COSO

トレッドウェイ委員会支援組織委員会

ガバナンスと内部統制

ブロックチェーンと内部統制

ＣＯＳＯの視点

デロイト社

ジェニファー・バーンズ | エイミー・スティール | エリック・E．コーエン | シュリ・ラマムーティ博士

本稿に記載している情報は一般的な内容であり、変更される可能性のある情報源に基づいている。特定の状況へ本稿の情報が適用できるかは、専門家との協議を通じて決定すべきである。また、本稿は専門家のサービスに代わるものではなく、組織に影響を与える可能性のある意思決定や活動の根拠として使用すべきものでもない。

著　者

デロイト＆トウシュ社
パートナー
ジェニファー・バーンズ

デロイト＆トウシュ社
パートナー
エイミー・スティール

寄稿者

コーエン・コンピュータ
コンサルティング社
エリック・E．コーエン

デイトン大学
准教授
シュリ・ラマムーティ博士

謝　辞

本稿の作成にあたり、ご意見、ご支援および貴重なフィードバックを提供してくださったデロイト＆トウシュ社マネージャーのヨランド・シンクレア氏、ＣＯＳＯ理事会およびＣＯＳＯ会長ポール・ソーベル氏に謝意を表したい。また、技術的なご意見とご助言をくださったデロイト＆トウシュ社プリンシパルのティム・デービス氏、マネージングディレクターのシェルビー・マーフィー氏およびシニアマネージャーのギリーシュ・シヴァクマール氏にも謝意を表したい。

ＣＯＳＯ理事会は、本稿のアイデアを発案したシュリ・ラマムーティ博士とデロイト＆トウシュ社の支援に感謝する。

トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）理事

ポール・Ｊ．ソーベル
ＣＯＳＯ会長

ダグラス・Ｆ．プラット
米国会計学会

ロバート・Ｄ．ドーラー
米国公認会計士協会

ダニエル・Ｃ．マードック
国際財務担当経営者協会

ジェフリー・Ｃ．トムソン
管理会計士協会

リチャード・Ｆ．チェンバース
内部監査人協会

序　文

本プロジェクトは、トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）から委嘱されたものである。ＣＯＳＯは、組織のパフォーマンスや監督を改善するとともに、組織における不正を減らすために立案された内部統制、全社的リスクマネジメントおよび不正抑止に関する包括的なフレームワークとガイダンスの開発を通じて先進的な考え方を提供することに取り組んでいる。ＣＯＳＯは、次の団体の協賛と資金提供によって運営されている民間部門主導の団体である。

米国会計学会（American Accounting Association）

米国公認会計士協会（American Institute of Certified Public Accountants）

国際財務担当経営者協会（Financial Executives International）

管理会計士協会（Institute of Management Accountants）

内部監査人協会（Institute of Internal Auditors）

COSO
トレッドウェイ委員会
支援組織委員会

coso.org

ガバナンスと内部統制

ＣＯＳＯの視点

調査委嘱者

トレッドウェイ委員会支援組織委員会

2020 年 7 月

一般社団法人日本内部監査協会および公益財団法人日本内部監査研究所は、著作権保有者、トレッドウェイ委員会支援組織委員会（「ＣＯＳＯ」）から、この翻訳物を翻訳することを許可されており、実質的な内容は原文と同じです。

本書の一部またはすべてを、著作権保有者の事前の書面による許可を得ずに、複製、検索システムに蓄積、および伝送することは、いかなる形式や手段（電子的、機械的、複写、録音、その他の方法）においても禁止されています。

Copyright © 2020, Committee of Sponsoring Organizations of the Treadway Commission (COSO).
1234567890 PIP 198765432

COSO images are from the COSO Internal Control - Integrated Framework ©2013, The American Instituteof Certified Public Accountants on behalf of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO is a trademark of the Committee of Sponsoring Organizations of the Treadway Commission.

All Rights Reserved. No part of this publication may be reproduced, redistributed, transmitted, or displayed in any form or by any means without written permission. For information regarding licensing and reprint permissions, please contact the American Institute of Certified Public Accountants, which handles licensing and permissions for COSO copyrighted materials. Direct all inquiries to copyright-permissions@aicpa-cima.com or AICPA, Attn: Manager, Licensing & Rights, 220 Leigh Farm Road, Durham, NC 27707 USA. Telephone inquiries may be directed to 888-777-7077.

Design and production: Sergio Analco.

COSO
coso.org

目　次

	ページ
エグゼクティブサマリー	1
１．はじめに	3
２．ブロックチェーンという変革の波	4
３．構成要素と原則の概要	7
結論と次のステップ	20
付録１：技術的な付録	22
付録２：重要な洞察：ブロックチェーンについて知っておくべき 10 項目	25
付録３：ブロックチェーン、財務報告のアサーションおよび監査証拠	27
補足資料と出典（ＣＯＳＯ支援団体が提供したものを含む）	29
著者について	30
ＣＯＳＯについて	32
デロイト社について	32

エグゼクティブサマリー

ブロックチェーンがより主流になっているため、このテクノロジーと事業体の内部統制との関わり方に注目することは適切である。ブロックチェーンの導入と統合を慎重に行うことで、ブロックチェーンの特徴的な機能を活用して組織のより強固な統制が実現できる。さらに、ブロックチェーンで強化されたツールには、業務の効率性と有効性を促進し、財務報告やその他の報告の信頼性と応答性を向上させ、また、法令遵守を向上させる可能性がある。同時に、ブロックチェーンは新たなリスクを生み出し、新たな統制の必要性を生じさせる。トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）の『内部統制の統合的フレームワーク』[i]（*2013 年版フレームワーク*、図１参照）は、ブロックチェーンに関連する特有のリスクに対応するための統制の設計と導入に活用できる、効果的かつ効率的なアプローチを提供している。

図１．2013 年版ＣＯＳＯフレームワーク

組織がＣＯＳＯのレンズを通してブロックチェーンの利用を評価する場合、取締役会と上級幹部はその状況をよりよく理解し、このテクノロジーの可能性と内部統制への適用可能性について、より多くの情報に基づいた評価が行えるようになる。これにより、組織は詳細なリスク分析が行えるようになり、ひいては、そのようなリスクに対応するための適切な統制活動を策定して、ブロックチェーンの効果的な採用と利用が促進できるようになる。

本稿では、*2013 年版フレームワーク*を使用して、財務報告という状況におけるブロックチェーンの利用に関連するリスクを評価し、当該リスクに対応するための統制を設計して導入するための視点を示す。これは、監督、リスクおよび財務報告に係る内部統制（ＩＣＦＲ）に関する意思決定に資することを意図している。そのため、本稿では、財務報告に関与するさまざまな利害関係者が、各自の置かれた環境に合わせて価値を発揮することが期待されている（表２参照）。本稿の目的は、ブロックチェーンの複雑な仕組みや主要なプラットフォーム間の技術的な違いを詳細に説明することではない。しかし、付録１では、本稿で使用した重要な概念のいくつかを説明しており（付録１の概念は、「エグゼクティブサマリー」と本文で最初に登場する箇所を太字で表記している）、「補足資料と出典」には、追加の資料が掲載されている。

所見と影響

ブロックチェーンの利用によって生じるより大きな変化の１つは、事業体の階層に関するものである。図１に示すように、*2013 年版フレームワーク*で示された階層の最上位は全社レベルであり、部門、業務単位、機能へと掘り下げられているが、ブロックチェーンには、異なる事業体にまたがる、分散ベースで動作しながらも共有データで結合された（すなわち、**分散型データベース**）新しい協働単位を作成する機能が備わっている。共有台帳や記録管理から包括的なガバナンス（おそらく監督や組織横断的な内部統制のための**スマートコントラクト**の活用）まで、ブロックチェーンは内部統制環境における「事業体」の概念だけでなく、関連する責任と要件も変える可能性がある。

*2013 年版フレームワーク*の３つの目的である「業務」「報告」「コンプライアンス」は、目的の達成方法という点でブロックチェーンによって大きな影響を受ける可能性がある。特に、多くの支持者は、記録管理が完全に変革され、完全にアドホックで自動化されたオンデマンドの報告活動やコンプライアンス活動につながると考えている。こうした変革に伴い、経営者、管理会計士、財務幹部、内部監査人および外部監査人の役割やスキルセットも変化していく可能性がある。

[i] 訳注：邦訳は、八田進二・箱田順哉監訳、日本内部統制研究学会新ＣＯＳＯ研究会訳『ＣＯＳＯ内部統制の統合的フレームワーク』日本公認会計士協会出版局、2014 年。

さらに、ブロックチェーンを事業環境へ導入すると、*2013 年版フレームワーク*の 5 つの構成要素に対して、以下のような影響があると考えられる。

表１．ブロックチェーンが５つの構成要素に及ぼす影響

構成要素	ブロックチェーンの影響
統制環境	ブロックチェーンは、（例えば、最小限の人的介入でトランザクションを記録することで）効果的な統制環境を促進するのに役立つツールとなり得る。しかし、この構成要素内の原則の多くは、経営者による誠実性や倫理観の促進など主に人間の行動を扱っており、他のテクノロジーを用いたとしてもブロックチェーンでは評価できない。より大きな課題は、ブロックチェーンに参加する他の事業体や人々と事業体が関わり合うことで、その結果、統制環境をどのように管理するかに関するものである。
リスク評価	ブロックチェーンは新しいリスクを生み出すが、同時に、説明責任の促進、記録の完全性の維持および反論の余地のない記録の提供（すなわち、個人や組織は、メッセージや記録の承認や送信における自らの役割を否定したり異議を唱えたりできない）により、既存のリスクの軽減に貢献する。
統制活動	ブロックチェーンは、統制活動を促進するためのツールとして機能できる。ブロックチェーンとスマートコントラクトは、（例えば、人的ミスや不正の機会を最小化することで）グローバルビジネスを効果的かつ効率的に行うための強力な手段となり得る。しかし、ブロックチェーンの協働的な側面は、特にテクノロジーが分散化され、ＩＣＦＲに影響するシステムに対して説明責任を負う単一の当事者が存在しない場合、さらなる複雑性をもたらす可能性がある。
情報と伝達	ブロックチェーン固有の特性は、トランザクションの可視性とデータの可用性の向上を促進し、経営者が主要な利害関係者に財務情報をより迅速かつ効果的に伝達するための新たな手段を生み出せる。経営者がブロックチェーンを適用する際に特に考慮すべき点の１つは、財務帳簿や記録を裏づける情報の可用性と、ブロックチェーン上で処理される情報の監査可能性である。
モニタリング活動	より頻繁な、より多くのテーマの、より詳細なモニタリングを促進するブロックチェーンへの期待は、実務を大幅に変える可能性がある。スマートコントラクトと標準化されたビジネスルールをモノのインターネット（ＩｏＴ）デバイスと組み合わせて使用することで、モニタリングの実施方法が変わる可能性がある。

ブロックチェーンの未来と財務報告やＩＣＦＲへの影響

ブロックチェーンの用途は今後も発展と進化を続け、採用が拡大すれば企業の運営方法を変える可能性がある。ブロックチェーンが財務報告や内部統制に及ぼす潜在的な影響について、多くの人々が慎重な楽観論を表明している。あらゆる破壊的テクノロジーと同様に、各組織は、自らの具体的な状況において、課題を評価し、関連するリスクをよりよく理解し、最善の行動を決定して、それらのリスクを是正するために協力する必要がある。

ブロックチェーン採用の支持者がブロックチェーンによってもたらされるとする変化の多くは、単独で見られるものではない。ブロックチェーンと何かを足したものが最もうまくいくのである。ブロックチェーンは基盤となるテクノロジーとして、世界のデジタルビジネスの状況を根本的に変える可能性があり、その結果、他のほぼすべてのものに大きな影響を与えることになる。

組織はブロックチェーンの利用を考える際に、以下の 10 項目を知っておくべきである（補足説明は付録２を参照）。

1. ブロックチェーンに関するニュースやインターネット上の情報は、誤解があったり間違っていたりすることがよくある。
2. ブロックチェーンは**デジタル資産**以上のものを含んでおり、それが組織にもたらす恩恵は相当なものになり得る。
3. ブロックチェーンは魔法ではなく、コストがかかり、すべてのリスクを排除できるわけではない。実際は、新たなリスクをもたらす。
4. ブロックチェーン・テクノロジーの仕組みを知ることは、ブロックチェーンが内部統制や組織全体に与える影響を評価し、準備し、管理する上で非常に重要である。
5. ブロックチェーンは、テクノロジーとガバナンスの両方への影響がある。
6. ブロックチェーンによって、経営者、会計士または監査人の存在意義が薄れることはないが、彼らが何をどのように行うかには影響を与える。
7. ブロックチェーンは、新しいスキルセット（例えば、より優れた事後的知見、洞察力および先見性のためのデータサイエンス）と、組織内および組織を超えた新たな協働を必要とする。
8. 今こそ、組織全体の利害関係者を啓発して巻き込むべき時である。
9. ブロックチェーンはまだ流動的であり、進化を続けている。
10. ブロックチェーンの採用は選択の余地がないかもしれない。

財務報告に対するブロックチェーンの潜在的な恩恵は、財務報告、内部統制および監査を理解して責任を負う人々が、ブロックチェーンに関する議論に積極的に関与し、共通の議題を進展させるために協力する場合にのみ最大化される。

1．はじめに

本稿では、ＣＯＳＯの『内部統制の統合的フレームワーク（*2013 年版フレームワーク*）』を使用して、財務報告という観点からブロックチェーン[1]に関するリスクを評価し、当該リスクに対応するための統制を設計する方法について説明する。本稿では、ブロックチェーンに関連するハイレベルな概念（その一部は付録 1 で説明）について説明しているが、ブロックチェーンに関する、あるいはブロックチェーンの利用に関連する、すべての問題、リスクおよび内部統制に関する包括的なガイドとなることは意図していない。以下の表は、本稿の対象読者と意図した用途に関する追加情報を示すものである。

表 2．**対象読者と意図した用途**

対象読者	意図した用途
取締役会 **監査委員**	（ガバナンスレベルで）以下を理解すること • ブロックチェーンに関する重要な概念 • 監督責任を強化するのに十分なレベルで、ブロックチェーンが内部統制に与え得る影響
経営幹部（最高経営責任者（ＣＥＯ）、最高財務責任者（ＣＦＯ）、コントローラー） **内部監査人、管理会計士、内部統制関係者**	（業務レベルおよび／または技術レベルで）以下を理解すること • ブロックチェーンに関する重要な概念 • *2013 年版フレームワーク*を活用して、ブロックチェーンの利用に関連する考慮事項を評価し、ブロックチェーンの利用についてより多くの情報に基づいた意思決定を行う方法 • ブロックチェーンを導入した場合に、*2013 年版フレームワーク*の各構成要素が受ける影響の例
外部監査人	（業務レベルおよび／または技術レベルで）以下を理解すること • ブロックチェーンに関する重要な概念 • ブロックチェーンに関する経営者の統制を評価する方法
教育関係者	（基礎研究や応用研究の関心に応じて）以下を理解すること • ブロックチェーンに関する重要な概念 • ブロックチェーンが内部統制に与え得る影響 • 概念や実際の適用について学生と共有する方法

本稿では、ＣＯＳＯの各構成要素について、以下を説明する。

- その構成要素を強化するためにブロックチェーンを使用する方法
- ブロックチェーンを使用することで発生する新たな脅威やリスク
- そのような脅威やリスクを軽減する方法の例

最後に、協働を強化する観点から、ブロックチェーンがより広く採用されるにつれてとり得る次のステップを示して締めくくる。

[1] 本稿では、ブロックチェーンや分散型台帳テクノロジーを指す言葉として「ブロックチェーン」を使用する。より広い意味では、これらの用語は互換的に使用されることもあれば、明確に区別されることもあるが、本稿での考え方は、概念レベルではどちらにも適用可能である。

2．ブロックチェーンという変革の波

ブロックチェーンが事業環境や運営環境にもたらす潜在的な変化を考慮すると、成功要因と推進力の両方として、内部統制への影響を検討することは賢明であると思われる。ブロックチェーンの導入により、既存の内部統制の弱点に対処する、あるいは弱点を解消するかもしれず、既存の統制を改善するために利用されるかもしれず、また、特に認知されたベストプラクティスがない場合には、実務の場面で新たなリスクや課題をもたらすかもしれない。

ブロックチェーンとは何か

ブロックチェーンには多くの相反する定義があるが、本稿では、さまざまな情報源を参考に、次の実用的な定義を用いる。*ブロックチェーンとは、追記専用台帳であり、チェーンへの追加に同意する責任を負うユーザの**分散型**ネットワークによって維持され、暗号化[2]によって保護された連続したデータベースである。*わかりやすく言うと、ブロックチェーンとは、参加者間で共有される安全で透明性の高い不可逆的なデジタル台帳のことである。ブロックチェーンにはさまざまな種類があり、唯一の「ザ・ブロックチェーン」は存在しないことに留意することが重要である。

ブロックチェーン採用の支持者がブロックチェーンによってもたらされるとする変化の多くは、単独で見られるものではない。「ブロックチェーン＋何か」（つまり、他の新興テクノロジー）が変化を可能にしているのである。これらのテクノロジーは、手作業を補完または排除し、関連情報をより適時に報告する、より合理的な財務報告の状態へと移行することに重点を置いている。ブロックチェーンの潜在的な進化をさらに引き出すのに役立つ可能性のあるツールやテクノロジーには、次のようなものがある。

人工知能（ＡＩ）

ＡＩは、意思決定、問題解決、感覚の模倣、学習、計画のようなタスクや、視覚認識や音声認識のような活動について、知的な機械が人間のように働いたり反応したりするコンピュータサイエンスの分野である。特に、パターンや異常値を識別するのに有効である。ＡＩは、人間の関与を補強するために、あるいはその代替として使用できる。例えば、ブロックチェーン上のリアルタイムの貿易取引データなどをＡＩで分析し、分類、記録、解析および意思決定において人間の判断をシミュレートできる。

モノのインターネット（ＩｏＴ）

モノのインターネットは、インターネットに接続できるモノのリストを広義に捉えたものである。ホームオートメーション機器のような、電源のオン・オフが可能なあらゆるものがインターネットに接続されると、周囲の環境をモニタリングし、報告し、対処できる、モノのネットワークの一部となることが可能である。ＩｏＴデバイスは、ブロックチェーンへ情報を書き込んだり、ブロックチェーンの情報に基づいて対処したりして、監査人の作業を支援できる可能性がある。

ビッグデータ・オープンデータ

事業体自身の帳簿や記録以外のデータ、いわゆる外部データが利用可能になれば、より広範な業界分析が促進され、高度な監査データ分析に大きな背景情報を提供できる。ビッグデータとは、ＩｏＴやソーシャルメディアなど、従来のアプリケーションでは処理できないほど大規模または複雑なデータソースからもたらされる多種多様なデータを指す。オープンデータは、ビッグデータのサブセットであり、一般に、構造化された大規模なデータセットで、通常、政府によって提供されている[3]。ビッグデータ、ＩｏＴ、ＡＩおよびブロックチェーンは、将来、すべて一緒に使われる可能性があり、内部統制プロセスと連動して、強力なツールセットとなる可能性がある。

[2] 暗号技術は、ブロックチェーンにトランザクションが入力される前に、コンセンサス・プロトコルを通じて合意されなければならないという点で関連がある。各ブロックは、一意の識別子（すなわち「**ハッシュ**」）で前のブロックにリンクされている。

[3] www.data.gov.（訳注：日本政府のものは、https://www.data.go.jp/）

内部統制への影響

ブロックチェーン対応の世界では、内部統制環境も異なる可能性が高い。そのため、ブロックチェーンの機能、特性、リスクおよび恩恵を考慮して、その違いを活用することが重要である。ブロックチェーンの機能を活かして内部統制を強化することで、以下を高める可能性がある。

- 業務の有効性と効率性
- 財務報告やその他の報告の正確性、一貫性および信頼性
- 適用される法令のコンプライアンス

多くの点で、ブロックチェーンソリューションの導入と運用に関する統制上の考慮事項は、新しいエンタープライズ・リソース・プランニング（ＥＲＰ）や文書管理システムの導入と運用に関する統制上の考慮事項とよく似ている。財務報告の統制を考える場合、一定の「主要」財務統制（例えば、照合）とプロセス（例えば、財務報告書の作成）は、おそらく根本的に変わる。さらに、新たなリスクが発生し、新たな統制が必要となる。財務報告の統制とプロセスがどのように変更されるかについての例示は、サイドバー（補足説明）を参照されたい。

財務報告の統制とプロセスの変更例

統制環境に関連する内部統制

異なるブロックチェーン環境内で、事業体が課すことのできる統制の量はさまざまである。多くの場合、統制はもはや事業体内にはとどまらない。このことは、事業体が統制環境内の問題を検討して評価する方法に影響を与える。

照合

照合の多い分野（例えば、会社間取引）に対応するためにブロックチェーンソリューションを活用することにより、照合は高度に合理化と効率化がなされ、取引の全当事者の可視性を高める結果となる。

確認

ブロックチェーン上で取引の再計算ができるようになれば、ある種の確認は必要なくなるかもしれない。しかし、新たなサービスプロバイダとの別の確認の必要性が高まる可能性もある。

ベンダーやサプライヤーの承認

ブロックチェーンの利用は、組織とベンダーやサプライヤーとの関係のあり方（例えば、取引の処理方法、価格に対する可視性、情報の報告や透明性）を変える可能性がある。

第三者のサービスプロバイダ

他のテクノロジーソリューションと同様に、ブロックチェーンソリューションも内部で管理される場合と外部から調達される場合がある。外部調達されたシステムの多くは、通常、業務受託会社である特定の第三者によって監督される。経営者は、「業務受託会社のシステムに関する『第三者の』経営者確認書の表現の公正さ、および特定期間を通じて確認書に含まれる関連する統制目的を達成するための統制の設計と運用の有効性の適合性」に関する情報を提供する業務受託会社のシステムおよび組織統制（ＳＯＣ）のタイプ２[4]の報告書を要求できる。したがって、こうした環境での何らかの形のＳＯＣ報告書に対する需要は増加すると思われる。

分散型外部システム

ブロックチェーンの世界では、特定のブロックチェーンを監督する単一の中央管理者が存在しない場合がある。設計者が事前に定めたルール（プロトコル）や当事者の合意による変更は伝えられるが、統制目的の達成に説明責任を持ち、問題があった場合に責任を負うような、単一の外部機関が存在しない場合がある。この説明責任の欠如は、深刻な問題である。一元管理されていなければ、ＳＯＣ監査人を雇う簡単な方法がないかもしれず、ＳＯＣ報告書がない場合、企業は代替策を検討しなければならない。

[4] www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html.

財務報告の統制とプロセスの変更例（続き）

デジタル資産の統合

ブロックチェーンが従来のテクノロジーソリューションとは異なるもう１つの点は、デジタル資産をシステムに統合することである。ブロックチェーンの中には、他のどこにも存在せず他の方法では追跡できない、独自に統合されたデジタル決済や価値を持つものがある。従来のシステムは、銀行や他の金融システムにリンクできるが、ブロックチェーンは、時にはシステムそのものである。

電子的監査証跡

ある種のブロックチェーンから得られる重要な恩恵は、すべてのトランザクションの電子的記録（すなわち、監査証跡）が自動的に作成されて存在することである。とはいえ、所有権や権利の決定に関してはさらなる課題が存在し、ブロックチェーン上にトランザクションがあるからといって、必ずしも帳簿や記録の目的でトランザクションが検証されるわけではない。さらに、監査人が見つけたい証拠がチェーン自体（「オンチェーン」）にはない可能性もあるが、他の情報源（「オフチェーン」）が存在し容易に入手できる場合には、その情報を入手できる十分な状況が存在する可能性もある[5]。

内部監査と外部監査の業務

内部統制を実施するための基盤となるブロックチェーン対応のプラットフォームを考えると、統制の自動化や他の新興テクノロジー（ＡＩ、ＩｏＴなど）との相互作用が高まることで、外部監査人と内部監査人の両方の業務が促進される可能性がある。ブロックチェーンによって促進される内部統制環境は、外部監査人がよりよく依拠できる内部監査環境を可能にするかもしれない。外部監査人と内部監査人が行う業務の連携が強化され、対象とする範囲が拡大する可能性がある。

継続的でリアルタイムな財務報告

より実質的かつ実態に即した継続的リアルタイム財務報告が可能になり、日常的なものとなる可能性がある。組織から事前に合意した定期的な報告書を受け取るのではなく、ブロックチェーンにアクセスして独自のアドホックな報告書を作成したい（そして、リアルタイムの情報にアクセスできるようにしたい）当事者もいるかもしれない。

モニタリングが唯一の「事後」統制となる

トランザクションがシステムにヒットした時点で、最終的な報告書があらかじめ決定されるほど内部環境が合理化されると、モニタリング以外のすべてが「事前」、つまりトランザクションの処理前とみなされ、「事後」、つまり処理後に必要な統制はモニタリング統制のみというケースもあり得る。

ブロックチェーンの世界における統制の種類

統制は、予防的（リスクが顕在化する前）と発見的（リスクが顕在化している最中または後）に特徴づけられる。ブロックチェーンでも、これらの統制の種類は関連性があり、当てはまる。

表３．**ブロックチェーンが統制の種類に及ぼす影響**

統制の種類	ブロックチェーンの影響
予防的統制	ブロックチェーンに記録されたトランザクションは不変であることを認識し、トランザクションを最初に正しく記録することに重点を置いている。
発見的統制	ブロックチェーンの世界におけるトランザクションの可視性は、必要な情報が**オンチェーン**で入手できるか、オンチェーンの記録から**オフチェーン**の情報を発見できる場合、発見的統制の新たな手段を提供する。さらに、相当量のデータが利用可能であるため、ブロックチェーンとＡＩ、ＩｏＴおよびデータアナリティクスのような他の新興テクノロジーの分析能力を組み合わせることで、異常を発見する手段として利用できる可能性がある[6]。ブロックチェーンの世界では、問題が確認されたときにどうするかが課題である。一般に、修正はこれまでどおり可能だが、ブロックチェーンの追記専用という特徴を考えると、修正は既存のトランザクションを直接修正するのではなく、調整として反映させる必要がある。ただし、これは使用している特定のブロックチェーンの仕様に依存することになる。

ブロックチェーン上でトランザクションが処理され記録されるスピードと、そのようなトランザクションの不変性と不可逆性を考慮すると、企業が重大な損失やエラーのリスクを軽減する支援をするためには、発見的統制よりも予防的統制の実施がより普及する可能性が高い。また、企業は、より適時にエラーを特定するために、発見的統制の実施頻度を高めることを検討してもよい。

[5] オンチェーンとは、ブロックチェーン自体に格納されている情報を指す。これに対し、オフチェーンとは、ブロックチェーン上に格納されていないが、オンチェーン上の情報と直接的または間接的につながっている情報を指す。

[6] 例えば、社内で作成したデータと社外で作成したデータの比較は非常に効率的で、矛盾があればすぐに発見して明らかにできるようになる。これは強力なモニタリングの手段になる。４ページのサイドバー（補足説明）も参照されたい。

3．構成要素と原則の概要

ブロックチェーンを導入する際は、ＣＯＳＯの各構成要素と原則（表４参照）を考慮した上で、ＩＣＦＲへの潜在的な影響を分析すべきである。以下を検討することは有益である。

- *2013 年版フレームワーク*の原則を達成する上でのブロックチェーンの有用性
- ブロックチェーン導入で発生し得る、当該原則に影響を及ぼす新たな脅威やリスク
- 最大の利益を追求しながら、それらのリスクを軽減する方法の例

表４．**2013 年版フレームワークの統制の構成要素と原則の要約**

構成要素	原則
統制環境	1．誠実性と倫理観に対するコミットメントの表明 2．監督責任の遂行 3．組織構造、権限・責任の確立 4．業務遂行能力に対するコミットメントの表明 5．説明責任の履行
リスク評価	6．適合性のある目的の特定 7．リスクの識別と分析 8．不正リスクの評価 9．重大な変化の識別と分析
統制活動	10．統制活動の選択と整備 11．テクノロジーに関する全般的統制活動の選択と整備 12．方針と手続を通じた統制活動の展開
情報と伝達	13．関連性のある質の高い情報の利用 14．組織内における情報伝達 15．組織外部との情報伝達
モニタリング活動	16．日常的評価および／または独立的評価の実施 17．不備の評価と伝達

ブロックチェーンに関連する内部統制の機会とリスクは、導入するブロックチェーンの特性と種類、ならびに組織がさまざまなブロックチェーン環境内で課すことのできる影響力、監督および統制の量によって異なる。*2013 年版フレームワーク*をブロックチェーンに適用するにあたっては、以下の点に留意することが重要である。

- **プライベート型**の**許可型ブロックチェーン**を単一の企業内に導入することは、いくつかの新たな考慮事項とリスクをもたらすが、経営者に入力、処理および出力を含め、ブロックチェーンを統制する能力があれば、これまでのテクノロジー採用とよく似た経験となるだろう。
- **コンソーシアム型ブロックチェーン**や別の組織のプライベート型ブロックチェーンに参加すると、リスクや統制が組織間で共有され、より協調的な意思決定が求められるなど、組織間の新たな課題が発生する。
- **パブリック型**の**許可不要型ブロックチェーン**を財務報告環境の一部にすると、意思決定が分散化され、個々の影響力の余地が少なく、個々の説明責任がほとんどないため、まったく異なるリスクと課題が発生する。これは外部の業務受託会社の利用と比較されるかもしれないが、経営者はこれらの「外部委託した」プロセスについて、より広範かつ可能な限り深い見識を持つ必要がある。

統制環境

概要	原則
1．誠実性と倫理観に対するコミットメントの表明	組織は、誠実性と倫理観に対するコミットメントを表明する。
2．監督責任の遂行	取締役会は、経営者から独立していることを表明し、かつ、内部統制の整備および運用状況について監督を行う。
3．組織構造、権限・責任の確立	経営者は、取締役会の監督の下、内部統制の目的を達成するにあたり、組織構造、報告経路および適切な権限と責任を確立する。
4．業務遂行能力に対するコミットメントの表明	組織は、内部統制の目的に合わせて、有能な個人を惹きつけ、育成し、かつ、維持することに対するコミットメントを表明する。
5．説明責任の履行	組織は、内部統制の目的を達成するにあたり、内部統制に対する責任を個々人に持たせる。

統制環境とは、主にリスクと統制を意識したカルチャーの存在と、誠実性と倫理観に対する事業体のコミットメントに合致した方法で責任を遂行するよう、あらゆる階層の人々を導く方針、プロセスおよび構造に関するものである。ブロックチェーンを（刺激的でおそらく革命的ではあるが）単なるテクノロジーの１つと認識すると、統制環境に対する潜在的な影響を過小評価する結果になりかねない。ブロックチェーンは、人間の本質や、統制環境全体に大きな影響を与えるガバナンスの行動面を変えるものではない。これらは利用するテクノロジーを問わず、ほとんど変わらない。

とはいえ、ブロックチェーンを利用する際には、重要な統制環境上の影響がある。経営者は、ブロックチェーンの利用が事業体の誠実性や倫理観へのコミットメントを支えるかを評価するために、事業体におけるブロックチェーンの利用計画や、特定のブロックチェーンのガバナンス構造（すなわち、独自のガバナンス構造およびその構造の継続的な健全性や運用の有効性）を十分に理解できる適切なスキルセットを持つことが重要である。また、取締役会が監督責任を果たすためには、ブロックチェーンを十分に理解することも重要である。

ブロックチェーンを活用した統制環境の強化

- ブロックチェーンは、最小限の人的介入でトランザクションを実行して記録する方法を組織に提供できる。さらに、ブロックチェーンの高度に自動化された特性と、共有台帳上で変更不可能なトランザクションを検証して記録する機能は、人的ミスを回避し、取引や報告の不正に対処する機会を組織に提供する。
- ブロックチェーンでは、プロセスは通常、暗号によって検証可能な**不変性**と不可逆性がある。したがって、適切に設計され導入されたブロックチェーンでは、経営者は活動の証拠を信頼して提供できるはずである。
- 共有台帳システムによる可視性の向上は、透明性の向上に寄与し、強固な統制環境を促進するとともに、リアルタイムの財務報告を容易にする。
- ブロックチェーンは、ＡＩやデータアナリティクスのような他の新興テクノロジーの分析能力と組み合わせると、組織の行動基準からの逸脱をより適時に特定できるようになるかもしれない。これは、大規模および／または分散型の組織において効果的な監督を実施する際に、特に有用であることが証明される可能性がある。
- 場合によっては、ブロックチェーンによって、経営者の手作業によるプロセスへの介入を排除し、経営者の意思決定、誠実性および倫理観の影響をほとんど受けないようにすることを促す可能性がある。

ブロックチェーンの活用がもたらす新たな脅威やリスク

- ブロックチェーン上でトランザクションを行う当事者の擬似匿名性[7]は、オープンな特性と防御策が欠如している可能性と結びつくと、許可不要型ブロックチェーンが倫理にもとる悪用をされ得るという脅威を引き起こす[8]。
- 各ブロックチェーンには、独自のガバナンス構造が設定されており、その健全性や運用の有効性を積極的にモニタリングする必要がある。ある種のブロックチェーンでは、分散型であり、当事者の行動に責任を持たせる中央の管理者、システムまたは監督機関がないため、文字どおり「管理者

[7] パブリック型ブロックチェーンでは、ブロックチェーン・アドレス間で資産のやりとりが行われ、認証には秘密鍵が使われるが、そのアドレスや鍵に人名や組織名が明示的に関連づけられることはない。このため、個人を特定できる情報を与えずにトランザクションを行えるので、身元を偽装したような状態になる。しかし、さまざまな非匿名化手法により、身元を明らかにすることは可能である。

[8] ブロックチェーンに取引主体識別コード（ＬＥＩ、組織を識別するための国際的な固有シリアル番号）を組み込む取り組みが進められており、これにより利益相反の特定と評価が容易になる一方で、疑似匿名性を考えると、現在の仮想空間では倫理にもとる悪用のおそれが残っていることを認識すること。

不在」状態になる。物事がうまくいかないとき、ある種のブロックチェーンでは、誰にも頼ることができず、したがって説明責任もなく、ガバナンスに関する重大な欠点となる。

- 一般に、ブロックチェーンの利用は先進的で前向きなものと考えられているが、ブロックチェーンを提唱、採用および受容する行為や、特定のグループと関わることは、組織の従業員、顧客、アドバイザーおよび監督者から否定的に捉えられる可能性がある。さらに、ブロックチェーンの特性やブロックチェーンに参加する仲間によっては、参加することでグループの最低限の倫理観を共有していると受け取られ、組織が評判リスクに直面する可能性もある（つまり、関連づけによる評判）。ある種の取り決めについては、参加者やシステムの**コンセンサス**の変更を管理することは、経営者の統制の範囲外となる。

- ブロックチェーンの新規性と複雑性は、有能な人材がなかなか見つからず、能力へのコミットメントを保証したり評価したりすることが難しいことを意味する。ブロックチェーンが広範な自動化を促進する可能性があることは、より多くの作業を自動的に行えることを意味し、人々の責任と関連する能力の特性が、時には劇的に変化する可能性がある。同様に、経営者やガバナンス担当者は、ブロックチェーンの導入と利用を効果的に監督するための適切なレベルの理解と専門知識を得ることが難しい場合もある。

ブロックチェーンの導入に伴う新たな脅威やリスクの軽減

識別された特定のリスクへの対応として、経営者と取締役会は以下の措置を検討することができる。

- 適用可能であれば、ブロックチェーン内の当事者の行動を規定する行動規範を策定し、コンプライアンス違反に対処するためのガイドラインを確立する。プライベート型ブロックチェーンの導入やコンソーシアム型ブロックチェーンの開発を目指す組織は、そのような行動規範や、（１）倫理観と誠実性に対する各メンバーのコミットメントを検証する仕組み、（２）行動規範に基づく説明責任の遂行や逸脱の報告、対処および是正の仕組み、を整備するとよい。組織は、ガバナンスプロセスを明確に理解し、それが効果的であるかを積極的にモニタリングして評価すべきである。また、可能であれば、確立した行動規範の監督と遵守の検証を行うために、独立した外部者を関与させることを検討してもよい。このような場合、組織は、外部者が各当事者のガバナンス担当者に直接報告するよう、明確な報告経路を確立することが重要である[9]。

- また、外部委託のサービスプロバイダの行動規範、責任および権限に関する期待も検討する。外部委託のサービスプロバイダに関連する活動の多くはブロックチェーンの外で行われるが、外部委託のサービスプロバイダに関連する信頼性の低いデータがブロックチェーンに入り込むと、その結果は厄介なものになり得る。

- 組織がトランザクションを行う当事者、組織がブロックチェーンへのアクセスを許可する当事者および組織がトランザクションの実施に使用することを選択できるパブリック型ブロックチェーンを決定するための、ガイドラインと基準を確立するデューディリジェンス方針を策定する。これらの方針には、取引相手の身元と健全性を把握するための身元確認（ＫＹＣ）手続、マネーロンダリング防止（ＡＭＬ）手続、ＳＯＣレポートの要求および他のデューディリジェンス手続が含まれる場合がある。このような手続には、ブロックチェーン内の当事者の行為を管理するために設けられた方針を把握することも含まれる。ガバナンスプロセスを常に把握して、その有効性を継続的にモニタリングすることが特に重要である。

- ブロックチェーンの効果的な導入と導入後の適切な利用や更新を確実にするために、ブロックチェーン・テクノロジーに関する専門知識を入手または修得する必要性を評価する。さらに、ブロックチェーン・テクノロジーは急速に進化し続けるため、そのような能力の再評価とモニタリングを継続すべきである。

- 新しいテクノロジーやプロセスを評価して判断する能力を組織が持つようにする。これは、社内のリソースや外部委託のリソース、またはその組み合わせにより達成できる。

[9] 行動規範を確立することは、パブリック型ブロックチェーンでは実現不可能である可能性が高い。そのため、経営者やガバナンス担当者は、パブリック型ブロックチェーンの使用に関連するリスクと、そのリスクに対する許容度を評価する必要がある。

- ブロックチェーンの専門家と、ブロックチェーンの導入に影響を受けるビジネスの各分野（例えば、ＩＴ、会計、財務、オペレーション、内部監査）の代表者を含む、分野横断的なチームを設置する。このようなチームは、計画、開発および導入の各プロセスを通じて関与すべきである。

- 取締役会と監査委員会がブロックチェーンに関連する潜在的な用途とリスクを理解する能力と、ブロックチェーンの導入と利用を効果的に監督する能力を評価して、必要に応じて強化する。

- 職務分掌に関する懸念（例えば、アクセスレベルの特権、**秘密鍵**へのアクセス、トランザクションの承認機能、関連する財務報告）を考慮して、ブロックチェーン・テクノロジーを取り巻く責任と権限の程度や水準を定義する。内部統制の鍵となるブロックチェーンをめぐる権限と責任について、割り当てた程度や水準に対する適切な後継者計画を策定する。

- コンソーシアム型またはプライベート型ブロックチェーンにおいて、基盤となるプロトコルに組み込まれていない場合、ネットワークのメンバー間で発生する紛争を処理する責任を負う個人またはグループを特定する明確な報告経路を確立する。これには、紛争解決の管轄裁判所や相互に合意した手続に加え、「和解しがたい相違」が生じた場合の離脱の可能性を定義することを含む場合がある。

リスク評価

概要	原則
6．適合性のある目的の特定	組織は、内部統制の目的に関連するリスクの識別と評価ができるように、十分な明確さを備えた内部統制の目的を明示する。
7．リスクの識別と分析	組織は、自らの目的の達成に関連する組織全体にわたるリスクを識別し、当該リスクの管理の仕方を決定するための基礎としてリスクを分析する。
8．不正リスクの評価	組織は、内部統制の目的の達成に対するリスクの評価において、不正の可能性について検討する。
9．重大な変化の識別と分析	組織は、内部統制システムに重大な影響を及ぼし得る変化を識別し、評価する。

リスク評価には、目的達成に対する脅威を識別して評価する反復プロセスが含まれる。ブロックチェーンは、対処すべき新たな目的とリスクをもたらす可能性がある。ブロックチェーンに関連する特有のリスクを理解して、継続的にリスクを識別、評価し、かつ、かかるリスクに対応するために、組織は適切なスキルとリソースを持つことが重要である。

ブロックチェーンを活用したリスク評価の強化

- ブロックチェーンを他の新興テクノロジーと統合することで、経営者、取締役会および外部関係者に、リアルタイムな報告を提供することができる。これにより、さまざまな事業体目的（例えば、業務、外部財務報告、コンプライアンスまたはその他の内部目的）の達成度を識別して評価する、より機動的な事業環境を創出することができる。

ブロックチェーンの活用がもたらす新たな脅威やリスク

- 従来のリスク評価は、事業体に焦点を当てたものであったが、ブロックチェーンの利用により、企業はより広範にリスクを検討する必要がある。例えば、事業体は、ブロックチェーン・ネットワーク内の他の当事者がリスクに曝される可能性や、それが各々の事業に及ぼし得る影響を検討する場合がある。さらに、ブロックチェーンのメンバー間でリスク選好やリスク許容度が異なると、ブロックチェーン用のモニタリング統制を設計する際に対立が生じる可能性がある。ある種のブロックチェーンでは、誰１人として担当者がいない場合に誰がリスク管理に責任を持つのか、適切な説明責任をどのように果たすのか、といった疑問が生じる可能性がある。

- ブロックチェーンの導入により、企業は新たな不正スキームや従来の不正スキームを実行するための新たな手段に対して脆弱になる可能性がある。例については、右のサイドバー（補足説明）を参照されたい。

- ブロックチェーン対応の環境では、データ量が管理しきれないほど膨大になる可能性があり、あまりにも多くのデータを管理しようとすると、データ過多となり、データガバナンスの問題が深刻化する。

- **スマートコントラクト**は、潜在的なリスクでもあり、リスク軽減のための重要なツールでもある。一旦導入されると、自己実行されて停止することは難しい。そのため、不正に開発されたり操作されたりすると、その影響でエラーや大規模な損失が発生する可能性がある。

- ブロックチェーンの利用は、組織の財務記録に記録された取引を裏づける十分かつ適切な証拠の取得をめぐる（すなわち、電子環境下でのトランザクションの監査証跡の喪失による）問題を生じさせる可能性がある。

- **デジタル資産**は、リスクの管理や異常行動の特定に関して、過去の経験がほとんど、あるいはまったくなく、意味のある類似性もほとんどない新しい種類の資産である。デジタル資産の保有を検討している企業は、ある種のデジタル資産の市場の変動や市場の欠如、秘密鍵の保護に関するサイバーセキュリティリスク、このような資産の会計や財務報告、進化する規制要件など、資産そのものに関する追加的な検討事項がある。

新たな種類の不正スキームの例

- デジタル共有台帳に格納される財務情報の信頼性は、基盤となるテクノロジーに依存する。ブロックチェーンの基盤となるコンセンサス・メカニズムや他の部分が改ざんされた場合、台帳に格納された財務情報が不正確で信頼できないものになる可能性がある。

- ブロックチェーン上の当事者の擬似匿名性は、共謀の機会を増やしたり関連する当事者間取引をわかりにくくしたりする可能性がある。このリスクは、そのようなネットワーク上の多数の未知の当事者による、より擬似匿名性の高い環境の可能性を考慮すると、パブリック型ブロックチェーンに関してより当てはまるかもしれない。

- 信頼性の高いブロックチェーンはトランザクションのセキュリティを提供するが、アカウントやウォレットのセキュリティは提供しないため、組織の秘密鍵が盗まれたり危険に曝されたりした場合、どのアカウントに保存されている価値でもアカウント乗っ取りの影響を受ける可能性がある。

- ブロックチェーンに対する、サイバーセキュリティ上のリスクが高まっている。サイバー攻撃の結果、基盤となるテクノロジーが侵害された場合、組織の資産が盗まれる可能性がある。さらに、サイバー攻撃の影響は、組織を超えてネットワーク内の他の組織にまで及ぶ可能性がある。また、ブロックチェーンは暗号技術やウォレットを利用し、分散型であることから、サイバーリスクに影響を与える固有の側面がある。

- ブロックチェーンと既存の旧システムとの統合という課題が発生する可能性がある。ブロックチェーンは、より大きな中核インフラの一部のツールになる可能性が高く、従来のインフラと一体となって動作する必要がある。ブロックチェーンと事業体の他のシステムとの統合がうまくいかないと、顧客体験の低下や規制違反の問題など、あまり望ましくない結果になる可能性がある。右のサイドバー（補足説明）を参照されたい。

- ブロックチェーン、スマートコントラクトおよびデジタル資産を取り巻く規制環境は進化を続けており、法域によって異なる可能性があるため、（税金、データプライバシーおよび保護、報告、またはその他の規制要件を含む）規制要件についての不確実性が生じる可能性がある。

- ブロックチェーンの事業環境も進化を続けており、テクノロジーの改善、ベストプラクティスおよび新たなユースケースが日々確認されている。目まぐるしく進化する環境をモニタリングすることは、困難だがやりがいのあるものかもしれない。

- 現存する断片的なソリューションは、すぐに取って代わられるかもしれない。テクノロジーとその手法に時間、人材、資金、そして、マスコミ報道が多大な投資を行った結果、ソリューション市場は非常に断片化し、機能が重複し、相互運用性がほとんどない状態になっている。ブロックチェーン開発に対する行き当たりばったりで協調性のないアプローチが続いていることから、ガートナー社は、2019 年に導入したブロックチェーンの 90%は、2021 年までに置き換えが必要になると予測している [11]。

また、高度に自動化されたテクノロジーの特性上、ブロックチェーン環境では、以下の領域において、一般的なＩＴリスクやその他のリスクが悪化または増大する可能性がある。

- システムへのアクセス権やデータとプログラムの完全性といった問題は、他のテクノロジーソリューションにも共通するものだが、ブロックチェーン上では不適切なアクセス問題の影響が企業間の共有問題となり得るため、テクノロジーのアクセス権に関する懸念が高まっている。

ブロックチェーンの相互運用性

企業が複数のチェーンの統合を重視していることが示唆されるものの、ブロックチェーンの相互運用性に関連する成功例は限られている [10]。ウェブがプラットフォームの不可知性をもたらし、Ｍａｃ、ＰＣおよび携帯端末のすべてが重要なリソースにアクセスできる時代において、現在のブロックチェーンの利用は大部分が独立型である。今後の利用は、価値ネットワークがサービスネットワークと情報を交換し、サービスネットワークがコンテンツネットワークと情報を交換し、すべてがＡＩやＩｏＴ、あるいは従来のデータベースやシステムと連携するような相互運用性が求められるようになる。採用がさらなる採用や機能強化を生み、それがさらなる採用を生むというネットワーク効果は、これまで市場が証明してきたことである。

- ブロックチェーンが多くの関係者に可視化される場合、可視化されることによってサイバーセキュリティ上の課題やサイバー攻撃がもたらされる可能性がある。

- 大部分のパブリック型ブロックチェーンでは、ユーザは導入されている一般的なＩＴ統制とその有効性について把握できないかもしれない。さらに、プロトコルの修正を管理して執行する中央機関が存在しない場合、テクノロジーの開発プロセスや保守プロセスの統制活動を確立することが難しくなる可能性がある。

- ブロックチェーンにトランザクションが記録されるスピードと、トランザクションの不変性と不可逆性を考慮すると、ブロックチェーンに係る内部統制の不備を適時に識別して修正しない場合、組織は重大な損失やエラーが発生するリスクの高まりに直面する可能性がある。さらに、中央集権的な監督者や仲介者がいないことで、エラーや損失が発生した場合に企業が救済手段を失い、ガバナンス上の課題が生じる可能性がある。ブロックチェーンベースのトランザクションを行う企業は、不正行為があった場合、資金を取り戻すために銀行のような中央の仲介者に頼ることはできない。そのため、企業は内部統制インフラの強化が必要かどうかを検討する必要がある。

[10] Deloitte's 2019 Global Blockchain Survey, Blockchain Gets Down to Business. Deloitte Insights.
[11] https://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain.

- 組織がブロックチェーンを取り入れ始めると、移行期間が設けられることになる。この間、旧システム、ＥＲＰまたは第三者のクラウドベースシステムがフロントエンドの処理とデータ収集を行い、その後ブロックチェーンと接続して追加の処理や記録を行うことになる。ブロックチェーンに格納されたデータはほぼ安全で改ざんできないものの、ブロックチェーンの外にいる間は一般的なＩＴリスクに対して脆弱なままである[12]。上流システムからブロックチェーンへのデータのインターフェース送信は、こうした新しい環境において慎重に扱うべき統制ポイントになる。

ブロックチェーンの導入に伴う新たな脅威やリスクの軽減

識別された特定のリスクへの対応として、組織は以下のような措置を検討する必要があるかもしれない。

- 適切な会計処理と効果的な財務報告を可能にするために、信頼し得る検証可能な帳簿と記録を裏づけるようなブロックチェーンの使用目的を確立する。

- 組織のあらゆる側面にブロックチェーンが及ぼす影響を考慮した、より強固なリスク評価プロセスを策定する。このような評価を策定する際、企業は、（組織の統制環境、ブロックチェーンおよび一般的な不正スキームに関する知識に基づいて）潜在的な脅威、リスク領域および不正スキームの特定を支援するために、関連するＩＴやブロックチェーンの専門家に依頼することが有用である。ブロックチェーンの導入前に、このようなリスク評価プロセスを実施することは、このテクノロジーに関連する潜在的な恩恵とコストを評価する上でも有用である。

- ブロックチェーンを取り巻く事業環境と規制環境の変化を把握するための手続を策定する。テクノロジーの導入に際して、事業体の法律顧問や内部監査部門を早期に関与させることは、規制環境の変化について情報を得るのに役立つ可能性がある。

- ブロックチェーンが組織のビジネス情報プロセスに統合され、その統合が財務報告に影響するようになると、経営者は、財務報告、内部統制、適切な会計処理および監査への影響（例えば、監査可能性についての課題がある可能性）に関連する新たなリスクを特定するために、適切な関係者（例えば、内部監査人や外部監査人）を関与させるべきである。

- ブロックチェーンの導入に先立ち、事業体の既存システムに精通した適切なＩＴやブロックチェーンの専門家を関与させ、ブロックチェーンが事業体の既存のＩＴインフラにどのように統合され、その一部として運用されるかを評価する。

- 新しいスマートコントラクトの導入や既存のスマートコントラクトの修正、あるいはブロックチェーンへの変更を行うために、強力なガバナンスプロセスと変更管理プロセスを策定する。このようなプロセスでは、インシデント対応管理や、スマートコントラクトとブロックチェーンの運用における不具合の特定と対応の方法についても考慮すべきである。

統制活動については、次章でより詳細に説明するが、不正行為やサイバーセキュリティのリスクを軽減するための統制の例には、以下が挙げられる。

- ブロックチェーンのトランザクションを承認する機能（すなわち、秘密鍵へのアクセス）と、事業体の総勘定元帳内の取引を記録する機能との間で適切な職務分掌を導入し、さらに基盤となるテクノロジーへの変更を承認して実行する機能を取り巻く適切なアクセス統制を確立する。
  - 望ましくない結果を避けるために、職務分掌を含め、ブロックチェーンのプロトタイプや現実的なユースケースを通じてユーザ受入テストを実施すべきである。

- ブロックチェーンと事業体の総勘定元帳システムおよびその他のオフチェーンシステムとの間の情報授受に係る統制を確立する。

- マルチシグネチャや鍵のシャーディング技術[13]を使用して、ブロックチェーンベースのトランザクションを承認する機能を管理する。

[12] M.D. Sheldon, "A Primer for Information Technology General Control Considerations on a Private and Permissioned Blockchain Audit," Current Issues in Auditing, Vol. 13, No. 1, (Spring 2019: A15–A29).
[13] 鍵のシャーディングは、マルチシグネチャと同様に、複数の関係者が関与することで、リスクと統制を分散させる鍵管理方法である（秘密鍵の一部を分割するなど）。

- 侵入者が情報システムにアクセスするのを防ぐために、また、侵入が発生した場合、最初の防御層が侵害された後、迅速に発見してさらなるアクセスを防止するために、予防的統制と発見的統制を組み合わせて展開する。
- 組織とブロックチェーン・ネットワークの他のメンバーが共有するサイバーセキュリティリスクの識別と対応の方法についての評価を含む、サイバーセキュリティリスクの識別と評価を管理する体系的なアプローチを策定して導入する。

統制活動	
概要	**原則**
10. 統制活動の選択と整備	組織は、内部統制の目的に対するリスクを許容可能な水準まで低減するのに役立つ統制活動を選択し、整備する。
11. テクノロジーに関する全般的統制活動の選択と整備	組織は、内部統制の目的の達成を支援するテクノロジーに関する全般的統制活動を選択し、整備する。
12. 方針と手続を通じた統制活動の展開	組織は、期待されていることを明確にした方針および方針を実行するための手続を通じて、統制活動を展開する。

統制活動は、目的の達成に対するリスクの軽減に役立ち、組織のあらゆる階層、ビジネスプロセス内のさまざまな段階およびテクノロジー環境にわたって実施される。統制活動は、予防的または発見的な特性を持ち、許可や承認、検証、照合または業績のレビューのような、手動または自動で行われるさまざまな活動を含む場合がある。統制活動のゴールは、目的の達成に対するリスクを許容可能な低水準まで十分に軽減することである。

ブロックチェーンは、暗号化手法の使用、スマートコントラクトの作成機能および可視性の向上機能を備えており、統制活動を可能にし、そうした統制をより信頼性の高い安全なものにし、この状況下で必要な手順を実行するための強化されたツールや新しいツールを提供する重要な補助手段となり得る。同時に、統制活動やＩＴ全般統制に特化した検討を必要とする新たな課題も出現している。

ブロックチェーンを活用した統制活動の強化

- 適切に設計され導入されたブロックチェーンは、企業の内部統制をさらに強化する機能を提供する可能性がある（例えば、説明責任の促進、記録の完全性の維持、反論の余地のなさなど）。適切に導入されたブロックチェーンは、過去のデータの記録、修正または削除への直接アクセスに対する懸念を軽減できる。例えば、ある種のブロックチェーンでは、一旦あるブロックが十分に覆われ（すなわち、より新しい検証済みのブロックがその上に存在する）と、運営管理者が変更を行うことに同意するか、（ブロックチェーンのセキュリティ違反がないと仮定して）チェーンが**分岐**しない限り、過去のデータが変更されるリスクは最小限に抑えられる。
- ブロックチェーンには高度に自動化された特性があり、共有台帳上で変更できないトランザクションを検証して記録するテクノロジーの機能と組み合わせることで、財務報告プロセスにおける人的介入を減らし、企業は取引や報告の不正に対抗する機会が得られる。ブロックチェーンの利用により、従来の不正行為や手作業によるミスの機会が減少し、損失リスクが軽減される。さらに、複数のメンバーがコンセンサス・プロトコルに参加することで、転記前に多くの当事者が取引の正確性を検証するため、誤りが特定される可能性が高くなる。
- ブロックチェーンは、データ損失のリスクを最小限に抑えるため、ある種のＩＴ全般統制が不要になる。そのため、プラットフォームが放棄されたり使われなくなったりしない限り、データのバックアップ、**ノード**間のバッチ処理および災害復旧といった従来の統制は不要になる可能性がある。ブロックチェーンの台帳はネットワーク上の複数のノードで共有されるため、最新バージョンの台帳はネットワーク上の影響を受けていない他のノードから復元できる可能性があり、バックアップへの依存はあまり重要ではない。
- ブロックチェーンを使用すると、特定のブロックチェーンによっては、ほぼリアルタイムでトランザクションを処理して記録する機能を組織に提供できるため、トランザクションの処理や記録が適時でなくなるリスクも軽減される可能性がある。この機能により、エラーを大幅に減らせる。

- スマートコントラクトは、統制活動を強化し、（契約条項の実行を自動化することにより）不正の機会を防止できる。ただし、スマートコントラクトはツールであるため、スマートコントラクトが使用するツールや（ブロックチェーンの**オラクル**からの入力を含む）入力は、不正を行うために操作される可能性があることに留意が必要である。

ブロックチェーンの活用がもたらす新たな脅威やリスク

- ブロックチェーンの適切な機能は、基盤となるテクノロジーの信頼性と、補完的なビジネスプロセスおよび一般的なＩＴ統制の導入状況に大きく依存する。ブロックチェーンの導入が不十分であったり、適切な支援統制がなかったりすると、スマートコントラクト、鍵管理、コンセンサス・プロトコル、チェーンの**ロールバック**、分岐に関する問題など、ブロックチェーンに関連する問題が新たに発生したり、より広範に発生したりする可能性がある。

- スマートコントラクトは強力だが、複雑性を増す可能性がある。他のプログラミングアプリケーションと同様に、スマートコントラクトにはプログラミングエラーやバックドアが含まれる可能性があり、また他の課題にも直面する可能性がある。ビジネスロジックに欠陥があり、設計や導入に問題のあるスマートコントラクトは、無効なトランザクションの大規模な自動実行や記録につながり、それに対する救済措置がない可能性があり、非常に好ましくない結果となり得る。

- ブロックチェーンは、組織の秘密鍵へのアクセスに対して経営者に保護を提供しないため、組織のデジタル資産を直接統制することはできない。秘密鍵やブロックチェーンベースのトランザクションを開始する機能に対して適切な統制が行われていない場合、組織の資産の損失や不正流用の可能性がある。エンタープライズ鍵管理ソフトウェアは、鍵管理ガイドライン[14]と同様に、まだ始まったばかりである。

- ブロックチェーンのコンセンサス・プロトコル（またはメカニズム）は、合意されたルールに従ってトランザクションを検証するためのルール、前提条件および要件を設定するものである。コンセンサス・プロトコルの設計や導入に問題があると、合意されたルールに則ってトランザクションを適切に検証するこのテクノロジーの機能が損なわれる。そのような場合、共有台帳に記録された情報は無効で信頼性に欠ける可能性がある。効果的なコンセンサス・プロトコルを導入しても、ある１人以上のグループメンバーがコンセンサス・プロトコルを支配できるような、ネットワークのメンバー間の計算能力の分散状態（通称「51％攻撃」[ii]）などの多くの理由により、ブロックチェーンに記録されたトランザクションが無効になるリスクは依然として存在する。

- コンセンサス・プロトコルは、システムの更新と変更を推進する。チェーン・ロールバックはブロックチェーンの大きなエラーを「修正」するための主要な方法であるが、以前の時点から再開することによってチェーンの不変性を回避するために使用されることもある。そのため、チェーン・ロールバックは、ブロックチェーンに記録されたトランザクションを変更する機能を経営者に提供する可能性がある。

- 組織がオフチェーン・トランザクションの記録を行っている場合、ブロックチェーンに記録されたトランザクションの完全性が疑問視される可能性がある。オフチェーン・トランザクションはブロックチェーンに取り込まれないため、オンチェーン・トランザクションと関連する財務報告とを照合するためには、さらなる検討と統制が必要となる。

[14] NIST Key Management Guidelines.

[ii] 訳注：悪意あるマイナーがブロックチェーン上で膨大な計算を行い、パワープレイで不正な取引の承認を正当化したり、正当な取引をわざと承認しなかったりする不正行為。

ブロックチェーンの導入に伴う新たな脅威やリスクの軽減

ブロックチェーンの重要な特徴に係る統制

ブロックチェーンの導入は、事業体の統制活動の有効性を高めることも損なうこともあり得るが、これらのリスクを軽減し、ブロックチェーンを最大限に活用するために講じられる具体的な措置がある。例えば、方針と手続の改訂では、ブロックチェーンの使用に関連する新たなリスク、内部統制および会計に対応すべきであり、方針と手続を実行するための責任と説明責任も確立すべきである。さらに、組織は必要に応じて、以下の表で概説しているものを含む、ブロックチェーンの重要な特徴に係る関連統制を特定して導入することを検討すべきである。

表５．**ブロックチェーンの重要な特徴に係る統制**

ブロックチェーンの特徴	統制活動の検討事項
ノード	ブロックチェーン・ネットワーク上の各コンピュータは、「ノード」として知られている。企業にとって、データベースのコピーを保存し、トランザクションを検証し、チェーンに追加するデータの準備作業を行い、あるいは他のサービスを実行するために、ノードの活動を管理する統制を確立することが重要である。 統制は、以下の目的に関連する場合がある。 • 一部のノードが共謀してシステムを攻撃する機会を最小化するために、十分な数のノードが動作していることを確認する。コンセンサス・プロトコルが支配できないように、計算能力がすべてのノードに適切に分散されていることを確認する。 • ネットワーク内の異なるノードからブロックチェーンデータが利用できるかをテストする。 • ネットワーク内の異なるノードから取得したデータの一貫性を検証する。 • チェーンにデータを追加することに同意する前に、ノードが関連する検証を実行しているかをテストする。 • 正しい検証に対するインセンティブと不正確な検証に対するペナルティを追跡して提供する。 （注：パブリック型ブロックチェーンに関しては、ネットワーク上で動作するノードの数が多いため、組織はこれらを実行できない場合がある。）
コンセンサス・プロトコル	ある種のブロックチェーンのコンセンサス・プロトコルは、定期的に評価し、以下の点を判断する必要がある。 • 適切なノードがコンセンサスに参加することを許可されている。 • プロトコルは適切に設計され、効果的に運用されている。 • 不正行為を軽減するために、プロトコルを遵守するためのインセンティブと遵守しない場合の罰則が適切に設計されている。 コンセンサスには、プルーフ・オブ・ワーク、プルーフ・オブ・ステーク、多数決などの種類がある[15]。
秘密鍵	企業は、秘密鍵へのアクセスを管理するための手段を講じるべきである。これらの統制は、鍵の保管方法（例えば、ホット**ウォレット**かコールドウォレットか）により異なる。場合によっては、鍵管理を支援するために、あるいは資産を直接管理するために、第三者のカストディアンに委託することがある。カストディアンは、秘密鍵へのアクセスを複数の関係者に分割し、それによって複数の関係者によるトランザクションの承認（マルチシグネチャ）を要求する場合がある。また、ブロックチェーンのトランザクションを承認する者が、組織の帳簿や記録に取引を記録する機能を持たないように、組織が適切な職務分掌を検討していることを確認することも重要である。
スマートコントラクト	スマートコントラクトに関連するリスクを軽減するために、企業は以下が行える。 • スマートコントラクトの設計の適切性と導入の有効性を検証し、統制された方法で変更と更新を追跡し、また、説明責任を果たすための適切な文書と履歴記録があることを確実にするために、統制を導入する。 • ブロックチェーンオラクルからの入力を含む、スマートコントラクトへの入力に係る統制を導入する。 スマートコントラクトに係る統制は、すべてが意図したとおりに動作することを確実にし、離脱や逸脱が速やかに適切な関係者に報告されるように、適時な警告と例外報告を提供すべきである。

[15] 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特性に関する詳細は、イーサリアムの創設者の１人であるヴィタリック・ブテリン氏の 2015 年のブログへの投稿「On Public and Private Blockchains」を参照。https://ethereum.github.io/blog/2015/08/07/on-public-and-private-blockchains/ で閲覧可能。

情報と伝達	
概要	**原則**
13. 関連性のある質の高い情報の利用	組織は、内部統制が機能することを支援する、関連性のある質の高い情報を入手または作成して利用する。
14. 組織内における情報伝達	組織は、内部統制が機能することを支援するために必要な、内部統制の目的と内部統制に対する責任を含む情報を組織内部に伝達する。
15. 組織外部との情報伝達	組織は、内部統制が機能することに影響を及ぼす事項に関して、外部の関係者との間での情報伝達を行う。

*2013 年版フレームワーク*の「情報と伝達」の構成要素は、内部関係者と外部関係者との間で関連情報を特定し、処理し、伝達することに焦点を当てている。ブロックチェーンは、組織を協働のために結びつけて効果的かつ適時な情報伝達を支援する機会がある一方で、新たなリスクや脅威をもたらす可能性もある。同時に、組織はブロックチェーンの利用を踏まえて、必要と見込まれる情報とコミュニケーションの変化を考慮しなければならない。例えば、現在導入されているブロックチェーンの大部分は、取引の種類、事象または勘定残高に関する経営者確認書を裏づけるのに役立つすべての情報をオンチェーンに含んでいるわけではない。

ブロックチェーンを活用した情報と伝達の推進

- ブロックチェーンは、トランザクションの可視性を高め、経営者が主要な利害関係者に（例えば、アドホックでリアルタイムの財務報告を通じて）財務情報を伝えるための新たな手段をもたらす。

- 包括的な共有データベースとして、ブロックチェーンは、財務報告と意思決定の両方に関連するトランザクションに関するデータを提供するための基盤となり得る。

- ブロックチェーンの導入が適切に行われれば、アクセス可能で、正確で、一貫性があり、最新で、保持され、適時なデータの利用が促進できる。

- データは、共通の包括的なデジタル台帳に入力または集約される際に失われる可能性が低いため、可視性の向上を促進し、補完的な来歴の証拠を提供する。

ブロックチェーンの活用がもたらす新たな脅威やリスク

- ブロックチェーンの全機能、ブロックチェーンとは何か、そして、ブロックチェーンで何ができるのかが不明なため、ブロックチェーン上の情報は常に正しく、情報は入手可能で、人々に通知され、フィードバックを受け取っているという誤った安心感を抱くことがある。実際には、ブロックチェーン上の情報は入力されたものの完全性を維持するだけであり、他のすべてのものと同様に、「ごみを入れれば、ごみしか出てこない」が成り立つのである。さらに、ブロックチェーンに保存されるデータの信頼性は、基盤となるテクノロジーの有効性に依存する。欠陥のあるテクノロジーに支えられたブロックチェーンは、信頼性に欠けるデータを提供する可能性があり、根本的な欠陥を治すことができない。

- ブロックチェーンは大量のトランザクションデータを適時に記録する機能を備えているが、このデータは有用で実用的な情報に加工する必要がある。

- 財務報告に関連して、企業は、ブロックチェーンで処理されたデジタル資産やデジタル資産トランザクションについて行うアサーションを裏づける十分かつ適切な証拠を収集するという課題に直面する可能性がある。さらに、企業は、監査人が帳簿や記録が適切に裏づけられているかを評価するために必要な証拠を入手する能力に課題を抱える可能性がある（アサーションに関する詳しい説明については、付録３を参照されたい）。

ブロックチェーンの導入に伴う新たな脅威やリスクの軽減

情報の授受に関わる新たなリスクや脅威への対応として、組織は以下を検討する必要があるかもしれない。

- （ガバナンス担当者を含む）主要な利害関係者に対して、ブロックチェーンがビジネスで使用される方法と、このテクノロジーを使用することに関連する恩恵とリスクについて啓発する。ブロックチェーンは、リアルタイムで検証済みのトランザクションを提供することを目的として、トランザクションの実行と記録プロセスを改善するために設計されているが、データの信頼性を低下させ得るリスクがあることを利害関係者が理解することが重要である。
- 取締役会と監査委員会が、関連する監督責任を果たすために必要な情報を持っているかを判断する。
- ブロックチェーン・ネットワークのメンバーが懸念事項を報告するための方法を確立する。その方法には、まだ設置されていない場合、内部告発用ホットラインを含める場合がある。
- ブロックチェーンの使用に関連する運用上およびその他の変更や更新が適切な担当者に伝達され、内部統制に関連する責任を理解して遂行できるようにするために、コミュニケーション方法を整備する。
- 内部統制の機能を支援するための関連性のある質の高い情報を作成するために、ブロックチェーンの利用を踏まえて必要となる新たな情報要件を決定する。
- ブロックチェーンから関連性のある質の高いデータを特定して取得するためのデータアナリティクス手続を策定し、その後、経営者のビジネスプロセスと報告目的を支援するために使用する情報に加工できるようにする。
- 事業体のプロセスで使用するブロックチェーンを開発または特定する際に、内部監査人と外部監査人の両方と議論に参加する。これらの議論の一環として、経営者は、ブロックチェーンの使用に関連する典型的な監査可能性の問題と、そのような問題を軽減するために導入される対応プロセスを理解し、トランザクションのための適切な情報と裏づけを利用できるようにすることが重要である。

モニタリング活動

概要	原則
16. 日常的評価および／または独立的評価の実施	組織は、内部統制の構成要素が存在し、機能していることを確かめるために、日常的評価および／または独立的評価を選択し、整備および運用する。
17. 不備の評価と伝達	組織は、適時に内部統制の不備を評価し、必要に応じて、それを適時に上級経営者および取締役会を含む、是正措置を講じる責任を負う者に対して伝達する。

モニタリング統制は、各構成要素と原則を含む内部統制が有効かつ機能しているかを判断するために使用される。発見事項は、適切に評価され伝達される。ブロックチェーンを利用しても、構成要素と原則が存在し、機能しているかを評価する必要性は変わらないが、ブロックチェーンの利用を考慮すると評価方法が変わる可能性がある（例えば、内部統制環境を複数の企業で共有し、組織間の連携がより必要になる可能性がある場合など）。

ブロックチェーンを活用したモニタリングの強化

- ブロックチェーンは、人的介入を最小限に抑え、より統合されたフロースルー環境を促進するため、評価自体を、スマートコントラクト、ＡＩおよび標準化されたルールエンジンを用いてブロックチェーン対応のプロセスに組み込める。さらに、ブロックチェーンは他のテクノロジーと併用することで、効果的な監督のための情報の特定に役立てることができる。例えば、ＩｏＴデバイスは、これまで人的介入が不可能だった場所に作用し、環境の変化に基づくトランザクションのリアルタイムの記録を可能にできる[16]。ブロックチェーンは、さまざまな方法で集約できる詳細なデータを保持し、さまざまな範囲と頻度の評価を完了できる。

[16] 例えば、輸送用コンテナに搭載されたＩｏＴセンサーは、乱暴な動きや温度変化による損傷の可能性をモニタリングし、保険やその他の契約上の賠償のための適切な請求が行える。

- ブロックチェーン上にリアルタイムで情報の収集や集約がされるため、モニタリング活動によって不備の発生の近くで問題を把握し、エクスポージャーの最小化と改善の迅速化が図れる。

- ブロックチェーンの導入が効果的に行われれば、より適時にエラーを特定し、より全体的にパフォーマンスレビューを行えるようになる可能性がある。高度なアナリティクス、ＡＩおよびその他のツールを使用して詳細を分析することで、経営者はよりリスクの高い分野に集中できる。また、内部監査人が行う独立した評価も、自らの用途に最も関連性の高い情報に焦点を当てられる。

ブロックチェーンの活用がもたらす新たな脅威やリスク

- 頻繁に更新される大量のデータを扱うことは、情報過多に関連するリスクのレベルや脆弱性を高め、適切なモニタリングにさらなる課題をもたらす可能性がある。

- 統制環境の構成要素で確認された課題と同様に、ブロックチェーンに係る効果的なモニタリング統制を設計して実行する有能な人材を見つけることは難しいかもしれない。

- ブロックチェーンのユースケースは、ブロックチェーンを取り巻く規制や法律と同様に、その数と複雑さを増している。継続的な変化に後れをとらず、テクノロジーやモニタリングに関するものを含め、必要とされるその他の手続上や運用上のプロセスに対する適切かつ適時な更新を確保することは難しい。

- ある種のブロックチェーンは分散型であり中央の仲介者がいないため、モニタリング統制の実行に責任を持つ当事者や組織が確立されておらず、ガバナンス上の問題が生じる可能性がある。

ブロックチェーンの導入に伴う新たな脅威やリスクの軽減

新たなリスクや脅威への対応として、組織は以下を検討する必要があるかもしれない。

- ブロックチェーンで処理される大量のデータと、これらのトランザクションが高い頻度で処理されることを考慮して、従来の手作業とは異なり、コンピュータによる継続的なモニタリング技法を使用して継続的な評価を行う。

- 継続的な評価により、テクノロジーの変化や更新を特定し、内部統制の構成要素が存在し、機能しているかを検証する。

- １）適切なモニタリング統制の設計と導入を支援し、２）当該モニタリング活動の結果と効率を評価するために、事業体の基本的な統制環境、ブロックチェーンのテクノロジーおよびモニタリング技法を取り巻くベストプラクティスについて必要な知識を持つ人材を特定して獲得する。

- コンセンサス・プロトコル、スマートコントラクトおよび秘密鍵のようなブロックチェーンの固有の特徴や、使用中のブロックチェーンの継続的な健全性、ガバナンスおよび全般的な信頼性に関する要素を評価する。

- コンソーシアム型やプライベート型のブロックチェーン内で、モニタリング統制の実行を担当する個人を特定し、不備が確認された場合に伝達して是正措置を講じるための合意された方針と手続を確立する[17]。

- 場合によっては、コンソーシアム型ブロックチェーンを評価するために客観的な第三者を確保する。例えば、構成要素が機能しているかの判断、欠陥の評価および欠陥の伝達のために個々の事業体から専有情報が必要な場合、信頼できる仲介者がそのような情報にアクセスできる。

- 外部委託先とのサービスレベル合意書や、外部委託先からの管理報告書をモニタリングする。前述のとおり、こうした関係に関連する信頼性の低いデータがブロックチェーンに入り込むと、結果が大きく損なわれ、破滅的な事態に陥る可能性さえある。

[17] パブリック型ブロックチェーンに係るモニタリング統制の確立は、分散化の程度や経営者がテクノロジーの管理と監督を統制できないことを考慮すると、不可能かもしれない。

結論と次のステップ

多くの企業、産業および政府は、ブロックチェーンが目的の達成にどのようなプラスの影響を与えられるかについて、投資や調査を進めている[18]。組織がＣＯＳＯのレンズを通してブロックチェーンの利用可能性を評価する場合、取締役会と上級経営者は、その状況をよりよく理解し、このテクノロジーの可能性と内部統制への適用可能性について、より多くの情報に基づいた評価が行えるようになる。これにより、組織内の他の者は詳細なリスク分析が行えるようになり、ひいては、そのようなリスクに対応するための適切な統制活動を策定して、ブロックチェーンの効果的な採用と利用が促進できるようになる。

ブロックチェーンの可能性を活用するためには、多くの課題に対処する必要がある。これらの課題や問題点は、１）透明性がありアクセス可能なブロックチェーンベースのシステムを持つことに意欲的な組織、２）ブロックチェーンによって破壊されつつある産業に属する組織、によって整理されると考えられる[19]。これらの組織は、解決策の特定に大きな負担を抱え、将来的に他のブロックチェーン採用企業の助けとなる新しい道を照らすことになる。さらに、新しいユースケースを開発し、自らの組織を発展させるだけでなく、（規制当局や他の利害関係者を含む）他の人々がブロックチェーンの潜在的な恩恵を理解する支援をするのもこれらの組織である。

「はじめに」では、潜在的利害関係者（対象読者）のリストと、本稿が意図した用途を示した。以下の表は、同じ利害関係者がとり得る次のステップを示したものである。

表６．主要な利害関係者のための次のステップ

利害関係者	次のステップ
取締役会 **監査委員**	• 本稿および適切なブロックチェーン関連情報、教材、ウェブキャスト、研修などを活用し、このテクノロジーに関する基本的な理解を深める • 取締役会において社内の専門知識を構築し、組織内のブロックチェーン活動や潜在的な恩恵と課題に関するリーダーシップレベルでの議論を支援する • ブロックチェーン対応のプロセスが、報告の効率とリスクをどのように促進または低減させるかを理解する • 内部監査人と外部監査人がテクノロジーの可能性をどのように考えているかを理解する
経営幹部（最高経営責任者（ＣＥＯ）、最高財務責任者（ＣＦＯ）、コントローラー） **内部監査人、管理会計士、内部統制関係者**	• 社内の専門知識を構築し、ブロックチェーンの潜在的な恩恵と課題に関する部門および／または部署レベルでの議論を支援する • 同業他社でのブロックチェーンの利用方法や、利用されている革新的な手法について洞察を得る • ブロックチェーン開発者と連携し、内部統制に対応できるブロックチェーン・テクノロジーの優先順位づけと設計を支援する • ブロックチェーン対応の世界で適切な監査証拠を入手する方法など、ブロックチェーンが監査に与える影響について理解するために外部監査人と協議する • ブロックチェーンの使用に関連するリスクと統制の影響を評価するために、*2013 年版フレームワーク*を実践する
外部監査人	• ブロックチェーンに関する知識と専門性を修得する • ブロックチェーン対応の世界で十分かつ適切な監査証拠を入手する方法や、ブロックチェーンを監査目的に使用する方法など、ブロックチェーンが監査に与える影響を理解する • 監査法人内および第三者の監査ツール開発会社と連携し、（例えば、内部統制の理解やブロックチェーン・トランザクションの監査などに）必要なツールを開発する
教育関係者	• 情報、教材、ウェブキャスト、研修などを活用して、学生の教育に役立てる • ブロックチェーンの導入とそのユースケースに関連した研究プロジェクトの可能性を検討し、ブロックチェーンの影響と効果的な内部統制の評価に役立てる • この進化する空間における新たな知識、革新的な実務および基準や規制を調査する

[18] Deloitte's 2020 Global Blockchain Survey, From Promise to Reality. Deloitte Insights.

[19] ブロックチェーンによって破壊される産業について語られるとき、特定の産業がリストの上位に上がる傾向がある。これらの産業の特徴としては、サプライチェーン、長期的な記録保持の必要性および大量の反復的な詳細情報を持つ産業（例えば、金融サービス、医療、貿易、サプライチェーンマネジメント）などが挙げられる。

ブロックチェーン・テクノロジーが進化している最中でさえ、財務報告関係者コミュニティは、潜在的な恩恵を実現するための課題やリスク、是正方法および先進事例をよりよく理解するために共同で取り組める。利害関係者は、このような活動が行われるか否かにかかわらず、（関連するリスクを考慮しても）採用が進む可能性が高いことを認識しなければならない。今努力しなければ、知識、学習および適用のギャップが拡大し、このテクノロジーとその採用に関する課題に対応するために、後でより多くの労力が必要となる。

財務報告の信頼性に特有のブロックチェーンの恩恵は、財務報告、内部統制および第三者による保証を理解する人々が、ブロックチェーンエコシステムの進化や関連する規制とガイダンスに積極的に関与する場合にのみ最大化される。さらに、ブロックチェーンが財務報告関係者にもたらす潜在的な恩恵は、ＡＩやＩｏＴといった他のテクノロジーとの組み合わせによってのみ最大化される。

付録１：技術的な付録

ブロックチェーン小史

初期のブロックチェーン採用は、主にビットコインであった。サトシ・ナカモト氏の代表的な論文「Bitcoin: A Peer-to-Peer Electronic Cash System」（2008 年）で強調されているように[20]、ビットコインは中央銀行や仲介者を必要としないピアツーピアの支払い（価値交換）のために設計された。このため、デジタル資産が従来の金融サービスに対して正面切っての脅威となり得るという興奮と懸念が一部で起こっている。

デジタル資産とその価値の変動が話題になる一方で、市場参加者はその基盤となるテクノロジーであるブロックチェーンと、当事者間の新たな接続手段としてのブロックチェーンの可能性について調査を開始した。ブロックチェーンのユースケースは急速に進化していることから、ビットコイン以外のさまざまな目的でこのテクノロジーを標準化して活用するためのグローバルな取り組みが活発化している。ブロックチェーンの機能（例えば、ほぼリアルタイムでデジタル資産の転送を容易にすること）により、組織は新しいビジネスモデルやバリューチェーン、製品や配送のスピードアップなど、これまでとは異なる働き方をする機会を得ている。

ブロックチェーンの始まりはいつか

最初のブロックチェーン

ブロックチェーンの始まりは、1990 年代初頭、スチュアート・ハーバー博士とスコット・ストルネッタ博士が、数学と暗号学を用いて、新しい文書のメタデータを既存のチェーンにリンクすることで文書の完全性を証明するという学術研究論文[21]を多数発表したことに遡る。この追記専用構造は、タイムスタンプとデジタル署名を活用し、チェーン全体のデータの完全性を確保することを目的としている。

ビットコインのブロックチェーン

ブロックチェーンという言葉を使わないナカモト氏の論文は、電子キャッシュとピアツーピアのトランザクションを支援するためのハーバー氏とストルネッタ氏の画期的な研究を引用して、それを発展させたものである。そのゴールには、単一の金融仲介機関を不要にすること、二重支出を防止すること[22]、分散型参加者が分散型ネットワークを維持して新しい記録を追加する作業を行うインセンティブを与えること、などが含まれていた。「ビットコインは**オープンソース**であり、その設計は公開されており、誰もビットコインを所有や管理しておらず、誰もが参加できる」[23]。ビットコインの機能は、参加者を信頼する必要がなくシステムに依存できることから、「トラストレス」という言葉の由来となっている。

その後のブロックチェーン、トークンの追加およびスマートコントラクト

ビットコインの後、別の多くのブロックチェーンが誕生した（例えば、イーサリアム[24]ブロックチェーン）。これらは、トークンと呼ばれる独自のデジタル資産を設計する機能を追加し、スマートコントラクトと呼ばれる強力なプログラミング環境を導入した。

[20] https://bitcoin.org/bitcoin.pdf.

[21] "How to Time-Stamp a Digital Document" など。www.anf.es/pdf/Haber_Stornetta.pdf.（訳注：本稿を翻訳している 2022 年 5 月時点で、このＵＲＬは存在しない。）

[22] 物理的な硬貨や紙幣では、一度に 1 人しか所有することができない。しかし、「二重支出問題」に対処するように設計されていないデジタル資産を使用する場合、開設口座が利用可能であるという証明を複数の関係者に同時に約束できる。ビットコインは、これが引き起こすかもしれない問題を最小限に抑えようとした。

[23] https://bitcoin.org.

[24] イーサリアムについて、その開発のきっかけや、ビットコインのブロックチェーンをトークンとスマートコントラクトで拡張した経緯など、詳しくは https://ethereum.org/ を参照。

本稿で使用するブロックチェーンに関連する重要な概念には、以下のようなものがある。

表７．ブロックチェーンに関連する重要な概念

概念	説明
コンセンサス・メカニズム（またはプロトコル）	ブロックチェーンを分散管理する場合、１）トランザクションを基本的なルールと照らし合わせてチェックし、ブロックチェーンに一貫したセットが含まれていることを確認する方法、２）共有され分散された情報内で検証されたトランザクションの順序、について合意を得る何らかの手段が必要である。このように合意を得る手段を*コンセンサス・メカニズム*という。（ビットコインは「**マイナー**」と呼ばれる参加者に報酬を与えることで、インセンティブによる合意を達成した。）
コンソーシアム型ブロックチェーン	コンソーシアム型ブロックチェーンは、通常、許可型であるが、パブリック型ブロックチェーンをベースに構築されているものもある。コンソーシアム型ブロックチェーンには、ブロックチェーンを共同で使用することに合意した異なる組織が集まっている。
分散型データベース	ブロックチェーンは、「分散型」データベースと表現されることが多い。「データベース」とは、通常、検索に重点を置いて、簡単にアクセス、管理、更新および照会できるように整理された構造化されたデータのことを指す。これはすべてのブロックチェーンに当てはまるわけではなく、中には不透明で、いかなる形の第三者にも分析もできないように設計されているものもある。 デジタル資産を持つブロックチェーンとデータベースとの大きな違いは、ブロックチェーンがデジタル資産の唯一の記録保持装置になる可能性があることである[25]。ブロックチェーンは、情報を共有したいさまざまな人々のグループが、仲介者として機能する当事者の１人に依存しなくてよい点で優れている。
デジタル資産	本稿で使用するデジタル資産という用語は、検証やセキュリティのために暗号を使用して作られた、分散型台帳（例えば、ブロックチェーン）上のデジタル記録を広く指している。米国公認会計士協会[26]が定義するデジタル資産は、交換媒体として、商品やサービスの提供や利用のための表現として、あるいは証券などの資金調達手段としてなど、さまざまな用途に使用できることが特徴であると考えられる。デジタル資産に関連する権利と義務は、それらを説明するために使用される用語と同様に、大きく変化する。
フォーク（分岐）	フォークは、ビットコインやイーサリアムのようなパブリック型ブロックチェーンで広く使われてきた重要なツールである。その名が示すように、ブロックチェーンが分岐するとき何らかの決定がなされ、その結果、２つの潜在的に異なる経路が発生する。２つのチェーンは分岐点までは共通であるが、分岐後は異なるルールセット、異なるデータへの追加、時にはまったく異なる資産が適用されることになる。グループは、ベースとなる「変更不可能な」ブロックチェーンを修正するために、ブロックチェーンを分岐させることを選択する場合がある。 以下の例で示すフォークでは、元のデジタル資産の保有者は、元のチェーンを分岐して作成された新しいチェーンの別のデジタル資産の保有者にもなっている。ビットコインやイーサリアムでは、新しいルールを適用するためだけに分岐することもある。
ハッシュ	ハッシュとは、任意の大きさのデータを取り出し、固定長の一意の情報に変換するための暗号化された一方通行のアルゴリズムである。ブロックチェーンでは、ブロックチェーン上の各ブロックは、このような一意の識別子で前のブロックとリンクしている。
不変性と記録の完全性	不変性とは、ブロックチェーンが追記専用という特性であることを指す。ブロックチェーンが暗号技術によって追記専用に設計されていることは、一度ブロックチェーンに書き込まれた情報の改ざんが非常に難しいことを意味する。訂正は可能であるものの、既存のトランザクションの訂正として直接ではなく、調整として反映させる必要がある。ブロックチェーンは記録の完全性を保証するが、記録自体が合法的または適切に分類されたトランザクションを反映していることを保証するものではない。
マイナー	ビットコインは、実行が難しいが確認が容易な「プルーフ・オブ・ワーク」と呼ばれる方法で、計算が難しい数学パズルを解くために努力し、計算能力を提供する（マイナーと呼ばれる）参加者に報酬を与えることで、インセンティブを通じてコンセンサスを達成した。ビットコインのデザインは、意図的に難解なものとなっていた。他にも、プルーフ・オブ・ステークと呼ばれる、デジタル資産そのものを多く保有する人に信用を与えるなどの方法が用いられている。ビットコイン白書の原文にあるように、「必要なのは、信頼の代わりに暗号的証明に基づく電子決済システムであり、意思のある２つの当事者が、信頼できる第三者を必要とせずに直接トランザクションを行うことを可能にする」[27]。

[25] 例えば、ビットコインのエコシステムは、それ自体で価値がある（またはない）デジタル資産であるビットコインを追跡することに焦点を当てている。イーサリアム・プラットフォームには主要なデジタル資産であるイーサがあるが、カスタマイズされた（特注の）相互交換可能なトークン（ＥＲＣ 20）やその他の非代替性トークン（ＥＲＣ 721）の作成も許可されており、多くのデジタル資産はイーサリアムを使って作成されている（訳注：原文では「ＥＲＣ＊20」とあるが、「＊」は誤って入ったものと思われる。）。

[26] AICPA, "Practice Aid: Accounting for and Auditing Digital Assets," December 2019.（訳注：本稿を翻訳している 2022 年 5 月時点で、このＵＲＬは存在しない。）

[27] https://bitcoin.org/bitcoin.pdf.

表７．ブロックチェーンに関連する重要な概念（続き）

概念	説明
ノード	ブロックチェーン・ネットワーク上の各コンピュータは、ノードと呼ばれる。
オンチェーン・トランザクション、オフチェーン・トランザクション	オンチェーン・トランザクションは、分散型台帳で利用可能なトランザクションであり、ブロックチェーン・ネットワークの全メンバーが閲覧できる可能性もある。オフチェーン・トランザクションは、ブロックチェーン外での資産や関連情報の記録の移動を表す。
オープンソース	オープンソースモデルとは、協調的な分散型の開発モデルのことである。これは、共同開発に関心を持つ人々が協力して、個々の商業開発者が単独で作成するよりもコスト効率よく、かつ数をこなして品質を重視したものを作成することを奨励するものである。
オラクル	オラクルは、ブロックチェーンに情報を記録として書き込む手段であり、スマートコントラクトはその記録に変更がないかをモニターし、それに基づいて行動できる。オラクルは、スマートコントラクトの条件を実行するために使用される重要なインプットを提供するため、そのようなオラクルに対する統制を導入することが重要である。事業体が第三者のオラクルを使用している場合は、オラクルを保護するための安全対策について定期的に証拠を取得していることを確認することが重要である。さらに、ＩｏＴデバイスがオラクルの一部として外部活動を行うために使用されている場合、さらなるリスクと統制を考慮すべきである。
プライベート型（許可型）	プライベート型ブロックチェーンでは、ブロックチェーンの読み取り、書き込み、その他のアクセスには、所有者の許可または開発者が設定したプロトコルが必要である。プライベート型ブロックチェーンを許可不要型にすることは可能であるが、異例である。
パブリック型（通常、許可不要型）	許可不要型ブロックチェーンでは、ブロックチェーンの読み取りやその他のアクセスに許可を必要としない。しかし、コンセンサスと呼ばれる、誰が書き込めるかについての特定のルールがある。パブリック型ブロックチェーンを許可型にすることは可能である。
秘密鍵と公開鍵	ブロックチェーンでは、あるブロックチェーン・アドレスから別のブロックチェーン・アドレスへのデジタル資産の移動の承認に、公開鍵と秘密鍵（下図参照）を使用する。セキュリティ、特に暗号化[28]では一般的であるが、このような鍵の使用は、これまで日常の事業活動にはなかった。デジタル資産の移動は秘密鍵を使って承認されるが、これらの鍵の管理はブロックチェーン環境における新たな重要な責務である。銀行取引に複数の署名が必要なように、デジタル資産のトランザクションに複数の鍵が必要になる場合がある（マルチシグネチャまたはマルチシグ）。また、他人の署名を偽造する人がいるように、他人の鍵を入手できる人は、鍵の所有者の許可を得ずに行動できる。 下図に見られるように、大きな乱数が、秘密鍵（秘密にしておくが、特定のブロックチェーン・アドレスからのデジタル資産の移動を承認するために使用する）を作成するための標準化された数学アルゴリズムのシードに使用される。さらにアルゴリズムによって公開鍵が作成され、公開鍵からデジタル資産の残高の追跡番号であるブロックチェーン・アドレスが作成される。シードと鍵からアドレスを割り出すのは非常に容易である。しかし、アドレスから公開鍵、公開鍵から秘密鍵、秘密鍵からシードというように、その逆を行くことは事実上不可能である。
ロールバック	チェーンのロールバックは、データ破損などの問題で既存のデータベースを古いバージョンで上書きするのと同じようなものである。後のトランザクションを「取り消す」のに十分な裏づけがある状況が発生した場合、チェーンを以前の状態に復元し、その時点以降の必要なトランザクションを書き換える処理が行われる。 下図では、ブロック 125,998 以降の一連のトランザクションが無効化され削除され、ロールバックが発生している。ビットコインのようなパブリック型ブロックチェーンでは、ブロックチェーンが変更不可能であるという評価を考えると、これは簡単な処理ではなく深刻な影響を及ぼす。より中央集権的な統制が行われている場合は、このような行為は観察者には明らかであるものの、より容易に達成できる可能性がある。

[28] 暗号化とは、適切な知識やツールを持つ者だけが元のメッセージを再作成できるように、情報を変更する双方向のプロセスである。不正な傍受者が内容を理解できないようにするために使用される。

表７．**ブロックチェーンに関連する重要な概念**（続き）

概念	説明
スマートコントラクト	ブロックチェーンにおけるスマートコントラクトとは、ブロックチェーン上に格納された「自己実行型」のコンピュータプログラムであり、プログラムの実行結果はそのブロックチェーンに記録される。法的な契約のように制限されたり、特別に設計されたりしているわけではないが、これらのプログラムは、必要な入力があれば自動的にトランザクションの記録やデジタル資産の交換を推進できる。ブロックチェーンに自然に発生するトランザクションや、オラクルと呼ばれる外部ソースによって書き込まれたトランザクションなどの条件が満たされると、スマートコントラクトは自動的にトランザクションを生成する。
トークン	トークンはデジタル資産の一種であり、それ自体が新しいデジタル資産となることも、（議決権のような）無形資産を表すことも、物理的資産のデジタル代理人として機能することもある。
ウォレット	ウォレットは鍵を管理するために使用される。コールドウォレットは、インターネットに接続されていない。ホットウォレットは、インターネットに接続されている。

付録２：重要な洞察：ブロックチェーンについて知っておくべき 10 項目

ブロックチェーンについて組織が知っておくべき 10 項目は、以下のとおりである。

❶ ブロックチェーンに関するニュースやインターネット上の情報は、誤解があったり間違っていたりすることがよくある。

ブロックチェーンについて理解を深めるには、信頼できる情報源を参照すること。ブロックチェーンは１つではなく（つまり、固有名詞扱いの「ザ・ブロックチェーン」はない）、ブロックチェーンを使用しても、完全に信頼できる自己監査環境で、すべての組織が即座に魔法のように商取引でつながり、その中の暗号化されたデータが適切な人と適切なときにだけ利用されるわけではないことに留意すること。実際、多くのブロックチェーンが存在し、そのほとんどは互いに簡単にやりとりできず、うまくいかないことも多く、必要な情報の多くはブロックチェーン自体には存在しない。

❷ ブロックチェーンはデジタル資産以上のものを含んでおり、それが組織にもたらす恩恵は相当なものになり得る。

ブロックチェーン・テクノロジーはデジタル資産の枠を超え、ユースケースは産業を問わず幅広い。ブロックチェーンはビットコインで有名になったが、今やユースケースはもっと広い（例えば、サプライチェーン、金融、保険、その他の分野）。世界経済がデジタル資産に移行するにつれ、ブロックチェーン・テクノロジーは、組織が提供する製品やサービスとそれらの提供方法から、企業が内部の記録管理やデータ管理システムを管理し、トランザクション処理を行う方法まで、あらゆるものに影響を与える可能性がある。

❸ ブロックチェーンは魔法ではなく、コストがかかり、すべてのリスクを排除できるわけではない。実際は、新たなリスクをもたらす。

ブロックチェーンは、ＥＲＰシステムの全機能を置き換えることですべてのリスクに対応できるわけではないし、すべての規則や要件の遵守を保証するものでもない。実際、ブロックチェーンには、新たな資産クラスやプロセスについて考慮すべき新たなリスクが伴う。ブロックチェーンに参加する場合、各参加者は、責任、運営モデルとガバナンスモデル、トランザクションのルール、セキュリティプロトコル、インセンティブ、ペナルティ、また、必要に応じてコンソーシアムへの参加と脱退のプロセスを理解すべきである。

❹ ブロックチェーン・テクノロジーの仕組みを知ることは、ブロックチェーンが内部統制や組織全体に与える影響を評価し、準備し、管理する上で非常に重要である。

ブロックチェーンは、効率性の向上や人的ミスの削減など、適切なユースケースにおいて大きな恩恵を生み出す。一般に、ブロックチェーンが最も検討に値するのは、以下のような場合である。

- あるプロセスに対して複数の当事者や仲介者が存在し、全員が同じ情報を記録する

- ビジネスとその関係を管理するために、多くの調整を必要とするプロセスがある
- データの入力や追跡がかなり手作業で行われる
- 利害関係者が、さまざまな報告書の集計と頻繁なアドホックの報告を要求する

5 ブロックチェーンは、テクノロジーとガバナンスの両方への影響がある。

新しいブロックチェーン統制は、本質的にテクノロジーに重きを置くことになる。しかし、ガバナンス、文書やデータの保持、プライバシー法、競争優位性、評判、説明責任および情報の可視性などの問題を考慮することも重要である。

6 ブロックチェーンによって、経営者、会計士または監査人の存在意義が薄れることはないが、彼らが何をどのように行うかには影響を与える。

ブロックチェーンは、現時点では、判断、解釈、評価、発生主義会計、コミットメントや偶発事象の追跡または保証の提供の機能を備えていない。さらに、ブロックチェーンは、財務取引の記録と分析の方法、照合作業の方法および監査人が証拠を入手する方法を変えることになる。ブロックチェーンの利用により、テクノロジーに関する受託業務に係る内部統制の保証報告書の需要が高まる可能性がある（5ページのサイドバー（補足説明）を参照）。進化する会計や財務の報告規則を理解してモニタリングすることが重要である。

7 ブロックチェーンは、新しいスキルセット（例えば、より優れた事後的知見、洞察力および先見性のためのデータサイエンス）と、組織内および組織間で新たな協働を必要とする。

ブロックチェーンは、ブロックチェーンの開発、導入およびモニタリングのために、テクノロジー（とその影響）の専門知識を持つさまざまなスキルセットへの需要を生む。ブロックチェーンの教育とスキル向上は非常に重要となる。組織内と組織間の両方で、新たな協働スキルと、経営、技術および法律のスキルとの融合が必要になる。

8 今こそ、組織全体の利害関係者を啓発して巻き込むべき時である。

ブロックチェーンの潜在的なユースケース、必要となるスキルセットと研修、パフォーマンス要件、拡張性、現在のシステムとの統合、帳簿や記録の裏づけに使われる証拠への影響およびリソースの必要性を検討するには、組織全体での早期の関与が重要である。短期計画と長期計画の両方を作成することが必要な場合もある。

9 ブロックチェーンはまだ流動的であり、進化を続けている。

現在導入されているどのようなソリューションも、数年後にはやり直しが必要になるというアナリストもいる[29]。しかし、業界や規制環境がブロックチェーン、デジタル資産およびプログラミング言語に必要となる機能を明確にすれば、安定性は増す。

教育関係者は実務家と協働して、ソートリーダーシップを発揮し、現実世界の課題に対処し、解決策を提案する上で不可欠な存在となり得る。

10 ブロックチェーンの採用は選択の余地がないかもしれない。

ブロックチェーンは、デジタル資産への直接投資、デジタル資産への間接投資、自社の許可型ブロックチェーンの開発、外部の許可型ブロックチェーンへの参加、あるいはその他の活動を通じて、すべての組織に影響を与える可能性がある。顧客、サプライヤー、パートナーおよび政府から導入を迫られるかもしれない。

[29] ガートナー社は、2019年に導入されたブロックチェーンのうち、90%は2021年までに入替が必要になるとの見方を示している。
https://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain.

付録３：ブロックチェーン、財務報告のアサーションおよび監査証拠

経営者は、財務諸表と関連する開示における情報の認識、測定および表示に関して、黙示的または明示的にアサーションを行う。監査人の仕事は、監査人の意見を裏づける十分かつ適切な監査証拠を入手することである。監査証拠には、経営者のアサーションを裏づけて確証する情報と、そのようなアサーションと矛盾する可能性のある情報の両方が含まれる。

以下の表は、ブロックチェーンに格納された資産またはトランザクションに係る経営者のアサーションを裏づける十分かつ適切な監査証拠を企業が提供する方法に関して、ブロックチェーンが課題をもたらす可能性がある点を明らかにしている[30]。

表８．**経営者のアサーション（監査要点）とブロックチェーン**

アサーション	検討事項[iii]
評価の妥当性	ブロックチェーンの用途の多くは、（デジタル資産の残高などの）何かの量を追跡することであるが、追跡されるものの価値は必ずしもブロックチェーン内に保持されているわけではない。その上、デジタル資産の価値を裏づける観察可能な市場データがほとんどない、あるいは市場データの変動が大きい場合、その価値の決定が難しくなる可能性がある（例えば、ＡＳＣトピック 820[31] によると、最も流動性が低く価値が決まりにくいレベル３資産）。
実在性	デジタル資産の実在性は、ブロックチェーンから得られる証拠にのみ依存することが多い。ブロックチェーンは、トランザクションの処理と記録における改ざんを減らすために開発されたが、これ自体では、分散型台帳に格納された情報の信頼性は完全には確保できない。ブロックチェーンから得られる情報の信頼性は、システムを支える基盤のテクノロジーと導入された関連統制の有効性に大きく依存する。したがって、ブロックチェーンから情報を提供するだけでは、資産の実在性を検証するための十分かつ適切な証拠とはみなされない可能性がある。多くの場合、追加的な手続（例えば、ブロックチェーンに関連する内部統制やデジタル資産の秘密鍵のセキュリティのテスト）が必要とされる。
期間配分の適切性	ブロックチェーンによる株式、議決権またはその他の関係の追跡のようなブロックチェーン情報は、配分計算を裏づけるために使用できる。ただし、このような配分計算を裏づけるためには、ブロックチェーンから取得した情報の信頼性を裏づけるための追加の手続が必要となる場合がある。
発生	実在性と同様に、ブロックチェーンから取得した情報自体だけでは、発生のアサーションを裏づけられない場合がある。ブロックチェーンに格納された情報の信頼性、ひいてはトランザクションの発生を証明するためには、追加の手続が必要な場合がある。さらに、ブロックチェーンのトランザクションには疑似匿名性があるため、利用者が架空の取引や経済的実質のない関連当事者との取引を行い、収益を膨らませる機会を提供する可能性がある。
網羅性	ブロックチェーンが唯一の取引記録である場合は、完全な記録として機能し得るが、ブロックチェーンに保存された取引の完全性は、ブロックチェーン・テクノロジーの信頼性に加え、事業体の帳簿と記録がすべての取引を適切に捉えていることを保証するために事業体が導入した統制に依存することになる。さらに、情報の一部または全部が別のシステムに記録されている場合、ブロックチェーンは網羅性を裏づけられない。オンチェーンかオフチェーンかにかかわらずすべての活動と、オンチェーンかオフチェーンかにかかわらずすべての詳細が、利用可能で完全に記録されていることを確実にするための統制が必要である。
分類	デジタル資産の分類は、会計指針や判例がまだ進展中であるため、難しい場合がある。さらに、そのような資産の適切な分類を決定するためには、企業は資産の目的と用途を客観的に評価する必要がある。
理解可能性	ブロックチェーンは、何らかの報告や理解しやすい形での要約の必要性は考慮しておらず、そのような機能は備えていない。経営者は、ブロックチェーンからのどのようなデータが財務諸表の作成を支援するために有用であるかを判断し、そのようなデータを取得して要約するための適切な方法を決定する必要がある。分類のアサーションと同様に、このテーマを取り巻く会計指針や判例はまだ進展中であり、事業体の財務諸表内でのデジタル資産の表示を決定する際には十分な注意が必要である。
正確性	ブロックチェーンは、デジタル資産の記録として、すべてのトランザクションと残高の履歴を保存する。これは、ブロックチェーン内の情報が正確であることを意味するのではなく、記録が完全性を保つことのみを意味する。
表示の妥当性	「理解可能性」に関する検討事項を参照。

[30] Eric Cohen, "Will Blockchain Make Auditors Obsolete?", ThinkTWENTY20, Spring 2019. http://www.thinktwenty20.com/images/docs/Spring-Issue-2019.pdf, accessed June 16, 2020.
[31] 公正価値測定 (トピック 820), https://asc.fasb.org/imageRoot/81/118196181.pdf.

[iii] 訳注：この行、原文では表７と同様「Concept」「Explanation」だが、内容から判断すると「Assertion」「Consideration」であると思われるため、「アサーション」「検討事項」と訳した。

表８．経営者のアサーション（監査要点）とブロックチェーン（続き）

アサーション	検討事項
カットオフ	ブロックチェーンに書き込まれた記録やブロックにはタイムスタンプが押されるため、関連するすべてのトランザクションの完全な記録として、記録日のカットオフを評価する機能がある。しかし、会計上の認識時期や、発生主義、前払費用、費用収益対応の原則などの概念は、本来の機能として存在しない。
権利と義務の帰属	一般に、デジタル資産には、権利と義務のアサーションを裏づける書面での所有権の合意書は存在しない。署名付きメッセージングなどの手続は、秘密鍵に係る統制（ひいては資産に対する権利）を証明するために使用されるかもしれないが、運用上の制約により、これらの手続を完了することができないかもしれない。さらに、これらの手続は、基盤となるブロックチェーン・テクノロジーの信頼性に依存するため、追加の手続（例えば、内部統制のテスト）の実施を必要とする可能性がある。最後に、署名付きメッセージング手続は、秘密鍵に係る統制を示すかもしれないが、秘密鍵が組織によってのみ統制されていない可能性がある（すなわち、他の当事者が秘密鍵を入手でき、したがって関連資産の統制または所有権を持つかもしれない）というリスクが依然として存在する。

補足資料と出典（ＣＯＳＯ支援団体が提供したものを含む）

本稿は、支援団体や関連する利害関係者から提供された多くの有用な文書やその他のリソースを補完するために作成されたものである。この議論に関連するそれらの文書の例には、以下のようなものがある。

米国会計学会（ＡＡＡ）
https://aaahq.org/Meetings/2018/BlockchainAAA

米国公認会計士協会（ＡＩＣＰＡ）
https://us.aicpa.org/interestareas/informationtechnology/resources/blockchain [iv]

国際財務担当経営者協会（ＦＥＩ）
www.financialexecutives.org/Research/News/2017/Blockchain-and-the-Future-of-Financial-Reporti-(1).aspx

管理会計士協会（ＩＭＡ）
Frans Roozen, Ph.D.; Bert Steens, Ph.D.; and Louis Spoor, "Technology: Transforming the Finance Function and the Competencies Management Accountants Need," *Management Accounting Quarterly*, Fall 2019,
www.imanet.org/insights-and-trends/management-accounting-quarterly/maq-index/2019/fall-2019?ssopc=1

Reina G. Wiatt, CMA, CPA, "From the Mainframe To the Blockchain," *Strategic Finance*, January 2019,
https://sfmagazine.com/post-entry/january-2019-from-the-mainframe-to-the-blockchain/

Natalia Maslova, CMA, CTP, PMP, "Blockchain: Disruption and Opportunity," *Strategic Finance*, July 2018,
https://sfmagazine.com/post-entry/july-2018-blockchain-disruption-and-opportunity/

内部監査人協会（ＩＩＡ）
www.theiia.org/centers/aec/Pages/blockchain-risks-opportunities.aspx [v]

その他の関連資料

ACCA Global: Divided We Fall, Distributed We Stand
www.accaglobal.com/uk/en/technical-activities/technical-resources-search/2017/april/divided-we-fall-distributed-we-stand.html

ICAEW: Blockchain and the Future of Accountancy [vi]
https://www.icaew.com/technical/technology/blockchain-and-cryptoassets/blockchain-articles/blockchain-and-the-accounting-perspective

[iv] 訳注：原文に記載のＵＲＬから変更されているため、現在のＵＲＬを記載した。
[v] 訳注：本稿を翻訳している 2022 年 5 月時点で、このＵＲＬは存在しないことをＩＩＡに確認済み。
[vi] 訳注：原文に記載されていたＵＲＬでは該当文書が見当たらなかったが、ここに記載したＵＲＬが正しいと思われる。

著者について

デロイト＆トウシュ社、パートナー、ジェニファー・バーンズ

ジェニファーは、デロイト＆トウシュ社の米国国内事務所のパートナーであり、監査の実施に影響を与える規制、基準設定および品質に関する事項において 25 年以上の経験がある。現在、保証業務の新興分野（人工知能、ブロックチェーン、サステナビリティ、その他の第三者評価の分野を含む）に関する同社の米国国内事務所の取り組みを主導し、専門職基準の適切な適用に関して監査チームに助言している。また、専門職に影響を与える規制の動向について、監査委員会やクライアントと定期的に意見を交換している。

米国公認会計士協会（ＡＩＣＰＡ）の保証業務執行委員会の委員であり、専門職が進化する市場のニーズに対応できるよう、そのミッションを推進している。公開会社会計監視委員会（ＰＣＡＯＢ）、米国証券取引委員会（ＳＥＣ）、国際監査･保証基準審議会（ＩＡＡＳＢ）、トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）などの基準設定機関や規制機関とも交流し、同社の意見を代表している。また、ＣＯＳＯの「財務報告に係る内部統制ー小規模会社向けのガイダンス」（2006 年）、「内部統制システムモニタリングガイダンス」（2009 年）、「内部統制の統合的フレームワーク」（2013 年）の策定において、ＣＯＳＯに助言をするタスクフォースの委員も務めた。

それ以前は、ＳＥＣの主任会計官室で会計専門家フェローとして、専門職基準の策定とサーベインズ・オクスリー法に関連する要件の導入の監督に携わった。

カリフォルニア州クレアモントのクレアモント・マッケナ大学を優秀な成績で卒業し、ワシントンＤＣ、カリフォルニア州およびネバダ州の公認会計士資格を持ち、ＡＩＣＰＡの会員でもある。

デロイト＆トウシュ社、パートナー、エイミー・スティール

エイミーは、デロイト＆トウシュ社の米国国内事務所のパートナーとして、テクノロジー産業とメディア産業の上場・非上場企業の監査を主導している。規制、基準設定および監査品質において豊富な経験を持ち、同社のグローバル組織全体で品質を向上させ、監査を革新し変革するための戦略を主導している。ブロックチェーンとデジタル資産に関する同社の米国およびグローバルな監査手法のリーダーである。また、同社の新興保証業務（監査専門家の役割の拡大と監査におけるテクノロジーの影響に焦点を当てた業務）の主席パートナーでもある。さらに、収益に関する同社の監査手法を主導し、監査基準の複雑な適用について監査チームに助言をしている。これらの役割において、規制機関や専門家団体と頻繁に連携している。

ＡＩＣＰＡのデジタル資産作業部会の委員長を務め、デジタル資産に関する監査と会計指針の策定を主導している。また、新興テクノロジーの監査品質センター（Center for Audit Quality Emerging Technologies）のタスクフォースとサイバーセキュリティ・タスクフォースの委員でもある。実業界のソートリーダーとして活躍し、財務報告や監査業務に影響を与える問題についての意見を求められ、技術的なテーマについて幅広い聴衆や規制当局に情報を発信している。

以前は、ＳＥＣの主任会計官室で主任会計官代理を務め、監査業務全般およびＰＣＡＯＢの監督に関する委員会の主要アドバイザーとして、主任会計官室を支援するという貴重な機会を得ていた。さらに、この役割において、監査人やＳＥＣのさまざまな部署と監査や内部統制に関する技術的な議論を行い、ＣＯＳＯの「内部統制の統合的フレームワーク」（2013 年）の策定時にはＳＥＣの公式オブザーバーを務めた。

ワシントン大学を極めて優秀な成績で卒業し、専門会計修士号を取得した。ＡＩＣＰＡの会員であり、ワシントン州とコネティカット州の公認会計士資格を保持している。

エリック・Ｅ．コーエン

エリック・コーエンは、監査データ基準、ブロックチェーン、継続的監査、サステナビリティと企業責任、拡張可能な事業報告言語（ＸＢＲＬ）など、新興の会計・監査テクノロジーに焦点を当てたコンサルタント会社、コーエン・コンピュータ・コンサルティング社の経営者である。ＸＢＲＬ運動の共同創設者であり、ＸＢＲＬのグローバル元帳（ＸＢＲＬ ＧＬ）タクソノミーフレームワークの「発明者」でもある。ＸＢＲＬの大使として、会計・監査データの標準化を試みる他のほぼすべての標準化活動と協力し、国連貿易円滑化と電子ビジネスのための国連センター（ＵＮ／ＣＥＦＡＣＴ）との長い協力関係から、会計・監査ドメインのＵＮ／ＣＥＦＡＣＴドメイン・コーディネーターを引き受けるに至った。

多作で意欲的な講演者、教師およびトレーナーであり、数多くの書籍（Guide to Customizing Accounting Software (ＣＴＳ社) や Accountant's Guide to the Internet (ジョン・ワイリー社) など）を執筆または寄稿し、ビジネス誌、専門誌および学術誌向けに数百の記事を発表している。学界とは長いパートナーシップを築いており、ＸＢＲＬ、継続的監査および関連分野の研究やカリキュラム作成で多くの教授と協力している。

国際標準化機構（ＩＳＯ）のブロックチェーンと電子分散台帳技術に財務報告に係る内部統制ー小規模会社向けのガイダンス専門委員会（ＴＣ 307）米国国内専門家として、ガバナンス、相互運用性および監査指針に関する規格開発に注力している。ニューヨーク州公認会計士協会（ＮＹＳＳＣＰＡ）デジタル資産委員会の委員であり、2019 年にはＮＹＳＳＣＰＡの会計教育財団（ＦＡＥ）デジタル資産カンファレンスの議長を務めた。

シュリダハール・ラマムーティ博士

シュリダハール・ラマムーティ博士（ＡＣＡ、ＣＰＡ、ＣＩＴＰ、ＣＦＦ、ＣＧＭＡ、ＣＩＡ、ＣＦＥ、ＣＦＳＡ、ＣＧＡＰ、ＣＧＦＭ、ＣＲＭＡ、ＣＲＰ、ＭＡＦＦ）は、オハイオ州のデイトン大学で会計学の准教授を務めている。実務に携わり続けるために、リスクアドバイザリー業務を行うケツァールＧＲＣ社と、不正リスクの軽減、発見および調査業務を行うビヘイヴィョラル・フォレンジック・グループ社の２つのコンサルティング会社の代表として活躍している。以前は、ジョージア州ケネソーのケネソー州立大学マイケル・J・コールズ経営学部の会計学准教授と、コーポレートガバナンスセンターのディレクターを務めていた。

学問と実務が融合した独特の経歴を持ち、学問、監査およびコンサルティングの分野で 35 年以上の経験がある。オハイオ州立大学で博士号を取得後、イリノイ大学で会計学の教員を務めた。その後、イリノイ州シカゴで、アンダーセン社のプロフェッショナル・スタンダード・グループのプリンシパル、アーンスト・アンド・ヤング社の国内ＳＯＸアドバイザー、グラント・ソントン社のコーポレートガバナンス・パートナーを務めた。再び学界に戻る前には、イリノイ州ネイパービルのインフォジックス社でガバナンス・リスク・コンプライアンス（ＧＲＣ）の専門サービス部門を短期間率いた。

ＣＯＳＯの「内部統制システムモニタリングガイダンス（2009 年）」、情報システムコントロール協会（ＩＳＡＣＡ）のガイダンス「内部統制システムおよびＩＴのモニタリング（2010 年）」、「監査委員会ハンドブック（第 5 版、ワイリー社、2010 年）」、「内部監査：アシュアランス業務とアドバイザリー業務（第 4 版、内部監査人協会、2017 年）」および米国連邦捜査局（ＦＢＩ）アカデミーや複数のカンファレンスで発表した不正の心理に関する著書「A.B.C. of Behavioral Forensics (ワイリー社、2013 年)」の執筆・制作チームの一員であった。また、学術誌や専門誌に 60 を超える論文や記事を発表し、数多くの編集委員を務めている。

ＣＯＳＯの支援 5 団体すべての会員であり、内部監査人協会（ＩＩＡ）および国際財務担当経営者協会（ＦＥＩ）の研究財団の評議員を務めたこともあるなど、専門職として積極的に活動している。また、ＰＣＡＯＢの常設諮問委員会の元委員でもある。過去 20 年にわたり、16 か国[vii]で講演を行ってきた。

[vii] 訳注：日本では、2004 年 9 月「第 38 回内部監査推進全国大会」において、「現代内部監査の論点」と題して基調講演を行った。講演内容は、『月刊監査研究』2004 年 11 月号掲載。

ＣＯＳＯについて

1985 年に設立されたＣＯＳＯは、５つの民間団体の共同イニシアチブであり、全社的リスクマネジメント（ＥＲＭ）、内部統制および不正抑止に関するフレームワークとガイダンスの開発を通じて、先進的な考え方を提供することに取り組んでいる。ＣＯＳＯの支援団体は、内部監査人協会（ＩＩＡ）、米国会計学会（ＡＡＡ）、米国公認会計士協会（ＡＩＣＰＡ）、国際財務担当経営者協会（ＦＥＩ）、管理会計士協会（ＩＭＡ）である。

デロイト社について

Deloitte（デロイト社）とは、英国の保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（「ＤＴＴＬ」）と、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人の１つまたは複数を指す。ＤＴＴＬと各メンバーファームはそれぞれ法的に独立した別個の組織体である。ＤＴＴＬ（「Deloitte Global とも呼ばれる」）は、顧客に業務を提供していない。

ＤＴＴＬおよびメンバーファームの詳細については、deloitte.com/about を参照されたい。デロイト社およびその子会社の法的構造の詳細については、deloitte.com/us/about を参照されたい。一部の証明業務は、公開会社に関する会計の規則上、顧客に提供できない場合がある。

本稿には一般的な情報のみが含まれており、ＣＯＳＯ、その構成団体または本稿の執筆者のいずれも、本稿によって、会計、ビジネス、金融、投資、法律、税務またはその他の専門的なアドバイスやサービスを提供するものではない。ここに掲載されている情報は、このような専門的なアドバイスやサービスの代わりになるものではなく、ビジネスに影響を与える可能性のある意思決定や行動の根拠となるものではない。ここで述べている見解、意見または解釈は、関連する規制当局、自主規制機関またはその他の当局の見解とは異なる場合があり、また、時間の経過とともに変化する法律、規制または慣行を反映している場合がある。ここに掲載されている情報の評価は、利用者自身の責任で行っていただきたい。ここに記載されている事項に関して、利用者のビジネスに影響を与える可能性のある意思決定や行動を行う前に、関連する有資格の専門アドバイザーに相談していただきたい。ＣＯＳＯ、その構成団体および執筆者は、ここに記載されている誤り、脱落、不正確さ、あるいは本稿に依拠した人が被った損失について、いかなる責任も負わないものとする。

一般社団法人日本内部監査協会

内部監査および関連する諸分野についての理論および実務の研究、ならびに内部監査の品質および内部監査人の専門的能力の向上を推進するとともに、内部監査に関する知識を広く一般に普及することにより、わが国の産業、経済の健全な発展に資することを目的に活動。

また、国際的な内部監査の専門団体である内部監査人協会（The Institute of Internal Auditors：ＩＩＡ）の日本代表機関として世界的な交流活動を行うとともに、内部監査人の国際資格である“公認内部監査人（Certified Internal Auditor：ＣＩＡ）”等の認定試験を実施している。1957（昭和 32）年創立。

公益財団法人日本内部監査研究所

内部監査に関する研究調査を推進するとともに、わが国の内部監査の普及発展に貢献することにより、わが国経済、社会の健全な発展に資することを目的として、2020 年７月に設立。2021 年６月に公益財団法人としての認定を受け「公益財団法人日本内部監査研究所」となった。

監訳者

八田　進二　（大原大学院大学　会計研究科　教授　／　青山学院大学　名誉教授）

橋本　　尚　（青山学院大学大学院　会計プロフェッション研究科　教授）

訳　者

堺　　咲子　（内部監査人協会（ＩＩＡ）国際本部　北米外地域筆頭理事　／　インフィニティコンサルティング　代表　／
プレミアアンチエイジング株式会社　社外取締役　／　ＣＩＡ，ＣＲＭＡ，ＣＣＳＡ，ＣＦＳＡ）

ガバナンスと内部統制

COSO

トレッドウェイ委員会
支援組織委員会

coso.org

ガバナンスと内部統制

ブロックチェーンと内部統制：ＣＯＳＯの視点

COSO

トレッドウェイ委員会支援組織委員会

coso.org

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C103046