

# エンタープライズ向け ブロックチェーンの大きな可能性と クラウド・プラットフォームの必要性

ブロックチェーンの「分散台帳」と「P2P」という二つのコア技術が、  
新しいエンタープライズシステムとビジネス変革を生みだす。



# ブロックチェーンの特徴である「P2P」「合意形成」「分散台帳」「電子署名」の四つの技術から実現できる課題解決

仮想通貨の代表的な存在であるビットコインが、ブロックチェーン技術から構成されていることは、よく知られています。そのため、ブロックチェーン技術は仮想通貨のためだけの技術だと思っている方もまだ多いようです。というのも、ビットコインは2008年に発生したリーマンショック直後にSatoshi Nakamoto氏によって投稿された論文「Bitcoin: A Peer-to-Peer Electronic Cash System」を元に2009年からサービスが提供開始されており、当時は金融危機によって金融機関の信用リスク問題がクローズアップされ、信頼できる通貨システムへのニーズが高まったタイミングと重なっていたことがあります。ビットコインは、金融危機を踏まえ、従来の銀行による中央集権的な台帳管理(トランザクション管理)ではなく、ピア・ツー・ピア(P2P: Peer-to-Peer)によるネットワーク参加モデルで、合意形成のもとに確定される分散型の共有台帳を仮想通貨として利用するという非中央集権型の分散アーキテクチャーという特徴で、始まりました。

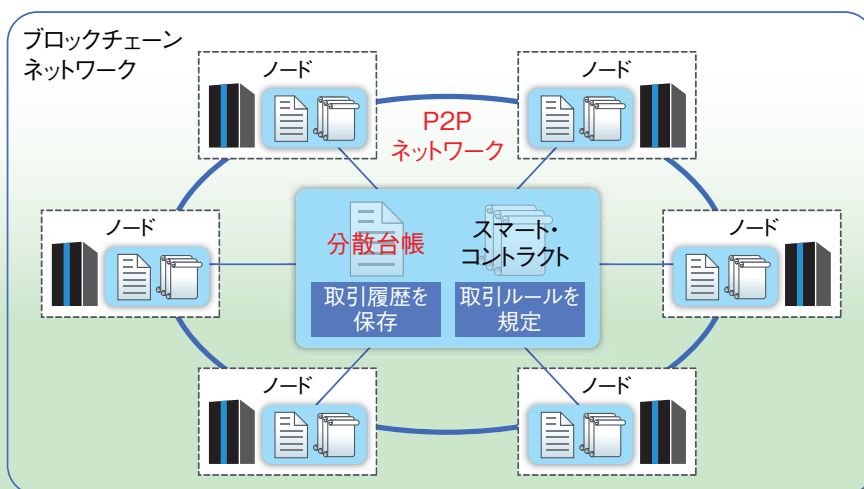
その後も、EU諸国で何度か発生した通貨危機は、大きく仮想通貨の価値を上げ、注目度が上がってきました。さらに2015年に入ると、FinTechブームもあり、そのコア技術として、構成する技術にも注目を浴びるようになりました。ブロックチェーン技術の特徴は、従来型の社会システムを構築する上での課題の多くを解決するものでもあります。

エンタープライズ・システムで、信頼性とセキュリティーを維持するために、高コストになりがちな要素は、主にネットワークとデータベースです。ブロックチェーンの特徴から、これらがどのように解決されていくかを説明していきます。

従来のシステムは、クライアントとサーバー間の通信が中心になります。このアーキテクチャーでは、サーバー側にデータを寄せることが中心になるため、サーバーが過負荷になりがちです。また、特定のサーバーが重要な役割を担うため、クライアントからの通信も信頼性を保つために複数の機器と複雑なプロトコルを使って冗長化を行う必要があります。

P2Pとは対応するコンピューター群が直接通信する中心のないネットワーク・モデルのことです。これによって、単一障害点をなくし、分散したネットワーク・アーキテクチャーを構成することができます。分かりやすく説明すると分散台帳とスマート・コントラクトは、従来のデータベースとアプリケーションに近いコンポーネントになります。一般的に、データベースとアプリケーションの分散は難しいものですが、ブロックチェーンでは、これらが一体となってP2Pネットワークに分散されて共有される点が特徴です。また、このデータ更新において、P2Pネットワークに参加者が合意のもとに更新する合意形成(コンセンサス)モデルや電子署名によるトランザクションの正当性を担保する仕組みがあるため、分散型であるにもかかわらず、データの一貫性や改ざん防止にも役立つという特徴があります。

このブロックチェーンのP2Pネットワーク・モデルと分散型共有台帳を活用することで、従来は複雑で高価な中央集権的なシステムで実現していた台帳の管理性が管理コストを低く実現できるようになります。これによって、複数の組織による新たなビジネスモデル・フローを簡単かつ低コストで創出し、プロセス効率化とユーザー利便性の向上を実現します。



図：ブロックチェーンの特徴

# 企業の業務に耐えうるブロックチェーン基盤 「Hyperledger Fabric」

IBMはこの特性に注目し、ブロックチェーン技術を仮想通貨以外の目的にも使える、エンタープライズ用途に耐えうるプラットフォーム技術として捉えています。

ブロックチェーン技術は、現在さまざまなプロジェクトによって開発されていますが、パブリック型とプライベート型の2種類に大別されます。パブリック型はビットコインを原型にしており、ネットワーク形態や参加者が自由にできるという特徴があり、「Ethereum(イーサリアム)」が有名です。一方の、プライベート型は参加者を許可制にしているのが特徴で、コンソーシアム型もこの中に含まれます。コンソーシアム型は特定の参加者が参加できるモデル、プライベート型は単位のモデルです。Ethereumも対応してきていますが、最初からこのモデルを前提にしておりIBMがLinux Foundationにコントリビュートしている「Hyperledger Fabric(ハイパーレジャー)」が有名です。

パブリック型の代表であるビットコインが提供している価値は二つあります。

一つ目は、ビットコインという「価値の創造」です。これは中央銀行が紙幣を発行するのと同様の価値の創造です。その価値の源泉は何かと言えば、ビットコインのユーザーが、自分以外のユーザーもビットコインに価値があると信じるだろうと信じられることです。これは中央銀行による通貨の価値の源泉と基本的に同じです。通貨自体に貴金属が含まれている場合や兌換紙幣の場合は異なりますが、近代通貨は基本的にこれが価値の源泉と言われています。ビットコイン・システムはビットコインの供給量を制限することで希少価値を確保し、価値を維持しています。

二つ目は、ビットコインの所有権の移動の「事実の確定」です。どうして確定されるかと言えば、これも1番目と同様に自分以外

のユーザーもその事実が確定したことを信じるだろうとすべてのユーザーが信じられることです。この信頼を生み出しているのがブロックチェーンであり、PoW によるブロック確定の仕組みです。

パブリック型に対して、コンソーシアム型/プライベート型であるHyperledger Fabric のスタンスの違いを見ていきます。

一つ目の「価値の創造」に関して、Hyperledger Fabricは、放棄しています。Crypto Currency(暗号通貨)の発行もアプリケーションの対象としていません(Digital Currency は対象としています)。二つ目の「事実の確定」についてHyperledger Fabric は、ビットコインの所有権移動だけでなく、非常に幅広い事実の確定ができるように設計されています。ここで言う事実とは、利用者同士が何らかの約束をしたという事実です。その約束とは、所有権の移動や契約締結などです。この事実の確定を参加者全員が自分以外も信じるだろうと信じられるような仕組みを提供していることが、Hyperledger Fabric の最大の機能だと言えます。

例えば、公証役場という仕組みがあります。Aさん、Bさんが何らかの契約をする時、当事者間だけ行くと後になって一方がそのような契約をした覚えがないとか、契約内容に瑕疵があるので無効である、などの主張をする恐れがあります。そこで公証人により、契約内容を確認し、正当な契約が締結されたという事実を保証して記録する制度で、Hyperledger Fabric が行っている役割に該当します。デジタルな契約をスマート・コントラクト(チェーンコード)で実装し、その正当性を指定の参加者が確認し、合意形成(コンセンサス)により事実の順序を確定させ、衆目監視が可能な複数の分散台帳に保存し、それらが系統的に改ざん不能であることを保証しています。

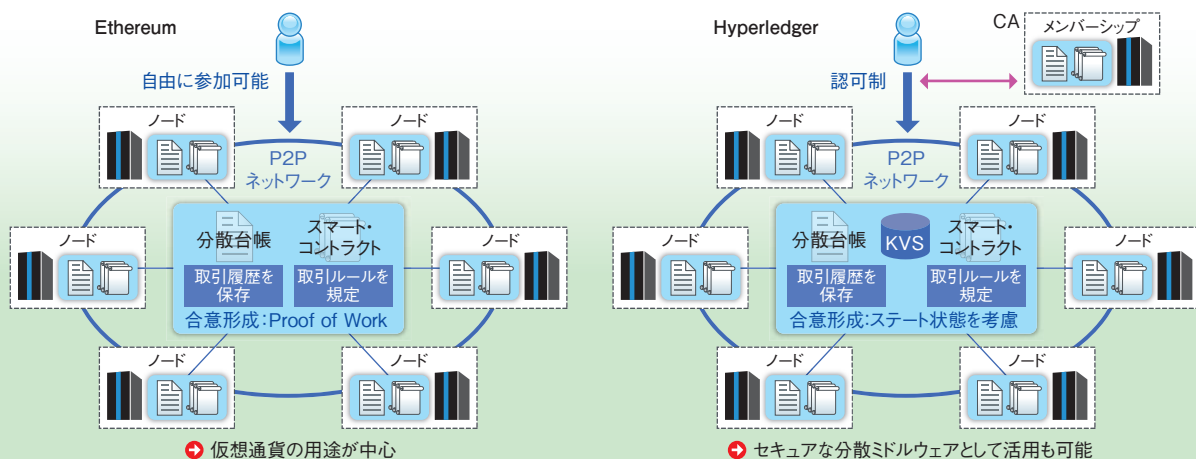


図: Ethereum と Hyperledger Fabric の違い

実装面での両者の特徴的な違いを見てみましょう。

### ■参加者認証による信頼度の高いプライバシーと機密保持

暗号技術に基づくコンセンサスのプロセスは、参加者の匿名性を支える必要がありました。パブリック型のブロックチェーンの参加者は不特定多数で、信頼に基づいていないシステムのため、匿名性にコストを費やすことになり全体的なコストが高くなります。しかし、ビジネス・ネットワーク内の参加者が信頼できる場合は、匿名性へのコストを低く抑えることが可能になります。Hyperledger Fabric には、CA(認証局)の仕組みが内包されており、このプロセスを円滑に処理できます。

### ■ワールドステートを活用した

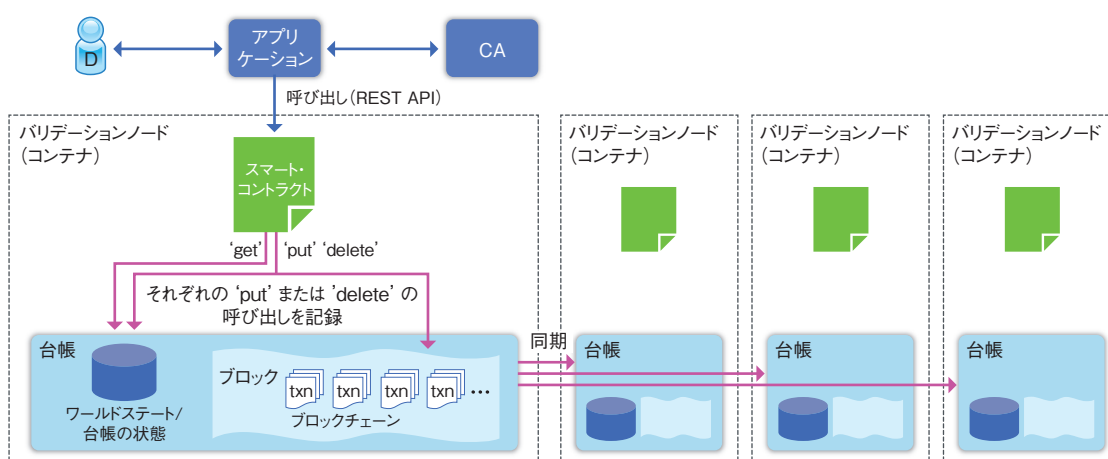
#### 高速かつ信頼性の高いコンセンサスモデル

Hyperledger Fabricの認証プロセスでは、信頼性が高まるにつれ、コンセンサスにかかるコストを下げることができ、コンセンサスにかかる時間も短時間で済みます。企業の業務利用を目的としているHyperledger Fabricではコストパフォーマンスと応答速度を高めるための機能を兼ね備えており、分散台帳の

データとスマート・コントラクトのデータを分離し、後者をワールドステートというデータベースに管理する特徴的なアーキテクチャーを採用しています。

Hyperledger Fabric の分散アーキテクチャーを簡単に解説します。Hyperledger Fabric は、CA(認証局)の機能を保持するメンバーシップ・サービスと、分散台帳やスマート・コントラクトを保持するバリデーションピアから構成され、Dockerコンテナベースで動作します。

通常のWebアプリやモバイル・アプリからHyperledger FabricにAPIを発行することでチェーンコードが実行されます。実行された処理は、メンバーシップによる合意形成(コンセンサス)のもと、チェーンコードが実行され台帳にブロックとして更新されています。台帳のブロックは追記型になる点が、ブロックチェーンの由来となっています。このようなアーキテクチャーであることから、分散型であるにもかかわらず、データの一貫性が保証され、ブロックは合意形成のもとに格納されるため、第三者による改ざんも行われません。



図：Hyperledger Fabric Logical Architecture

## コンソーシアム型ブロックチェーンによる台帳とスマート・コントラクトの共有のメリット

実際のビジネスにおいて、P2Pにセキュアかつ、特定の複雑な商取引を完成させるために、複数の参加者で台帳を共有管理できるブロックチェーンのメリットを生かせるモデルがHyperledger Fabric で採用している「コンソーシアム型」です。

コンソーシアムとは、共同で、ある目的にそって活動したり共通の目標に向かって活動したりする団体のことを指します。ブロックチェーンのビジネス活用を考えると、まず同じ業種でのコンソーシアム型を考えるのが現実的だと言えるかもしれません。ブロッ

クチェーンを利用し、個々の企業がバラバラに保持しているビジネスロジックとデータモデルを、スマート・コントラクト、分散台帳として共有することで個別の接続仕様の調整が削減できるため、商取引のプロセスを大きく効率化でき、改ざん防止にも効果があります。

例えば、航空機のように非常に多くの部品で構成されている部品管理台帳を、部品製造企業、組み立て企業、メンテナンス企業、利用企業、監督官庁などで共有できるようになると、製

造物に対する信頼度が高まることにつながります。製造者、製造日時、製造バッチ、製造に使った機械のプログラムなどを共有することで製造プロセスと使用部品の可視化が可能になるのです。航空会社や航空機メーカーが1社だけでこのシステムを構築しようとする、多大なコストがかかりますが、複数の航空関連会社によるコンソーシアムで、構築・利用すればコスト負担は下がります。また、コスト効果以上に関連企業間で部品管理を効率的に安全に行えるため、製造物の信頼性向上に加えて、保守内容・タイミング、部品製造・発注などの事前予測ができ、改ざん防止によるデータの信頼性向上など各企業にとっても多くのメリットが生まれます。

ブロックチェーンのコンソーシアム型によるスマート・コントラクトと分散台帳の共有によって、利用企業の利便性を大きく高め、新しいエコシステムが確立すると考えられます。

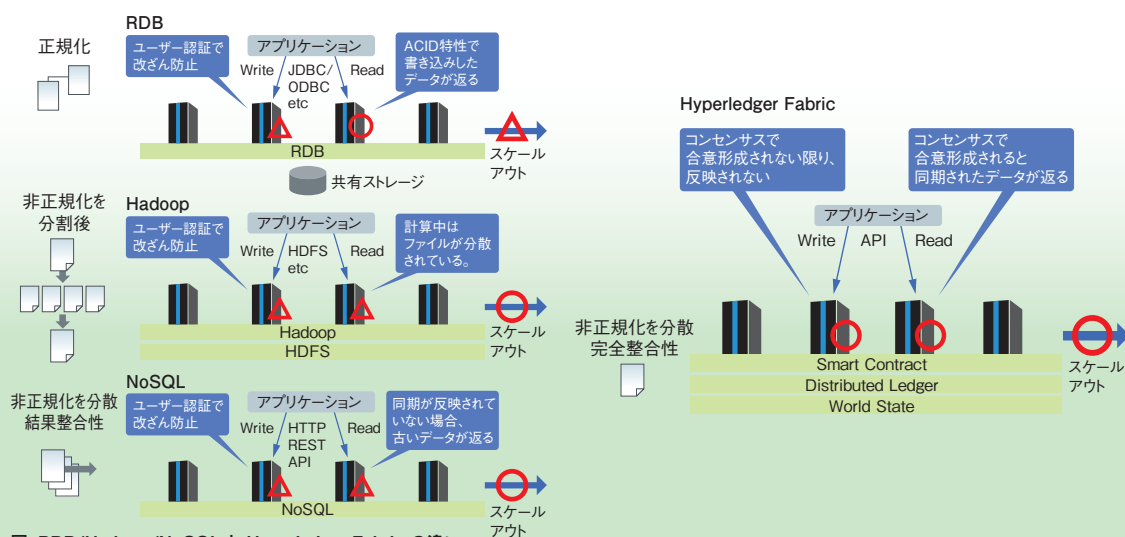
ブロックチェーンの価値は、特定の業界や団体のコンソーシアム単位で、ブロックチェーン・ビジネスネットワークを構成し、スマート・コントラクトと分散台帳を共有できるという、そのモデルにあります。そのため、コンソーシアム型を標準採用しているHyperledger Fabricは、そのモデルが要求される業界に最適な選択肢です。各業界に精通し、Hyperledger Fabricに精通するIBMが提供することで、コンソーシアムに対する支援も可能になります。

## 台帳管理において、RDBMS、Hadoop、NoSQLではなくHyperledger Fabricが優位な理由

台帳管理であればリレーショナル・データベース(RDBMS)の方が適しているのではないか、と思う方も多いでしょう。また、既存システムでは台帳管理にRDBMSが多く採用されているのも事実です。単独で台帳管理を行うのであればRDBMSでも良いのですが、複数の組織によって台帳管理をRDBMSで行うには、P2Pでやりとりを行うためには、RDBMSにおいてマルチテナントを考慮した設計が必要になります。また、分散化しにくいRDBMSではP2Pとの相性がよくありません。そうすると、それぞれの組織が個別に台帳をRDBに保有し、取引が発生するとRDBを更新するという手法を取らざるを得ず、参加者が増えてくると、双方向通信がメッシュ型となり、参加者ごとにRDBMSが増えていくため、複雑なアーキテクチャーとなります。加えて、RDBMSは、セキュアかつ高信頼性を保つためには、

データベース管理者が必須になります。RDBMSに依存した構成になるため、RDBMSのトラブルがビジネス・ネットワーク全体に及ぼす影響が大きいからです。中央のシステムの障害がビジネス・ネットワーク全体の障害となり、ビジネスがストップしてしまうリスクがあるのです。

分散台帳の管理であれば、Hadoopでよいと考える方もいるかもしれませんが。確かに、台帳データを対象にする点は共通していますが、Hadoopは分散計算のフレームワークであり、ファイルを分割して並列計算を行い、その結果を構造化データとしてアクセスするのが主体的な利用方法です。また、分散して台帳データを管理するという点ではNoSQLという選択肢もあるかもしれませんが、アーキテクチャーとしては近いものがありますが、NoSQLの多くは高いスケーラビリティの代わりにデータの



完全な一貫性を犠牲にしています。

RDBMS、Hadoop、NoSQLが、Hyperledger Fabricと決定的に違うのは、メンバーシップと合意形成の有無です。Hyperledger Fabricでは、メンバーシップによる合意形成がない限り、データの更新、すなわち改ざんができません。また、通常のデータベースでは、ユーザー権限で制御する必要がある

セキュリティや監査の機能をHyperledger Fabricでは、メンバーシップと合意形成で担保します。なおかつ、データの一貫性やスケーラビリティもあり、この複雑なデータ管理をHyperledger Fabricのミドルウェアにて行われる点もポイントです。

## ブロックチェーンを使ったサービスにおいて 必須となるクラウド環境

Hyperledger Fabricは、スケーラブルなアーキテクチャーで、コンソーシアムにネットワークの接続性が求められるので、スケーラブルに共有できるクラウド・プラットフォームが最適な実行環境と考えられます。ただし、クラウド・プラットフォームを推進する理由は、これだけではありません。Hyperledger Fabricのバージョンアップやセキュリティも含めた運用とチェーンコードの開発が、自社運用では手間が掛かるという点があります。

IBMは、Hyperledger Fabricをクラウド・サービスとして提供しています。このため、常に最新のバージョンのHyperledgerを使用でき、クラウドのメリットでもある、システム運用の工数がかからないこと、高度なセキュリティでのデータ保護、という観点でも利用価値は高いと言えます。特に、ミッションクリティカルな用途向けに「IBM LinuxONE」を基盤とした「High Security Business Network」も提供しています。高い可用性に加え、セキュア・サービス・コンテナ（SSC）と呼ばれる仕組みにより、システムリソースへのバックドアからの侵入を完全シャットアウトし、

高いセキュリティが求められる金融システムや公共サービスシステムなどの用途に最適です。ブロックチェーンで多用される暗号化やハッシュ処理が専用ハードウェアで実行されるため高速かつスケーラブルであり、ハードウェアにより暗号鍵を安全に保管されるメリットもあります。

また、IBM Bluemix（以下、Bluemix）でも提供されます。ブロックチェーンはチェーンコードがDockerイメージで提供されるという特徴があるため、IBM Container Services、DevOps Services、Open Toolchain等を中心にしたIBM Bluemixと親和性があります。ブロックチェーンにアクセスするアプリケーションを構成するために、Cloud Foundryを活用したクラウドネイティブ・アプリケーション、Mobile Foundationを活用したモバイル・アプリケーション、OpenWhiskを活用したサーバーレス・アプリケーションも簡単に開発でき、安定的に継続的インテグレーションをハイブリッドにもまわすことも可能です。

さらに、Bluemixのプラットフォーム上の「IBM Watson」、

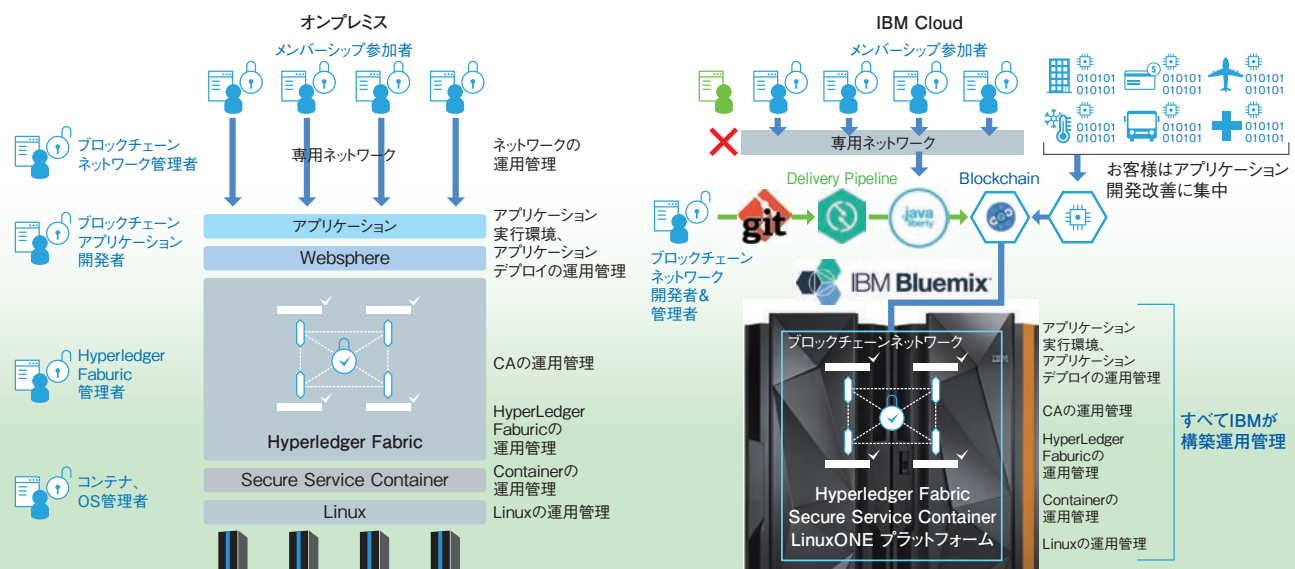


図:Hyperledger Fabric Physical Architecture on IBM Cloud の価値

「Watson IoT Platform」を利用し、ブロックチェーンと連動することも可能です。IoTデータを必要に応じてIBM Watsonで学習、分析させ、ブロックチェーンに蓄積し、共有することもできます。

IoT、AI、ブロックチェーン、これらすべてを組み合わせることで大きな価値を生み出し、提供するためにも、Hyperledger FabricはIBM Cloudでの実行が最適だとIBMは考えています。

## ブロックチェーン活用のための 開発支援サービス「IBM Bluemix Garage」

PaaSの世界では、クラウドネイティブやDevOpsといった比較的新しい考え方が必要なため、支援サービスが提供されています。IBMは、IBM Bluemix Garageというサービスを提供しており、要求分析を整理し、実装までを短期間にBluemix上でプロトタイプ開発するために、デザインシンキングを重視しています。特に、ブロックチェーンに関しては、どのような業務で活用すればよいかイメージしにくいお客様も多く存在しています。そこでIBMでは、多くの可能性をもつブロックチェーンの活用についても、お客様のビジネス要件にそって、このGarage

Methodを適用しています。企業ユースのブロックチェーンHyperledger Fabricに興味を持たれ、自社ではどのような活用方法があるのかを知りたい、素早くブロックチェーンを試してみたい、という方に適したサービスとなっています。東京で提供しているBluemix Garageにおいては、ブロックチェーンは最も引き合いの多いトピックになっており、既に多くの実績がある点も、Bluemixで提供されるHyperledger Fabricを推奨する理由です。

### 制作監修

日本アイ・ビー・エム株式会社  
クラウド事業本部 エグゼクティブ・ITスペシャリスト  
紫関 昭光 (しせき あきみつ)

日本アイ・ビー・エム株式会社  
クラウド事業本部 コンサルティング・アーキテクト  
平山 毅 (ひらやま つよし)

日本アイ・ビー・エム株式会社  
IBMシステムズソリューション事業部 先端テクノロジー・センター担当  
高田 充康 (たかだ みちやす)

### お問い合わせはこちら

電話番号 : 0120-550-210 (平日9時30分~17時30分)

E-mail : [cloudedm@jp.ibm.com](mailto:cloudedm@jp.ibm.com)

### お問い合わせ

このカタログの情報は2017年2月現在のものです。仕様は予告なく変更される場合があります。サービスや製品の詳細については、弊社の営業担当員にご相談ください。



日本アイ・ビー・エム株式会社

[www.ibm.com/industries/jp/ja/blockchain/](http://www.ibm.com/industries/jp/ja/blockchain/)

IBM、IBMロゴ、ibm.com、Bluemix、IBM Watsonは、世界の多くの国で登録されたInternational Business Machines Corporationの商標です。他の製品名およびサービス名等は、それぞれIBMまたは各社の商標である場合があります。現時点でのIBMの商標リストについては、[www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)をご覧ください。