AICPA

受託会社に関するSOC業務[1]における

ブロックチェーンの使用がもたらす影響

[1] 「System and Organization Controls for Service Organization Examinations」を指し我が国においては、受託業務に係る内部統制の保証業務と呼ばれることが多い。本文書においてはSOC業務と記載することとしている。

目次

序説

「ブロックチェーン」[2]とは、暗号化技術により結び付けられた複数のブロックに整理された、取引に関するデジタル記録の増大し続けるリストを意味する。各ブロックには、その前のブロックを*暗号化した*[3]ハッシュと、ブロックチェーンのユーザーが以前のブロックの改ざんを容易に検出できるようにするその他の情報が含まれている。ブロックチェーン*分散型台帳*は、*P2P ネットワーク*全体で取引を共有し、それによって参加者（事業体、企業、組織又は個人）は集中清算機関を必要とせずに記録の読み取りや書き込み、及び取引の確認を行うことができる。

ブロックチェーンネットワークは、受託会社がそのシステム内で使用できる他の技術とは異なる多くのユニークな特徴を有している。個々の特徴はブロックチェーンネットワークの種類により異なるが、一般的に以下のような特徴を有する。

- データ、情報又はコンテンツを、セキュアで検証可能かつ最新であり、かつ信頼可能で正確であるよう構造化できる。
- 暗号化関数の応用により、不正な変更や破壊のリスクを減らす。
- 取引記録に参加者がアクセスできるようにしたり、要求に応じて利用できるようにしたりする。
- 参加者が取引データを線形で時系列的な順序で更新及び記録して、取引の記録と監査証跡を残せるようにする。
- 第三者がデータを保持する必要性がない。

以上の、及び本文書の「ブロックチェーンのユニークな特徴」セクションで論じたその他の特徴により、ブロックチェーンの使用は、受託会社にとって新たな業務（例えば、新システムを開発してサプライチェーンの効率性を支援する等）の提供や、委託会社に対する既存業務の提供コストを削減する（例えば、照合に費やす時間の除去、取引の各当事者が保持している複数の台帳間の相違の調査と解消、業務記録に対する不正な変更のリスクの削減、業務記録が必要な際に利用できないリスクの削減）機会を提供する可能性がある。

2 「ブロックチェーン」という言葉は、しばしば「分散型台帳」と同義で用いられるが、必ずしもすべての分散型台帳がブロックチェーンであるわけではない。本文書は分散型台帳一般ではなく、ブロックチェーン分散型台帳のみに焦点を当てている。

3 本文書において、各関連用語は初出の際に斜体で記載され、ブロックチェーン及びデジタル資産に関連した当協会のすべてのコンテンツに関する参照資料として作成されたブロックチェーン共通用語集において定義されている。

しかしながら、ブロックチェーン技術を使用することで得られる機会は、受託会社とその委託会社にとってリスクの増大ももたらすことになる。受託会社のマネジメントは、そうしたリスクを許容可能な水準まで軽減する内部統制のデザイン及び適用を通じて、それらリスクの特定、評価、文書化、及びそれらリスクへの対応に責任を負う。

それらのリスクと、それらリスクの軽減のために受託会社のマネジメントにより実施される内部統制を理解することは、SOC 1®（SOC for Service Organizations:(ICFR)）（受託会社に関する SOC：（ICFR））業務）、又は SOC 2®（SOC for Service Organizations: Trust Services Criteria）（受託会社に関する SOC：Trust サービス規準）業務（以下、集合的に「受託会社に関する SOC 業務」という）を実施する受託会社監査人にとっても極めて重要である。本書は SOC1 及び 2 の業務を特に取り扱うが、サプライチェーン SOC 業務の実施者にとっても本書は有益となる可能性がある。実施者はそれら業務の指針を、AICPA 指針「*SOC for Supply Chain: Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System*」（*サプライチェーンに関する SOC：生産、製造又は流通システムにおけるセキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに係る内部統制の保証報告書*）で確認できる。

ブロックチェーンは比較的新しい技術であるため、受託会社監査人はブロックチェーンの仕組みについて限られた経験しか有していない可能性がある。加えて、この技術が複雑であることから、受託会社がブロックチェーンを使用している場合には、当該受託会社に関する SOC 業務の実施に求められる能力はより高度なものとなる。そうした業務を受託する前に、受託会社監査人は監査チームが、ブロックチェーンに関する十分な知識を含め、職業的専門家としての基準及び適用される法令等に従って業務を実施する上で適切な資格と能力を有していることについて納得すべきである。納得できない場合、受託会社監査人は、業務の実施を支援する上で関連する知識及び技能を具備した専門家の利用が必要であると決定するかもしれない。この点については、本文書の「監査チームが適切な資格及び能力を具備しているかどうかの判断」と題したセクションでより詳細に論じている。

「ブロックチェーン」とは、暗号化技術により結び付けられた複数のブロックに整理された、取引に関するデジタル記録の増大し続けるリストを意味する。各ブロックには、その前のブロックの暗号化されたハッシュと、ブロックチェーンのユーザーが以前のブロックの改ざんを容易に検出できるようにするその他の情報が含まれている。

本文書の目的と構成

ブロックチェーンが受託会社のシステムの不可欠の要素になっている、又は当該システムがブロックチェーンとインターフェースで接続されている場合、ブロックチェーンのユニークな特徴とそれが受託会社及び委託会社にもたらすリスクを理解することにより、受託会社監査人は (a) そうしたリスクを特定及び評価し、(b) 受託会社監査人としての意見を裏付ける上で十分で適切な証拠を入手するための手続をデザインし、実施することができる。

本文書の目的は二つある。すなわち、ブロックチェーンのユニークな側面のいくつかについて受託会社監査人を啓発するとともに、委託会社への業務の提供を目的としたシステムにおいてブロックチェーンを使用することが SOC 報告書にもたらす影響を論じることである。

これらの目的を達成するため、本文書は二部構成となっている。

本文書パート 1

- 複数の種類のブロックチェーンネットワークに関する議論やそのユニークな特徴等、ブロックチェーンの概要を紹介する。
- ブロックチェーンの使用に固有のリスクを特定する。ただし、本文書はそうしたリスクに対処するために受託会社が適用できる特定の内部統制を識別しておらず、受託会社監査人がそうした内部統制のデザイン又は運用状況に関する証拠を入手するために実施する可能性のある手続についても説明していない。

本文書パート 2

- 受託会社に関する SOC 業務に適用される職業的専門家としての基準及び規準の概要を示す。
- 監査チームが、適切な場合における専門家の利用を含めて、ブロックチェーンに関する知識並びに業務を実施するための技能及び資格を具備する必要性について論じる。

本文書の目的は二つある。すなわち、ブロックチェーンのユニークな側面のいくつかについて受託会社監査人を啓発するとともに、委託会社への業務の提供を目的としたシステムにおいてブロックチェーンを使用することが SOC 報告書にもたらす影響を論じることである。

- ブロックチェーンが受託会社のシステムに不可欠であり、インターフェースを通じてこのシステムに接続されている場合における、当該システムに関する受託会社監査人の理解に関する独特の要素について説明する。
- ブロックチェーンを含む受託会社のシステムに関する記述書、内部統制のデザインの適切性、及びタイプ 2 業務における内部統制の運用状況に関する意見を形成する際における独特な検討事項について論じる。

また、本文書には以下の付属資料が含まれる。

- 付録 A には、受託会社が、委託会社に対する業務の提供のために使用されるシステムにおいてどのようにブロックチェーンを使用できるのかについての例を収めている。
- 付録 B には、ブロックチェーンについてより詳しく学びたい受託会社監査人のために、追加的な AICPA の資料をリスト化している。

本文書では、保証業務に関する基準に基づくブロックチェーンの検証について取り扱っていない。ただし、もし業務実施者がそうした検証業務の提供を担当した場合、本文書の情報の一部は、業務実施者が AT-C セクション 205「*Assertion-Based Examination Engagements*」(*主題情報の提示を受ける検証業務*)に沿って業務の実施方法を決定する上で有益となる可能性がある。

ブロックチェーンの概要

ブロックチェーンネットワークは、複数のデバイス（PC、ノート PC 又はサーバー等。ノードと呼ばれることが多い）にわたる取引の記録に使用できる、デジタルの、一元的でない分散化された台帳である。取引を遡及的に改変しようとする試みがあれば、参加者は警告を受け、然るべく対応（例えば、提案されている改変の理由について理解し、それに同意するかどうかを判断する等）できる。

ブロックチェーンは、参加者に取引の台帳への書き込みや台帳からの読み取りを可能にし、お互いに知り合ったり信頼したりする必要なしに、独立して取引を検証できるようにする。かつては集中型台帳で保持されていた情報をコンピューターによるネットワーク全体に分散させることにより、ブロックチェーンは第三者の媒介（例えば、金融取引における銀行、土地の権利者や車両の所有者の記録における法廷書記官、あるいは証券取引の決済における決済会社等）の必要性を減少させる可能性がある。

異なる種類のブロックチェーンの分類[4]

ブロックチェーンネットワークには、以下を含む複数の異なる種類がある。

- **パブリック型ブロックチェーン（自由参加型）：**インターネットにアクセスできる参加者なら誰でもブロックチェーンに参加し、取引を読み取り、書き込み、送信できる。参加者が取り得るいかなるアクションに関しても許可は必要とされない。パブリック型ブロックチェーンは、取引をすべてのフルノードに分散させる[5]。デジタル資産の売買等の取引に用いられる最も一般的な種類のブロックチェーンである。最も有名で広く保有されているデジタル資産である*ビットコイン*は、パブリック型ブロックチェーンの一例である。しかし、パブリック型ブロックチェーンに関連するリスクの一部が理由で、企業間（B2B）商取引では他の種類のブロックチェーンに比してあまり用いられない。

- **プライベート型ブロックチェーン（許可型）：**お互いに知っており信頼している参加者のグループのために、セキュアで隔離された環境に存在する。参加者のアクセス権は、参加者間の合意に従って割り当てられる。参加者が許可制のため、合意に従って許可されたものしか閲覧できない。

  特定のプライベート型ブロックチェーンに関しては、ブロックチェーンの管理者がプロトコル[6]を変更する権能を有する中央機関を指定する場合がある。プライベート型ブロックチェーンの主要な特徴の一部がパブリック型ブロックチェーンに固有のリスクを軽減するため、営利事業は多くの場合、B2B 取引の記録と処理にプライベート型ブロックチェーンを使用する。

- **ハイブリッド型ブロックチェーン：**パブリック型ブロックチェーンとプライベート型ブロックチェーン両方の特徴を利用する。ハイブリッド型ブロックチェーンでは、ブロックチェーンに記録された情報へのアクセス及び他の機能が特定の参加者に対して制限される可能性がある一方、その他の情報は全参加者が利用できる。例えば、ハイブリッド物流ブロックチェーンにはプライベートコンポーネント（すなわち、読み取り、書き込み、取引、及びブロックチェーンプロトコルの変更に対する投票を許可されているごく少数の大規模なサプライヤーが利用できる情報と機能）とパブリックコンポーネント（すなわち、取引ステータスのクエリやレポート生成といった、多数の再委託業者、顧客、及びより小規模なサプライヤーが利用できる情報と機能）の両方が含まれる場合がある。

4 （訳註）保証業務実務指針 3701（以下「保証実 3701」という。）における非パブリック型ブロックチェーンの類型による定義は、ブロックチェーンの管理主体によって分類されている一方、本稿における定義は、参加者を主体として分類されている。このため、保証実 3701 における「コンソーシアム型ブロックチェーン」は、本稿での「プライベート型ブロックチェーン」及び「ハイブリッド型ブロックチェーン」の双方に含まれる。

5 フルノードのみがすべてのブロックチェーン取引のコピーを有しており、それ以外のノード（*軽量ノード*と呼ばれる）は取引の正当性を検証するためだけにブロックヘッダーをダウンロードする。

6 プロトコルとは、取引の無効化やすべての参加者に影響を与える可能性のある他の決定の仕方を含め、ブロックチェーンの運用方法を規定した共通のコミュニケーションルールである。

ブロックチェーンのユニークな特徴

個々のブロックチェーンネットワークの特性は当該ブロックチェーンの種類によってさまざまであるが、本セクションではブロックチェーン技術のユニークな特徴のいくつかについて説明する。ブロックチェーンは分散型台帳であるが、ブロックチェーンでの取引は取引ブロックとしてグループ化され、時系列に整理される点で他の種類の分散型台帳とは区別される。ブロックは相互に結び付いており、暗号化技術を使用してセキュア化される。ブロックチェーンは本質的に、取引の連続した台帳である。データの追加のみが可能で、以前に記録された取引を変更や消去することが大きく制限された構造となっている。参加者はコンセンサス・メカニズムを使用して、ブロックチェーンへの取引の追加に同意する。*バリデーター*は取引を収集し、暗号機能を実行してそれらを検証する。コンセンサスが実現し、取引が承認されると、新しい取引ブロックが台帳に追加され、各フルノードに自動的に分散化される。

ブロックチェーンは分散型台帳であるが、ブロックチェーンでの取引は取引ブロックとしてグループ化され、時系列に整理される点で他の種類の分散型台帳とは区別される。ブロックは相互に結び付いており、暗号化技術を使用してセキュア化される。ブロックチェーンは本質的に、取引の連続した台帳である。

アクセス・コントロール・メカニズム

アクセス・コントロール・メカニズムとは、承認されたユーザー（個人、組織、参加者、メンバー、デバイス、ユーザー、ノード等）にのみアクセスを許可するとともに、不正なアクセスを防止・検知することにより、ブロックチェーンネットワークとその内部にある記録のセキュリティを保全する手段である。ブロックチェーンにおけるアクセス・コントロール・メカニズムには*暗号鍵*が含まれ、ハードウェア又はソフトウェア機能、運用手順、管理手順、及びそれらのさまざまな組み合わせも含まれる場合がある。アクセス・コントロール方法は、パブリック型ブロックチェーンとプライベート型ブロックチェーンの主要な相違の一つである。

- **パブリック型ブロックチェーンのアクセス・コントロール・メカニズム：**パブリック型ブロックチェーンには、中央管理者やセキュリティ管理者による承認を得ることなく、誰もが参加及びアクセスできる。パブリック型ブロックチェーンでのアクセス・コントロール・メカニズムは*ウォレット*であり、これによって参加者は新たな記録を書き込み、他のすべての参加者が作成した既存のすべての記録を読み取れる。誰がウォレットを取得できるかについての制限はない。
- **プライベート型ブロックチェーンのアクセス・コントロール・メカニズム：**プライベート型ブロックチェーンへのアクセスは、ユーザー・アクセス・ポリシー及びアクセス・コントロール・リストによりネットワークレベルで、ブロックチェーンのセキュリティ管理者によって各ユーザー及びリソースに付与される個々の許可によりアプリケーションレベルで、それぞれ設定される。

コンセンサス・メカニズム

ブロックチェーン内における記録の完全性は、ブロックの検証とブロックチェーンへの追加に用いられるコンセンサス・メカニズムに依存する。コンセンサス・メカニズムとは取引の認証・検証に用いられる手法をいう。コンセンサス・メカニズムは、*コンセンサス・アルゴリズム*[7]とプロトコルを使用してコンセンサスを実現する方法を定義する。

7 アルゴリズムは、バリデーターが相互に信頼し合う必要なく同一バージョンのブロックチェーンに同意できるようにする計算の実行に関する仕様として用いられる。

コンセンサス・メカニズム（続き）

コンセンサス・メカニズムにはさまざまな種類があり、そのすべてが、受託会社とそのビジネス相手にとって異なるリスクをもたらす。受託会社監査人は、受託会社のシステムが使用するコンセンサス・メカニズム及びその機能の仕方、関連リスク、並びにそれらリスクを軽減するために受託会社が実施している内部統制を理解する必要がある。

データの完全性

ブロックチェーンのコンセンサス・メカニズムは、過去に記録された取引に対する変更を検知し、そうした変更がネットワーク上のブロックチェーンの他のコピーに分散化されるのを防止することによって、ブロックチェーン内に記録された取引の完全性の保存に寄与する（通常、以前に記録された取引は変更できないが、一部のケースでは、例えば*ハードフォーク*がある場合やプロトコルが修正記入を許可している場合等、取引の当事者又はフルノードが変更に合意した場合において、コンセンサス・メカニズム及びプロトコルが以前に記録された取引に一定の変更を許可する場合がある）。

スマートコントラクト

スマートコントラクトは、ブロックチェーン内のデータを利用して、スマートコントラクトの契約当事者により合意された一連のルールを実行するコンピュータープログラムである。スマートコントラクトのルール（取引処理のルール等）は、合意や取引の履行を促進し、検証し、執行することを意図している。実行されると、取引結果はブロックチェーンに記録される。スマートコントラクトは人間による介入なしに機能し得るが、取引当事者の承認後に取引が可能になるルールを含む場合もある（例えば、購買請求を承認すると注文書となる、受領書を承認すると請求書に対する支払いが行われる等）。

多くの場合、スマートコントラクトは B2B ブロックチェーンの最初のブロックを形成する。他のブロックチェーン取引と同様に、通常、スマートコントラクトで実行された取引は不可逆である。（スマートコントラクトの一部には、誤って実施された場合や特定の条件を満たした場合に取引の無効化を可能にする機能が含まれる可能性がある。）なお、「受託会社によるブロックチェーンの使用に関連するリスク」のセクションで論じるように、スマートコントラクトに関連する重大なリスクが存在する。

モノのインターネット（IoT）

モノのインターネット（IoT）を使用してデータを収集するさまざまなブロックチェーン・アプリケーションにスマートコントラクトが含まれる可能性がある。例えば、生鮮食品が特定の温度及び湿度水準を維持した環境で用意、輸送、保管及び販売されていることを検証し、人間による消費に適していることを保証する目的でスマートコントラクトが使用される場合がある。IoT センサーを複数の地点に設置して、それら指標のほか、特定の場所、ベンダー、サプライヤー、取扱業者、バッチ番号、その他の関連情報を把捉できる。その結果をスマートコントラクトに報告できれば、確立されたパラメーターに従って維持されなかった安全でない食物について、自動的に警告を発することができる。このデータをブロックチェーンに書き込む際、ブロックチェーン内の承認された参加者は食品の状況その他の関連情報を確認できる。こうした、ほぼリアルタイムの透明性によって、サプライチェーンに関与するすべての当事者は食品の状況を確認し、データの正確性と完全性を検証できるようになる。なお、「受託会社によるブロックチェーンの使用に関連するリスク」のセクションで論じるように、データを IoT デバイスから取得するオラクル（次のセクションを参照）から伝達されたデータを使用するスマートコントラクトは、リスクや危殆化のポイントが集中しやすい可能性がある。

オラクル

ブロックチェーンとスマートコントラクトは、スマートコントラクトの中核となるコンピューターコードの実行に必要な外部情報を取得する内部メカニズムを有していない。そのため、ブロックチェーンオラクルはスマートコントラクトへのインプットとして、ブロックチェーン外のソースからの取得した情報を利用する。オラクルは、外部情報を記録する IoT デバイス等、外部ソースからの情報を伝えるコネクションを確立し、その情報をスマートコントラクトに伝達する。スマートコントラクトのみではブロックチェーン内のデータしか取得できないため、オラクルがなければスマートコントラクトの有用性は限定的となる。オラクルの中には、データをブロックチェーン外の目的地に伝達できるものもある。受託会社のブロックチェーンによるそうしたオラクルの使用について、概念化された例を以下に示す。

受託会社のブロックチェーンにおけるオラクルの使用例

ブロックチェーン

課題:
シトラス加工工場はコストを削減する必要があり、シトラスを供給する栽培業者は果実の納品から支払いまでの時間の短縮を望んでいた。

ブロックチェーンによるソリューション:
上記の目的を達成するため、工場と栽培業者は、工場に納品される果実に関する金融及びサプライチェーンに関するデータを提供し、栽培業者に対する果実の対価の適時での支払いを円滑化する受託会社である「OJ ブロックチェーン・コンソーシアム」(OJBC)を組織した。

栽培業者は、各工場に納品する果実の量及び品質についてのデータを、各栽培業者に支払われる価格と共に受け取る。工場は在庫、買掛金、及び栽培業者に対する支払いを記録するために利用するデータを受け取る。栽培業者に提供される情報は、栽培業者の売掛金、収益、及び銀行口座に記録される。これら取引はすべてブロックチェーンに記録されるので、情報はすべての参加者が確認できる。そのため、全参加者にデータの正確性及び完全性を検証する機会がある。

OJBC の最初のブロックはスマートコントラクトであり、それには栽培業者に対し、工場に果実が納品された時点で、栽培業者、果実販売業者及び加工業者の組合(「組合」)が管理するデータベースに報告される市場価格と、納品された果実の品質及び数量に基づいて支払いを行うというルールが含まれている。このシナリオには以下の 4 つのオラクルが関与している。

1 →
1 つ目のオラクルは、組合のデータベースにクエリを行い、現在の市場価格を返す。

2 →
2 つ目のオラクルは、果汁内の可溶性糖含有量(第 1 の品質尺度)を報告するデバイスに問合せを行う。

3 →
3 つ目のオラクルは、甘味比(第 2 の品質尺度)を計測するデバイスにクエリを行う。

4
4 つ目のオラクルは、納品されたオレンジの合計重量を報告する電子デジタル重量計にクエリを行う。

果実が工場に納品される際、4 つのオラクルが情報をほぼリアルタイムでスマートコントラクトに伝達する。

スマートコントラクトが栽培業者に支払われる金額を計算し、工場の銀行口座から ACH を通じて、栽培業者の銀行口座に振り込む。

ブロックチェーン、スマートコントラクト、そしてオラクルがなければ、取引の当事者たちは関連情報を照合し、相違を調査・解消しなければならない。OJBC が構築される以前、このプロセスは多くの場合 1 カ月又はそれ以上を要し、その分、栽培業者への支払いが遅れていた。

スマートコントラクトへの情報伝達に使用可能な複数の種類のオラクル（ソフトウェアベース、ハードウェアベース及び人間によるもの）がある。多くの場合、使用されるオラクルの種類は情報伝達が (a) コード又は物理的デバイスにより開始されるかどうか、 (b) アウトフローであるかインフローであるか、それとも両方であるか、 (c) 単一の機関によって管理されるか、それとも複数の機関によって管理されるか、又は (d) これらの組み合わせであるかに依存する。

各種のオラクルのリスクは、本文書の以下のセクションに記述している。

受託会社によるブロックチェーンの使用に関連するリスク

本セクションでは、受託会社が委託会社へのサービス提供を目的としたシステム内でブロックチェーンを使用する際における、ブロックチェーンの使用に関連したリスクの一部を取り上げる。前述したように、それらのリスクを理解することは、SOC1 業務における受託会社による内部統制の目的の達成、又は SOC2 業務におけるサービスコミットメント及びシステム要求事項の達成に影響を及ぼす、受託会社監査人によるリスクの特定及び評価にとって、極めて重要となる。本セクションで取り上げるリスクは包括的であることを意図しておらず、これら以外にも、特定の SOC 業務に関する特有の事実及び状況に関連するリスクが存在する可能性がある。

受託会社に関する SOC 業務において、受託会社監査人は (a) 主題（システムに関する記述書、内部統制のデザインの適切性、及びタイプ 2 業務における内部統制の運用状況）に重要な虚偽表示があるというリスクを特定し評価するため、及び (b) それらのリスクに対応する手続をデザインするために、受託会社のマネジメントがデザインし実施した内部統制を含め、システムについての理解を得る。受託会社がブロックチェーンを使用している場合、その使用に関するリスクは、受託会社監査人による当該システムの理解及び重要な虚偽表示のリスクの評価に関連する。

ほとんどのケースにおいて、本文書内で特定されているリスクは、受託会社により適切に軽減されない場合、以下につながる可能性がある。

- SOC1 業務において、受託会社が 1 つ以上の統制目的を充足できず、委託会社の財務諸表に潜在的な虚偽表示の可能性が生じる。
- SOC2 業務において、受託会社が 1 つ以上の主要な業務上の義務及びシステム要件を達成できない。

本文書は受託会社監査人を対象として執筆されているが、委託会社監査人にとっても、SOC1 業務における委託会社の財務諸表に対する重要な虚偽表示のリスクを理解しようとする際に有用である可能性がある。以下のリストは包括的なものではないが、本文書の「ブロックチェーンのユニークな特徴」セクションで論じたブロックチェーンのより重要な特徴に関するリスクが含まれる。

- **アクセス・コントロール・メカニズム**
  - アクセス・コントロール・メカニズムの不備は、不正な取引や、企業又は個人に関する機密情報の開示につながる可能性がある。認証又は認可されていない参加者が、ブロックチェーンに記録されている取引に対して不適切な読み取り・書き込みアクセスを有してしまう可能性がある。
  - **暗号鍵管理**
    - 暗号鍵を適切に管理できなければ、認証又は認可されていない参加者が、ブロックチェーンに記録されている取引に対して不適切な読み取り・書き込みアクセスを有してしまう可能性がある。
    - 暗号鍵に対するシャーディングを不正確に行うと、データの喪失や破損につながる重大なリスクがある。
    - マルチ署名暗号鍵[8]が同一のサーバーに保管されている場合、攻撃で 1 つの鍵が漏洩することで他の鍵も破られてしまう可能性がある。この場合、ブロックチェーンに不正な取引が記録されるリスク及び不正な開示が行われるリスクが増大する。

8 マルチ署名暗号鍵では、ユーザーがグループで単一の文書に署名できる。

- シングル署名の暗号鍵を使用すると、ブロックチェーン上の記録へのアクセスの喪失、不正な取引、及び不正な開示のリスクが増大する。
- セキュアでない、又は鍵へのアクセスに対する管理が不十分な場所に暗号鍵を保管すると、不正な個人がブロックチェーンに記録されている取引に対して不適切な読み取り・書き込みアクセスを有してしまうことにつながる可能性がある。
- 暗号鍵を喪失すると、受託会社又は委託会社がデジタル資産・記録にアクセスできなくなる可能性がある。
- 完全かつ正確な暗号鍵のインベントリが維持されていない、あるいはインベントリが受託会社のマネジメントによる定期的なレビューを受けていない場合、不正な組織又は個人が不正なアクセスを行う可能性がある。そうしたアクセスによって、ブロックチェーンへの不正な取引の入力が可能となる、又は不正な情報開示が可能となる可能性がある。
- 暗号鍵へのアクセスに関する監査ログが適切に有効化されていなければ、受託会社のマネジメントが、鍵に対する不正なアクセスの試みを検知・調査する上で十分な情報を得られない可能性がある。
- 暗号鍵へのアクセスを追跡するログへのアクセスが適切に制限されていない場合、そうしたログを改変しようとする不正な試みが適時に検知できない可能性がある。これによって、不正なユーザーがブロックチェーンに不正な取引を入力したり、不正な情報開示を行ったりすることを許してしまう可能性がある。
- 暗号鍵への不審な又は異常なアクセスについて、セキュリティ担当者、内部監査部門及び適切なシニアレベルのマネジメントに警告を発するようデザインされたログ分析ソフトウェアが有効化されていないか、又は不適切に有効化されている場合、不正な組織又は個人による、成功した又は不成功に終わった鍵の取得の試みが適時に検知されない可能性がある。このことが、不正なユーザーによるブロックチェーンへの不正な取引の入力や、ブロックチェーンに記録された情報の不正な開示を適時に検知できないことにつながる可能性がある。
- ログ分析ソフトウェアによる警告を受け取った個人が、異常な又は不審な活動の報告を受けた際に行動する上で不適格であるか又は十分な権限を有していない場合、不正な活動への適時の検知・対応ができない可能性がある。
- 暗号鍵へのアクセスを有するユーザーの再認証が定期的に実行されない場合、ブロックチェーンにおける不正な取引のリスク、又はブロックチェーンに記録された情報の不正な開示のリスクが適時に検知・防止できない可能性がある。

- **法令等の遵守**
  - 特定の SOC2 業務において、自由参加型パブリック型ブロックチェーンを使用して委託会社に業務を提供する受託会社は、法令等の遵守に関連した主要な業務上の義務及びシステム要件を達成できない可能性がある。受託会社がそうした義務や要件を達成できない状況の例には以下が含まれる。
    - パブリック型ブロックチェーンの全ユーザーは、すべての記録に対する無制限の読み取りアクセスを有しており、このことから、プライバシーに関する法令等の遵守、及び受託会社の業務上の義務及びシステム要件の達成に関する課題が生じる可能性がある。
    - パブリック型ブロックチェーンの主要な特徴及びメリットの一つは、ユーザーが真の身元を隠し、匿名のままに留まれることである。こうした特徴によって、金融サービス業界の委託会社は、顧客確認（Know Your Customer）ルール[9]、又は各顧客及び顧客の代理として行動する権限を有する各個人に関して詳細な記録を把握し、保持することを求める類似の法規制の遵守が困難になる可能性がある。

9 金融取引業規制機構（FINRA）規則 2090 はブローカーディーラーに対し、「あらゆる口座の開設及び維持に関して、すべての顧客及びそれら顧客の代理として行動する各個人の権限に関する基本的事実の把握（及び保持）を目的とした合理的な注意を払う」ことを求めている。

- **コンセンサス・メカニズム及びプロトコル**
  - 一部のコンセンサス・メカニズムの主要なリスクに「51%攻撃」がある。これは、当該ネットワークの計算能力の 50%超を支配するマイナーのグループによるブロックチェーンへの攻撃をいう。フルノードの数が少ないほど、51%攻撃の成功は容易となる。より少ないノードでコンピューターの計算能力の過半を支配できるため、攻撃者はブロックチェーンに追加的な操作を加えること、過去に記録された取引を無効化すること、さらには過去のデータのブロックを置き換えることもできる可能性があり、これらはすべて、ブロックチェーンの完全性を危殆化する可能性がある。
  - デジタル資産の取引に使用されるブロックチェーンは、バリデーターの出資金（すなわち、バリデーターが、ブロックのバリデーターに選ばれる機会を得るために担保とした資産額）に基づいたコンセンサス・メカニズムを使用する場合がある。バリデーターの出資金の額が大きいほど、バリデーターが個人的な利益のためにブロックを不正に認証する可能性は低くなる。しかし、誠実であることに対するバリデーターへのインセンティブは、バリデーターの純資産に対する出資金額の割合に直接関連する。例えば、2 人のバリデーターが、取引のブロックを検証する機会を得るためにそれぞれ 5 万ドル相当のデジタル資産を出資した場合を考える。5 万ドルが、一方のバリデーターの純資産の 1%にしか相当しないものの、もう一方のバリデーターの純資産の 50%に相当する場合、前者にとっては後者よりも誠実さを保つことへのインセンティブが少ない。
  - コンセンサス・メカニズムがブロックチェーンでハードフォークを認める場合、以前に無効とされたブロックが認証されるリスク、及び有効な取引が無効化されるリスクは増大する。
  - コンセンサス・メカニズム又はプロトコルが危殆化すると、委託会社が保有するデジタル資産の凍結につながる可能性がある。
  - コンセンサス・メカニズムの不備、アルゴリズムの脆弱性、陳腐化又は破損は、委託会社による資産の喪失又は不正確、不完全若しくは重複した取引の記録につながる可能性がある。
  - コンセンサス・メカニズムにおいて脆弱なハッシュ化手法を使用することは、情報の不正な変更、破壊又は開示につながる可能性がある。
  - コンセンサス・メカニズムは不正な形式のデータ（すなわち、読み取ったり正確に処理したりできないデータ）を防止できなかったり、無効な取引、不正な取引又は取引の無効化を許してしまったり、参加者間におけるデジタル資産の不適切な移転を可能にしたりする可能性がある。
- **二重支払い**
  - デジタル資産の取引に使用される、特定のコンセンサス・メカニズムを使用するパブリック型ブロックチェーンは、同一のデジタル資産が 2 回以上売却又は支出されることを許可してしまう可能性がある。これはしばしば二重支払いと呼ばれる。二重支払いを意図的に実行する者は、元々の資産の売却や支出を無効化する複数の取引を生成してバリデーターに送り、元々の取引が生じなかったかのように装う。
- **不変性**
  - 一部のコンセンサス・メカニズムのプロトコルは、以前に記録された取引の変更を許可する可能性がある。例えば、ブロックチェーンでのハードフォーク（正当な理由により、又は51%攻撃が契機となって生じる場合がある）により、以前に記録された取引が無効化又は改変される可能性がある。プライベート型ブロックチェーンが使用する他のコンセンサス・メカニズム、プロトコル、及びスマートコントラクトについては、そのプロトコルが台帳への記入の無効化を許可している場合、以前に記録された取引の無効化を許可する可能性がある。

- **統合及び相互運用性**
  - 受託会社と委託会社の既存の技術及びシステムを適切に統合し、ブロックチェーンと相互運用可能（すなわち、現在及び将来において他の商品、システム又はアプリケーションとシームレスに連携できる）にしなければ、処理の完全性と可能性が損なわれる可能性がある。
- **法的所有権**
  - プライベート型ブロックチェーンに参加する際、ブロックチェーンの取引記録の法的所有権を定義しなければ、参加者（所有者）による取引記録へのアクセスの拒否につながる可能性がある。
- **オラクル**
  - オラクルはブロックチェーンのセキュリティ管理によって保護されておらず、そのため不正確なデータが（意図的に又は意図せずに）スマートコントラクトに送られ、取引当事者の意図に反した取引が実行されることにつながる可能性がある。
  - **ソフトウェアオラクル**
    - コーディングエラーが、誤った情報がスマートコントラクトに伝達されることにつながる可能性があり、それが不正確な取引ルールの実行や、本来は有効であった取引の拒否につながる可能性がある。
    - オラクルとスマートコントラクトの間の通信チャネルの待ち時間はすべての種類のオラクルに影響を与え、取引が実行されない、あるいは情報を適時に伝達できないことにつながる可能性がある（例えば、オラクルから受け取った市場情報に基づくセキュリティ取引を自動的に実行できない、食品の買い手に腐敗状況を通知できない等）。
  - **ハードウェアオラクル**：コンポーネントの機能不全又は故障は、ユーザーへの誤った情報の報告や、ユーザーに重要な情報を報告できないことにつながる可能性がある。例えば、医療機器に組み込まれたオラクルの機能不全は、ブロックチェーンに入力された電子カルテにおける診断ミスのリスクを増大させる。もう一つの例として、食品加工工場で使用される機械に組み込まれたオラクルの故障により品質認証が遅れたり、環境条件が検知できなくなったりし、結果として食品の腐敗につながる。
  - **ヒューマンオラクル**：自動化された手段では報告できない特定の事象を報告するタスクを担うオラクルで、彼らの身元を確認できなければ、不適格な人物がデータをブロックチェーンに導入できるようになり、結果にバイアスが生じる可能性がある。
- **スマートコントラクト**
  - オラクルに依拠するスマートコントラクトは、オラクルが危殆化した場合に誤った決定を下す可能性があり、委託会社への金銭的損失や不正確な報告につながる可能性がある。
  - スマートコントラクトにより開始された取引がブロックチェーンに記録される際に、契約に規定された準拠法及び裁判管轄が全取引当事者の権利と義務を認識し、執行できないリスクがある。これは、スマートコントラクトで意図されている、当事者の資産への法的権利又は責任に影響を与える可能性がある。通常、受託会社は、委託会社が相補的な内部統制（CUEC）を確立することでこのリスクに対処することを期待するものと考えられる。これについては、本書の「受託会社監査人に関する追加的検討事項」セクションで論じている。
  - スマートコントラクトは必ずしも意図した通りに機能するとは限らない。コーディングエラーは、たとえそれがどれほど小さなものであっても、多額の金銭的損失をはじめ、被害者にとって取り戻す術がほとんどない、重大な結果につながる可能性がある。コーディングエラー、及びスマートコントラクトのテストが不十分であることによって、取引が意図されたシーケンス以外で処理されることにつながる可能性がある（例えば、商品の受領前に、あるいは支払いの承認前に代金が支払われる等）。
  - 不十分な又は非効果的な変更管理統制は、スマートコントラクトに不正な変更を許してしまい、それがさらに取引の処理に影響を与える可能性がある。条件の変更は、複数の取引当事者の金銭的損失、又はSOC1 業務における委託会社の財務諸表の虚偽表示につながる可能性がある。

受託会社に関する SOC 業務における受託会社によるブロックチェーンの使用がもたらす影響

受託会社に関する SOC 業務に適用される職業的専門家としての基準及び規準の概要

受託会社監査人が SOC1 及び SOC2 業務を実施する際に準拠する職業的専門家としての基準及び解釈上の指針を以下の表に示す。

SOC1 報告書：ICFR	SOC2 報告書：Trust サービス規準（TSC）
主題及び受託会社監査人の意見	
すべての重要な点において、受託会社確認書に記載された規準に基づき、	**すべての重要な点において、**
a. 受託会社のシステムに関する記述書は、*[日付]*から*[日付]*までの期間にわたってデザインされ業務に適用されているシステムを適正に表示している。	**a.** 記述書は、記述書規準に従って、*[日付]*から*[日付]*までの期間にわたってデザインされ業務に適用されている受託会社のシステムを適正に表示している。
b. *[日付]*から*[日付]*までの期間にわたって内部統制が有効に運用されていたならば、記述書に記載された統制目的に関連した内部統制は統制目的を達成することに合理的な保証を提供するよう適切にデザインされている。	**b.** 記述書に記載された内部統制は、*[日付]*から*[日付]*までの期間にわって有効に運用されていれば、適用される Trust サービス規準に基づいて、受託会社のサービスコミットメント及びシステム要求事項を充足するという合理的な保証を提供するように、当該期間にわたって、適切にデザインされている。
c. タイプ 2 業務において、内部統制は、*[日付]*から*[日付]*までの期間にわたって記述書に記載された統制目的が達成されていたという合理的な保証を提供するよう有効に運用されている。	**c.** タイプ 2 業務において、記述書に記載された内部統制は、適用される Trust サービス規準に基づいて、受託会社のサービスコミットメント及びシステム要求事項を充足するという合理的な保証を提供するように、*[日付]*から*[日付]*までの期間にわたって有効に運用されている。
審業務を実施する際に準拠する職業的専門家としての基準及び指針	
AT-C Section 105, Concepts Common to All Attestation Engagements（以下「AT-C105」という。）	AT-C105
AT-C Section 205, Assertion-Based Examination Engagements（以下「AT-C205」という。）	AT-C205
AT-C Section 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting（以下「AT-C320」という。）	
AICPA Guide, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting（SOC 1®）（以下「SOC1 Guide」という。）	AICPA Guide, SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (以下「SOC2 Guide」という。)
規準	
内部統制の規準：*AT-C320 第 16 項*に、内部統制が適切にデザインされているかどうかを評価する上での最低限の規準が示されている。AT-C320 17 項には、SOC1 業務において内部統制が有効に運用されているかどうかを評価する上での最低限の規準が示されている。	内部統制の規準：TSP100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality,and Privacy*
記述書の規準：AT-C320 第 15 項に、SOC1 業務における記述書に関する最低限の規準が示されている。	記述書の規準：DC200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*

監査チームが適切な資格及び能力を具備しているかどうかの判断

AT-C105 第 29 項 b は、業務を受嘱する前提条件の中でも特に、チームが業務を実施する能力と適性を有していることについて納得している場合に限り、業務実施者は証明業務を受嘱すべきであると述べている。しかしながら、前述のように、ブロックチェーンは比較的新しい非常に複雑な技術である。そのため、受託会社監査人が関連するリスクを特定、評価し、受託会社がそれらのリスクを軽減するために適用している内部統制を評価する上で必要となるブロックチェーンに関する知識が不足している可能性がある。

受託会社監査人は、正規の学校教育、継続教育、実務経験又は他者の助言を通じてブロックチェーンについての知識を得る可能性がある。しかし、ブロックチェーン技術は極めて複雑で進化しているため、継続教育のみでは必須の技能及び能力を得るのに十分ではない可能性がある。正規の学校教育や継続教育にはブロックチェーンの主要な特徴や利用に関するリスクについてのハイレベルな概説が含まれる可能性があるが、それらによっても受託会社監査人が受託会社に関する SOC 業務を実施する上で必要となる深い知識、技能及び能力を得ることができない可能性がある。

受託会社監査人が必須の知識及び技能を欠いている場合、受託会社監査人はそうした専門知識を有する内外の専門家の利用を検討できる。AT-C205 の A45 項によれば、業務における専門家作業の重要性が大きいほど、専門家は、特定分野の専門家とそれ以外の要員で構成される分野横断的なチームの一員として作業を行う可能性が高くなる。AT-C105 第 34 項 a から b 及び A63 項、並びに AT-C205 第 37 項から第 39 項、A17 項及び A39 項から A47 項において、SOC1 又は SOC2 業務における専門家の作業の利用が論じられている。SOC2 Guide の 2 章第 160 項から第 166 項でも、SOC2 業務における専門家の作業の利用が論じられている。

システムに関する理解の獲得

AT-C 205 第 14 項から第 15 項によれば、受託会社監査人は主題についての理解、及びその作成に対する内部統制についての理解を得る必要がある。受託会社監査人の主題に関する理解は、受託会社監査人に以下を可能とする上で十分なものである必要がある。

a. 主題における重要な虚偽表示リスクの特定及び評価

b. 評価されたリスクへの対応及び受託会社監査人の意見を裏付ける合理的な保証の獲得を目的とした手続のデザイン及び実施の基礎の提供

受託会社監査人がそうした手続から獲得する証拠は、SOC 業務における受託会社監査人の意見を裏付ける上で十分かつ適切なものである必要がある。

ブロックチェーンが委託会社へのサービスの提供に使用されるシステムの不可欠の要素である場合、ブロックチェーンの理解は極めて重要となる。SOC1 業務では、ブロックチェーンを理解することで受託会社監査人はそれが委託会社の ICFR に関連するかどうか、及び関連する場合、ブロックチェーンが委託会社のシステムにどのような形でインターフェースにより接続されているのかを検討できるようになる。さらに、そうした業務において、ブロックチェーンの理解は受託会社監査人に、ブロックチェーンに対する内部統制を含め、記述書で特定されている内部統制が適切にデザインされ実施されたかどうか、及びタイプ 2 業務において、そうした内部統制が統制目的を充足する上で効果的に運用されていたかどうかを検討することも可能にする。

SOC2 業務において、ブロックチェーンの理解は、ブロックチェーンに対する内部統制を含め、システムに関する記述書が当該業務に関連する記述書規準に沿って表示されているかどうかに関する意見の作成にとって極めて重要である。それはまた、受託会社監査人にデザインの適切性、及びタイプ 2 業務においては主要なサービスコミットメント及びシステム要求事項の達成に必要なブロックチェーンに対する内部統制の運用状況の評価を可能にする。

受託会社のシステムがブロックチェーンを使用している場合、通常、ブロックチェーンに関する受託会社監査人の理解には以下が含まれる。

- **ブロックチェーンのアーキテクチャ及びデザイン**
  - ブロックチェーンアーキテクチャの一部であるサービスの提供にクラウドプロバイダーが使用されている場合、サービスの内容（例えば infrastructure as a service（IaaS）、software as a service（SaaS）、platform as a service（PaaS）、又は blockchain as a service（BaaS））、及びクラウドプロバイダーがベンダー又は再受託会社とみなされるかどうか。SOC1 業務に関して、クラウドサービスプロバイダーがベンダー又は再受託会社であるかどうかの判断については SOC1 Guide の第 3.17 項から第 3.18 項及び表 3-1 で論じられている。SOC2 業務に関しては、SOC2 Guide の第 2.06 項から第 2.11 項で論じられている。
  - システムで使用されるブロックチェーンの種類（すなわちプライベート型ブロックチェーン、パブリック型ブロックチェーン、又はハイブリッド型ブロックチェーンのうちいずれか）及びブロックチェーンの種類に依拠する他の関連する情報（誰が参加できるか、メンバーの等級とその権利、メンバーがブロックチェーン上で他のメンバーと相互交流を行う方法等）
- **アクセス・コントロール・メカニズム**
  - アクセス・コントロール・メカニズムを管理する当事者（もしいれば）
  - SOC2 業務の対象範囲に機密保持又はプライバシーの Trust サービスカテゴリーが含まれる場合、
    - ブロックチェーン内に保管される機密情報又は個人情報を不正な開示から保護する方法
    - ブロックチェーン内に保存される機密情報又は個人情報に使用されている暗号方式（もしあれば）
    - 危殆化に対する暗号方式の脆弱性
    - 受託会社監査人による検証業務の対象期間内に暗号が破られる可能性の程度

- **コンセンサス・メカニズム**
  - コンセンサス・メカニズムのデザイン
    - コンセンサス・メカニズムを管理する当事者（もしいれば）
    - ハッシュ化と暗号化に使用される手法とその手法の強度
  - プライベート型ブロックチェーンにおいて
    - 受託会社又は委託会社が、ブロックチェーンのルールに従ってバリデーターを担うフルノードを管理している、又は管理を認められている場合
- **暗号鍵管理**
  - 以下に対する管理を含む暗号鍵のライフサイクル管理
    - デザイン及び開発
    - 実装
    - 鍵の生成
    - 保管
    - アクセス・コントロール
    - 鍵の廃棄
  - 以下を行った従業員、請負業者、又はコンサルタントの役職
    - 暗号鍵アーキテクチャのデザイン及び開発
    - 暗号鍵アーキテクチャの実装
    - 鍵の生成
  - 暗号鍵アーキテクチャのテスト方法及びテスト結果
  - 暗号鍵アーキテクチャが実装された日と鍵が生成された日
  - 鍵を保管する場所及び方法、並びに鍵へのアクセスが、その職務や機能の実行にそうしたアクセスを必要とする承認された個人及びシステムに制限されているかどうか
  - 受託会社が維持する暗号鍵のインベントリ（鍵にアクセスを有する個人の氏名及び役職、並びにインベントリの完全性及び正確性に対する管理を含む）
  - 暗号鍵へのアクセスに関する監査ログの記録及びレビュー、並びにログが鍵へのアクセス権のないユーザーのアクセスを制限した形で保管されているか
  - マネジメントの適切なメンバー（セキュリティ担当者、内部監査人その他の上級役職者）に対し、鍵への不審な又は異常なアクセス、及びログ改変（成功のみならず未遂も含め）について警告を発するログ分析ソフトウェア、並びに警告を受領しレビューした個人の氏名と役職
  - 鍵にアクセス権を有するユーザーの再認証の頻度、及び再認証を実行する担当者の氏名と役職
  - 暗号鍵が複数の部分に分割（シャード）されており、それら部分のサブセットがオリジナル暗号鍵の復元に使用されているかどうか、及び、使用されている場合、シャードが分配された個人の氏名と役職
  - マルチ署名暗号鍵が使用されている場合、取引が発生する前に合意しなければならない当事者の役職
- **相互作用と融合**：（もしあれば）システム間の情報と取引のフローに加え、交換されるデータの完全性と正確性に関する統制を含む、受託会社のレガシーシステムとブロックチェーンの間の相互作用と融合
  - ブロックチェーンが他のブロックチェーンと相互交流するようデザインされているか、及びそれが受託会社の内部統制の目的を充足する能力（SOC1 業務において）又は主要なサービスコミットメント及びシステム要求事項を達成する能力（SOC2 業務において）に影響を与える可能性
  - 受託会社のレガシーシステムの記録とブロックチェーンの記録の照合
  - IoT 等の他の技術との融合の度合い
- **監視**：実際に発生した取引を記録した証拠に関するブロックチェーンの監視方法

- **参加者**:
  - 参加者が単一の ID を有する個人か、複数の ID を有する個人か、それとも会社、組織、政府機関等の個別の事業体か
  - ブロックチェーンの参加者、メンバー及びユーザー間に利益相反の可能性があるか
- **プライバシー**:SOC2 業務の対象範囲に守秘義務又はプライバシーの Trust サービスカテゴリーが含まれる場合、受託会社が以下を含むブロックチェーンの主要な特徴によって生じる固有のコンフリクトに対処する方法
  - 忘れられる権利等、プライバシーに関する法規制に関して、記録が変更不可能とされること
  - コンセンサス・メカニズムが記録の変更を認めない場合、以前にブロックチェーンに追加された個人情報を訂正、修正又は編集する手順
  - パブリック型ブロックチェーンにおけるユーザーの仮名性(これが、ユーザーについて特定の情報の追跡を目的としたプライバシー関連の法令及び要件を毀損する可能性があるため)
  - データ主体に提示された選択肢と彼らが行った同意
  - 分散型ネットワークの使用の開示(個人情報が提供された取引の当事者ではない参加者が管理するデバイスに個人情報が保管されること)
- **スマートコントラクト**
  - 人間が介入することなく、スマートコントラクトにより開始される取引のデザインと内容
  - オラクルと、スマートコントラクトとの間で授受されるデータの種類(伝達される情報の正確性と完全性に対する管理を含む)
  - 契約が意図したとおりに機能しているか判断するため、スマートコントラクトが独立した第三者により監査されているかどうか
  - 取引及び事象に関する完全かつ正確な開始、記録、処理又は報告につながる、スマートコントラクトのルールに対する統制
  - ブロックチェーンの使用に関するルールが、スマートコントラクトの当事者に対し、法的に拘束力のある書面又は電子的な契約書を締結するよう求めているか、及びその契約書が電子的又は物理的な署名を必要としているかどうか
  - スマートコントラクトにより実行された取引が無効化可能か、及び、可能である場合、取引を無効化する手順があるかどうか
  - スマートコントラクトがブロックチェーンと他のシステムや技術との統合の促進に使用されているかどうか
  - スマートコントラクトが取引又は条件に関する情報を委託会社に伝達する場合、その情報の完全性と正確性に対する管理

ブロックチェーンにおいてスマートコントラクトが使用される際の追加的検討事項

受託会社のシステムが、スマートコントラクトによる取引を開始し実行するブロックチェーンを使用している場合、受託会社監査人は以下の追加事項の検討を希望する場合がある。

- 「受託会社によるブロックチェーンの使用に関連するリスク」セクションで論じたように、スマートコントラクトは必ずしも意図した通りに機能しない可能性があり、そのため受託会社は、本番環境への移行に先立って、スマートコントラクトの機能を独立した第三者に監査させるよう義務付ける内部統制を具備する可能性がある。この場合、受託会社監査人は記述書において、スマートコントラクトの監査についての開示が示されることを期待すると考えられる。
- スマートコントラクトは、必ずしもすべての要件が準拠法及び裁判管轄に基づいて合法的に執行可能とは限らない可能性がある。そのため、受託会社のシステムにスマートコントラクトが含まれる場合、受託会社のマネジメントは委託会社に、それが準拠法及び裁判管轄に基づき合法的に執行可能かどうかを判断する目的で、委託会社の法務顧問にスマートコントラクトのレビューを義務付ける委託会社の相補的な内部統制の実行を期待する可能性がある。

受託会社のシステムに関する記述書、内部統制のデザインの適切性、及びタイプ 2 業務における内部統制の運用状況に関する意見の形成

「受託会社に関する SOC 業務に適用される職業的専門家としての基準及び規準の概要」セクションで示したように、受託会社監査人は (a) システムに関する記述書、(b) 内部統制のデザインの適切性、及び (c) タイプ 2 業務において、内部統制の運用状況について意見を表明する。

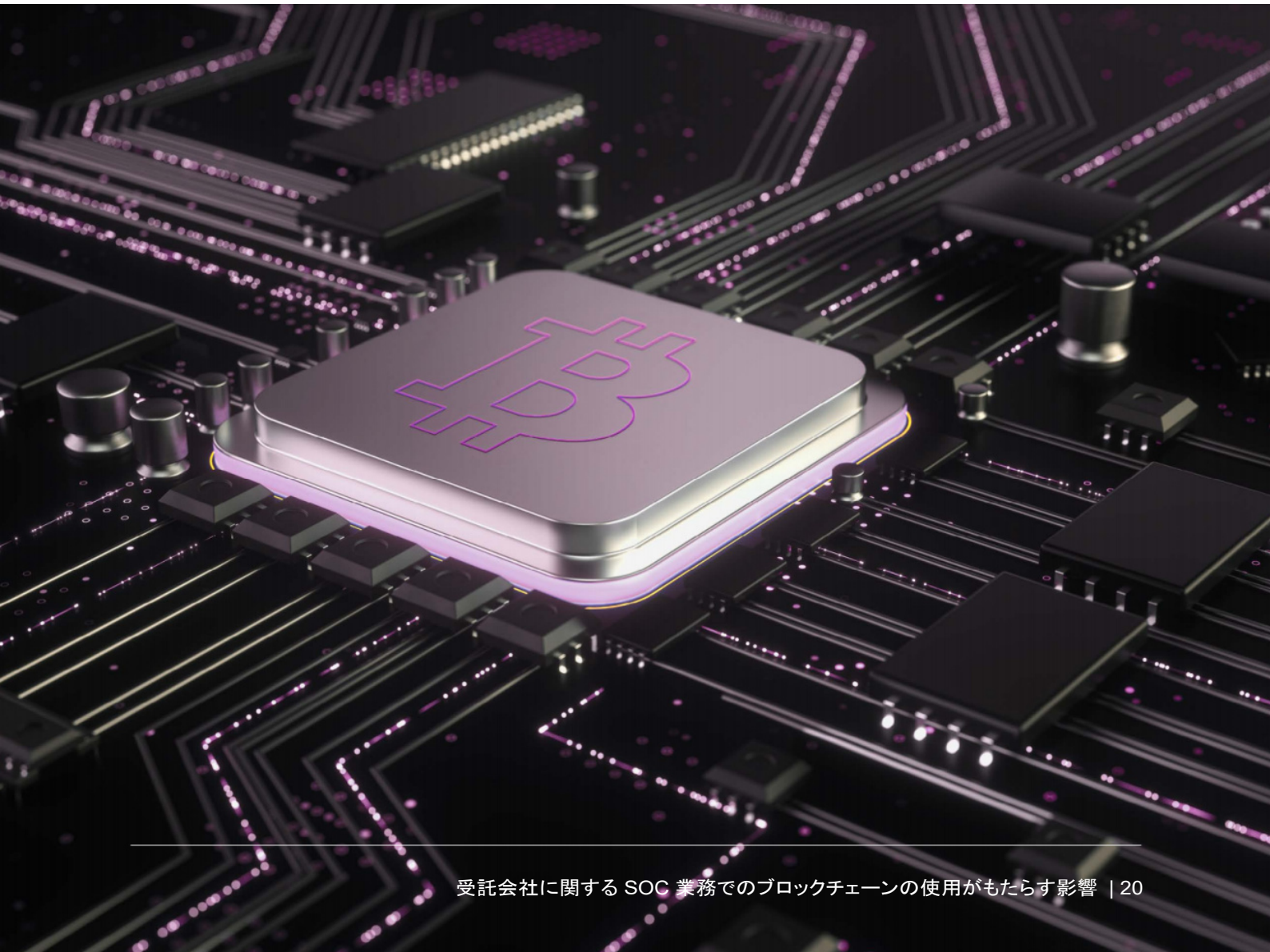
システムに関する記述書の目的は、委託会社に、受託会社と事業を行うリスクの評価に使用できる情報を提供することにある。ブロックチェーンの使用に関連するリスクを理由として、記述書には、記述書の規準を満たす上で関連するブロックチェーンの諸側面を開示することが期待されると考えられる。システムに関する記述書は、通常、本文書の「システムに関する理解の獲得」セクションにリスト化した関連する事項を、ブロックチェーンの使用に関連するリスクを軽減するためにデザイン、実行及び運用された統制等の他のシステム要素と併せて開示する。受託会社監査人の手続は、ブロックチェーンの使用に関連する諸側面を含め、規準に求められる開示事項がシステムに関する記述書に含まれているという十分かつ適切な証拠を取得するためにデザインされると考えられる。

デザインの適切性、及びタイプ 2 業務において内部統制の運用状況に関する意見を作成するため、受託会社監査人はブロックチェーンに関連する諸側面に関連するものも含め、システムに関する記述書に含まれる内部統制に焦点を当てる。デザインの適切性に関する意見を形成するため、受託会社監査人はデザインの適切性を裏付ける十分かつ適切な証拠を得るために手続をデザインすると考えられる。同様に、タイプ 2 業務において、受託会社監査人の手続は運用状況を裏付ける十分かつ適切な証拠を得るためにデザインされると考えられる。実施されたテスト及びその結果は、SOC 報告書のセクション 4 に含まれると考えられる。

要旨

本文書では、受託会社によるブロックチェーンの使用が、受託会社に関するSOC業務にどのような形で固有のリスクをもたらすかについて論じた。受託会社監査人は、受託会社監査人にそうしたリスクの特定と評価を可能とし、評価されたリスクに対処する手続のデザインと実施のための基礎を提供するものとなる、受託会社のシステムについての理解を得ることが求められる。

受託会社のシステムがブロックチェーンを使用している場合、受託会社監査人の理解には、ブロックチェーンがシステムにどのように統合されているか、及びそれに対する内部統制が含まれる。本文書に記述されている事項の理解は、証明基準に従って受託会社に関するSOC業務を実施する上で受託会社監査人を支援する。



付録 A

受託会社によるブロックチェーン使用の例

本文書全体を通じて論じたように、受託会社が委託会社に業務を提供する上で使用するシステムにブロックチェーンを統合することにより、新たな課題が提起され、ユニークかつ重大なリスクがもたらされる。例示のみを目的とし、本付属資料では、受託会社が委託会社に業務を提供するシステムにおいてブロックチェーンをどのように使用するかについて、4 つの例を示している。

例 1: 給与支払処理	給与支払業務受託会社で構成される「給与 BC コンソーシアム[10]」は、BaaS を使用してプライベート型ブロックチェーンを構築及び実装し、メンバーの委託会社のために給与支払取引を処理している。ブロックチェーンユーザーの ID とアクセス権は、取引の承認とコンセンサスの達成に使用されるコンセンサス・メカニズムにより承認され、確立されている。 給与 BC コンソーシアムのブロックチェーンの最初のブロックは、委託会社の取引を開始し、記録し、処理し、報告するスマートコントラクトである。税務当局のシステムに組み込まれているオラクルが、税コードの変更をスマートコントラクトに伝達し、スマートコントラクトが雇用者と従業員の課税額を計算する。コンソーシアムのメンバーによる、委託会社の給与支払処理に関連するすべての取引はブロックチェーンに記録される。
例 2:従業員給付制度の記録管理	上場企業である大手銀行（受託会社）が、顧客に対して包括的な退職給付制度を提供している。退職給付制度とその参加者により高い価値を提供するため、及びプロセスをより効率的なものにするために、銀行はブロックチェーンを開発し、実装した。銀行は、プライベート型ブロックチェーンコンポーネント（プライベートコンポーネント）のメンバーが所有及び管理するハイブリッド型ブロックチェーンを利用している。 プライベートコンポーネントは、プライベート型ブロックチェーンプラットフォーム上で稼働する。各ノードはメンバーのサーバーに保管される。 プライベートコンポーネントの最初のブロックはスマートコントラクトであり、取引処理のためのロジックを含み、特定の条件が生じた場合に実行すべきアクションを特定する。スマートコントラクトはオラクルから受け取ったデータを基に、ポートフォリオのリバランス、報告のアップデート、及び必要な場合、委託会社の制度の加入者に対して変更（例えば退職ポートフォリオの変更）についての警告を自動的に行う。制度の加入者は、このプラットフォーム上で稼働する銀行のパブリックコンポーネントに参加する選択肢を有する。加入者は、各自の退職制度に関する選択をブロックチェーン上で入力及び更新できる。これにより、特定の条件を満たした場合、各加入者のポートフォリオが自動的に変更されるとともに、セキュアなウェブサイトから報告書や納税申告用紙をダウンロードできる。

10 コンソーシアムは会社又はその他の組織で構成され、個々のメンバーのリソースを超える活動を引き受けることを目的として結成される。

例 3：ブローカーディーラー・ブロックチェーンコンソーシアム

受託会社とその同業他社が、中小規模のブローカーディーラーに対して金融業務を提供する。そうした業務には記録管理、取引記録簿の維持、株式台帳、取引、評価、及び報告が含まれる。競争力を維持するため、受託会社及びその同業他社、並びにそれらのクライアントは団結し、取引コストの軽減と決済時間の短縮を目的としてブロックチェーン・コンソーシアム（「BD・BC コンソーシアム」）を結成した。

BD・BC コンソーシアムのブロックチェーンはプライベート型ブロックチェーンで、そのメンバーが所有し管理する。メンバーは適用されるルール及び使用されるコンセンサス・メカニズムのプロトコルについて投票を行い、所有権と投票権はメンバーが処理する取引の価額に比例する。

BD・BC コンソーシアムのブロックチェーンは、メンバーの投票権の決定とバリデーターの選任に、(a) メンバーの市場価格、 (b) メンバーの株式が公開されているかどうか、及び (c) ブランド認知の 3 つの主要素を使用したコンセンサス・メカニズムを使用している。要因 (a) に関して、上場企業でないメンバーは将来予想キャッシュフローの割引額を市場価格の代わりに使用できる。要因 (b) に関しては、SEC への登録及び米国の金融業規制機構（FINRA）への加盟によりこの要件が充足される。要因 (c) に関して、ブランド認知は、金融関連メディア及びソーシャルメディアで各メンバーが好意的に又は非好意的にメンションされた回数を報告するデータ分析により測定される。すべてのバリデーター候補は、BD・BC コンソーシアムの「コンセンサス・メカニズム検証委員会」（「検証委員会」）により事前に承認されなければならない。

例 4：商業不動産管理業務

不動産管理業務会社（受託会社）が、商業不動産市場に関して不動産投資会社（家主）にサービスを提供する。受託会社のブロックチェーンシステムはプライベート型ブロックチェーン上に構築されており、バリデーターに政府が発行した有効な ID の提示を求めるコンセンサス・メカニズムを使用している。ブロックチェーンの参加者には、受託会社、家主、テナント及び銀行が含まれるが、フルノードとなり、新たなブロックのバリデーターを務めることができるのは受託会社、家主及び銀行である。

このブロックチェーンの最初のブロックはスマートコントラクトである。受託会社は参加者に、スマートコントラクトがいかなる法的地位も有しておらず、業務会社、家主及びテナントをいかなる権利又は義務に対しても拘束しないことを通知する。ただし、スマートコントラクトには、取引のいずれかの当事者が誤りを犯した場合、又はスマートコントラクトのロジックに欠陥があり、記録された取引が当事者の意図に反する場合に取引を無効化する選択肢が含まれる。スマートコントラクトへの合意に加えて、参加者は従来的なリース契約も締結しなければならない。契約の条件は、実行に先立って家主とテナントにより合意される。

受託会社の従業員にブロックチェーンへのアクセスを可能にする暗号鍵は、セキュアなサーバーに保管される。家主及びテナントは、各自の暗号鍵のセキュリティに責任を負う。

付属資料 B

追加的な AICPA の資料

AICPA は、ブロックチェーン及びデジタル資産に関する知識の向上を支援するため、以下を含む複数の資料を作成している。

White papers

- Blockchain and Internal Control: The COSO Perspective
- Blockchain and Its Potential Impact on the Audit and Assurance Profession
- CPAs Leveraging Blockchain
- 2019 Blockchain Symposium: Experts' Insights Indicate Growing Use Cases and Value for the Technology

CPE

- Blockchain for Financial Advisors
- Blockchain for Financial Services
- Blockchain for Healthcare
- Blockchain for Insurance
- Blockchain Implications for Audit and Assurance Services
- Blockchain for Not-for-Profits
- Blockchain for Supply Chain
- Digital Mindset Pack (2019-20)

Certificate program

- Blockchain Fundamentals for Accounting and Finance Professionals Certificate Program

Additional resources

- Blockchain Legislation Emerging in State Legislatures
- Emerging Technology Report: Blockchain
- How will blockchain change accounting?

AICPA と CIMA により設立された国際公認職業会計士協会（Association of International Certified Professional Accountants）は、全世界の会計及び金融分野のリーダーを支援している。