踊るバズワード ～Behind the Buzzword（11）ブロックチェーン（5）：

「ブロックチェーン」に永遠の愛を誓う ～神も法もかなわぬ無敵の与信システム

https://eetimes.jp/ee/articles/2102/08/news054.html

今回は、ブロックチェーンについて“技術用語を使わずに”説明してみました。さらに、ブロックチェーンを使用するアプリケーションとして、「借家システム」「ブロックチェーン投票」「ブロックチェーン婚」を紹介します。

2021年02月08日 12時30分 更新

[江端智一, EE Times Japan]

「業界のトレンド」といわれる技術の名称は、“バズワード”になることが少なくありません。“M2M”“ユビキタス”“Web2.0”、そして“AI”。理解不能な技術が登場すると、それに“もっともらしい名前”を付けて分かったフリをするのです。このように作られた名前に世界は踊り、私たち技術者を翻弄した揚げ句、最後は無責任に捨て去りました――ひと言の謝罪もなく。今ここに、かつて「“AI”という技術は存在しない」と2年間叫び続けた著者が再び立ち上がります。あなたの「分かったフリ」を冷酷に問い詰め、糾弾するためです。⇒連載バックナンバー

ビットコインに期待し過ぎた？

これまでの3回の連載において、私のビットコインに対するスタンスは、かなりネガティブだったと思います。ビットコインの製造プロセス、信用システム、与信システム、現状のビットコインの運用に至るまで、一貫してネガティブです。

このネガティブについて、自分なりに考えてみたのですが、どうやら、私は、「**ビットコインに過大な期待を持ち過ぎた**」ように思えるのです。

今となっては、ITに詳しくない人ですら知っている用語、**OSS（オープンソースソフトウェア）** ―― この概念が世間に公表された時、世界中のITエンジニア（私も含めて）から「**アホじゃないか**」と、あきれたものです。

プログラムのソースコードは、ソフトウェア技術の集大成です。そのソースコードを誰でも見られるようにオープンにしたら、自分の仕事をわざわざ他人にくれてやっているようなものです*）。

*）特許出願も、自分の考えを公開するという点では同じですが、その代わり、一定期間（出願から20年間）の独占的な実施権が与えられます。

まさに「**気が狂っている**」としか表現しようがありませんでした。多くの人が、そんなことしたらソフトウェア産業が崩壊してしまう、と考えたものです。

そんな中、PC/AT互換機（いわゆるIBM互換機）のCPU上で動く、オペレーティングシステムLinuxがOSSとして公開されました。この時の、私たちITエンジニア達の衝撃は、言葉では語り尽くせないものでした。

そもそも、**当時の私たちには、「オペレーティングシステム（OS）を自作する」という発想がありません**でした。

OSを作ることができるのは、バチカン秘密文書館の中に収められている秘密の書「IA-32 アーキテクチャ仕様書」に触れることのできるローマ教皇ただ1人*）であり、われわれ下々の司教（ITエンジニア）は、その神の恩恵を枢機卿（API）を通じて得られるのみ、とあると思っていました。

＊）現在は、厳しい条件をクリアした者であれば、バチカン秘密文書館の限定された資料にアクセスできるようです。

しかしLinuxがOSSとして公開されたということは、その文書館の秘密の書「IA-32仕様書」が、世界に公開されて、全てのITエンジニアにOSを自作する可能性が与えられた、ということを意味しました。

これを形容することは、本当に難しいのですが、「**生まれて始めて地動説を聞かされた、敬虔なカトリック教徒**」くらいの衝撃だったと思います。少なくとも、私にとっては自己の価値観を揺がすほどのパラダイムシフトだったのです。

そして、あの時が、神聖にして不可侵の「神器（じんぎ）」であったコンピュータが、私たちITエンジニアが改造を加え続けて、一生涯をかけて遊ぶことのできる「玩具（おもちゃ）」として生まれ変わった瞬間だったのです。

そして、このLinuxという玩具は、文字通り、PCのデスクトップとして、制御システムのカーネルとして、マイコン（ラズパイ）のコアとして、そしてクラウド（AWS）で選択されるOSの一つとして、私の人生を、劇的に変えました ―― それは、私に無限の課題を与え、それを解決する楽しさを与えてくれる、最高の玩具になったのです。

ビットコインは、私に人生2度目のパラダイムシフトを与えてくれるに違いない ―― 私は根拠もなく、そう信じていました。

いかなる宗教も成し得えなかった、全世界人類共通の価値観「お金」 ―― これは「神器」というレベルを軽く超える統一的な信仰の対象です。

「ビットコイン」は、その「お金」を、私たちにとって楽しく遊べる「玩具」となって具現化してくれるものに違いない ――

- 例えば、国家の暴力装置や、既成の与信システムにベタベタの関係にある現在の「お金」を、私たちの自由意志で管理・運用し、現在の「マネー=権力」の価値観すらも、変えてしまうものとして ――
- または、Linuxがコントリビュータたちによってバージョンアップを続けてきたように ―― あたらしい「お金」の価値のパラダイムシフトが行われ続ける世界を作り出すものとして ――

私は、そんなことを期待していたのです。

ところが、調べてみれば ―― 新しい時代の、新しいネット世界の、新しいパラダイムであるはず（と私が信じていた）ビットコインは、市場（ネットを含む）に流通すらしておらず、その大半が投機目的で所有者に蓄えられているだけ、そして、世界最古の貨幣である法定通貨とベタベタに癒着した、最も醜悪な姿で、私の目の前に現れました。

私は、失望しました。

つまるところ ――私は、ビットコインに、**勝手に期待して、勝手に理想を押しつけて、そして、勝手に失望した** のです。そして、こんなにも勝手な私は、もうこれ以上、ビットコインについて語るべきではないと思います。

というわけで、ビットコインについて語ることは、ここまでとして、今回からは、本命の「ブロックチェーン」の話に注力していきたいと思います。

技術用語を使わずに「ブロックチェーン」を説明したい

ブロックチェーンとは、ビットコインから生まれた技術の一つです。逆に言うと、ビットコインから、ビットコインの生産量を調整するアルゴリズム「半減期」を取り除いて、関係者全員から同意を得るアルゴルズム「コンセンサスアルゴリズム」の内容を換えて残ったモノです。

さて、ここで私は考えました ――「ハッシュ関数」「公開鍵」「秘密鍵」「電子署名」という技術と、「P2P（Point to Point）ネットワーク」について、一つも説明しないままで、**ブロックチェーンを理解したような気になることはできないか**、と。

なぜなら、ネットや書籍に記載されているブロックチェーンの解説は、「技術的に完全に間違っている」か、「技術的に正しいが、技術的に理解できる内容になっていない」かの2つしかないからです。

ちょっと話は横に逸れますが ――

（1）私は以前、上司（博士号取得者）に「オブジェクト指向プログラム」を何度も口頭で説明を試みて、最後まで理解してもらうことができませんでした。最後には「すみません。もう自力でコーディングを試みてください」と言い残して、私はサジを投げました。

（2）私の父は、スキー教室のビデオを見ただけで「もう分かった」と豪語した揚げ句、スキー場で転倒を繰り返し、滞在1時間で撤収しなければならなくなりました。帰宅中の車内で、父は酸欠のチアノーゼ状態になっていました。

残念ですが、「**技術は口伝（くでん）では伝えられない**」のです。

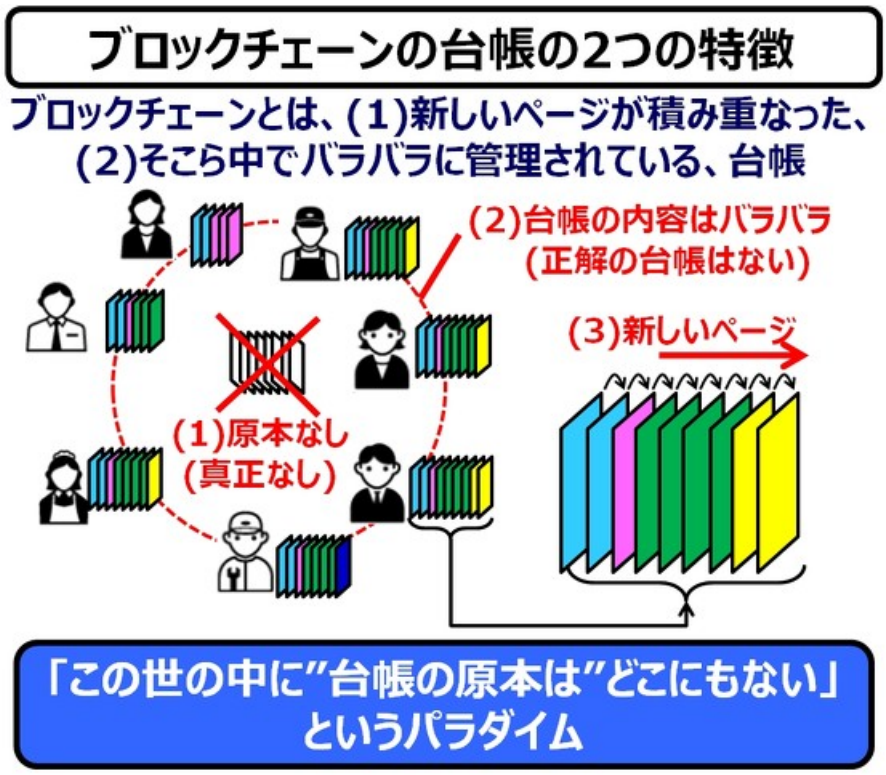
＊）プログラムを書いて理解を試みる方には、この辺の書籍をお勧めしておきます。

閑話休題。

“全てが偽物の台帳”であるブロックチェーン

さて、それではブロックチェーンの解説を始めたいと思います。

ブロックチェーンとは一言で言えば「台帳」です。しかも、「本物の台帳」は世界のどこにも一つとしてなく、**全てが「偽物の台帳」であるという、ものすごい割り切り方をします。**



台帳は、世界中の複数の人間にバラバラに管理されていて、かつ、「本物」はありません。そして、たった一つだけルールを決めておきます。

―― 複数の台帳が手元にあったら、一番厚い台帳だけを残して、残りの台帳は全て捨てる

これだけです。

人生における「長いものに巻かれろ」という処世訓、領土問題における「実効占拠」、そして、某国の元大統領が実施し続けた、証拠が添付されていない*)「盗まれた選挙」の主張の繰り返しこそが、ブロックチェーンの本質です。

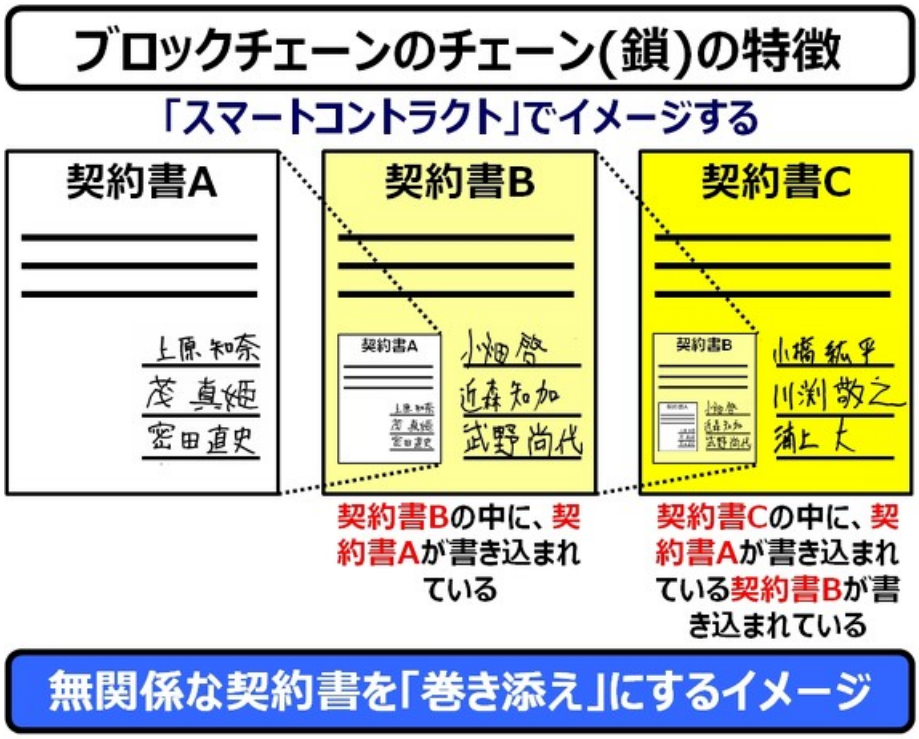
*)証拠の提示のない訴訟は、審理に入る以前に"却下"(訴えの内容を審理せずに門前払い)されます。"却下"と"棄却"は全然意味が違います。興味のある人は調べてみてください。

ちなみに、ナチス・ドイツの宣伝大臣であったヨーゼフ・ゲッベルスの有名なセリフで「うそも百回言えば真実となる」という言葉は、真偽が不明(出典がない)らしいのです。しかし、これが世界で100回以上引用されたことで、世界中の人が「ゲッペルスがそう言ったと信じている」ことになっています ―― これが、「**人工信用***)」であるブロックチェーンの機能と言えます。

*)「人工信用」については、「日本最高峰のブロックチェーンは、世界最長を誇るあのシステムだった」をご参照ください。

次に、台帳のページをどうやってチェーンにするかという問題ですが、乱暴に一言で言えば、ブロック(という名前の台帳のページ)に、前のページの縮小コピペを張りつけるだけです。

これで、自分のブロック(ページ)が、前のブロック(ページ)の次のブロック(ページ)であることが、バッチリと分かります。



上の図で言えば、この縮小コピペによって、契約書Bの前のページは契約書Aがあって、契約書Cのページの前には、契約書Bがあること、つまり「チェーン」となっていることが明らかになります。つまり、この台帳は、契約書A→契約書B→契約書Cの順番で契約が締結し、それがチェーンになっていることが分かるのです。

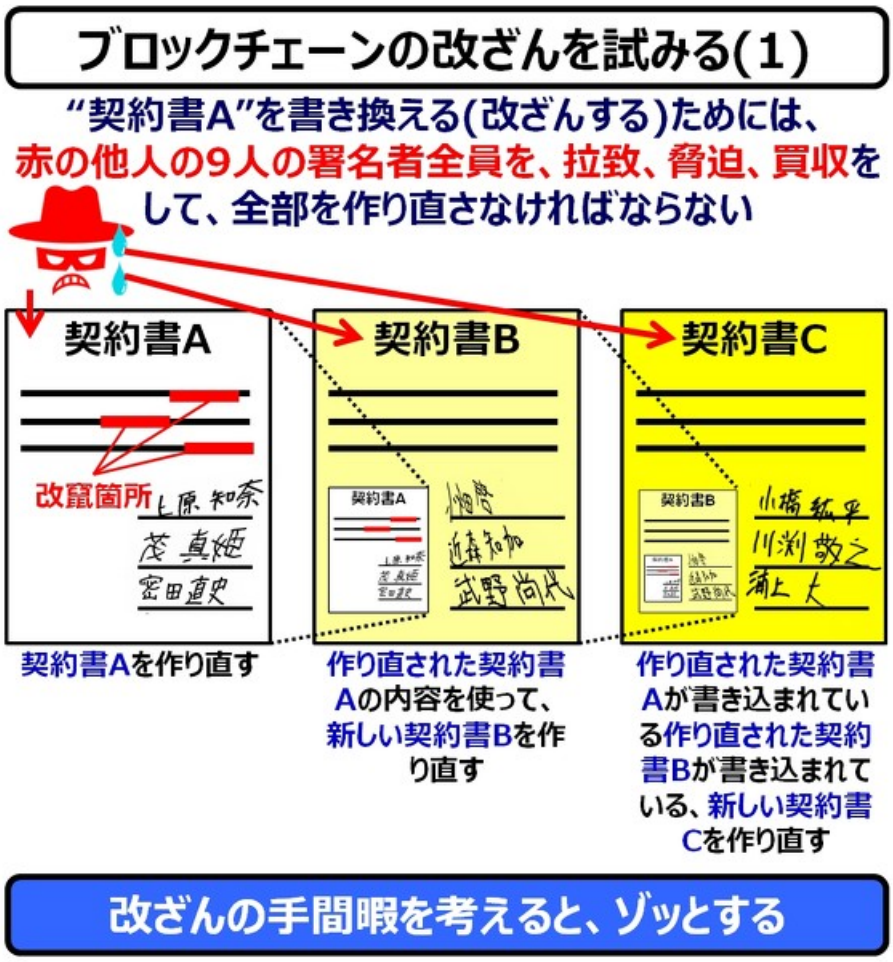
「そんなことしたら、全然関係のない人に、契約書の内容が丸見えになるじゃん」と思われるかもしれませんが、実は、契約書の中の縮小コピペの内容は、暗号化されて、その契約と無関係の人には、何が記載されているか見えません。

「見えないなら、チェーンにならないだろう?」と思われるかもしれませんが、これ、きちんとした手順を踏めば、必ずちゃんと見える状態に戻せます。ただし、**どえらい面倒くさい上に、ものすごく時間がかかります**。

加えて、この暗号は必ずしも解読する必要はないのです。解読できることが「証明」できれば、それで十分です(これがハッシュ関数によるハッシュ値の使い方です)。つまり、暗号化された契約書本体を解読して開示する必要はないのです。

ブロックチェーンの改ざんは「とにかく面倒くさい」!

で、この「**どえらい面倒くさい上に、ものすごく時間がかかる**」が、ブロックチェーンの改ざんを不可能とする仕組みの根幹なのです。



例えば、契約書Aの内容を改ざんしてやろうという悪意の第三者が存在するとします。

普通なら、契約書を金庫から盗んで、すりかえるなりすれば良いでしょう。契約書については、契約書Aに関わる3人を抱き込む（拉致監禁、脅迫、買収、その他いろいろ）ようにすれば、実現できそうです。うん、それでも応じないやつは、拷問して偽造書類に署名を書かせた上で殺害してしまいましょう。

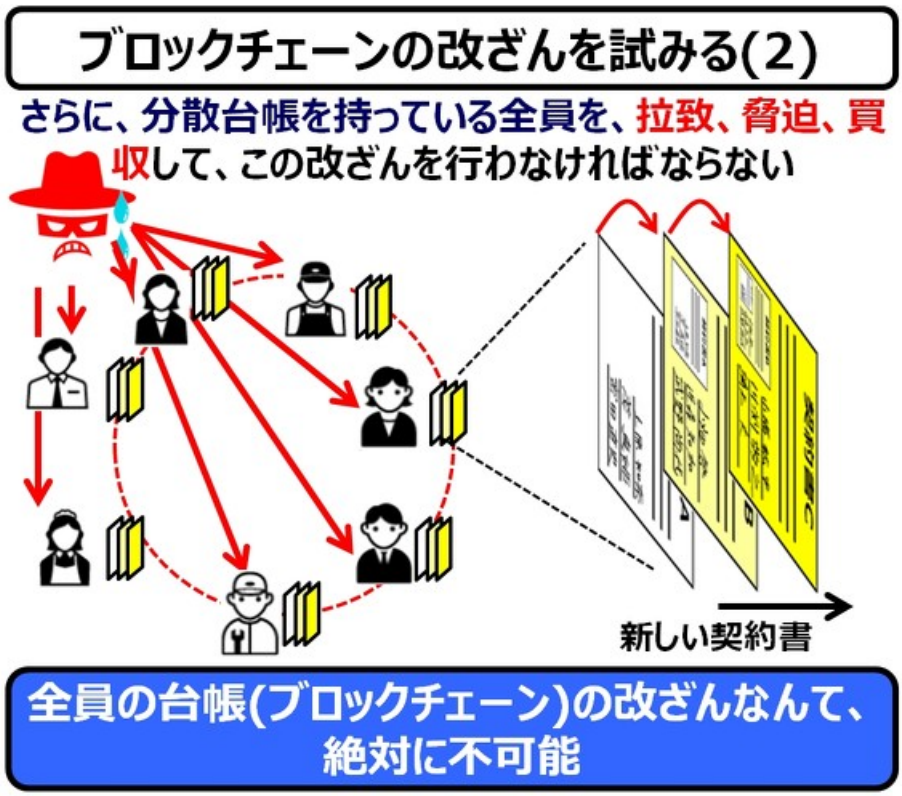
ところが、契約書Aを含むブロックチェーンが契約書Cまで繋っているとすると、話は恐ろしく面倒になります。

契約書Cには、契約書Aの内容がコピペされた契約書Bのコピペが添付されているからです。

契約書Aを改ざんするためには、契約書Bと契約者Cの関係者全員の同意を得て、もう一度、最初から、契約書A→契約書B→契約書Cの順番で契約を締結させて、それをチェーンとして再構築しなければなりません。

関係者総勢9人を巻き込んだ、一大改ざんプロジェクト —— それも1人足りとも欠けてはなりません。そんな面倒くさいこと、誰が試みようとするでしょうか？

しかし、悪意の第三者の仕事はこれでは完了しません。なぜなら、契約書A→契約書B→契約書Cの順番で契約を締結させたブロックチェーンは、**既に世界中にバラまかれている**からです。



世界中にバラまかれているブロックチェーンの全部を書き換えるということは、関係者9人を引き連れて、世界中を旅行しなければならないということになります。当然そんなことは、できっこありません。

それに、契約書Aの改ざんをやっている間に、契約書D、契約書Eが追加されでもしたら、ブロックチェーンルール「**複数の台帳が手元にあったら、一番厚い台帳だけを残して、残りの台帳は全て捨てろ**」に基づき、苦労して改ざんしたブロクチェーンは、その「薄さ」故に、世界中でゴミ箱に廃棄されることになります。

ならば、契約書D、E、Fを偽造して、契約書A→B→C→D→E→Fのブロックチェーン全体を偽造して、ネットワークにぶん投げれば、「厚さ」で勝てそうな気がします。

しかし、D→E→Fには、コンセンサスプロトコルを実施して、複数の関係者の証明書が付与されなければ、チェーンにつなげられないので、これも実現できません。

結局のところ、契約書Aを改ざんする現実的な手段を考えるくらいなら、**全面核戦争を引き起こして人類を「最初からなかったこと」にした方が簡単です**。

ブロックチェーンのアプリケーション

さて、技術的な話(?)はここまでとして、ブロックチェーンのアプリケーションの話をしましょう。どんな技術であれ、**その技術がアプリケーションで使われてこそ、意味がある**からです。

ブロックチェーンを使う可能性のあるアプリケーションを、下記のように分類してみました。

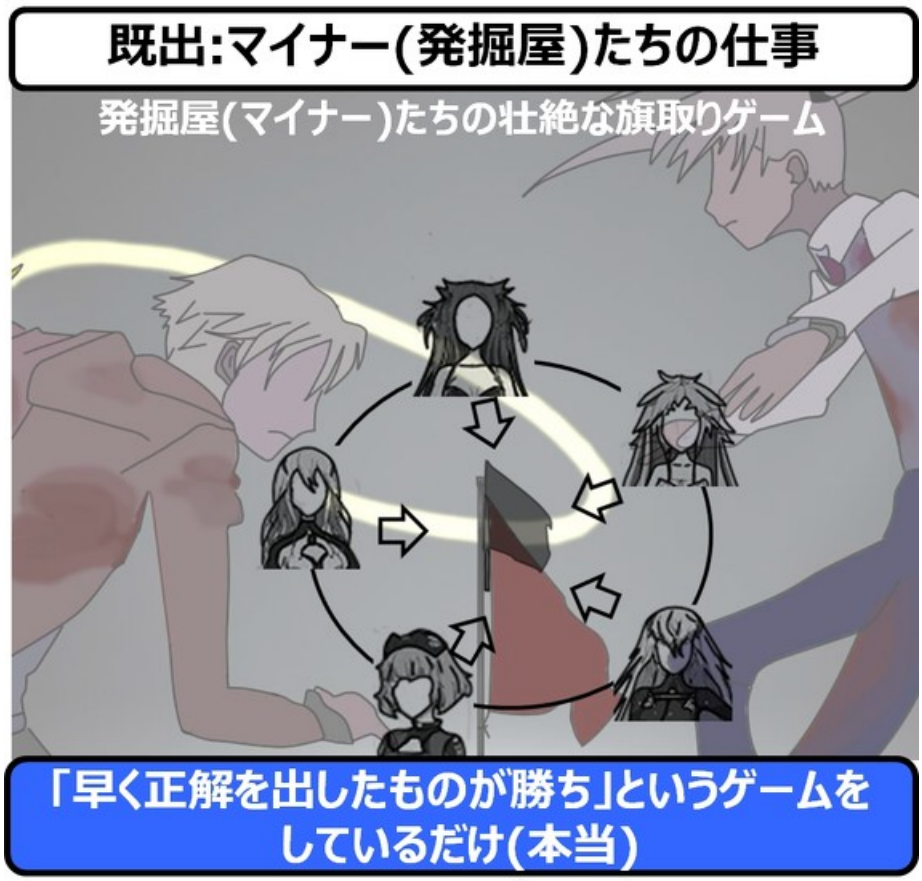
ブロックチェーンのアプリケーション

台帳を使う業務/サービス/アプリであれば、何だってブロックチェーンを使える

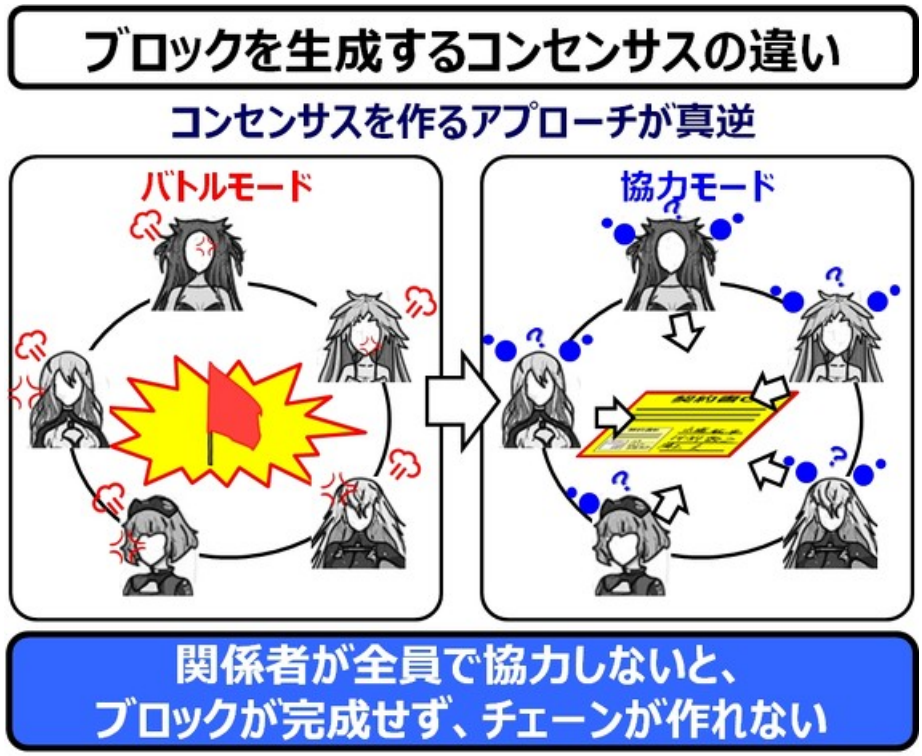
#	項目	内容	ヒット数	江端にヒットした事案
0	仮想通貨	(省略)	2,570K	■ビットコイン、その他の暗号資産
1	決済	貸借関係の解消	1,990K	■安価な国際送金 ■地域通貨
2	取引	金品や事柄のやり取り	2,340K	■個人での電力売買 ■秒単位の動画配信
3	証明・署名	証拠による確定/本人の証明	1,411K	■著作権管理(公証役場不要)、遺言
5	契約	権利/義務関係の発生	1,830K	■スマートコントラクト
6	投票	団体としての意思表示	1,770K	■スマホ投票 ■スマホ株主総会
7	ニュース	新規の出来事の報道	3,890K	■ファクトチェックによるフェイクニュース対策 ■撮影場所/時間の証拠化
8	娯楽	人を楽しませ慰めるもの	121K	■オンラインカジノ(各種の法解釈あり)
9	追跡	現在位置を確認	474K	■美術品の追跡 ■食品輸送
10	マッチング/婚活/結婚	マッチング/法律の枠外のカップル認定	1,100K	■就職/恋愛マッチング ■「永遠の愛」の宣誓 ■現時点で非合法化な結婚の証明(LGBTカップル等)

台帳を使う業務／サービス／アプリであれば、何だってブロックチェーンを使えます。しかし上記#0の仮想通貨（ビットコイン）と、それ以外の他のアプリケーションは、コンセンサス（同意）アルゴリズムの内容が決定的に異なります。

ビットコインでは、台帳ページを追加する権利が、ビットコインの発掘屋（マイナー）たちの壮絶なバトルで発生する、という話は、「ビットコインの正体 ～電力と計算資源を消費するだけの“旗取りゲーム”」でしました。



ところが、ビットコイン以外のブロックチェーンでは、こういう野蛮なコンセンサスアルゴリズムは採用しません(というか、アプリケーションの性質上、採用できません)。



ビットコインは、取引のラウンドが発生する度に、電力とコンピュータリソースを使った「数当てゲーム」行い、たった1人の勝者の勝利宣言と、敗者の敗北宣言で、1ラウンドが終了し、勝者が賞金(6.25BTC, 現時点のレートで2200万円相当)

を総取りする「**バトルモード**」です。

しかも、ビットコインの取引を行う人間と、けんかしている人間が、全く別々に無関係に存在している（完全に赤の他人）という、奇妙な構成となっています（参照）。

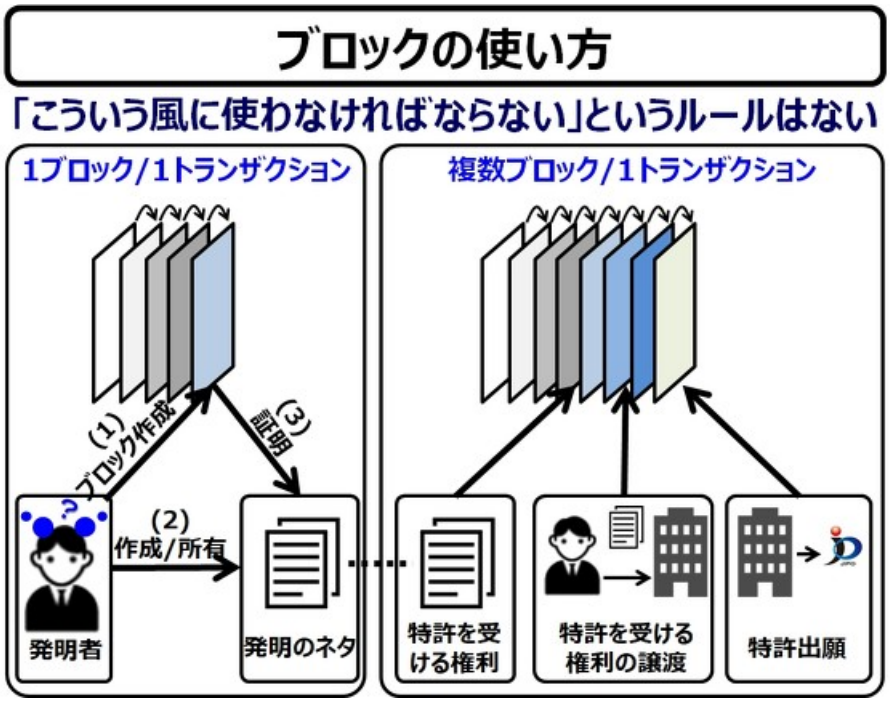
例えば、前回の例では、私がBitFlyer社からビットコイン5000円分の購入を申し入れた直後にから10分間、中国奥地に設置された数千台のビットコイン専用マイコンが、膨大な電力を消費しながら数当てゲームを行い、その勝者に2200万円（分のビットコイン）が付与されます ーー この強烈な非日常感に眩暈（めかい）がしそうです。

しかし、普通に考えれば、そんなプロトコルの方が変なのです。

本来、ブロック（台帳のページ）の生成に関わる人物は、アプリケーションのユーザーであり、そして、台帳のページ（例えば契約書）を作るためには、ユーザー全員で知恵を出しあう「**協力モード**」であるべきです。

この「協力モード」のブロックチェーンを調べてみると、大きく2つのパターンがあるようです。

この2つのパターンを、発明の登録のプロセスと、特許を受ける権利の発生から特許出願までのプロセスを例として説明します（ちなみに、特許庁の審査官とのバトルは、私の業務の一つです）。



まずは、一つのブロックに全ての処理を記載してしまう方法です（左図）。ここでは、新しいアイデアを思い付いた人が、特許庁に特許出願するのではなく、その発明について記載したメモ（発明者と発明の内容の両方が記載されている）を、**ブロックとしてまとめて、チェーンにつなげる方法**です。

もう一つは、処理の流れ（ワークフロー）そのものを、ブロックチェーンとしてしまう方式です（右図）。特許手続（特許を受ける権利の発生）→会社への譲渡→会社による特許出願の、**それぞれをバラバラにブロックにするという方法** です。

ちなみに、ブロックチェーンにも国際標準化活動があるようです。標準化ができれば、異なる組織同士でブロックをつなぐことができて便利かもしれませんが、インターネットの通信プロトコルなどとは違い、「何がなんでも、標準化が必要」という空気は（私には）感じられませんでした。

通信の場合、両方のプロトコルが一致していないと、1ビットも情報の伝送ができませんが、ブロックチェーンは、ブロックをつなげるだけですので、不細工で取り扱いが面倒くさくなったとしても、なんとかなりそうに（私には）思えるのです。

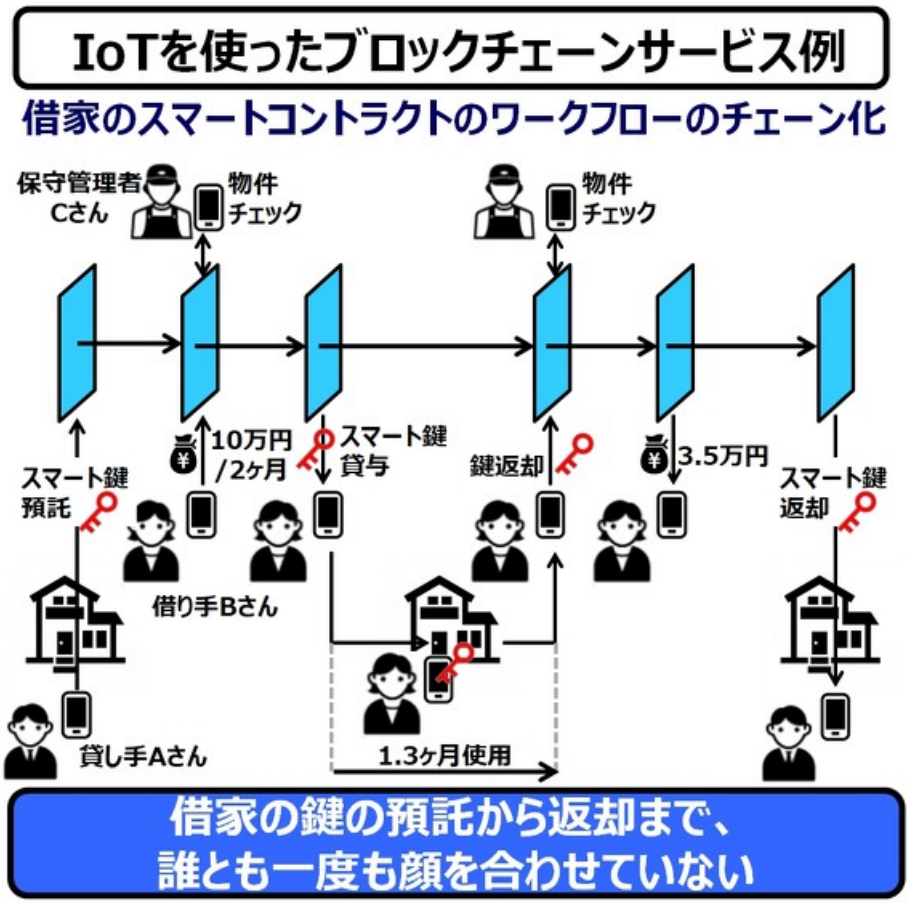
まあ、今後、ビットコインが他の通貨とマージして使えるようにする、というような話が出てれくれば、一気に標準化の流れ

が進む可能性もあると思います。

直接会わずに家が借りられる「スマートコントラクト」

さて、ブロックチェーンを使った契約（スマートコントラクト）について、もう少し具体的な例で説明してみたいと思います。

こちらの事例は、借家の契約の開始から完了までを、関係者（貸し手Aさん、借り手Bさん、保守管理者Cさん）が一度も顔合わせすることなく完了してしまう、IoT（モノのインターネット）を活用したスマートコントラクトの一例です。



まず、技術的な前提として、**スマホで開錠／施錠ができるスマート鍵があるもの**とします。このスマート鍵は、ネットワーク経由で第三者に転送が可能であり、最後に受けとった人だけが利用できます。

貸し手Aさんは1年間の海外出張のため、自宅を貸し出すことにしました。そこでAさんは、自宅のスマート鍵をブロックに添付し、借り手が現われるのを待ちます。

そこに、ブロックチェーンを見ていた、借り手Bさんが、2カ月間の貸与契約と電子マネーをブロックに添付します。さらに、そのブロックから連絡を受けた保守管理者Cさんが物件のチェック（貸与前のダメージチェック等）を行い、ブロックが生成されます。

次に生成されるブロックから、借り手Bさんにスマート鍵が送付されて、貸与期間が開始します。Bさんは予定の2カ月前に退去が決まり、鍵を返却し、保守管理者Cさんが、貸与後の借家のチェックを完了することで、ブロックが生成されます。

期間前の貸与による残金からダメージによる物件の現状復帰に必要な金額を差し引かれた金額（3.5万円）が、電子マネーで元借り手のBさんに返金されて、ブロックが生成されます。

帰国後、貸し手Aさんにスマート鍵が返却されて、ブロックが生成され一例の処理が完了します。

―― ぶっちゃけ、これ、普通のワークフローシステムでもできるよね

と言われれば、その通りだと思います。

これは別段ブロックチェーンでなくても、スマート鍵の配送さえできれば、実現できるような話です。しかし、この方式の特徴は、**『人間は、ブロックチェーンプログラムの中に記載されているオブジェクトの一つ』**であり、そのメリットは**『関係者が所定の場所に集って、契約書を取り交さなくても、条件に応じて契約条件が履行されていく』**という点にあります。

問題は、このブロックチェーンの契約が法的な効力を持つか、あるいは、**契約不履行の場合、例えば損害賠償の訴訟における証拠能力を有するか**ということにあります。

Google scholarで「ブロックチェーンと裁判」でちょっと検索して、いくつか論文を読んでみたのですが、「そんなもん大丈夫に決まっとろうが」という楽観論ものから、「裁判官がブロックチェーンプログラムコードを理解する必要があるのではないか（そんでもって、『それは絶望的だ』という主張）」という悲観論まで各種ありますが、現時点では過去の判例はないようです。

エンジニアとしての私は、「そんなもん大丈夫に決まっとろうが」という楽観論派です。根拠は上記で説明した、―― **契約書Aを改ざんする現実的な手段を考えるくらいなら、全面核戦争を引き起して人類を「最初からなかったこと」にした方が簡単** ―― と、思っているからです。

ただ、裁判所において、裁判官、検察、弁護人、そして傍聴者に対して、「ハッシュ関数」「公開鍵」「秘密鍵」「電子署名」を含めたブロックチェーン技術を、分かりやすくプレゼンしろ、と裁判所から命令されたら、**全力で逃げます**。

さて、先ほど、「某国の元大統領が実施し続けた、証拠が添付されていない『盗まれた選挙』の主張の繰り返し」について述べました。

『証拠なしで訴状を出すなどということを、現職大統領の法務担当チームがする訳ない』と思っていましたので、私は、訴状と証拠が開示されたら、その全文を読もうと腹を括っていました。（「英語に愛されないエンジニア」の私にとっては、おそろしくツラい作業になるとは思いましたが）。

ですが、現時点でも、訴状の内容の開示は確認できておりません（私が見落していたら、誰か教えてください）。原告（元大統領）に訴状の開示義務はありませんが、訴状を公開することによって、裁判所の理不尽な”却下”を、世間に訴えることもできただろうに、と、不思議に思っています。

あと、私にできそうなことと言えば、投票結果から、統計を使って不正投票の可能性を調べることです ＊）ちなみに「日本の大相撲が八百長である」という事例が、米国の統計学のテキストの演習問題で使われているそうです。。

この「統計を使った不正投票の可能性」についてはEE Times Japan編集部からGoを貰えれば、調査を開始したいと思っています。

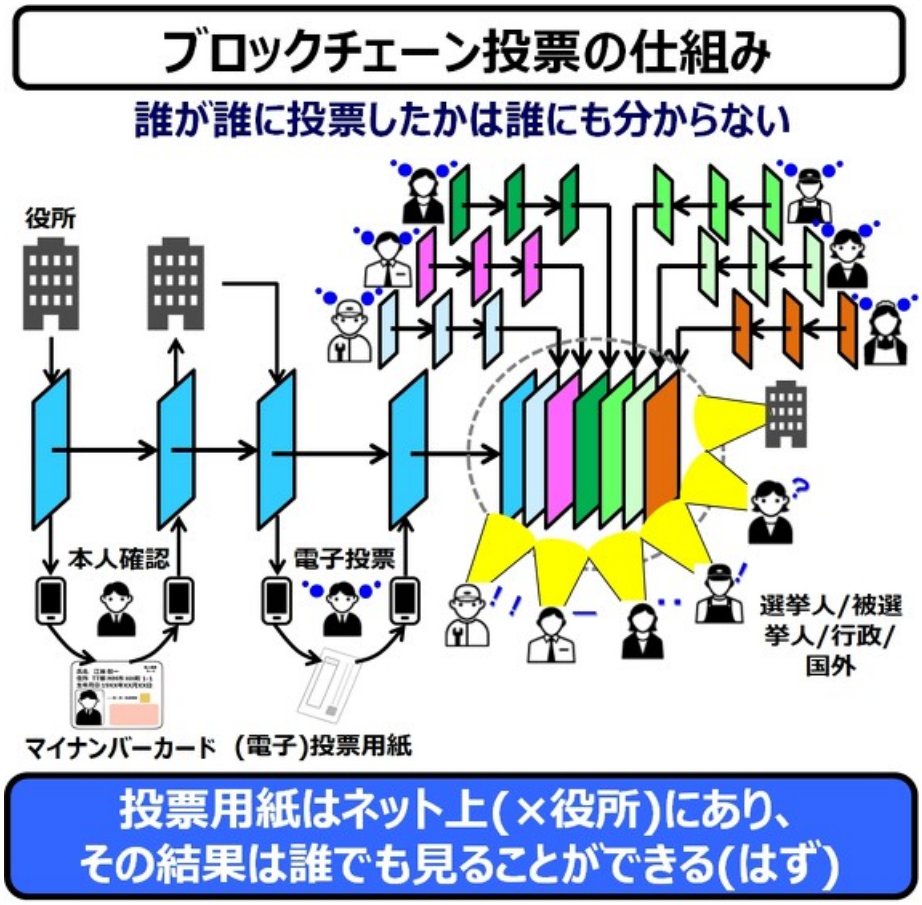
閑話休題。

郵便投票がイヤ？　ならば「ブロックチェーン投票」を導入してみよう

さて、ここからは、

―― 郵便投票が嫌なら、ブロックチェーン投票を導入すればよかったのに

について、お話したいと思います。



ブロックチェーン投票は、一言で言えばスマホやパソコンによる投票です。役所からスマホに送られてきた本人確認に対して、身分証明書で本人認証をすることで、スマホに電子的な投票用紙が送付されてきて、それを使ってスマホで投票を行うものです。

ブロックチェーン投票のすごい点は、投票結果を、選挙管理委員だけでなく誰でも、投票者も非選挙人も、もちろん現職大統領も見ることができて、それにもかかわらず、誰が誰に投票したかは誰にも分からない、という点にあります。

これは、ビットコインのアドレスから本人の特定が（事実上）できない、という仕組みから、実現可能であることが分かります。

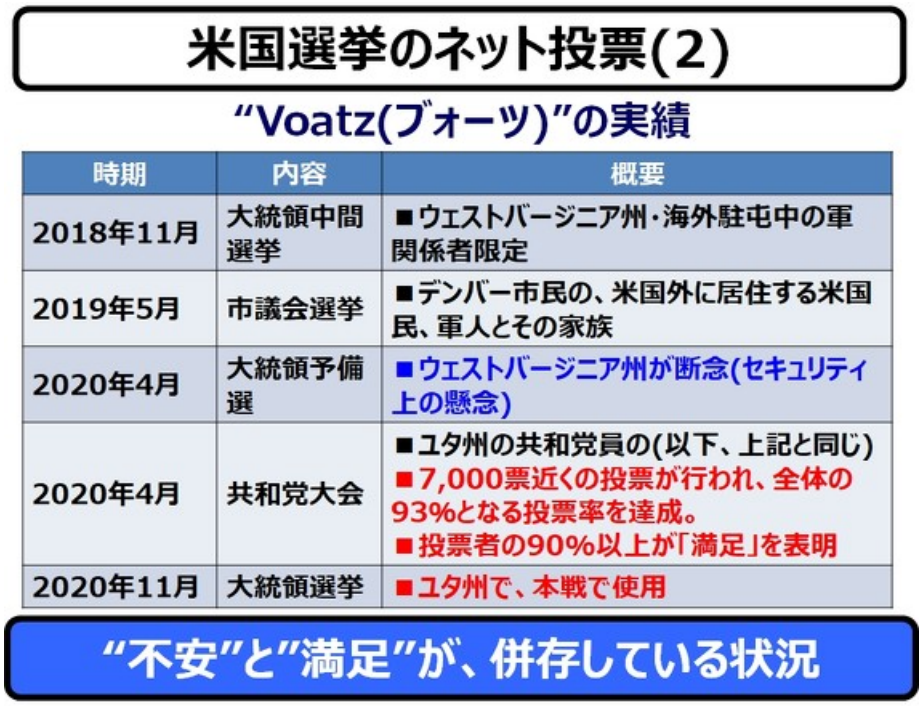
もちろん、これまで述べてきたように、**ブロックチェーン投票の改ざんは不可能**です。まあ、それでも、”システムで選挙が盗まれた”という人は一定数出てくると思います ―― 例えば、どっかの国の元大統領とその支持者のように。

しかし、ブロックチェーン投票の結果を否定することは、技術的には絶望的に難しいと断言できます。世界中の人間が、複数の投票所の開票作業を24時間でずっと見守り続け、その開票結果には1票のそごも生じない ―― そういう選挙になるからです。

実際に今回の米国合衆国大統領選挙では、ブロックチェーン投票が実現できたはずなのです。米国では、既にブロックチェーン投票のシステムが動いているからです。モバイル投票アプリの「Voatz（ヴォーツ）」です。

画像:Voatz

Voatzは、ウェストバージニア州の2018年の大統領中間選挙から使われて、数回の使用実績もあります。



当初、このVoatzの導入は、海外駐屯中の米軍関係者が投票できるようにするためでした。米軍(家族を含む)は世界各国に展開していますので、期日前投票の票の回収が、投票日当日までに間に合わない問題があったからです。

私が調べた範囲では、Voatzは数千人単位の投票で、トラブル等も発見されず、高い投票率と満足が得られていることが分かっています。実際に、ユタ州では、今回の大統領選挙(本戦)で使用されたようです。

そもそも、スマホでブロックチェーン投票ができれば、投票所が不要（3密解消）となり、世界中がリアルタイムで投票状況を把握でき、開票作業すら不要です。今回の2020年の米国大統領選挙で、Voatzが使われていれば、**ものすごく安全で安価な選挙が実施できただろう**に、と思います。

しかし、2020年4月の、ウェストバージニア州の大統領予備選挙においては、Voatzの使用が断念されました。これは、議会において専門家からセキュリティ上の不安が表明されたからです。もちろんVoatz社は、この理由について反論をしています。

人間が作るシステムに”絶対”はありません ーー しかし、ブロックチェーン技術とは、「ハッシュ関数」「公開鍵」「秘密鍵」「電子署名」からなるシステムです。私たちは気がついていませんが、私たちはこれらの技術を、毎日、使い倒しています。

ホームページを見に行くだけで「ハッシュ関数」「公開鍵」「秘密鍵」が動きますし、スマホを使って銀行から振込をする時には「電子署名」も発動しています。そもそも、私たちが使っている（or 政府に使わされている）**マイナンバーカードは、これらの技術の集大成**といっても過言ではありません。

ブロックチェーン投票が広まっていない理由を、一言で言えば、以前ご紹介した、行動経済学における「現状維持バイアス」です。

既出：行動経済学のアプリケーション(2)

<table>
<tr><th>例</th><th>手法</th><th>例</th><th>使用例</th></tr>
<tr><td rowspan="2">(6)確実性効果</td><td rowspan="2">“0%”か”100%”だけ</td><td>×「50%の確率で貰える30万円」</td><td rowspan="2">100%メニューの追加</td></tr>
<tr><td>○「100%貰える10万円」</td></tr>
<tr><td rowspan="5">(7)プロスペクト理論</td><td rowspan="2">利益を得る場面ではリスク回避</td><td>×「50%の確率で20万円貰える」</td><td rowspan="5">場面単位で、提案方式を変える</td></tr>
<tr><td>○「100%の確率で10万円貰える」</td></tr>
<tr><td colspan="2">だが</td></tr>
<tr><td rowspan="2">損失を被る場面では損失回避</td><td>×「100%の確率で10万円失う」</td></tr>
<tr><td>○「50%の確率で20万円失う」</td></tr>
<tr><td rowspan="2">(8)現状維持バイアス</td><td rowspan="2">「変更なし」を入れる</td><td>×「いいか悪いかわからない変化」</td><td rowspan="2">席替え、異動</td></tr>
<tr><td>○現状維持</td></tr>
<tr><td rowspan="3">(9)ギャンブラーの誤謬</td><td rowspan="3">「過去のデータ」をささやく</td><td>ルーレットで赤ばかり出ている時、</td><td rowspan="3">ギャンブルの最中</td></tr>
<tr><td>×「赤：50%、黒50%と考える」</td></tr>
<tr><td>○「黒に賭ける」</td></tr>
</table>

これは、30年前、大学のキャンパスで、「**電子メールを使う江端は、オタクな奴**」と、石を投げつけられた（暗喩）日々の再来です ーー ちなみに私は今でも、「現状維持バイアス」から抜け出せなかった、いわゆる、大学キャンパスの低能な”陽キャ”を許していません。

この低能な"陽キャ"の迫害に屈しなかった私（たち）の、地道な電子メール等に関する啓蒙活動が、今のスマホ文化を開花させ、我が国にデジタル庁を設立させるに至ったと確信しております ーー 私たちの貢献に対して、ことしの「紫綬褒章」を大いに期待しております。

とまあ、冗談はさておき ―― 実は、これ（「現状維持バイアス」）もバズワードの大きな性質の一つです。

Wikipediaでは、バズワードとは「技術的な専門用語から引用したり、それをまねた言葉で、しばしば、素人がその分野に精通しているように見せるために乱用される、無意味だが、かっこいい、それっぽい言葉」と定義されています。

しかし、バズワードの技術が、ひとたび私たちの利害に関わるところで使われることになると、私たちは手のひらを返したかのように、それを拒絶し出します。「実績がない」とか、「不安要素が残る」とか、後になって、いろいろ言い出し始めるのです。

つまりバズワードは、**『恣意的に、自発的に、ひとごとのままにしておきたい』**ものであり、**『私と関係のない世界で、私の知らない間に、勝手に終結する（うまく回っている）こと』**が期待されているという技術です*）。

*）関連記事：「ある医師がエンジニアに寄せた“コロナにまつわる現場の本音”」

つまるところ「**バズワードとは、ひとごとの技術名称**」 ―― この一言に付きるのです。

閑話休題。

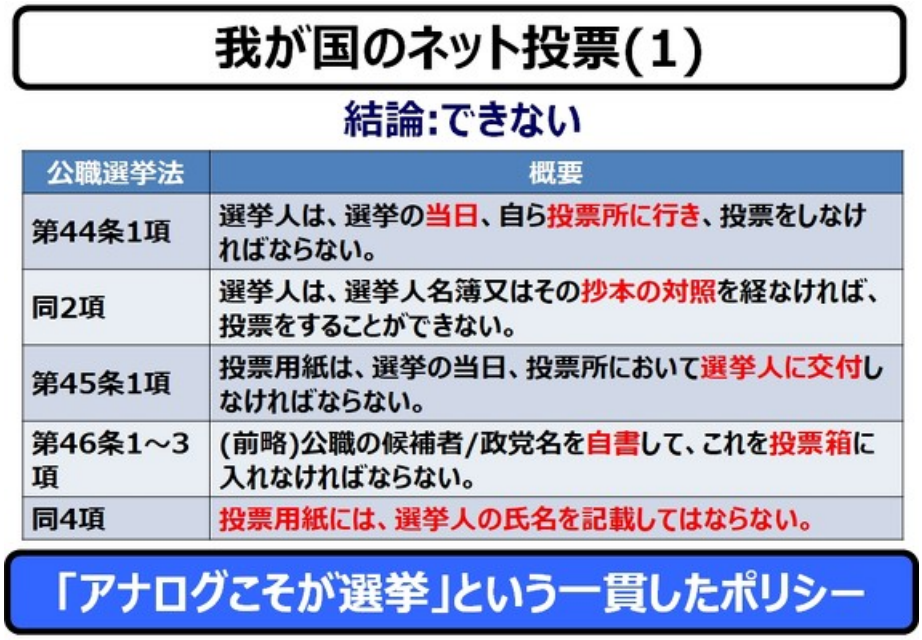
日本ではどうなのか

人様のお国の事情を、エラそうに語っているのもどうかと思いましたので、我が国のネット投票（ブロックチェーン投票に限定しない）がどうなっているかを調べてみました。その結果 ――

現時点での、我が国でのネット選挙の実現可能性はゼロ

ということが分かりました。

理由は明快です。法律でネット選挙が禁じられているからです。



ネット投票を可能とする法解釈の余地はありません。ここまではっきり言われたら、逆にすがすがしいくらいです。

もっとも今後は、米国のVoatz（ヴォーツ）の成功例、日本の少子高齢化、デジタル庁の創設、なにより、このコロナ禍などを勘案すれば、法改正に動く可能性はあると思います。

逆に、ネット投票の妨害勢力としては、「高齢者等の、デジタルデバイド問題」「システム障害の可能性」「IT教育（公開鍵方式の仕組み等）の不備」などがあると思いますが ―― 『マイナンバーカードの普及を促しながら、ネット投票による選挙を否定し続ける』というのは、**なかなか派手な矛盾**ですので、私は比較的楽観視しています。

「スマホが使えない」「USBが何のことか分からない」「自分でパソコンを使えない」ことを、まだ”笑える自虐”と信じている ―― 実際は、国民の多くから、心底”軽蔑”されている*) ―― 政府与党の老人たちが政界から消えれば、なんとかなる、と思っています。

*)著者のブログ

もっとも、公職選挙法は、公職の選挙にのみ適用されるのですから、民間が導入する分には構わないはずです。

私は、IT教育(スマホの利用を前提とした授業等)とセットにして、まずは中学、高校の生徒会役員選挙あたりで導入してはどうかと思います。(そんでもって、できれば、生徒自身が「ブロックチェーンの投票システムを自作する」ところまで持っていければ望ましいですが、ちょっと難しいかもしれません)

また、国内で行われたネット投票の実証実験では、以下の良好な実験結果が得られているようです。

我が国のネット投票(2)

2018年8月28日 茨城県つくば市での実証実験

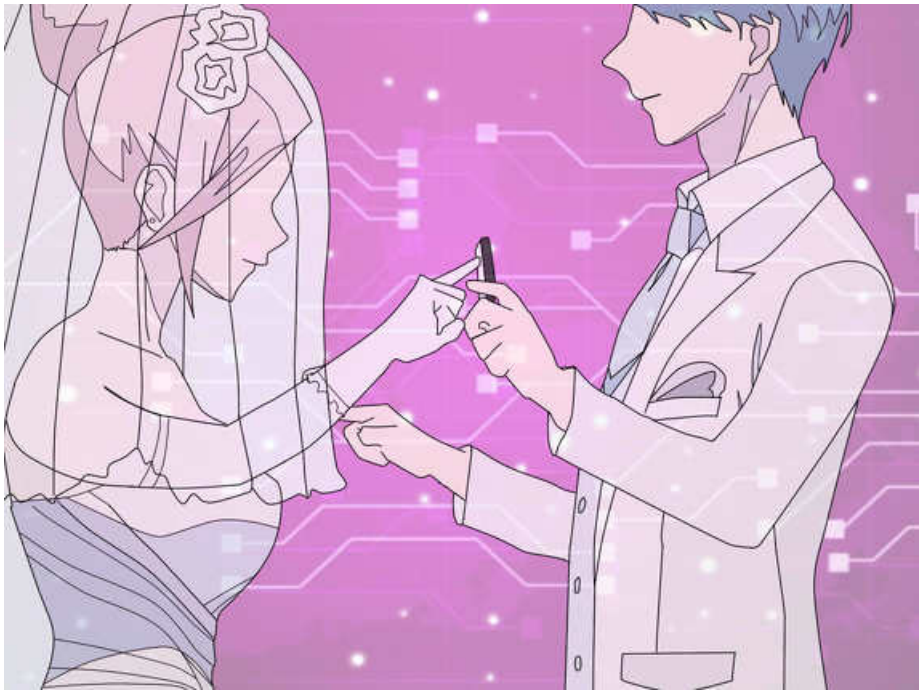
観点	項目	概要
特徴	本人確認	マイナンバーカード(秘密鍵)と本人写真
	匿名性	ブロックチェーン技術を用いて、各票を匿名化し、記録する
実験条件	選挙対象	社会実装トライアル支援事業13件中、1件を投票
	有権者数	119名(マイナンバーカード所有者)
実験結果	マイナンバーカードが”使える”	マイナンバーカードによる本人認証で「投票の正当性」が証明された
	データの非改ざん性が”証明”	■投票者情報と投票内容は別々のサーバで管理 ■改ざんが困難なブロックチェーン技術によって投票データの改ざんや消失を防止
	“上書き投票”の実現	二重投票による、後発的な投票変更を実現

現時点で実現可能である目処は立っている

法律が追い付かないなら「ブロックチェーン婚」で認定してみよう

では、最後に、ブロックチェーンという「人工信用」技術の社会的意義を、ピンポイントに示すアプリケーションを紹介したいと思います。

ブロックチェーン婚です。



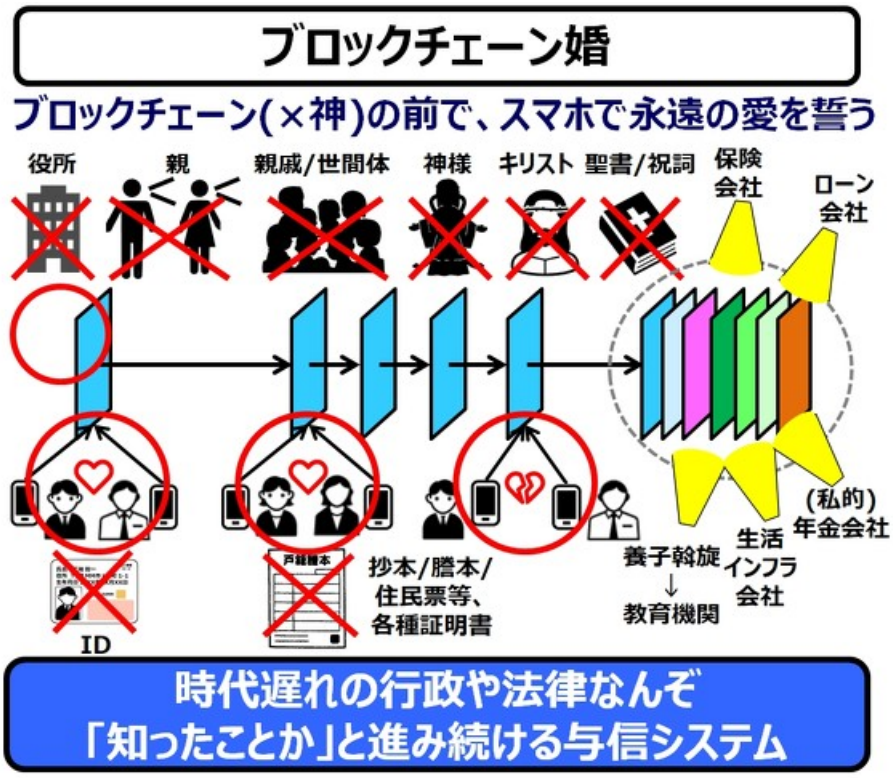
ブロックチェーン婚については、ググって頂ければ、結構な数の記事がヒットしますが、その背景を一言で言えば「**結婚の多様化に対して、社会システム（法律、行政）と、私たちの社会通念（常識、慣例）が追い付いていない**」です。

最も分かりやすいユースケースが、現時点では合法ではない「同性婚」です。

同性婚に関する私のスタンスは、もう何度も述べております*）ので、今日は、「モーリス・ウィリアムソンさんの議会演説」をご紹介するにとどめたいと思います。

*）技術的アプローチでは、こちらなど→https://biz-journal.jp/2014/03/post_4420.html

私が、この「ブロックチェーン婚」を重視しているのは、これからの社会は、法律、行政が揃わない状況下であっても、**社会システムの方が「勝手に整備されていく」という可能性**が、かなりはっきりと見いだせるからです。



前回、「天皇制とはブロックチェーンである」というテーゼを掲げて、それについて解説しましたが、今回は、その逆問題「**ブロックチェーンであれば、(天皇制に匹敵する)与信システムになる**」というテーゼになります。

ブロックチェーンは、それが「**過去にさかのぼって『なかったこと』にはできない**」という究極の「人工信用」の製造装置です。

そして、結婚とは、その成立に必ずしも規範や制度を必要としません。つまり「当事者が結婚である」と認定すれば、それは結婚として直ちに成立するものです。ただ、日本国において、法律上の保護(メリット)を受けるためには、日本国の法律に従った方が「いい」というだけのことです。

ブロックチェーン婚では、当事者の合意以外の全てのもの ―― 法律、役所への手続き(謄本、抄本、住民票、各種の証明書の提出)、両親の同意、親戚への報告、宗教上のイベントや規定など ―― 全て無視して構いません。

しかし、ブロックチェーン婚による結婚は、ネット上において多くの人に公開され、認定されることになります ―― そして、**それは大きなビジネスチャンスになります**。

まず、所帯を持つという意味では不動産業、家電製品なども販路開拓のきっかけになるでしょう。法上の結婚であろうがなかろうが、家族向けの保険の顧客になります。住宅や自動車ローンの需要もあるはずです。プライベートな年金システムも動き出すかもしれません。

行政は、住民の生活を保護する義務がありますので、事実婚(同性婚を含む)に対する各種の制度が拡充されて行くと思いますし、特に期待できるのは養子制度への橋渡しや、その被保護者への保護の充実が、さらに必要となっていくでしょう。

裁判所が、ブロックチェーンの証拠能力を公に認めれば、法律上の結婚制度の保護すらなくなるかもしれません。「事実婚=法律婚」がデフォルトとなれば、一体、どこの誰が面倒くさい行政手続きをしようとするだろうか、ということです。

さらに、立法府(国会)は、法律の作成をチンタラやっていると、議員(**特にジジイの政治家たち**)の望まないような社会の形成が勝手に進んでしまうという恐怖から、(同性婚等の)立法化が、加速化されていく可能性もあります。

以上のように、ブロックチェーンという「人工信用」システムは、**現在の立法と行政を無力化するほどのポテンシャル**を有する、かなり恐ろしいシステムであり、「ブロックチェーン婚」は、その端緒にすぎないのかもしれないのです。

では、今回の内容をまとめます。

(1) ブロックチェーンの解説を、技術用語を使わない方法で説明を試みましたブロックチェーンとは、分散された台帳であり、(A)「本物の台帳」は世界のどこにも一つとしてなく、**全てが「偽物の台帳」である**という、ものすごい割り切り方をしていること,(B)「複数の台帳が手元にあったら、**一番厚い台帳だけを残して、残りの台帳は全て捨てろ**」というルールだけがあること、(C)チェーンとは、台帳の**前のページの縮小コピペで実現している**こと、という説明をしました。

(2) 上記(C)の仕組みによって、ブロックチェーンの改ざんを行うことは事実上不可能であることを、「スマートコントラクト(契約)」の例を用いて説明しました。どのくらい不可能であるかというと、ブロックチェーンに関わる世界中の人間を、拉致、脅迫、買収をしなければならず、それを、極めて短い時間(例:10分以内)で行わなければならないなど、その難しさを**「全面核戦争を引き起こして、人類を『最初からなかったこと』にした方が簡単」**と表現しました。

(3)ブロックチェーンを使うアプリケーションを10カテゴリーに分類した上で、ブロックチェーンのコンセンサスアルゴリズムの違いを具体例で説明しました。また、スマートコントラクトを使った借家システムの具体例を示し、さらに、2020年に行われた米国大統領の選挙のドタバタを引例として、**「ブロックチェーン投票」の仕組みと、日米における運用例**をご紹介しました。

(4)「**結婚の多様化(同性婚等)に対して、社会システム(法律、行政)と、私たちの社会通念(常識、慣例)が追い付いていない**」ことを背景とした、「ブロックチェーン婚」について解説しました。この新しい婚姻与信の仕組みは、現在の立法と行政を無力化するほどのポテンシャルを有する、かなり恐ろしいシステムであることを具体例で説明しました。

以上です。

アメリカ合衆国第45代大統領、ドナルド・ジョン・トランプさんに対する、私の所感は控えさせて頂きますが(まあ、日常的に、私のブログやコラムを読んで頂いている方には、明らかでしょうが)、はっきり言えることは、「**この人ほど、私に膨大なコラムネタを提供してくれた人はいない**」ということでしょう。

彼の大統領就任なくして、この記事やプレゼンが、世の中に出ていくことはなかったでしょう。

地球温暖化について再度のレビューをすることもなかったと思いますし、新型コロナ禍におけるこれらの記事を自分なりの確信を持って執筆(シバタ医師の代筆)をすることもなかったでしょう。

それに、権力者によるSNSの濫……もとい、運用について、これほどのリアルをもって実施されることは、これまでになかったと思います。

私は、インターネットの構築に微力ながら参画したという自負のあるネットワークエンジニアですが、「**『私のインターネットによる理想の民主的社会』の幻想**」を、**これほど徹底的に破壊し尽くしてくれた人物はいない**と確信します。

さらに、今回のシリーズで解説している「人工信用」のメカニズムを、過去の事例ではなく、現在進行形の社会で実体験の中で体感するというレアなチャンスも与えてもらったと思っています。

加えて、私を、「不正選挙」というものの数学的、統計学的な観点から検証してみたいという気持ちに導いた、という点においても、高く評価しています。

そして、**誰が見ても、文句の付けられない、不正の発生する余地のない、安全で簡単でスケーラブルな投票システムを作らなければならないという危機意識**は、私のみならず、世界中のブロクチェーン研究者、そして、有権者と為政者にも共有できたと思います。

これから50年くらいの間で出てきたであろう、ネット社会の厄介な問題(他の問題については、知らん)、たった4年間で出し尽くした(?)という点において、彼の功績は大きいです。

ドナルド・ジョン・トランプさん。あなたは私たち人類に対して十分に貢献されました。

その貢献はあまりにも十分すぎて ―― もう、**ずっと休んでいてもいいと思えるほどです**。

元大統領へのディスリスペクト、「これはよくない」

後輩:「**米国元大統領についての、ディスリスペクト（いわゆる、”ディスる”のこと） ―― これは『よくない』**」

江端:「そうかなぁ。炎上する？　自分では、（ブロックチェーンと選挙システムを不正と言い張り続ける元大統領は）なかなか良い組み合わせだと思っているけど」

後輩:「炎上をさせるだけの知性のある奴は、江端さんのコラムには群がってきません。その点での心配は必要ありません ―― が、問題はそこではありません」

江端:「というと？」

後輩:「江端さんのコラムは ―― それが江端さんの主観に基づくものであったとしても、そのベースはあくまで **証拠とロジックによって導かれたものである、という形を取ってきたということ**です」」

江端:「ん？　どういうこと？」

後輩:「今回のコラムでは、『江端さんが、心底頭に来ている』という雰囲気がビシバシ伝わってきます。しかし、米国国民の有権者のほぼ半数が、元大統領の『盗まれた選挙』を ―― その真偽や事実や証拠はどうあれ ―― 信じているということは、厳然たる事実です」

江端:「……」

後輩:「私は江端さんに、『元大統領の主張を真実として受け入れろ』と言っている訳ではありません。『**元大統領の主張を真実として受け入れている人がいるという事実**』を、事実として認定しろ、といっているのです」

江端:「……」

後輩:「江端さんの『エンジニアリングアプローチ』とは、証拠第一主義でもなければ、正義などという相対的な概念でもないはずです。江端さんのコラムは、いつだって、自力の調査による膨大な情報の収集に基づく『事実認定』からスタートして、そこから、独自のロジックを組み立てるもののはずです」

江端:「……」

後輩:「今回は、そのプロセスがすっぽりと抜けています。これは、江端さん（のコラム）らしくない、と思う。私が心配していることは、江端さんのコラムが、そこらへんに転がっている有象無象のコラムや評論と一緒くたにされることです」

江端:「ふむ……」

後輩:「それは、江端さん個人の問題にはとどまりません。**長年にわたって、江端さんのコラムのレビューし続けてきた、監修者としての私のプライドの問題でもあるのです**」

江端:「おい！　ここまで長々と語ってきたオチがそれか！」

後輩:「まあ、ともあれ、違和感を覚えたのは事実です。江端さんが「不正選挙」について論じたいのであれ、別のコラムで徹底的にやればいいのですよ―― それこそ、江端さんの大好きな法律論や統計学をふんだんに突っ込めばいいと思います。こういう形で語るのは、やっぱり『よくない』と思うのですよ、私は」

後輩:「とはいえ、今回の『ブロックチェーン投票』の話は、かなり衝撃を受けました。これ、選挙管理委員会の事務局を作ることなく、選挙が簡単にできるようになりますよね。町内会の選挙も、町内で2台以上のPCを選挙用に貸してもらえれば、足ります。なんなら、ラズパイでブロックチェーンのクラスタ組むだけでも良いです」

江端:「『草の根ブロックチェーン投票システム』だな」

後輩:「江端さんも記載されていましたが、この投票システムは、高校の生徒会選挙あたりから始めるのが、良さそうです。高校のマイコンクラブあたりが、自前でブロックチェーン投票システムを作れるようになったら ―― **日本の未来は明るい**ですよ」

江端:「スクラッチから作るのは、ちょっと難しいかもしれなしから、AWS(Amazon Web Service)あたりでパッケージ提供してもらえれば、まるっきり夢物語ではないかもしれない」

後輩:「それにしても、『ブロックチェーンという人工信用システム』を熱く語る江端さんは、『人間嫌い』なんだなーと、実感しますねえ」

江端:「人間全般が嫌いなわけじゃないぞ。私が嫌っているのは、自分の価値観に懲り固まって、一向に知見を広げようとしないくせに、無駄に権力だけは持っている、**無勉強のジジイたち**(特に政治家)だ」

Profile

江端智一(えばた ともいち)

日本の大手総合電機メーカーの主任研究員。1991年に入社。「サンマとサバ」を2種類のセンサーだけで判別するという電子レンジの食品自動判別アルゴリズムの発明を皮切りに、エンジン制御からネットワーク監視、無線ネットワーク、屋内GPS、鉄道システムまで幅広い分野の研究開発に携わる。

意外な視点から繰り出される特許発明には定評が高く、特許権に関して強いこだわりを持つ。特に熾烈(しれつ)を極めた海外特許庁との戦いにおいて、審査官を交代させるまで戦い抜いて特許査定を奪取した話は、今なお伝説として「本人」が語り継いでいる。共同研究のために赴任した米国での2年間の生活では、会話の1割の単語だけを拾って残りの9割を推測し、相手の言っている内容を理解しないで会話を強行するという希少な能力を獲得し、凱旋帰国。

私生活においては、辛辣(しんらつ)な切り口で語られるエッセイをWebサイト「こぼれネット」で発表し続け、カルト的なファンから圧倒的な支持を得ている。また週末には、LANを敷設するために自宅の庭に穴を掘り、侵入検知センサーを設置し、24時間体制のホームセキュリティシステムを構築することを趣味としている。このシステムは現在も拡張を続けており、その完成形態は「本人」も知らない。

本連載の内容は、個人の意見および見解であり、所属する組織を代表したものではありません。