ブロックチェーン技術とIBMの取り組み

「情報の革命」から「取引の革命」へ
IBMの戦略とHigh Security Business Network

次世代の革新的技術としてブロックチェーンが注目を浴びています。特に金融業界においては、FinTechを支える主要技術として、国内外の銀行・証券会社/取引所を中心に積極的な検討や実証実験が盛んです。また最近では、金融業界だけでなく、公的サービスやサプライチェーンでの適用など、金融業以外への適用検討が広がってきています。

本稿では、ブロックチェーンの概要や最新の適用事例を紹介するとともに、IBMの取り組みとして、オープンソース・プロジェクトである「Hyperledger Project」での分散台帳技術の動向、ブロックチェーン・クラウド・サービスである「High Security Business Network（HSBN）」、そして、お客様との取り組みを紹介します。

1. ブロックチェーンの概要と最新動向

ブロックチェーンへの注目が非常に高まっています。特に、2015年からブロックチェーンの実ビジネスへの適用のための検討・検証が本格化し、メディアで取り上げられるケースが急増しています。ブロックチェーンは第2のインターネットとも呼ばれており、インターネットが「情報の革命」であるのに対し、「取引の革命」であるとも言われています。しかし、技術的にやや難解であるため、本質的な特徴やメリットがとらえづらい、何に適用すればよいのかよく分からないといった声も少なくありません。

ブロックチェーンは、分散台帳技術（DLT：Distributed Ledger Technology）であり、ピア・ツー・ピア（P2P：Peer to Peer）技術と暗号技術を使って、複数の参加者からなるビジネス・ネットワークでの各種資産の取引（取得・譲渡や移転・破棄など）の台帳を分散管理する技術です。取引を確実に実行するために、これまでは信用を担保する中央機関・仲介機関が介在していましたが、ブロックチェーンを使うことにより、これら中央機関・仲介機関を介さずに、複数参加者間の取引を安全に安価に、かつ迅速に実現できることが期待されています（**図1**）。

ブロックチェーンはもともと、仮想通貨であるビットコイン（Bitcoin）を支える要素技術として登場しました

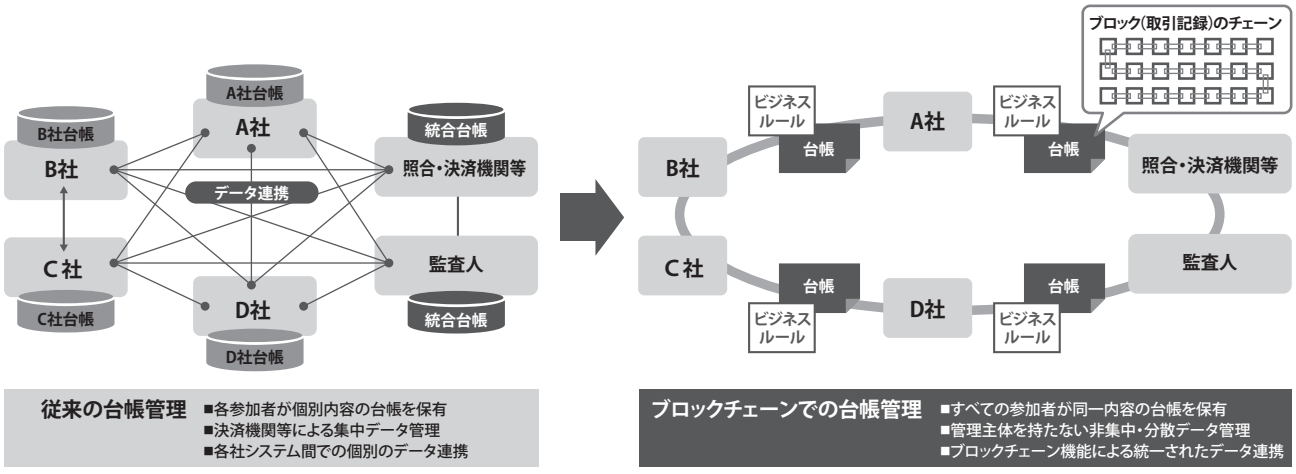

図1. ブロックチェーン～非集中・共有型の台帳管理

が、FinTechへの注目の高まりとともに、仮想通貨以外の金融資産の取引・移転にも幅広く適用できる技術として注目が高まってきました。

ブロックチェーンを活用することのできる資産（アセット）は、金融資産にとどまりません。自動車、美術品や農作物といった有形資産、不動産やデジタル・コンテンツといった無形資産、各種公的な権利・証明もブロックチェーンが扱うことができる資産です。インターネットがあらゆる情報を高速に、安価に、信頼性高く共有できる革新的な技術（「情報の革命」）であったのに対し、ブロックチェーンはあらゆる取引を、高速に安価に信頼性高くやり取りできる革新的な技術（「取引の革命」）として期待が高まっています。経済産業省の報告書でも、仮想通貨や海外送金のみならず、公的な記録、シェアリング・エコノミー、サプライチェーンなどさまざまな領域での適用が予想されています[1]。実際に、金融のお客様のみならず、行政機関や流通・小売業や製造業など、さまざまな業種のお客様で検討・検証が進んでいます。

2. Hyperledger Project

世の中にはビットコインやイーサリアム（Ethereum）をはじめとした、さまざまなブロックチェーン基盤があります。しかし、ブロックチェーンを多様な業務に適用しようとする場合のさまざまな要件を考慮した時、既存の基盤ではすべての要件を満たすことができません。また、さまざまなブロックチェーン基盤が乱立すると相互接続が困難となるばかりでなく、ツールやソリューションの互換性がなくなり非効率的です。 複数の企業で力を合わせて、オープン・ガバナンスの下に多様な業界で使える基盤を開発し、これをオープン・スタンダードとすることで、ブロックチェーンの普及を推進することができると考えられます。

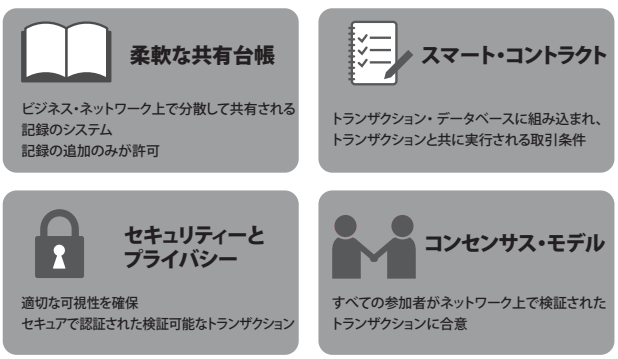

図2. Hyperledgerの4つの技術的な特徴

Hyperledger Projectは、このような目的のために設立されたオープンソースのコミュニティーであり、Linux Foundationの下で活動しています[2]。2015年12月の設立以降参加企業が急激に増加し、2017年1月現在、約100社のメンバー企業が参加しています。オープンソース・コミュニティーの参加企業はITベンダーが多いのが一般的ですが、Hyperledger Projectではそれに加えて、銀行や証券取引所などの大手金融機関が多いのが特徴です。また製造業の参加企業も徐々に増えています。IBMは、Hyperledger Projectの創立メンバーであり、44,000行に及ぶコード提供、技術ステアリング・コミッティーのリードなど、当プロジェクトを積極的に推進しています。

Linux FoundationはもともとLinux OSの開発を行っていました。Linux OS自体はオープンソースですが、多くの企業がデスクトップやサーバー、スマートフォン、さまざまな組み込み機器に使用して自社のビジネスに役立てることで世界標準的なOSとなっています。ブロックチェーンの基盤についても、コアとなる共通基盤はオープンソースとして各社が協力して開発することで、技術の迅速な発展と普及を促すことが期待されます。

Hyperledgerは企業間コンソーシアムなどの参加許可制（permissioned）のネットワークで、さまざまな業務に使用可能なブロックチェーン基盤の開発を目指しており、技術的な特徴として、「柔軟な共有台帳」「スマート・コントラクト」「セキュリティーとプライバシー」「コンセンサス・モデル」という4つが挙げられます（**図2**）。

2-1.柔軟な共有台帳

ビットコイン等の一般的なブロックチェーン基盤では、送金等のトランザクションが発生すると、そのトランザクションの履歴が帳簿のように記録され、共有されます。このとき、トランザクションを記録したデータの塊（ブロック）を、暗号的ハッシュ値で鎖のようにつなぐことにより、改ざんに対して耐性のあるデータ構造となります。

これが「ブロックチェーン」という名前の由来です。

Hyperledgerではそれに加えて、データを任意の形式で格納できるデータベースを持ち、後述するスマート・コントラクトから自由に読み書きができるため、より複雑なデータ構造を扱うことが可能になります。例えば、ブロックチェーンを使った送金システムを考えるとき、ブロック上のデータ は「誰がいつ、誰に、いくら送金したか」という一連の記録であり、データベースには各ユーザーの口座残高や、それ以外のさまざまな情報を格納することができます。

2-2.スマート・コントラクト

Hyperledgerでは、スマート・コントラクトという仕組みにより、データだけでなくビジネス・ルールやプロセスを共有することができます。例えば、車のリース契約をブロックチェーン上で実現しようとします。

- ●AさんはBさんに車をリースする
- ●BさんはAさんに毎月リース費用を支払う
- ●もしBさんが期日までにリース費用を払わなければ、10%の利子を上乗せして翌月支払う
- ●もしBさんが2カ月連続してリース費用を支払わなければ、車の使用を差し止める
- ●リース費用は、最初は月5万円だが、毎年1月1日に見直して新価格を決定し、両者が合意した後に新価格が有効となる

このような処理を実現するためには、単に送金するだけでなく、「もし、〜なら、〜する」という条件に基づいた処理や、利子などの数値計算、特定のイベントに基づくアクションの実行、過去の事象の記録と参照、特定のユーザーの合意の記録などの機能が必要になります。

スマート・コントラクトはこういった処理を可能にする、一種の分散アプリケーションの技術です。技術的にはビジネス・ルールやプロセスを実行可能なプログラムとして記述し、ブロックチェーン・ネットワークのすべてのノードが同じプログラムを実行することで実現します（**図3**）。

2-3.セキュリティーとプライバシー機能

ブロックチェーンを業務使用する場合に、セキュリティーが重要なのは言うまでもありません。Hyperledgerは参加許可制のブロックチェーン・ネットワークを指

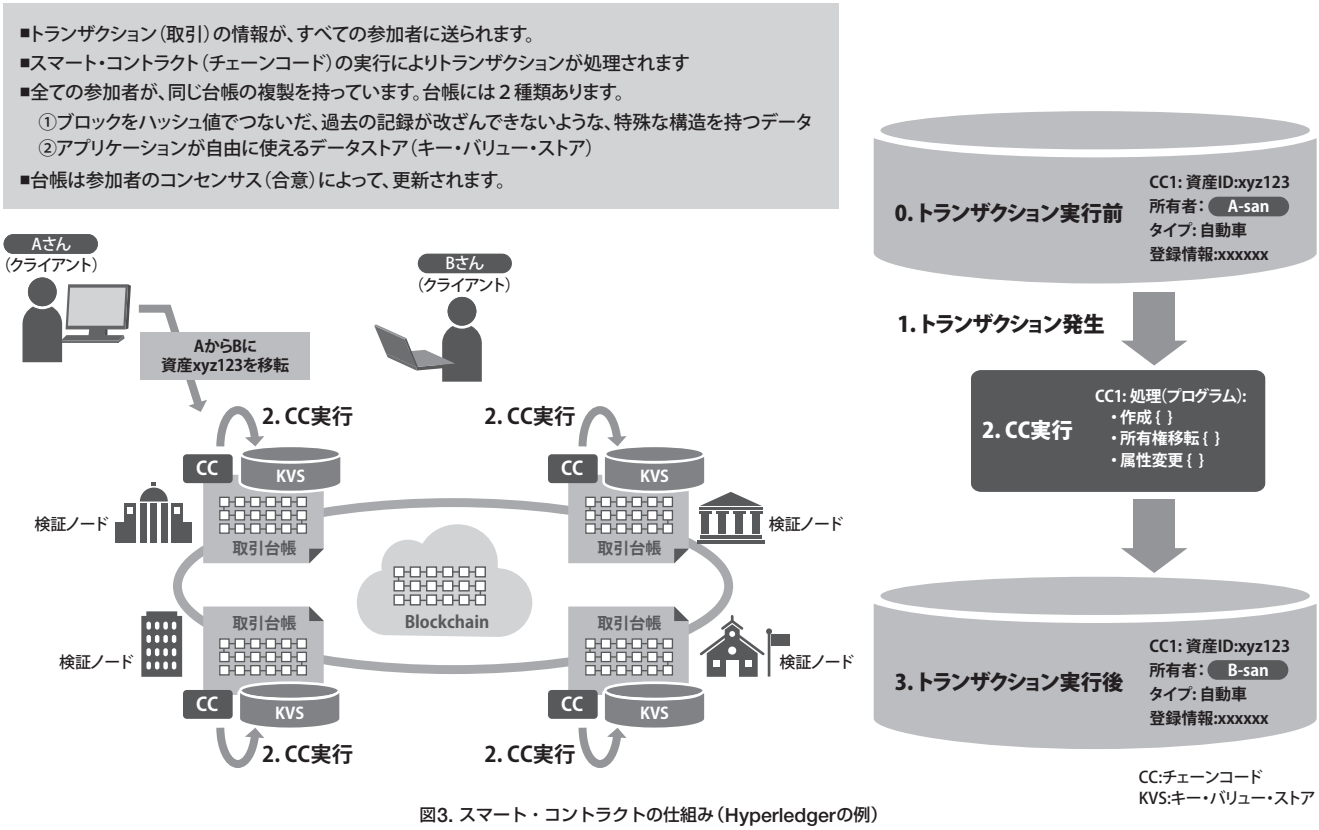

図3. スマート・コントラクトの仕組み（Hyperledgerの例）

向しているため、許可されたノードだけがネットワークに参加でき、また権限を持つユーザーだけがこれらのノードにアクセスできるようにする必要があります。Hyperledgerではメンバーシップ管理機能を持ち、公開鍵方式に基づくユーザー認証およびノード認証を行っています。また、参加者の認証を行いつつプライバシーを保護するための、匿名証明書の機能があります。

さらに、やり取りされるデータを暗号化するとともに電子署名を行うことで、データの秘匿性を保護し改ざんを防止する機能、データベースにアクセスした人の権限に応じてデータの参照・更新を許可するためのアクセス制御の機能があります。

2-4.安全で効率的なコンセンサス・モデル

コンセンサスとは、一般的に「合意」を意味しますが、ブロックチェーンにおけるコンセンサスは、それぞれのノードが持つデータの一貫性を保持するために、実行・承認するトランザクションの内容や順番について確認をするプロセスを指します。ビットコインなどで一般的に使われる「プルーフ・オブ・ワーク」(マイニングとも言う)も一種のコンセンサスの仕組みと言えますが、「消費電力が多い」「トランザクションのファイナリティーがない」(一度承認されたはずのトランザクションが、後に無効となりうる)という問題があります。このような性質は、特に既存の金融システム等と比較した場合に、大きなマイナスとなります。

HyperledgerではPBFT(Practical Byzantine Fault Tolerance)などのメッセージ交換型の分散コンセンサス形成アルゴリズムを採用しており、高速・低消費電力でコンセンサスを実行し、トランザクションのファイナリティーを保証することができます。

また、ビジネスの要件によって必要なコンセンサス・モデルは異なるという立場を採っており、さまざまなコンセンサス・モデルをプラグインして使えるようになっています。

3. IBMのブロックチェーンへの取り組み

3-1. IBMの「3つのC」の取り組み

IBMでは通称「3つのC」を通じたブロックチェーンへの取り組みを行っています(**図4**)。

1つ目のCはコミュニティー(Community)で、前述のようにオープンソース・コミュニティーのHyperledger Projectでの積極的な活動を行っています。

2つ目のCはクラウド(Cloud)で、Hyperledger Projectで開発したブロックチェーン基盤をIBMのクラウド上でサービスとして提供し、円滑なブロックチェーンの導入や運用を支援します。また、クラウド・サービス基盤である「IBM Bluemix」上において、後述する高セキュリティー基準のブロックチェーン・クラウド・サービスや、DevOpsサービスなどの付加価値サービスを提供します。

3つ目のCはクライアント(Client)で、ブロックチェーンの導入を支援するための「IBM Bluemix Garage for Blockchain」というサービスを東京、ニューヨーク、ロン

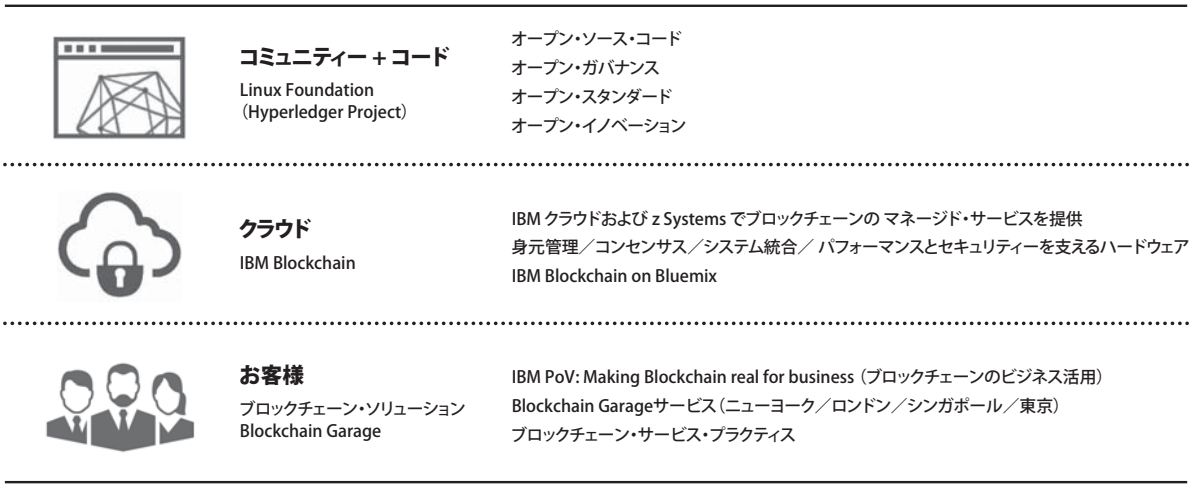

図4.「3つのC」を通じたIBMのブロックチェーンへの取り組み

ドン、シンガポールに展開しています。ここではデザイン・シンキングのワークショップを通じたユースケースの策定や、プロトタイプ開発による検証を行うことができます。

3-2. 業界最高水準のセキュリティー・レベルを誇るクラウド・サービス「HSBN」

ブロックチェーンは、暗号技術を用い、複数取引者間のビジネス・ネットワーク上の取引の安全性を確保しています。加えて、許可制ブロックチェーン・ネットワークを実現するHyperledgerにおいては、前述のとおり、特にアイデンティティー、プライバシー、アクセス制御の観点で、セキュリティーの強化が図られています。

しかし最近、ブロックチェーンの適用分野が金融や医療、公的機関などに広がり始め、より高いセキュリティー要件を満たす必要があるケースも増えてきました。特に、本格的なプロトタイプや本番適用では、データやアプリケーションの重要性、機密性も大幅に増します。外部からの侵入や内部犯行によるデータの漏えいや改ざんは決して許されません。

このような厳しいセキュリティー要件に応えるために、IBMはBluemix上に業界最高水準のセキュリティー・レベルを誇るブロックチェーン・クラウド・サービス「High Security Business Network(HSBN)」プランを提供しています。これは、メインフレーム・ベースのLinux専用機「IBM LinuxONE」にブロックチェーン・ネットワークをホスティングしたもので、ハードウェア・セキュリティー・モジュールによる安全な暗号鍵管理や監査機能、OS間の独立性確保など、LinuxONEで豊富な実績のある非常に高度で堅牢なセキュリティー機能を活用しています。これに加え、「Secure Service Container」という形でブロックチェーン・コンポーネントをソフトウェア・アプライアンス化し、たとえシステム管理者であってもOSの操作ができないなど、より堅牢なシステム構成となっています(**図5**)。HSBNにより、IBM Cloud上で非常にセキュアな最新のブロックチェーン基盤を迅速に構築し、簡単かつ安全に運用できるのです。

3-3. お客様との取り組み事例

IBMはさまざまな業界のお客様と連携し、それぞれの業界におけるブロックチェーンを使った実証実験を行ったりソリューションを開発したりしています。2017年1月時点で、以下のような取り組みが発表されています。

●IBM Global Finance(IGF)における、チャネル・ファイナンスへの適用

IGFはIBMのパートナー企業がサプライヤー企業から商品を購入する際に、その代金を融資するチャネル・ファイナンスを行っています。多数のパートナー企業とサプライヤー企業の膨大な数の取引の中で、商品の

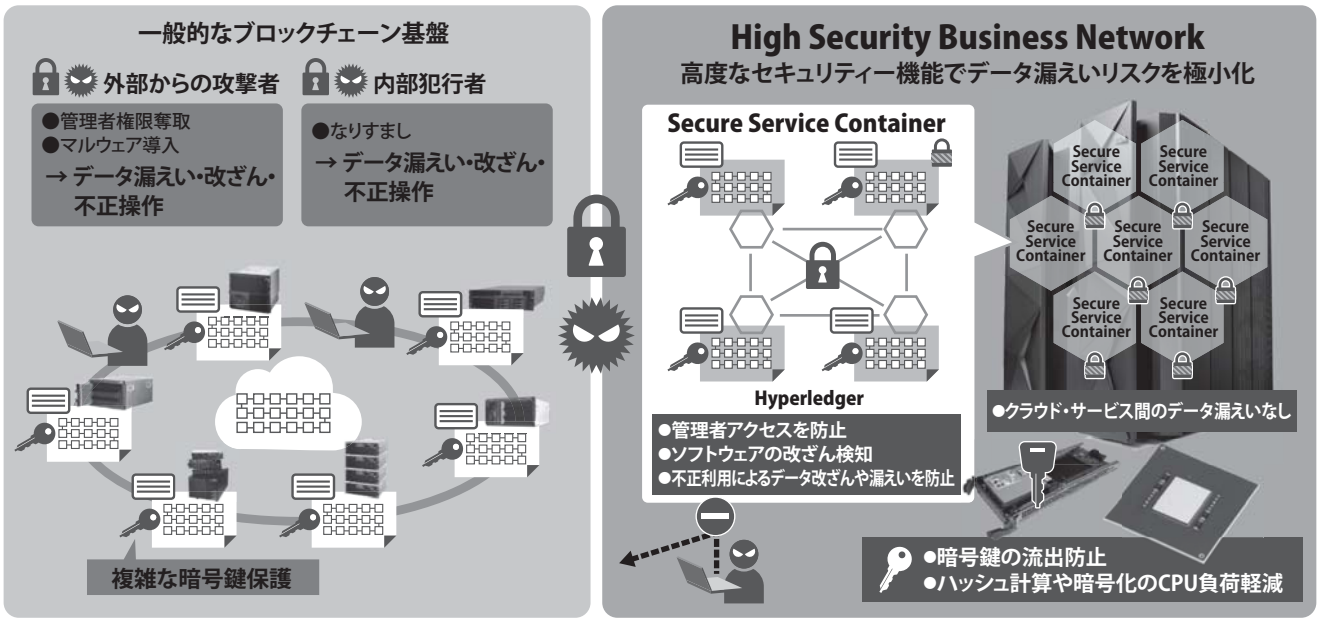

図5. HSBN – 堅牢なセキュリティー

配送ミスや請求書の記載事項の相違による争議が多く発生しています。ブロックチェーンを使用し、パートナー、サプライヤー、IGFだけでなく、運送会社や銀行など関連するすべての企業間のやり取りを記録することで可視化を行い、争議の削減と解決までの時間の短縮化を行っています[3]。

●日本取引所グループとの金融市場インフラに対するブロックチェーン適用に係る技術検証

証券取引における売買が成立した後の照合・清算・決済処理や配当金支払・株式分割等のコーポレート・アクションをブロックチェーンで実現することにおける、技術的な課題や可能性について検証しました[4][5]。

●三菱東京ＵＦＪ銀行シンガポール支店との、ブロックチェーンを使用した契約管理システム

現在、紙で扱うことの多い契約書を電子化してブロックチェーンに登録し、スマート・コントラクトで一連の合意や承認のプロセスを実行することで、複数社間にまたがり、契約文書の改ざん不可能な履歴を管理することができます[6]。

●Everledgerにおけるダイヤモンドのトレーサビリティー

ダイヤモンドの特徴データ（色、カット、重さ、透明度等）と、取引の履歴をブロックチェーンに登録し、売り手・買い手・保険会社などの間で共有することにより、盗品の売買を検出し、ダイヤモンドの保険金詐欺や盗難のリスクを削減することが可能になります[7]。

●ウォルマート社、中国の清華大学とIBMによる、食品サプライチェーンへのブロックチェーン適用

供給者から中間加工業者、小売などの流通経路における食品の情報をブロックチェーン上に記録し、関係者で共有することにより、サプライチェーンにおける透明性と効率性を高め、より細かな品質管理や、問題発生時の迅速な追跡が可能になります[8]。

4. 今後の展望

これまで述べてきたとおり、2015年後半から2016年にかけて、ブロックチェーンへの注目が一気に高まり、金融業をはじめとしたさまざまな業種のお客様で検討や本番展開を見据えた検証が数多く実施されてきました。一方で、Hyperledgerをはじめとしたブロックチェーン基盤は進化を続け、より機能が充実し、本格適用に耐えうるものになりつつあります。業種を越えた企業間連携や、オープン・コミュニティーを前提としたブロックチェーン技術のエコシステムもより進化していくでしょう。

2017年は、さまざまな業種のお客様で本格的な活用が始まると期待されます。IBMは3つのCを基本的な戦略に、技術、ビジネスの両面で、引き続き国内外のブロックチェーンの普及に貢献してまいります。

［参考文献］

［1］経済産業省：ブロックチェーン技術を利用したサービスに関する国内外動向調査，http://www.meti.go.jp/committee/kenkyukai/shoujo/blockchain/pdf/report_01_02.pdf（2016年4月28日）

［2］Hyperledger Project, http://www.hyperledger.org/

［3］YouTube：Blockchain in IBM Global Financing，https://www.youtube.com/watch?v=F0P7NM7d-ps（2016年3月15日）

［4］日本IBM：日本取引所とブロックチェーン技術の実証実験で合意，https://www-03.ibm.com/press/jp/ja/pressrelease/49070.wss（2016年2月16日）

［5］日本取引所グループ：金融市場インフラに対する分散型台帳技術の適用可能性について，JPXワーキング・ペーパー，http://www.jpx.co.jp/corporate/research-study/working-paper/index.html（2016年8月30日）

［6］日本IBM：IBMと三菱東京UFJ銀行　ブロックチェーンを活用した電子契約書の実用化へ，https://www-03.ibm.com/press/jp/ja/pressrelease/50547.wss（2016年9月16日）

［7］日本IBM：IBM、業界最高水準のセキュアなITインフラが支える新たなブロックチェーン向けクラウド・サービスを発表，https://www-03.ibm.com/press/jp/ja/pressrelease/50216.wss（2016年7月20日）

［8］IBM：Walmart, IBM and Tsinghua University Explore the Use of Blockchain to Help Bring Safer Food to Dinner Tables Across China, http://www-03.ibm.com/press/us/en/pressrelease/50816.wss（19 Oct. 2016）

日本アイ・ビー・エム株式会社
東京基礎研究所
ブロックチェーン・テクノロジー担当部長

吉濱 佐知子
Sachiko Yoshihama

日本IBM東京基礎研究所で情報セキュリティー関連の研究や新興国向け研究戦略の策定に携わる。現在はブロックチェーン技術を活用したインダストリー・ソリューションやツールの研究開発やビジネス創出に取り組んでいる。

日本アイ・ビー・エム株式会社
システム製品事業本部　ソリューション事業部
シニア・アーキテクト

町田 武夫
Takeo Machida

日本IBM入社以来、メインフレームから分散システムといった多岐にわたるプラットフォーム上でのオートノミック・コンピューティング、SOA、クラウドといった先進ソリューションの技術支援に従事。現在は、アナリティクス分野、およびブロックチェーン分野の担当として、これらシステムの提案・構築案件を支援している。