サプライチェーンマネジメントシステム構築のための ブロックチェーンプラットフォームの研究

A Study on Blockchain Platform for Construction of Supply Chain Management System

朝日大学大学院経営学研究科　修士課程２年　高橋弘樹
Graduate School of Business Administration, Asahi University, Master's Course 2nd Year, TAKAHASHI, Hiroki
朝日大学大学院経営学研究科　教授　奥山　徹
Graduate School of Business Administration, Asahi University, Professor OKUYAMA, Tohru

概要：サプライチェーンマネジメント（SCM: Supply Chain Management）は、サプライチェーンの維持・管理に必ず必要となる概念で、現在はICT（Information Communication Technology）を活用した、SCMシステムが構築されている。しかし、サプライチェーンは、それを構成するプレーヤー数が多くなり、複雑化している。また、B2Bを中心とする国際調達が激増し、サプライチェーンもグローバル化している。そのため、SCMシステムの標準化が進められている。現状では、標準化は業界ごとに行われており、他業種連携や国際連携による十分な標準化が行われていない。最近、SCMシステムの中核としてブロックチェーン技術を使う試みがある。本論文では、SCMシステムの中核としてブロックチェーンがどのように利用できるか調査したので報告する。

Abstract：Supply Chain Management（SCM）is a concept that is absolutely necessary to maintain and manage the supply chain. Currently, an SCM system utilizing ICT（Information Communication Technology）is being constructed. However, the supply chain is complicated by the large number of players that make it up. In addition, international procurement centering on B2B has dramatically increased, and the supply chain has become global. Therefore, standardization of the SCM system is in progress. At present, standardization is carried out for each industry, and sufficient standardization is not carried out by cooperation with other industry divisions or international cooperation. Recently, there are attempts to use blockchain technology as the core of the SCM system. In this paper, we investigate how blockchain can be used as the core of SCM system.

１．はじめに

企業が商品（モノ）を売りたいとき、モノを必要とする場所に、モノを届ける仕組みが必要となる。その際のモノとそれに付随する情報などの移動をすべてまとめて流通といい、流通システムは流通全体を表すためのものである。モノを作るための原材料から消費

者にモノを届けるまでの全行程をサプライチェーンと呼び、サプライチェーンの運用管理や効率化のための全ての作業をサプライチェーンマネジメント（以下「SCM」: Supply Chain Management と略記する。）と呼び、今日、流通システムにとって不可欠なものとなっている［1］。

SCM は流通の過程を記録する作業であると同時に、記録した情報を元に、需要と供給をバランスさせ、安定した品質の製品を安定して供給するための仕組みである。そして、どれだけのモノを、どこにどのようなタイミングで届けるかは需給計画と呼ばれ、最適な需給計画を施すことは、需給最適化と呼ばれる［1］。SCM の目的は、最終的に需給最適化を実現することであり、それにより、流通システムが安定し、消費者はより良い製品を適正な価格で手にすることができる。

SCM を取り巻く現実は、必ずしも需給最適化を達成できるレベルまで達していない。それどころか、ようやく紙を主体とした記憶媒体から電子データを交換する仕組みである EDI（Electronic Data Interchange）を使った電子的なシステムへの移行が始まり、メッセージ交換フォーマットが標準化される過程へと進んだところである［2］。現状の標準化は、業界ごとに標準規格が作られており、それらを横断的にまとめられてはいない［3］。また､国際的な標準化も進んでいるが［4］［5］［6］、業界横断的、全世界的な統一標準には至っていない［7］。

そこで、SCM の中心となる業界横断的にまた国際的に利用可能なプロトコルが必要である。そして、最近、Bitcoin 等［8］の仮想通貨等でデファクト標準となりつつあるブロックチェーン［9］に着目し､ブロックチエーンを SCM の中核として利用することとした。

本論文では最初に SCM の課題を洗い出し、それらの課題をブロックチェーンにより解決可能であるか研究した。その結果として、主要な幾つかの課題は解決可能である、また、解決が難しい課題も見つかったので、それらについて報告する。

2．サプライチェーンと SCM

サプライチェーンは「原材料から消費者までの効率的な供給チェーン」であり、その中心は「物流」となる［10］。しかし、モノを運ぶためには、単に輸送用デバイス（トラックや貨物車等）に荷物を詰めて運ぶだけではだめで、原材料の生産者の情報から始まり、そのモノに関する各種の情報が付随することとなる。モノの動きとその情報の伝達、及びそれに関わる全ての物事を管理することが SCM の役割である。

単純なサプライチェーンは図１（a）に示すように、単純なモノと情報の流れを一連の線図として表す。しかし、現在では図１（b）のように、複雑化した拡張サプライチェーンとして描かれることが多い［11］。

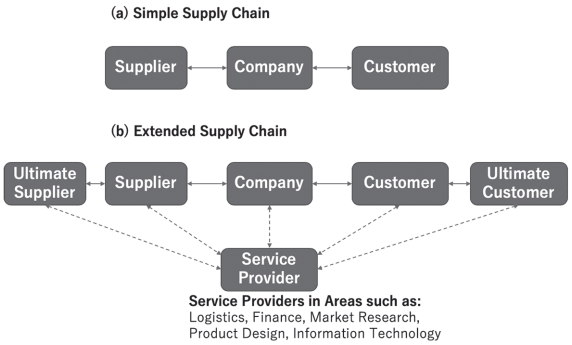

図１．簡単なサプライチェーン（a）と拡張されたサプライチェーン（b）［11］

図２は拡張されたサプライチェーンの例である。このようにサプライチェーンは、拡張し続け、より複雑になっている。また、途中で新しいプレイヤーが増加したり、役割を終えたプレイヤーが脱退したりすることもある。したがって、構造的に簡単で、なおかつ柔軟性と拡張性を備えたシステムを構築する

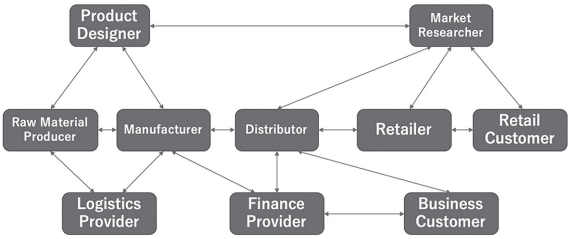

図2．拡張されたサプライチェーンの例［11］

必要がある。

図3は、サプライチェーンの「モノ」·「カネ」·「情報」の動きを図式化したものである。図に示すように、第1層の物流層としてのフィジカルレイヤ、第3層の情報層としてのサイバーレイヤ、そして第5層の金融層としてのファイナンシャルレイヤが実際の「モノ」、「情報」、「カネ」の流れを制御する層である。さらに、第1層と第3層を結ぶ第2層のサイバー・フィジカルレイヤは、モノを製造したり運んだりする実体である「Supply Chain Player」からサイバーレイヤへの情報の転写を制御する。一方、第3層と第5層の間のサイバー・ファイナンシャル層は、金融機関などの「Financial Entity」からのカネに関連する様々な情報の転写を制御する。

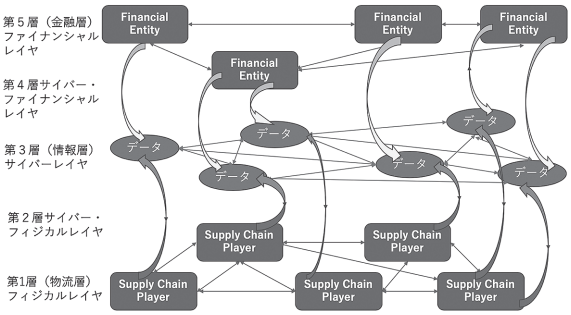

図3．サプライチェーンの5層構造

サプライチェーンをこのような5層構造で表した例はなく、このような考え方は本論文で著者が提案したものである。ただし、サプライチェーンの役割を商流・物流・金流の融合とする考え方は既に存在しており、例えばアメリカのウォルマートでは、2019年の9月までに葉物野菜の仕入先に対してブロックチェーン［8］を使った商流・物流・金流の融合したサプライチェーンへの参入を呼びかけている［12］。SCMとは、第2層から第4層にかけてのサイバーレイヤに関連した情報の取り扱いを包括的に行うもの考えることができる。そのため、これまでのような単なるチェーン構造の連結体としてのSCMとは異なる考え方が必要となる。

5層構造モデルを使う利点は、これまでSCMの中で個別に議論されることが多かった物流と金流の間を情報層でのデータの動きと連動させることで、それらの動きを簡単に把握できることである。一方、欠点として、サプライチェーンは簡単でもSCMのフェーズではサイバー・フィジカル、サイバー、サイバー・ファイナンシャルの三つの層でのデータの転写と管理を行う必要があり、複雑化することである。そのため、これまでのような単純なサプライチェーンを取り扱うようなSCMでは制御が難しい。また、サイバーレイヤに高いセキュリティを確保できる技術を導入すれば、各企業や金融業は、インターフェイスの部分のセキュリティだけ注目すればよく、導入コストや運用コストに占めるセキュリティ対策費を圧縮できる可能性がある。

3．サプライチェーンの課題

本節ではサプライチェーンの課題についてまとめた。(1) サプライチェーン内の情報共有の問題、(2) サプライチェーンの最適化の問題、(3) サプライチェーンのセキュリティとガバナンスの問題、これら三つが重要な課題と考えている。以下にそれぞれの課題について詳細に述べる。

3.1. 情報共有の問題

初期のサプライチェーンのプレイヤー間の

情報伝達は、紙媒体、電話やFAXを使用していた［13］。そのため自社内の在庫管理などや受発注の業務システムへ入出力する際に人手を必要としていた。その結果、人為的ミスの発生や時間のロスが生じていた。特に紙媒体は、物理的な制約が大きく管理や手間が増え、業務の効率を下げてしまう。一方、電子媒体であれば、納品書などの電子化されたデータからそのまま自動で記録を作成できる。また、一部では未だに印鑑を使用しているところもあり、電子化の普及の妨げになっている。印鑑自体は紙媒体であれば便利であるが､電子化には不向きである。したがって、押印を電子署名などの電子的技術［14］に変更する方が電子媒体には有効である。

サーバ－クライアントモデルを使ったサプライチェーンマネジメントシステムを想定する。例えWeb-EDIを使ったシステム等が該当する。このようなシステムでは、サーバ上のEDIゲートウエイ上でデータが集中管理されているので、情報は正しく共有されていると考えられる。しかし、実際のデータアクセスは、ACL（Access Central List）に従った制約がかかる。例えば、サーバの管理主体が、サプライチェーンを取り仕切っている場合、必ずしも全てのデータが開示されているとは限らない。基本的な取引データ以外は開示されないと考える方が一般的である［15］。したがって、サーバ－クライアントモデルによるシステムは、その構成上の欠点から、情報共有が制限される可能性がある。

図4は、原料（Raw Material）そのものあるいはその加工品を集めて、部品（Parts）に組み上げ、製品（Products）を作る場合の典型的なサプライチェーンの例である［11］。図中の「Raw Material Producer」は原料の供給業者、「Parts Supplier」は原料を元にした工業部品群の製造業者､「Parts Assembler」は工業部品からより大きな部品を組み立てる中間業者、そして、「Product Maker」は製品の製造業者である。例えばパーソナルコンピュータ（以下「PC」と略記する。）の製造を考える。PCの組み立てには様々な部品が必要となる。例えば、マザーボード、電源、筐体、CPU（Central Processing Unit）、MMU（Main Memory Unit）、磁気記憶装置、光学機器、その他様々な周辺機器である。これらは一つの企業で製造できないため、必ず他の企業から調達することになる。そこに、他社を含めたサプライチェーンができあがる。

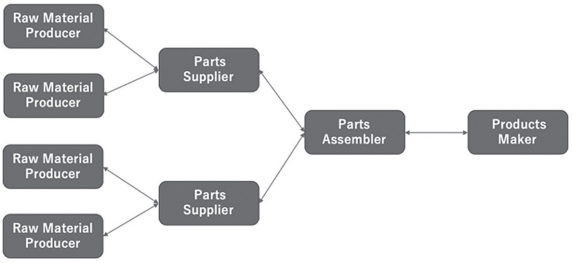

図4．原料から製品を製造する場合のサプライチェーンの例［11］

例えば、マザーボードについて考える。マザーボードの組み立ては「Parts Assembler」が行うとする。部品として、VLSI（Very Large Scale Integration）、抵抗、電解コンデンサ等が必要となる。それらは「Parts Supplier」が供給元となる。また、「Parts Supplier」はそれらの電子部品の原料（シリコンウエハーや電解液等など）を「Raw Material Producer」から調達する。製品の信頼性を上げるには、これらの部品や原料に至るまでの品質管理が必要となる。しかし、原料と中間製品との間での原料に関する情報共有はなされても、図のような構成では、それが「Parts Assembler」に正しく伝達されるかはわからない。ましてや、その下流にある「Products Maker」は､「Parts Assembler」から提供されるテクニカルノートのテストデータが許容範囲に収まっていれば、上流工程の個々の部品の詳細は、一般には気にしな

い。ましてや、その下流の販売店や消費者も特に気にすることはない。

2005 年に起きたマザーボード上の電解コンデンサの事故［16］は、まさにそのような企業間の SCM の盲点を突いたものであった。この事故は、マザーボードの VLSI のような主要部品ではなく、電解コンデンサというありふれた部品の不良（電解液の不良と言われている。）により、液漏れや発火、寿命の減少等の様々な事象が観測され、PC が使用不能に陥った。それ以来、PC メーカーは上流工程で利用されている細かな部品の信頼性や寿命等の情報を共有するようになった。また、消費者も仕様書などで、使用部品の耐久性や信頼性の提示を求めるようになった。

加工食品の原産国表示［17］も、食品偽装［18］からの教訓として、同様な流れで義務付けられることとなった。

このように、サプライチェーン内での情報の共有は必須の機能として位置づけられるようになった。しかし、図 4 のようなチェーン構造をしたシステムの場合、チェーンを構成するプレーヤー間で情報開示を繰り返すこととなり、必ずしも効率の良いシステム構成とはなっていない。そのため、Web-EDI による集中化などが必要となる。本論文では、これらの手法に代えて、現在、仮想通貨などでのデファクト標準となっているブロックチェーン技術[9]を適用することを提案する。

3.2. 最適化問題

さて、サプライチェーンは、運ぶ「モノ」や関連する企業間の関係を考慮すると様々な形態のものが存在する。そのため、一律な標準化は不可能とされている［19］。標準化されるべきは、製造プロセスや関連する部品、それらの受発注過程やそれに付随するメッセージ交換の仕様やデータ転送プロトコルである。サプライチェーンはそれらの標準化された種々の規格を使い、「モノ」・「カネ」・「情報」の流れを最適化する。

サプライチェーンの最適化問題は何を最適化するかにより大きく様相が異なる［20］。この場合、単純なグラフ理論による最大流（運ぶ「モノ」の量を最大化する。）問題や最小費用（かかる費用を最小化する。）問題［21］を解くことによる最適化は難しい。例えば最大流問題は、図 5 のような有向グラフを考え、始点 X から終点 Y にモノを運ぶ際、有向線上に示された各点間の最大運送量を元に一回で最も量を運べる経路を探索するものである。X を部品の供給企業 Y を最終製品の製造企業 A ～ E を中間業者とするならサプライチェーンの最適化問題として、そのまま適用できると考えられる。

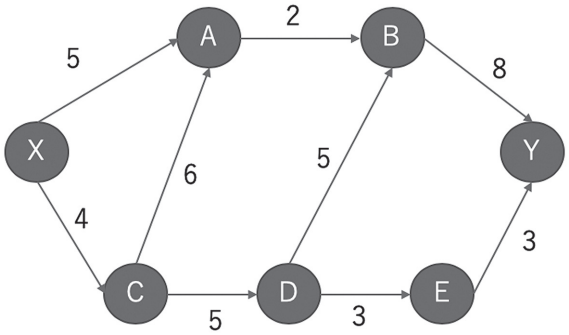

図 5．最大流問題のグラフの例

しかし、サプライチェーンでは X が供給した部品をそのまま Y が使うわけではなく、中間業者が何らかの加工を行い、異なった形態の部品として次の業者に送ることになる。したがって、B と E の業者が届ける部品は、両方とも Y では必要とするものである可能性が高い。それゆえ、有向線上の数値は単純な一つのモノを指しているのではなく、部品の質と量の両方を含んだものとなる。このような質と量の両方を含んだ有向線を持つグラフの最適化は一般に難しい［21］。ここでは、さらに Y が必要とする質と量の部品が必要時に届いていることが重要となる。すなわち、

最適化要因は、必要とする部品の種類、質、量、経過時間、輸送コストなど、複数存在する。もちろん、部品ごとにサプライチェーンを分割管理することは可能であるが、サプライチェーンはより複雑になり、管理のコストは大きくなる。

このように、サプライチェーンの最適化問題は、一般には「需給最適化問題」として知られており、論理的に解くことが難しい。そのため、遺伝的アルゴリズムや発見的アルゴリズム［22］を始めとした、様々な最適化手法が検討されている［23］。

3.3. セキュリティとガバナンス問題

SCM システムに限らず、情報システムに対するセキュリティ問題は技術的に解決可能な問題と、ガバナンスとして解決すべき問題（情報管理的に解決すべき問題）がある。例えば、通信路の暗号化は、通信途中でのパケットの搾取攻撃（「スニファ攻撃」とも呼ばれる［24］。）から通信途中のデータの漏えいを防止できる。これには、SSL（Secure Socket Layer）を使った VPN（Virtual Private Network）の構築が有効である。そして、これらの技術の中核となっているのが暗号技術、特に公開鍵暗号技術である。つまり、サプライチェーンに関する情報セキュリテイの技術的問題は、暗号技術を中心として幅広く研究されている［25］。

4．ブロックチェーンの概要

ブロックチェーンは、仮想通貨である Bitcoin の基本技術として考案された。しかし、その元となる技術やアイデア群はそれ以前から存在している技術を組み合わせたものである。図 6 はブロックチェーンに影響を与えたとされる技術体系をまとめたもの［9, p.16］である。

図 6 に示すようにブロックチェーンは、幾つかの既存の技術体系を集約したものとして生まれた。

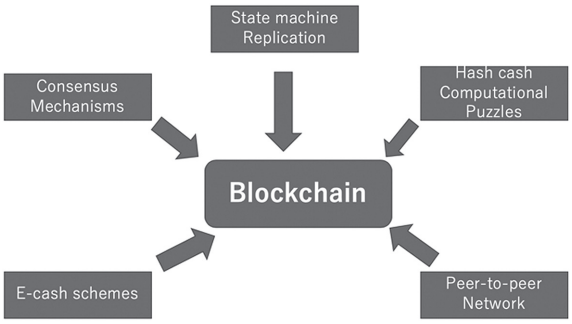

図 6．ブロックチェーンに影響を与えた様々な技術［9, p.16］

1．E-Cash Schemes：電子マネーを始めとするキャッシュレス体系［27］である。実際には、全ての取引を電子媒体上に移した形態を e-cash と呼び、適切な金融取引手段と組み合わせることで、キャッシュレスで取引を終えることができる体系である。
2．Consensus Mechanisms：正当性を担保するための合意形成メカニズムのことであり、P2P ネットワークでは特に重要となる。不正 Peer や故障 Peer に対するフォールトトレラント制御［28］のために必要不可欠である。狭義にはビザンチン将軍問題［29］の解法として定義されることが多い。Nakamoto の論文［1］では Proof of Work と呼ばれるリソース消費型のコンセンサス・アルゴリズム［30］が利用された。
3．State Machine Replication：SMR とも呼ばれ、システムの対障害性を向上するための技術の一つである［31］。サーバークライアントモデルでは、レプリカと呼ばれるシステムのコピーを複数作成し、レプリカ間で処理順序を同期させることで、一部に障害が発生しても、処理を継続できるようにすることである。

4．Hash cash Complutational Puzzles：Hashcash［32］は、1997 年に Black が提唱した。当初は匿名リメーラーからの DoS 攻撃対策［33］として利用されていた。現在では、Bitcoin のマイニングに利用されている。

5．P2P（Peer-to-Peer）Network：P2P は［34］、インターネット上のサービスモデルの一つである。P2P は、サーバークライアントモデルのようにサーバとクライアントの役割の異なる二つのコンピュータでサービスを構成するのではなく、全て対等な Peer 同士の結合体としてサービスを行うモデルである。

上で示した技術は、ブロックチェーンが登場する前から存在しており、これらの技術的な体系を組み合わせてブロックチェーンが作られている。ブロックチェーンは、図 7 に示すように、ベースとなる P2P ネットワーク上に形成されるアプリケーションプロトコル･スタックの総称であり、内部要素的には、トランザクション、ブロック、コンセンサス、状態マシン、ブロックチェーンアプリケーション（スマートコントラクト）などのプロトコルモジュールを持つ［9, p.17］。

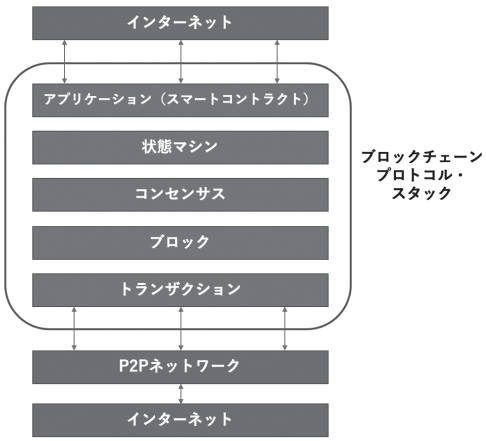

図 7．ブロックチェーンのプロトコルとしての位置づけとプロトコル・スタック［9 , p.17］

4.1. P2P ネットワーク

P2P ネットワーク［34］は、サーバークライアントモデルとは異なるコンセプトに従ったサービスモデルである。P2P は、サーバとクライアントのような機能の異なるシステム間の連携によりサービスを実現するのではなく、それぞれの情報デバイスを対等な関係を持つ一連の Peer と定義し、その間でデータを交換するものである。

4.2. P2P と分散型台帳

本論文で定義するブロックチェーンの一つの特徴として、「P2P で各ノードが分散型台帳を保持していること」とした。それぞれの Peer に台帳を管理することで、分散型台帳は保持できる。ここで、分散型台帳技術（Distributed Ledger Technology）は、ネットワークで分散されたデータベースの管理技術である。通常、データベースを管理する場合、データベースサーバにおいて一元管理することが多い。しかし、分散型台帳技術は、中央の管理サーバを置かずに、ネットワーク上に分散させる。P2P は、分散型台帳の実装プラットフォームとして最適なネットワーク系である。

分散型台帳を使うことで、データベースを集中管理する必要がなく、また対障害性が高くなる。また、不正取引や改ざんに対して耐性をもたせることも可能となる。今日、Bitcon を始めとするブロックチェーンの応用には分散型台帳技術は必須となっている。

4.3. ブロック、トランザクションとハッシュチェーン

二つ目の特徴は、「ハッシュチェーン構造を持つこと」であり、三つ目は、「電子署名されたトランザクションを実装し、木構造の根データを保持していること」となっている。

ブロックチェーンにおいて「ブロック」、「ト

ランザクション」と「ハッシュ関数」は重要な要素技術である。トランザクションは、分散型台帳の取引を記述する。ブロックは、トランザクション（一般的に、トランザクションは、その内容の完全性チェックのために、トランザクションを発行する者の鍵で電子署名されている。）とナンス値、直前のブロックのハッシュ値を格納する。図８はブロックの基本構造である。ブロック内の複数のトランザクションの管理は、電子署名されたトランザクションをマークル木［35］で一つにまとめる。マールク木はマールクが発明し、ハッシュ木とも呼ばれる根付き木で、その役割はデータの要約と検証である。トランザクションは電子署名されているので、木構造で接続されたブロック内のトランザクションの正当性を検証するには、全ての電子署名に対して検証しなければならない。しかし、それでは時間がかかりすぎるので、マールク木で電子署名を要約し、全ての電子署名を検証するのではなく、マールク木の根（root）だけを検証すればよいようになる。これが、電子署名されたトランザクションとそれらが木構造の根データを保持している、の意味である。

「ナンス値」は、Number Used Once の略で、一度しか使わない値のことである。ナンス値は、Bitoin では 32 ビットの数値で、マイニングの時に使用される。マイニングは、過去のトランザクションデータや新しくブロックに入れるトランザクションデータにナンス値を入れてひたすらハッシュ値を探す作業である。計算されたハッシュ値に制約条件（これをブロックチェーンでは「Difficulty」と呼ぶ。）を付けて、その制約条件を満たすハッシュ値をひたすらナンス値を代えて計算を繰り返す。ここで、Difficulty としては、「計算されたハッシュ値の先頭からの幾つかの桁にゼロ（0）が並ぶ」等である。

図８．ブロックの基本構造［９, p.18］

見つかったナンス値を入れたブロックから計算されたハッシュ値を、チェーンを接続するポインタとして使う。接続の様子を図９に示す。このようにハッシュ値を使ったブロックの接続構造をハッシュチェーンと呼ぶ［9, p.19］。

図９．ブロックチェーンの接続構造［９, p.19］

4.4.　コンセンサスアルゴリズム

ブロックチェーンの最後の条件が、「コンセンサスアルゴリズムが実装されていること」である。

ブロックチェーンは、分散型台帳として参加する Peer が同じデータを同じ量だけ保持することになる。このとき、データの正当性を担保する仕組みが必要となる。コンセンサスアルゴリズムは、「どのようにお互いのデータが正しいかを担保する」ために必要となる。

仮想通貨の場合、その取引が正当であるかどうかを担保して、正当であればデータをトランザクションとしてブロックに格納し、そうでなければ排除しなければならない。Bitcoin で使われている Proof of Work（以下「PoW」と略記する。）は、簡単に言えば「膨大な計算量を使って発見困難な値を見つける

表１．代表的なコンセンサスアルゴリズム［9, pp.28-29］

	PoW	PoS	PoI	PoC
名称	Proof of Work	Proof of Stake	Proof of Importance	Proof of Consensus
正当性の担保	仕事量	一定以上のコイン	総合信用スコア	一定数以上のバリデータの承認
代表的仮想通貨	Bitcoin	Ethereum	Xem	XRP
利点	・非中央集権 ・公平性の担保	・電力消費を抑える	・公平性の担保	・高速送金 ・低消費電力
欠点	・消費電力が高い ・51%攻撃の可能性	・資金力のあるものが占有する可能性	・信用スコアの計算に問題あり	・バリデータ間の悪意のある取引

とブロックを作ることができる。」というアリゴリズムであり、様々な分野で応用できる。

PoX（X というリソースを使うリソース消費型のコンセンサスアルゴリズム）には、PoW の他に、様々なものが知られている［9, pp. 28-29］。表 1 は、これまでに報告されている PoX 型のコンセンサスアルゴリズムの一部である。

PoW は Bitcoin［8］で採用されたコンセンサスアルゴリズムであるが、その起源は Hashcash［32］以前まで遡ることができる。PoW は、ナンス値のところで説明したように。ナンス値を入れたブロックを決められたハッシュ関数によりハッシュ値を計算し、それが Difficulty を満たすまで繰り返す。まさに、計算機の仕事量が問題となるプロトコルである。PoW は、非中央集権的で公平性が担保されており、知名度も高いために、他の仮想通貨でも使われている。一方、消費電力の問題や 51％攻撃の可能性が欠点として指摘されている。

PoS は仮想通貨 Ethereum［36］で採用されたコンセンサアルゴリズムである。PoS は、PoW の力技による消費電力を抑えることを目指して開発された。PoS は、「一定量のコインを保持している」がマイングの条件となるため、資金力が高いものが占有する危険性がある。そのため、新しい Ethereum の規格では、PoI や PoC への移行が示唆されている。

PoI や PoC は単純な力技やコイン量という指標ではなく、総合的な判断を種々のパラメータを使って下す（PoI）方式や、バリデータと呼ばれる取引の承認作業を行う特別な Peer が存在しており、それらの承認を一定数必要とする（PoC）といった方式が開発されている。

いずれにしても、コンセンサスアルゴリズムは一長一短があり、ブロックチェーンを活用する対象によって、適切なものを選択しなければならない。

4.5. 状態マシン

ブロックチェーンは、ブロックをハッシュチェーンで連結したものである。そのため、本来は状態（state）を持たない。しかし、技術的には、全ブロックを記述した状態から、新しいトランザクション（状態遷移関数とみなすことができる。）により、新しい状態へ遷移する状態遷移マシンとみなすことができる。面白いトピックであるが、本論文の議論とは大きく関連しないので、詳細は省く。詳しくは Ethereum の White Paper［36］を参

照せよ。

4.6. アプリケーション（スマートコントラクト）

スマートコントラクトは、1994 年に Szabo が提唱した概念 [37] である。広い意味では、契約の存在保証、契約の一意性、契約の自動化を実現するものである。Szabo は、例として、自動販売機を上げている。

ブロックチェーンでは、ブロックチェーン上で動作するアプリケーションと定義する。ブロックチェーンに影響を及ぼすアプリケーションは、広い意味では対象とするブロックチェーンと暗黙の契約の結ぶと考えられる。したがって、ブロックチェーンに影響するすべてのアプリケーションは、スマートコントラクトであると考えられる［38］。

5 . ブロックチェーンの SCM への適用

ここでは、サプライチェーンの課題が、ブロックチェーンを適用することで解決するかどうかについて考察する。

5.1. コンソーシアム型ブロックチェーンの適用

優れた流通システムを構築するためは、コンソーシアム型ブロックチェーンを適用することが良い。コンソーシアム型は、コンソーシアムに参加しているメンバーがブロックチェーンの Peer を形成するため、ガバナンスの脆弱性がシステムに影響ことはないと考えられる。そのため、逆に、実用段階で優れた組織運営を行えない場合、ブロックチェーンは秘匿性が増すので、導入を見送るべきである。ブロックチェーンの管理はコンソーシアムメンバーでの共同管理となるため、パブリック型のような非中央集権制は薄れるが、メンバー相互が監視することで、一つの権威に権限が集中することは避けられる。

5.2. 情報共有の問題

通常のサプライチェーンでは、フィードバックプロセス（下流側のプレイヤーがより上流に存在するプレイヤーの情報を参照するようなデータ参照の流れ）が起きない。しかし、消費者は商品の安全性を求めて、より深いデータの参照を要求する可能性がある。これは、情報管理に関する要素の中の、説明責任性、特にその中でも、食品などの起源を明らかにするトレーサビリティ（追跡性）に関わる重要な問題である。

製品のトレーサビリティを確保することで信頼性、透明性を高めることができる。製品の価値は完成品だけでなく製品の製造プロセスや原材料、社会的費用により変動する。正しい価値を反映させるには、トレーサビリティを高めることが必要である。

例えば、製品には生産国が記入されるが、複数の生産国に分かれていたりする場合、実際の表記と消費者のとらえ方にずれが生じる場合がある。ワインを例に上げると製造国Ａと製造国Ｂのワインを C 国でブレンド後ボトリングした場合、生産国の表記はＣになる［39］。消費者がブレンド工程より元となったワインの生産国の方が重要と考えている場合、判断が難しくなる。いずれにせよ、消費者に製品のプロセスのトレーサビリティを確保することは消費者に正しい選択肢を与えることとなる。

情報の流れを一元化することで様々な情報収集は容易となる。サプライチェーン間の情報は、従来であれば情報管理が一元化されていないため量・質ともに集めることが難しい［40］。ブロックチェーンを介して情報を集めれば容易に実現できる。各拠点間に配送する際、時間同期を正しく行っておけば、時間を記録して、正確な所要時間があらかじめ分かる。このようなタイムスタンプによる時間管理も、ブロックチェーンの適用により可能と

なる。

5.3. 最適化問題

P2P によるブロックチェーンは、通常のサーバ−クライアント方式に比べ可用性に優れる。サーバ−クライアント方式は冗長化することで高可用性を持つことができるが、P2P なら初めから冗長化されている。そのため、耐障害性が高い。SCM システムの障害は、製品の製造に大きく影響するため、このような冗長構成による保護は重要となる。

ところで、P2P となったことで可用性は上がるが、情報探索には、冗長性を持たせるためには P2P のルーティングを実装しなければならない。また、解析的に、データ探索のパスの最適化が難しいことも指摘されている。

実際のサプライチェーンの最適化は、需給最適化問題となる［41］。需給最適化問題は、サプライチェーンの基礎技術として、ブロックチェーンを使うことで解決しない。したがって、最適化問題は、この論文の取り扱い範囲外とする。現在は、AI を応用した最適化の試み［42］等がなされている。

5.4. セキュリティマネジメント

セキュリティ問題に関しては、SCM への適用を考えた場合、仮想通貨で使われている、CPU パワーやコイン量を指標とする厳密なコンセンサスアルゴリズムは必要ない。どちらかといえば、情報の漏えいや改ざんを防止するための情報管理的なセキュリティが重要となる。

鍵管理の問題は、プライベート CA を中心とした、プライベート PKI を使う方式が主流である。しかし、実運用を考えると信頼性のある第 3 者機関の運営するパブリック CA によるパブリック PKI を使う方法もある。

5.4.1. 所有権移転トランザクション

サプライチェーン内の製品のトランザクション処理は製品 ID、事業者 ID、タイムスタンプ等の種々の ID や時間管理データと実際の取引の帳票で構成される。前者の管理データを「メタデータ」、後者の取引データを「帳票データ」と便宜的に呼ぶ。サプライチェーンは、実際にモノが移動するので、製品の所有権は、次々と移動する。メタデータには、製品 ID と事業者 ID により、所有権移転の様子がブロック内に保持されることとなる。このようなトランザクションの形態を所有権移転トランザクションと定義する。所有権移転トランザクションを使うことで、サプライチェーンに事故が起きたとき、その商品の所有権がどこなるかが明確となり、説明責任性が厳密に保たれることとなる。

所有権移転型とする理由は、実装が単純であり、サプライチェーンの企業からもわかり安く、コストも安く抑えられるからである。また、所有権が明確になっていると、事故が起きたとき保険等の救済サービスを受けやすくなる。サプライチェーンに加盟している金融系の企業がブロックチェーンの情報を読み取り、審査の労力を大きく省くこともできる。保険の契約もブロックチェーン上で完結すれば、審査や契約の時間の短縮につながる。

所有権を移転していく処理手順は、あらかじめコンソーシアム内の企業 ID をブロックチェーン内に記録しておき、製品の ID と企業 ID、タイムスタンプ＋取引情報を含めたトランザクションを発生させる。トランザクションはブロックチェーンに記録される。製品がサプライチェーンの次のプレイヤーに渡れば同じようにトランザクションを発生させ、ブロックチェーンに記録する。製品 ID は QRcode に記録しておけば QRcode を読み込むだけで所有権移転のトランザクションを発生させるよう設定しておけばよい。QRcode

であればカメラ機能と通信できる一般的な端末、例えば、スマートフォンを利用することで実現できる。最終的に消費者が製品を受け取ったとき、QRcode をブロックチェーンで検索すると製品の追跡ができるようになる。消費者とコンソーシアム、サプライチェーン内の企業との距離が近くなることにより製品の評価、不良品やリコールの管理が迅速になる。ただし、一般消費者をどのように SCM に取り込むかについては、検索権限の設定などを含めて議論が残る。

5.4.2.　リスク耐性

分散型台帳技術が基盤になっているブロックチェーンでは災害などによってデータ損失する可能性が低く、極端に狭い地域に Peer が集まっていない限り、一つの災害によってデータが損失する可能性は低い。無論データのバックアップなどはリスク管理の視点から必要ではあるが基礎技術の部分で災害への強さは、小さなコンソーシアムにとっては重要な利点になる。

5.4.3.　対改ざん性

P2P システムには中央集権的ではなく分散管理なので不正 Peer や故障 Peer が混入した場合にデータの整合性が取れないリスクがある。ブロックチェーンは P2P システムでありながら、コンセンサスアルゴリズムの実装等により、通貨に使われるほど不正 Peer や故障 Peer への耐性が高い。

SCM は、受発注や金銭の授受に関する業務上重要な取引情報を扱うことになる。SCM には、コンセンサスアルゴリズムとは別に、PKI 等による厳密な鍵管理を含めたセキュリティモデルを使った対改ざん性対策が必要となる。

5.5.　ガバナンス問題

サプライチェーンの不祥事は、情報の非対称性や断絶が原因になることが多い。消費者は、SCM の中では末端であり、消費者が適切な情報を得るのは従来の EDI をベースとするシステムでは困難である。それどころか、消費者に正しい情報が伝わるかどうかも怪しい。本論文では、コンセンサスアルゴリズムであり、なおかつコンソーシアムの合意形成の手段として、トークンと呼ばれるものを定義し、その利用方法を示す。

企業内の内部統制［43］も含めた情報の統制と開示はコンソーシアム内のガバナンスの問題［44］と捉えることができる。また、直接製品を取引しない金融機関や監査機関に対して、どこまで情報を公開するかの決定も、ガバナンスの役割である。コンソーシアム型を採用することにより、このような統制は取りやすくなっているが、それらを技術的な要素として組み込むことは難しく、実体としてのプレイヤー間のガバナンスの問題は重要である。

5.5.1.　トークンによるコンソーシアムの管理

コンソーシアムの管理とブロックチェーンの管理のためトークンを使用する。トークンは、コンソーシアムが発行し、PoX 型の採掘権に利用でき、ネットワークを介した意思決定（ガバナンスの強化）に使われる。トークンを多く保有している Peer ほど意思決定に寄与する割合を多くする。トークンは初期状態では、プレイヤーに均等に配布され、意思決定が必要なときに投票券として機能する。このようなコンセンサスアルゴリズムを本論文では Proof of Token（PoT）と呼ぶ。トークンを多く保有している企業はトークン紛失リスクとコンソーシアムへ多く出資（資源提供）を行うことでブロックチェーン内の取引の手数料を受けることができ、同時に、

内部における発言権を強化できる。発言権の強化は、ブロックチェーンの非中央集権性と相反するものであるが、サプライチェーンへの適用を考える場合、このような緩和は必要である。

Peer 内部での処理速度やトランザクションの処理数は、Peer の構成を決める一つの要素であるが、一般の消費者や末端の原料供給者に投資コストを強いることはできない。末端では、スマートフォン程度の情報端末で参加できることが望ましい。したがって、本論文では、ネットワーク系はメッシュ型の P2P の構成を前提としているが、この点でも見直しが必要である。適切なネットワーク系とデバイスの配置は、コンソーシアム内のコンセンサスで決められることになる。

このように、SCM へのブロックチェーンの適用は、セキュアプロトコルの事実上のデファクト標準を使用することで、SCM そのものの安全性と透明性を高め、サプライチェーンの健全化に寄与すると考えられる。さらに、本論文で示した所有権移転トランザクションとトークンによるコンソーシアムの管理を行うことで、サプライチェーンで管理されているモノの管理主体が明確となり、責任の追求やモノの追跡が容易となり、保険などの周辺支援体制の強化に繋がると考えている。

5.5.2. スマートコントラクト

ブロックチェーンのスマートコントラクトにより、これまでの商慣習より効率的に契約を行える。ブロックチェーンのシステム内では発注側が発注用のスマートコントラクトを発行し、受注側が履行するだけになる。ブロックチェーンのシステム外ではスマートコントラクトの履行とともにスマートコントラクトの履行内容をそのまま実行する。従来は注文書、注文請書など複数回の情報の往復があったが、スマートコントラクトでは必要なく、一往復で契約を完結できる。スマートコントラクトを使用すれば、契約をオークション制や競争入札制、抽選制、先着制など様々な方法での契約が可能となる。SCM の管理項目内で、このような実際の契約行為の管理、さらにはキャッシュフローまでも一元管理できることは、ブロックチェーンを利用する大きなメリットとなる。

6．まとめ

本研究の結論は、「ブロックチェーン技術は、幾つかの修正を必要とするが、SCM に応用可能である」、というものである。本来 SCM は、フィジカルレイヤの物流（モノを運ぶこと）と商流（モノを売ること）と強く結びついている。そのために、業界ごとの商習慣が入りやすく、これまで標準化が遅れていた。しかし、グローバル化の進展により、SCM は、複雑化、国際化してきた。残念ながら現在行われている多くの標準化の試みは、完全に業界横断的な仕様となっていない。ブロックチェーンは多くの仮想通貨に使われているように、分散型台帳の管理のためのデファクト標準になりつつある。したがって、SCM にブロックチェーンを応用することは、業界横断的な標準化を達成するために、必要であると結論づけられる。

しかし、ブロックチェーンそのものをいきなり SCM に組み込むことは、サプライチェーンの性質上、難しいこともわかった。特に、セキュリティ問題は重要であり、本来、中央集権的な権威機構を持たないブロックチェーンに CA を中心とした信頼性モデルを組み込む必要があることがわかった。

しかし、そのような一部修正をするとしても、ブロックチェーンの SCM への適用は、魅力的で、効果的であると結論づけることができる。

引用・参考文献

[1] 石川和幸、『この1冊ですべてわかるSCMの基本』、日本実業出版、61頁、2017年。

[2] IT+ビジネス、「サプライチェーンマネジメント（SCM）とは何か？基礎からわかる仕組みと導入の方法」、SBクリエィティブ、2018年。
URL: https://www.sbbit.jp/article/cont1/34345（アクセス日：2019年12月12日）

[3] 宮下真一、「サプライチェーン・マネジメントにおける情報化と国際化の機能に関する実証分析」、『関西大学商学論集』、54巻、41-57頁、2009年。

[4] GXS Tutorial for the Active Business, Ed. “ANSI ASC X12 Standards Overview Tutorial”, *GXS Proprietary and Confidential Information,* 1980。
URL: https://www.gxs.co.uk/wp-content/uploads/tutorial_ansi.pdf（アクセス日：2019年12月20日）

[5] 安東一真、「【解説】ebXML Webサービスの利用をより簡単に　先行するSOAP/UDDIとは共存か」、『日経XTECH』、日経BP、2001年。
URL: https://tech.nikkeibp.co.jp/it/members/NIT/ITARTICLE/20010306/1/（アクセス日：2019年12月10日）

[6] 伊藤通晴、「ebXML MSを用いた流通コラボレーション」、XMLコンソーシアム、2002年。

[7] R. P. Cohen（IT Leaders 編集部翻訳）、「[基礎から分かる『EDI再入門』～グローバル企業のビジネス情報連携方法～]【第5回】EDIドキュメントと最新のグローバル標準」、『IT Leaders』。Impress、2015年。
URL: https://it.impressbm.co.jp/articles/-/11823（アクセス日：2019年12月20日）

[8] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008。
URL: https://bitcoin.org/bitcoin.pdf（アクセス日：2019年4月5日）

[9] I. Bashir, “Mastering Blockchain -Distributed Ledgers, Decentralization and Smart Contracts Explained-”, Packt Publishing Ltd. 2017.

[10] 石川和幸、『SCMの基本』、日本実業出版社、14頁、2017年。

[11] M. Hugos, “Essentials of Supply Chain Management, 4th ed.”, Wiley, p.26, 2011.

[12] F. Yiannas, “A New Era of Food Transparency Powered by Blockchain”, *Innovations: Technology, Governance, Globalization,* Vol.12, pp.46-56, 2018.

[13] 寺前俊孝、「SCMの変遷に見る2つの方向性と知識経営の視点による考察―知識経営の視点による付加価値創造型SCMの考察―」、『経営情報学会　全国研究発表大会要旨集』、2009f（0）、8-8、2009年。

[14] M. S. Ford and W. Baum, “Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption, 2nd Ed.”, Prentice Hall, 2000年。

[15] 総務省、「政府認証基盤（GPKI）について」、総務省、2001年。
URL: https://www.e-gov.go.jp/help/shinsei/flow/setup04/manu_certificate.html（アクセス日：2019年12月20日）

[16] M. Singer、「デル1社では済まない--PCメーカーを揺るがす不良コンデンサ」、『CNET News』、CNET Japan、2005年。
URL: https://japan.cnet.com/article/20091696/（アクセス日：2019年12月19日

[17] 消費者庁、「食品表示基準の一部改正の

ポイント」、消費者庁、2017 年。
URL: https://www.caa.go.jp/policies/policy/food_labeling/quality/country_of_origin/pdf/country_of_origin_171027_0003.pdf（アクセス日：2019 年 12 月 19 日）
[18] 増田佳昭、「食品偽装問題の諸段階と食品表示の課題」、『農業と経済』、68 巻、pp. 5–11、2002 年。
[19] 三菱 UFJ リサーチ＆コンサルティング、「平成 28 年度商取引適正化・製品安全に係る事業　サプライチェーン最適化に向けた物流の実態調査等　報告書」、経済産業省、2017 年。
URL: https://www.meti.go.jp/meti_lib/report/H28FY/000608.pdf（アクセス日：2019 年 12 月 20 日）
[20] 久保幹雄、『サプライチェーン最適化の新潮流（サプライチェーンマネジメント講座)』、朝倉書店、2011 年。
[21] 金谷健一、『これなら分かる最適化数学―基礎原理から計算手法まで』、共立出版、2005 年。
[22] 伊理正夫、「ネットワーク問題の理論と手法の最近の進歩」、『経営科学（日本オペレーションズ・リサーチ学会邦文機関誌)、16 巻、75–87 頁、1972 年。
[23] 和田健、清水良明、「ハイブリッド型メタ戦略によるサプライチエーンネットワークの全体最適設計」、『システム制御情報学会　論文誌』、19 巻、69–77 頁、2006 年。
[24] 山田忠史、繁田健、今井康治、谷口栄一、「在庫費用を考慮したサプライチェーンネットワーク均衡モデル：消費需要の不確実性に伴う物資流動量とネットワーク効率性の変化」、『土木学会論文集 D』、66 巻、359–368 頁、2010 年。
[25] 出口雄一、「情報収集の手法（2）--- キーロガー、スニファリング、ウォーダイヤリング、ウォードライビング」、『日経 XTECH』、日経 BP、2006 年。
URL: https://tech.nikkeibp.co.jp/it/article/COLUMN/20061108/253053/（アクセス日：2019 年 12 月 22 日）
[26] 久保知裕、原田要之助、「サプライチェーンにおける情報セキュリティの研究」、『情報処理学会研究報告、EIP、［電子化知的財産・社会基盤］』、65 巻、1–8 頁、2014 年。
[27]「キャッシュレス革命 2020」研究会編、『キャッシュレス革命 2020 電子決済がつくり出す新しい社会』、日経 BP、2014 年。
[28] 南谷崇、『フォールトトレラントコンピュータ』、オーム社、1991 年。
[29] L. Lamport, R. Shostak and M. Pease, “The Byzantine Generals Problem”, *ACM Trans. Program. Lang. System,* Vol. 4, pp. 382–401, 1982.
[30] 勝木健太著、ブロックチェーン白書編集委員会編、『ブロックチェーン白書 2019』、N.Avenue、2019 年。
[31] F. B. Schneider, “Implementing fault-tolerant services using the state machine approach: A tutorial”, *ACM Computing Surveys,* Vol. 22, pp. 299–319, 1990.
[32] A. Back, “hash cash postage implementation”, 1997.
URL: http://www.hashcash.org/papers/announce.txt（アクセス日：2019 年 12 月 20 日）
[33] A. Back, “Hashcash - A Denial of Service Counter-Measure”, 2002.
URL: http://www.hashcash.org/papers/hashcash.pdf（アクセス日：2019 年 12 月 20 日）
[34] G. Camarillo, Ed. “Peer-to-Peer（P2P）Architecture: Definition, Taxonomies, Examples, and Applicability”, *IETF,* RFC5694, 2009.

[35] R. C. Merkle, “Secrecy, authentication, and public key systems”, UMI Research Press, 1982.
[36] V. Buterin, “Ethereum White Paper: A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM”, 2013.
URL: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf（アクセス日：2019年1月30日）
[37] N. Szabo, “Formalizing and Securing Relationships on Public Network”, First Manday, 1997.
URL: https://firstmonday.org/ojs/index.php/fm/article/view/548/469（アクセス日：2019年1月30日）
[38] 濱田優、「ブロックチェーン、スマートコントラクトが金融ビジネスにもたらす影響は？ ―― STOとICOの違い」、coindesk、2019年。
URL: https://www.coindeskjapan.com/19863/（アクセス日：2019年12月5日）
[39] 消費者庁、「食品表示基準の一部改正のポイント」、消費者庁、2017年。
URL: https://www.caa.go.jp/policies/policy/food_labeling/quality/country_of_origin/pdf/country_of_origin_171027_0003.pdf（アクセス日：2019年12月19日）
[40] 大居由博、「ブロックチェーンが与えるサプライチェーンマネジメントへのインパクト」、DIGITAL INSIGHT、2019年。
URL: https://www.nttdata.com/jp/ja/data-insight/2019/0221/（2019年12月26日）
[41] 宮下真一、「需給チェーン・システムの事例分析：ディマンド・サイドとサプライ・サイドの比較考察」、『経済と経営（札幌大学経営学部紀要）』、37巻、59–80頁、2007年。
[42] 西竜志、「サプライチェーンにおける分散協調型最適化技術」、『人工知能学会』、19巻、571–578頁、2004年。
[43] 経営ハッカー編集部、「【内部統制の4つの目的と6つの基本要素】上場準備に必要不可欠な内部統制とは」、経営ハッカー、2019年。
URL: https://keiei.freee.co.jp/articles/c0501665（アクセス日：2019年12月15日）
[44] 竹本佳弘、「サプライチェーン・ガバナンス」、『日本貿易会　月報』、No. 665、21–24頁、2009年。