自身のスマートフォン	▶自身のスマートフォンにウォレット機能を有する専用アプリをダウンロードして利用する
ウェブウォレット	ホットウォレット※2	業者による管理	▶ブラウザ経由で業者（暗号資産交換所等）が管理しているウェブ上のウォレットを利用する

※1　ネットワークから切り離してコールドウォレットとして利用できるものもある。
※2　コールドウォレットを併用する等の対策をしている業者も存在する。

けで利用できるため，利用者の負荷軽減や利便性の高さがある一方，秘密鍵管理をウォレット事業者が行うため，その安全性は当該事業者の管理態勢に影響を受ける。

⑵　ウォレットの評価における留意事項

ホットウォレットは，ブロックチェーンネットワークに接続された環境に秘密鍵を置いているため，アクセスしやすいというメリットがある。タイムリーな対応が必要な場合には有益である。半面，常時インターネットに接続された環境に秘密鍵を置くことはサイバー攻撃等により搾取されるリスクが高まる。サイバー対策に重点を置くことはもとより，搾取されたとしても大きな影響を及ぼさないようリスク分散対策も望まれる。たとえば，複数の秘密鍵の組み合わせによる電子署名を求めるマルチシグ（マルチシグネチャー）といった技術を利用することによりリスク分散を図るケースが考えられる。

一方コールドウォレットの場合，無断で使用されないように内部管理態勢を構築することが重要である。一般的に金庫や施錠できるロッカー等で保管することになるが，利用・返却の記録を取り，実施状況をモニタリングする，といった貸出管理を行うことが望ましい。コールドウォレットの保管場所を社内の限られた者にのみ公開する対策も有効であるが，この際受託会社監査人はコールドウォレットの保管体制を評価することが容易でない場合もあるため，十分な証拠を入手する方法を検討する必要がある。

Ⅲ　コンソーシアム型ブロックチェーンにおける受託会社の特定に係る留意事項

複数の会社が共同でシステムを運営するコンソーシアム型ブロックチェーンでは，会社間の関係は従来型の垂直的な受託・再受託の関係ではなく，並列的な関係として識別したほうが合理的であることも考えられる。各社がシステム運営の主要な役割を果たす場合，運営に関わるすべての会社を受託会社として取り扱うと想定

されるが，非承認ノードしか持たない会社が運営主体として関与している場合，当該会社を受託会社に含めないとすることも考えられる。また，委託会社自らがノードを立てて参加する場合，当該ノード管理は委託会社の相補的な内部統制と位置づけられることも考えられる。受託会社監査人は，コンソーシアム型ブロックチェーンにおける受託会社の範囲の妥当性について十分検討する必要がある。

保証報告書に求められる「受託会社確認書」は，受託会社監査人が対象となる受託会社すべてから受領する必要がある。この場合，連名の受託会社確認書を受領する場合もあれば，各社から個別に受領する場合も考えられる。

複数の組織が運営に関与するコンソーシアム型ブロックチェーンでは，規定されたルールを関与者に徹底させるためのガバナンスが構築されているかどうかは，受託会社監査人として重要な観点となる。システムの理解には，ここまで触れてきた観点以外にも，たとえば次のものが含まれる。

- ノードの選定，追加，変更，および削除に関するルール
- 通常の取引とは異なるブロックチェーン上のデータの操作をする特例処理の有無，またそれを提供する機能の概要および実行に関するルール
- コンソーシアム参加者に要求されるセキュリティ条件等およびその維持に関する監視の方法
- スマートコントラクトを利用する場合のその内容と利用状況

《おわりに》

いま話題になっているメタバース，NFT，Web３等はいずれもブロックチェーン技術との関わりがある。こうしたサービスが近い将来に社会基盤に取り込まれると目されるなか，安心・安全に活用するためには技術的基盤に対する「信頼」が不可欠である。そのためには運営主体の内部統制を含めた業務の透明性が重要となる。保証報告書はそのための有効な手段の１つであり，ブロックチェーン技術を利用したシステムが社会実装されるにつれ，今後その必要性は高まってくるものと想定される。