PatentIsland

ブロックチェインとセンシングデータ流通市場について

作成：２０１６年５月２６日　http://www.patentisland.com/memo369.html
著者：　Ｐａｔｅｎｔ Ｉｓｌａｎｄ株式会社（Web: http://www.patentisland.co.jp）
　代表取締役社長　久野敦司　（E-mail: atsushi_hisano@patentisland.co.jp ）

【背景説明】

「ブロックチェイン技術の本質機能とその発展型について」と題した論考を、前回は行ないましたので、今回はブロックチェイン技術とセンシングデータ流通市場が 日本の国家戦略において占める位置づけを中心に説明します。

http://www.patentisland.com/memo368.html

２０１６年５月１２日に自民党ＩＴ戦略特命委員会から「最新テクノロジーの社会実装による世界最先端ＩＴ国家の実現に向けた提言　デジタル・ニッポン２０１６　～まず、やってみよう～」 が発表されました。（参考サイト１）

デジタル・ニッポン２０１６による提言の全体像を示した参考サイト１の第４４ページは、「経済再生」と「治安・テロ」と「規制・行政改革」の ３つを柱としています。この３本柱を実現する手段の中身として、提言１．１から提言４．２までの１２個のテーマが挙げられています。（下図を参照）

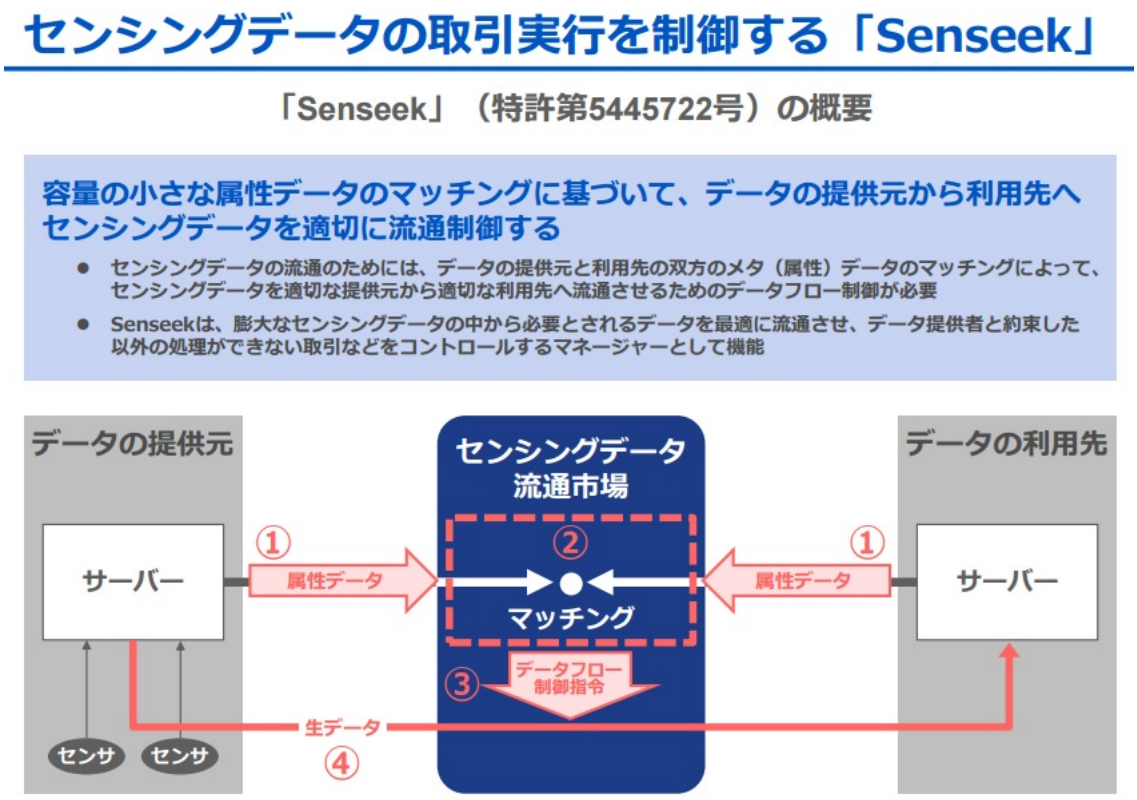
図１　デジタル・ニッポン２０１６の提言の全体構成図

１２個のテーマの中では、私はブロックチェインとセンシングデータ流通市場に注目しました。その理由は、次のとおりです。

ブロックチェインは下記の「１．　ブロックチェイン技術の本質の説明」にて述べている「データ無変更の保証」の機能に基づいて、ＩＴシステムの利活用において、ビジネス上や情報セキュリティ上の信頼の土台となる確定データを、 分散型システムで維持します。その結果、ブロックチェインは上図の「提言２．１　シェアリングエコノミーの本格化」において、シェアリング対象の属性を示すデータの信頼性の土台を実現できます。
また、「提言２．２　Ｆｉｎｔｅｃｈの本格化」もブロックチェインの有力アプリの１つであるビットコインが主役を占めます。
さらに、ブロックチェイン技術による「データ無変更の保証」の機能に基づいて、「提言３．１　国家的なサイバー／ＩｏＴセキュリティの強化」も実現しやすくなります。

また、センシングデータ流通市場は、分散型システムにおいて、様々な対象の不確定な状態を観測して得た情報をセンシングデータとして確定させた上で、 センシングデータを用いた最適制御などを、広い範囲で可能とします。（参考サイト２）

図２　センシングデータ流通市場



（上図の出典：　参考サイト２）

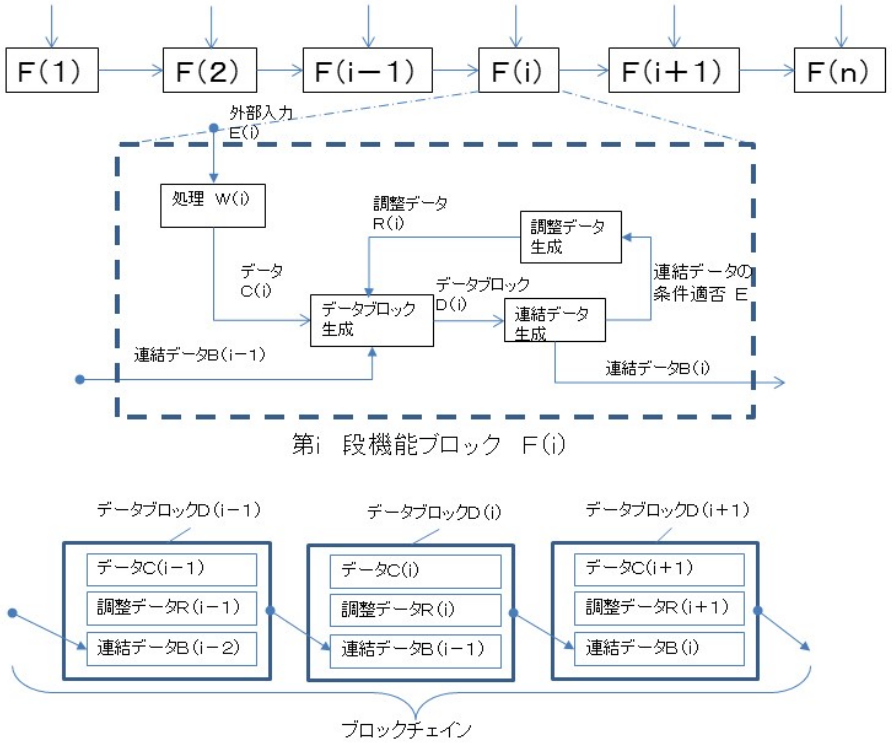
例えば、「提言１．１　ＩｏＴサービスプラットフォームの社会実装」は、センシングデータ流通市場の存在なしには、企業または企業グループの内部に閉じた小規模なシステムの開発効率を 向上させるにすぎないものにしかなりません。
「提言２．１　シェアリングエコノミーの本格化」は、センシングデータ流通市場の存在なしには、シェアリング対象やシェアリング利用者のシェアリング前後の状態の センシングのためのシステムをシェアリング対象分野別に開発し運営しなければならなくなります。
また、「提言３．１　国家的なサイバー／ＩｏＴセキュリティ強化」は、センシングデータ流通市場の存在なしには、センシングデータの流通経路が複雑になりすぎることと、 データフロー制御の統一的手段が実現できないため、効果的にサイバー／ＩｏＴセキュリティの強化をすることができなくなります。

すなわち、ブロックチェインとセンシングデータ流通市場は、日本のＩＴ戦略の基本構造を与えるものと言えます。しかし、ブロックチェインとセンシングデータ流通市場は完全に独立の関係にあるのではなく、ブロックチェインを用いてセンシングデータ流通市場を強化することも できることが判りましたので、その説明も行ないます。

その前にまず、ブロックチェインの基本構造を図３に示して、ブロックチェイン技術の本質部分を説明します。

１．　ブロックチェイン技術の本質の説明

図3　データブロックが所定条件を満たす連結データで結合してブロックチェーンを形成する仕組み



まず、ブロックチェイン技術を実行するシステムの構造は、時系列の順序番号である「ｉ」ごとにデータを獲得する処理Ｗ（ｉ）を内蔵する機能ブロックＦ（ｉ）が、 一列に連結した多段処理システムであり、各段の間は情報が流れていると、します。
そして、機能ブロックＦの動作を、次のようなプロセスＰ１，Ｐ２の組み合わせとして記述します。

Ｐ１：　前段である機能ブロックＦ（ｉ－１）が保持するデータブロックＤ（ｉ－１）によって一意に決定される連結データＢ（ｉ－１）と、 処理Ｗ（ｉ）で獲得したデータＣ（ｉ）と調整データＲ（ｉ）と組み合わせて、データブロックＤ（ｉ）を形成します。

Ｐ２：　前記のデータブロックＤ（ｉ）によって一意に決定される連結データＢ（ｉ）が所定条件を満足しなければ、調整データＲ（ｉ）を変更して、 前記Ｐ１に処理を戻します。

連結データＢ（ｉ）が所定条件を満足していれば、Ｅの値に成功フラグを設定し、 Ｂ（ｉ）を後段の機能ブロックＦ（ｉ＋１）に与えます。

ここで、「機能ブロックＦ（ｉ）がデータＣ（ｉ）を確定させる」とは、前記のプロセスＰ１によって形成されたデータブロックＤ（ｉ）から生成されるとともに、 所定条件を満足する連結データＢ（ｉ）を生成して外部に出力することであるとします。所定条件を連結データＢ（ｉ）が満足するようにするために、調整データＲ（ｉ） が調整手段となります。
次に、データＣ（ｉ）の確定の後にＣ（ｉ）を変更することの困難性を説明します。
データＣ（ｉ）は、調整データＲ（ｉ）および連結データＢ（ｉ－１）と組み合わされてデータブロックＤ（ｉ）を形成しています。
そのため、Ｃ（ｉ）の変更は、データブロックＤ（ｉ）によって一意に決まる連結データＢ（ｉ）以降の各連結データの変更が必要という形で影響を後段にもたらします。
もし、後段の機能ブロックＦ（ｉ＋１）以降に気付かれないように、機能ブロックＦ（ｉ）においてＣ（ｉ）を変更しようとするならば、 Ｃ（ｉ）を変更しても連結データＢ（ｉ）を変更しなくても済むようにしなければならないことになります。

連結データＢ（ｉ）は、データＣ（ｉ）と前段からの連結データＢ（ｉ－１）と調整データＲ（ｉ）の組み合わせからなるデータブロックＤ（ｉ）から生成されますので、 データＣ（ｉ）の変更の影響が連結データＢ（ｉ）以降の後段に発生しないようにしようとするならば、適切な連結データＢ（ｉ－１）の値を探索して発見し、 そのような値に連結データＢ（ｉ－１）を変更することが必要となります。
連結データＢ（ｉ－１）の変更は、さらにその前段の連結データの変更を必要とするというように、前段方向に変更の影響が波及します。
すなわち、データブロックがプロセスＰ１とＰ２で実現されるチェインを構成しているという枠組みのもとでは、データＣ（ｉ）の変更は、 前段または後段の連結データに影響を与えてしまうので、その影響の存在を検知するプロセスと組み合わせるならば、データＣ（ｉ）の変更が困難となります。

ここで、データＣ（ｉ）の確定後にデータＣ（ｉ）を変更し、Ｃ（ｉ）の変更に応じて連結データＢ（ｉ）も変更し、連結データＢ（ｉ）を後段の機能ブロックＦ（ｉ＋１）に 与えていない状態を想定します。
その状態では、機能ブロックＦ（ｉ）が保有する連結データＢ（ｉ）と、後段の機能ブロックＦ（ｉ＋１）が前段から受け取ったものとして保有する連結データの値が相違 しますが、どちらが正しいのかの判別がつきません。
そこで、連結データＢが満足すべき条件であって、そのような条件が成立するデータブロ

ックＤの内容は滅多に見つからないものを設けることで、データＣの確定後に データＣを変更しにくくしています。
すなわち、図１に示すように、調整データＲ（ｉ）を内部で自動生成してデータブロックＤ（ｉ）の内容を自動調整して、データブロックＤ（ｉ）に対応する連結データＢ（ｉ） が大変に多大な計算パワーを用いて初めて適切な調整データＲ（ｉ）が発見できるような難度の高い所定条件を満たす内部構造を持たせることで、 機能ブロックＦのチェインによって、データの変更がされにくいという信頼性の高いシステムを実現できることがわかります。

２． ブロックチェイン技術のセンシングデータ流通市場への適用

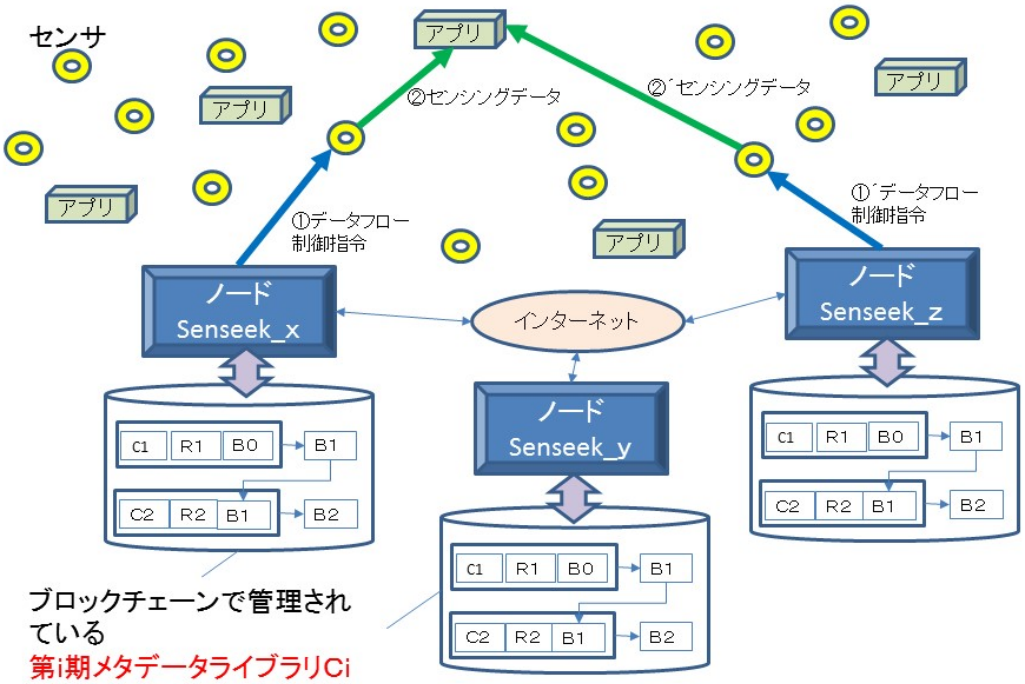
ブロックチェインは、ブロック内のデータについて「データ無変更の保証」を与えますので、ブロックチェイン内にセンシングデータ流通市場に関する確定データを設定し、 その確定データの基盤の上で、センシングデータ流通市場を動作させることが、信頼される市場の実現には必要です。

なお、ここで言う確定データとは、所定の時刻以降はデータ無変更の保証がされている確定したデータのことです。
センシングデータ流通市場において、ブロック内に確定データとして設定すべきデータ（以下、メタデータと言う）には、次の（１）～（３）があります。
（１） センシングデータ流通主体を特定する情報（例：名前またはＩＤ符号,取引口座情報,ＩＰアドレス，連絡用の電子メールアドレスなど）
（２） センシングデータ流通主体が流通対象とするデータの属性（例：データ種類,センシング対象の位置,データサイズ，データの発生時刻，データの有効期限，データの信頼度，データアクセス方法など）
（３） センシングデータ流通主体が実行を希望する取引条件（例：提供側／利用側の区分，売却／ライセンスの区分，データ移転の対価，データの利用可能な形態や分野の範囲，データの利用可能期間など）

注） 上記の（２）と（３）においては、センシングデータ流通でのデータの提供側の希望条件と、データ利用側での希望条件があります。

図４に基づいて説明します。

図4　ブロックチェインにてデータ流通のためのメタデータを共有管理する仕組み



センシングデータ流通に関する上記（１）～（３）のメタデータを、ブロックチェインを構成するブロックに設定し、インターネットで接続されたノードが、同じ内容の ブロックチェインを保有するようにします。
このようにメタデータを管理することで、センシングデータ流通の基礎となるメタデータの「データ無変更の保証」ができますし、多数のノードでメタデータの共有が できます。その結果、各ノードはブロックチェイン内のブロック内に記録されたメタデータを用いて、センシングデータの提供側のメタデータと 利用側のメタデータを自動的にマッチングして、マッチする提供側と利用側のペアを抽出し、センシングデータの提供側にデータフロー制御指令を与えます。
データフロー制御指令を受け取ったデータ提供側であるセンサは、データ利用側であるアプリに対してセンシングデータをＰ２Ｐ通信で送信します。

また、各ノードは、メタデータを内蔵する同じブロックチェインを有していますので、センシング対象の位置によってマッチング処理を分担する形態で、 各ノードは計算パワーの節約をしたり、各ノードが共同で広い範囲をサービス範囲とするセンシングデータ流通市

場を実現することもできます。

また、センシングデータ流通の対価の支払いが利用側から提供側に対して行われるように価値情報のフローも制御します。価値情報の移転にはビットコインを用います。

【参考サイト】

１．　最新テクノロジーの社会実装による世界最先端ＩＴ国家の実現に向けた提言　デジタル・ニッポン２０１６　～まず、やってみよう～
http://jimin.ncss.nifty.com/pdf/news/policy/132264_1.pdf
２．　センシングデータの取引実行を制御する「Senseek」
http://activeictjapan.com/pdf/20160324/jimin_it-toku_document_20160324.pdf#page=13
３．　特許第 5445722 号　アプリの要求に合致したセンサをアプリに結合する機能
https://web.archive.org/web/20151002100249/http://www.omron.co.jp/about/ip/patent/17.html