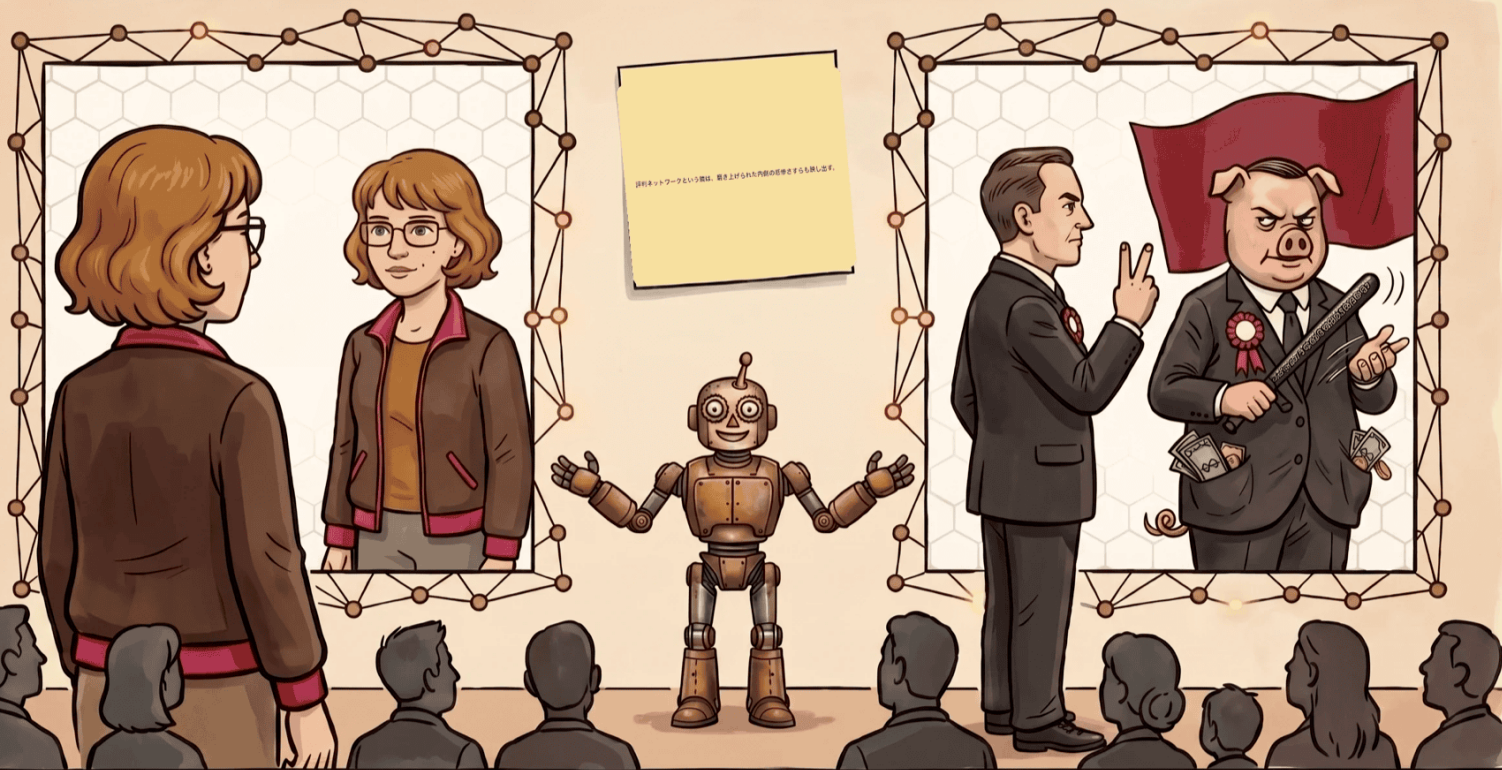


Personix



検閲不能かつ腐敗不能な分散型評判ネットワーク
国家の進化的後継者

Personix —妥協なき変革

検閲不能かつ買収不能な分散型評判ネットワーク

© 2025–2026 Pavel Kudrna, プラハ

バージョン 6 (2026-05-21)

初稿は 2025 年 6 月～11 月、2026 年 4 月～5 月に書き直し。

L^AT_EX (Tectonic) で Palatino と Helvetica Neue を用いて組版。
A5 横判 (210 × 148 mm)。

クリエイティブ・コモンズ表示-継承 4.0 国際 (CC BY-SA 4.0) のもとでライセンスされる —
creativecommons.org/licenses/by-sa/4.0/。留保される要素、ソースリポジトリ、および制作ツールについての注
記は本書の巻末に記載されている。

Contents

はじめに	7
この本は何についてのものか	9
変革のための不可欠な前提条件	17
変革のための不可欠な前提条件	17
ツール	27
評判に基づくソーシャルネットワーク	27
なぜネットワークは検閲不能なのか	51
当然の疑問に答える	53
技術への依存	53
ネットワークに公開することで私は金を窓から捨てているのか	53
誰かが複数のアイデンティティを作ったら	55
富める者は単により多くのアイデンティティを「買える」（あるいは仮想的な共同体を作る）のではないか	58
ただ読むだけで共同体に何も与えないフリーライダーはどうなのか	61
金銭的中立性	62

自発性、責任、そして自由	64
自由と全体主義のスイッチ（そして委任）	65
オラクル問題 — デジタル世界と物理世界を橋渡しする	72

検証はどのように機能するか 74

コンセンサスと検証プロセス	74
-------------------------	----

Roles in the verification transaction and authorities 80

役割の概観	80
発行者	82
権威	82
検証者	86
主体	88
オブザーバー	91
仕組み：タイムスタンプとチャレンジコード	91
落ち：本物のオブザーバーは要らない	93
委任	93
役割間のコミュニケーション	99

創発する社会契約 — 方針	99
-------------------------	----

自分についての情報を提供する	103
--------------------------	-----

犯罪と罰	104
犯罪と罰	104
金の流れを追え	116
金の流れを追う	116
国家の弱点 — 金	116
Proposed transition to the state's successor	118
革命ではなく進化	118
互いを支え合う四つのツール	120
単純な税制 — 入口の誘い	121
電子支出登録（ESR）	121
市民による税の配分 — 決定の重み	123
国家との交渉プラットフォーム — 梃子	127
身分証明書のない市民権	129
重なりと可逆性	132
結論	135
道は存在する	135
謝辞	137
インスピレーション	137

レビューとフィードバック	137
ツール	137

用語集	140
------------	------------

用語集	140
---------------	-----

はじめに

あなたは国家を頼れると感じているだろうか。

私や私の家族、あるいは私の共同体の誰かに明白な不正（身体的な危害、詐欺、不当な制限など）が加えられたとき、国家が「たしかに不正ではある、しかし何もするな、さもなくば我々ともっと大きな問題を抱えることになるぞ」と応じる — そんなことを私は受け入れない。そのような状態は病んでおり、それに従う人々は共犯者である。

その結果生じるのは、相互の疎外であり、共同体ごとであり、国家ごとであり、深刻な対立を予感させる社会のますますの崩壊である。

国家は技術と社会の変化のペースについていけるのか、それとも禁止を貼り付けるほうを好むのか。

停滞、無能、腐敗を、法の支配と伝統がもたらす公言された安定として扱うふりをすることもできようが、私はもうそうしたくない。それは自分自身への嘘であり、あなたへの嘘でもある。

自分が金を払っているものを批判しようとあえてしたとき、役人や選ばれた代表者たちの見下しを感じることはないだろうか。

私は、今日の国家に成文化された諸制度において選ばれた代表者となるための唯一にして十分な条件であるソフトスキルに秀でていないというだけの理由で、社会の人々を社会全体の規則を形づくるに値しないとみなすことを拒む。私は、大多数の人が自分自身、愛する者たち、そして自分の共同体の面倒を見ることができ、そこに自らの人生哲学の一片を見出していると信じている。私が周囲で知り合ってきた人々のほとんどはそうである。



納得できない。

しかし私は、まさにゲームのやり方を心得ていたがゆえに嫌な奴だった、正真正銘の嫌な奴たちにも出会ってきた — 共同体が彼らにフィードバックを与えることを許されないゲーム、国家が彼らを守り、国家のまさに本質を脅かすであろう秩序を誰も乱さないようにするゲーム。その本質とは、権力の階層とその制度の階層の上層階にいる者たちに楽な暮らしを保証することである。封建制は、ポピュリストとエリート主義者の支配に取って代わられた。

他人があなたの人生の生き方を指図してくるのが好きだろうか。

私は現状を完璧で最終的な所与として受け入れない。私は自分の振る舞い方に責任を持たねばならないが、それでも誰かが私にどの正しい価値観を抱くべきかと指図してくると、私は過敏になる。あなたはどうか。

この本は何についてのものか

自分でその を作りたい者が作れる（自分のアイデンティティを作れる）評判ソーシャルネットワークを想像してほしい。共同体のメンバーに招待されてもいいし、自分ひとりで飛び込んでもいい。あなたは自分の評判を築き上げ、必要なときには他者についての有用な評判データを引き出す。不正が起きたときには共同体の支援を求める — 自分の言い分を述べ、その件について手元にあるものを提示し、共同体はそれを見て、関連性に基づいて他者に伝えるべきかどうか、そして違反者をどう制裁するかを判断する。

この短い本全体は、外側でこれほど単純に機能するために、内側で何が必要ならなければならないのかについてのものである。最後まで付き合ってくれるなら、今は多くの点で複雑で理解しがたく見えるかもしれない世界が、より理解しやすく、より明確なものとして開けてくることを約束する。多くの悪いことが、悪い行為者にとってもはやそれほど不当に割に合わなくなるように設計できることが見えてくるだ

ろう。そしてそれは、四六時中オンラインに張り付いていなければならないようなツールではない — 必要だと感じたときに手を伸ばすだけで十分である。

さらに私は、ここに記した仕組みが人々の本当の動機により近く感じられること、そして何らかの主義の名のもとに人々を作り変える必要がないことを約束する。

そして最後に、共同体が再び完全に機能する社会単位となり、もはやただふりをしなくてもよくなる状態への、非革命的な移行をどう成し遂げるかを示す。

■ 技術論文

この本は、原典である技術論文『分散型評判ネットワーク：自発的で買収不能な社会組織のためのフレームワーク』（**Pavel Kudrna, 2026**）の解説的な伴侶である。形式的なアーキテクチャの記述、検証者選定アルゴリズム、および経済メカニズムの正当化に関心があるなら、そちらから始めることをお勧めする。

■ 各章は互いの上に積み重なる

本書は連続した議論として書かれている — 各章は前の章の上に積み重なる。一つの部で導入された概念は、脚注を含め、後の部で用いられる。順序を無視して読むことはお勧めしない。

■ この本は誰のためのものか

視覚的に親しみやすい体裁にもかかわらず、主たる対象読者は、人間社会のありうる社会・経済・政治的な仕組みの原理に関心を持つ、より専門的な読者である。この主題全体を最も広い一般の人々に平易に説明できる地点に到達するには、なお完全なコミュニケーション戦略を構築するための長い道のりが必要である。

この小さな著作、あるいはこれに続く改訂版を、より理解しやすくするための提案を歓迎する。

警告

私はあなたが誰なのか、いくつなのか、人生でどれだけ多くの破られた約束を耐え忍んでこなせばならなかったのかを知らない。私はここでそれをするのをやめた。代わりに私が警告したいのは、ここで学ぶことの唯一の帰結が、おそらく誰か他人があなたのために今日の混乱を片付けてくれる道など存在しない、という認識かもしれないということである。私はただ、その片付けをより単純で透明にし



この裏にはまだ続きがある。ついてきてほしい。

うるフレームワーク／ツールを記述しているにすぎない。それに基づいて、私は社会実験／シミュレーションの準備を試み、潜在的な欠陥を修正し、あるいは根本的な設計上の亀裂があると判明すればアイデアそのものを葬るつもりである。

お願い

この本を読み終えたあとも、このアイデアに対して開かれた心を保ち、それがどこへ向かい、実質的な批判にどう耐えるかを追ってくれるなら、私は深く感謝する。さらにありがたいのは、その後のあなた自身の関与である — 提案された均衡の原理をあなた自身のアイデアで打ち破ろうと試み、それによってこのシステムが現実の人間の振る舞いにどれほど備えているかをよりよく検証することである。

あなたとあなたの関与なしには、アイデアは引き出しの中の理論のままである。あなたとあなたの貢献と資金的な寄付なしには、私たちはこのプロジェクトを現実の社会実験へ、したがって現実の準備完了へと押し進めることができない。あなたとあなたの実質的な批判なしには、私たちは今いる場所で停滞するか、中道主義者たちの聖杯 — 絶対的で不可逆的な全体主義 — に飲み込まれるままとなる。どの道を選ぶか、あるいは傍観するかは、私たち次第である。

挑戦

私たちはあなたの肩に決して軽くはない荷を載せている。あなたはすでに、社会は中央集権的に運営されるのが最善だと主張するオカルト的で呪文めいた手引きを通じて、放漫に運営された社会のコストを負担している — それなのに私は、あえてさらに多くを求め、こうした傾向に逆らうよう頼む厚かましさを持っている。私たちが歴史上最大のねずみ講 — 賦課方式の年金制度 — の崩壊を、いくつもの世代を飢えさせることなく乗り切らねばならないことは承知している。

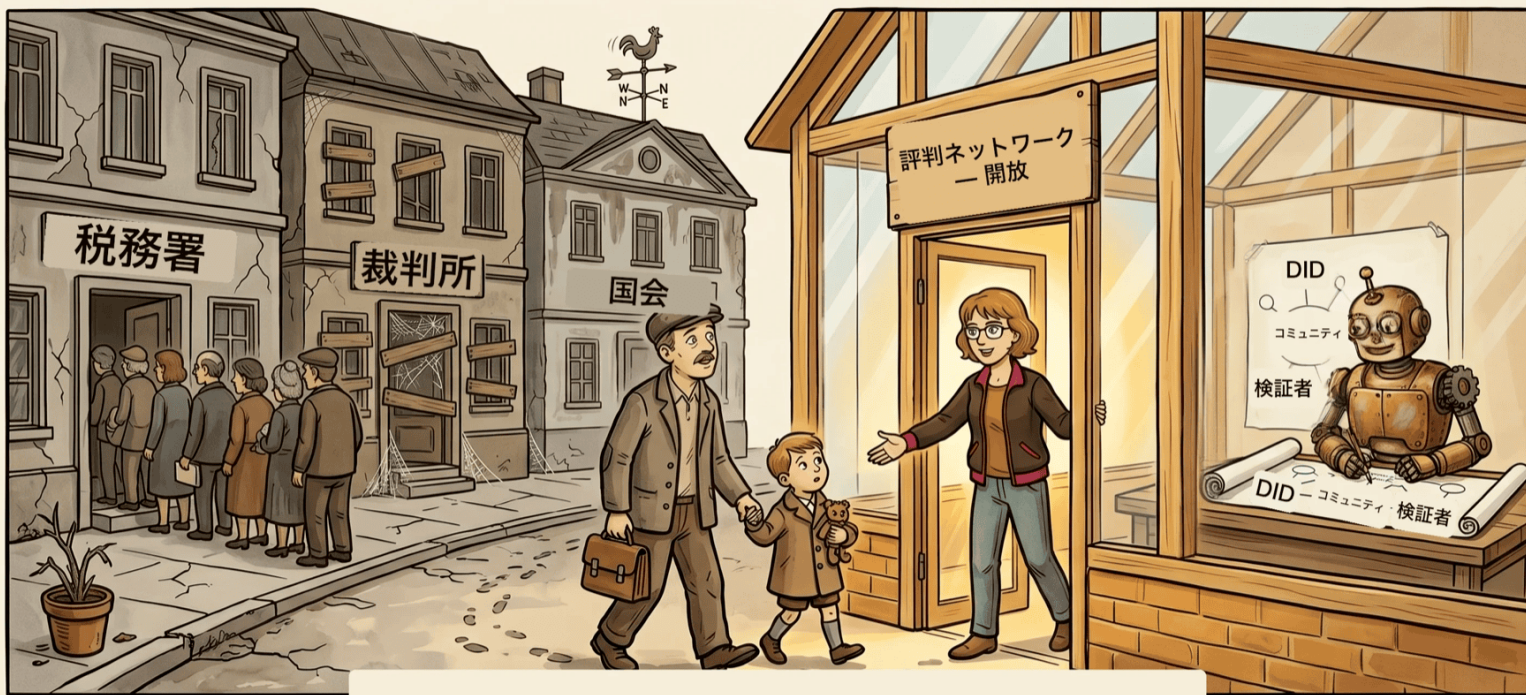
それでもなお私はあなたに頼む。私たちの子どもたちにようやくよりよい世界を手渡し、私たちがその変革をやり遂げたという遺産を残そう。経済成長を解き放つことは、地平線上に迫る苦境への部分的な解決策になりうる。そうすれば私たちは子孫に、それは途方もない旅だったし無駄ではなかったと語れる。



より良い世界にはその重みの価値がある。

■ 問題

直接的な責任によって釣り合いを取られた自由だけが、世界がかつて見たことのない巨大な潜在力を真に解放することができる。



どうぞ入って。計画はもう用意してある。

変革のための不可欠な前提条件

変革のための不可欠な前提条件

より良い方向への変革の根本的な前提条件は、従属する者が優位に立つ者になること — あるいは少なくとも対等なパートナーになることである。これは、優位と従属の関係を規定する最も重要な諸課題を引き受けることを意味する。これらの課題は、国家の市民を構成する諸共同体への帰属の証明に立脚している。それは情報であり、そしてそれらの共同体内で相当の評判を持つ権威によるその検証可能性である。

現行のシステムを乗り越えるために、私は五つの前提条件にたどり着き、それらを私が理解するやり方で説明する。これらの前提条件は、本書の残りの部分で記述されるシステムの構築を支える柱と考えることができる。私は最初、自分の好みで柱を選び、それらについて考えを巡らせながら、それぞれの理解を以下の形へと少しずつ精緻化していった。

これら五本の柱を一つずつ見ていこう。

変化のための前提条件

自発性



自発性

自分のことは自分で決める。

組織化



組織化

誰かの下ではなく、共に。

レジリエンス



レジリエンス

検閲できない。

合意



合意

圧力による妥協。

腐敗耐性



腐敗耐性

金銭を買収することはできない。

この5本の柱がなければ、どんな変化も時間の浪費に終わる。

■ 自発性

私たちの場合、自発性とは、私が分散型評判ネットワークの運営に参加することを強制されない、ということを意味する。しかし私は、ネットワークが私についての情報を記録しないという肯定的に構成された権利を要求することはできない — 私についての情報が評判ネットワークに載るかどうかは、私自身、私の振る舞い、私の行動、そして私の責任だけにかかっている。

■ 組織化

一人の個人ではシステムを打ち破れない。だからこそ国家は、自らの構造と機能を脅かしうる活動を防ぐ手段として、人々の結社を統制する。人々が賛成のために組織するか反対のために組織するかは問題ではない。組織化を通じて、誰かが国家をその意に反してあえて変えようとしたときの見せしめの罰の衝撃を和らげることができる。

共通の目標を掲げるのはやめよう。だが私たちは道の一部を共に歩むことはできる。最も自然な形は共同体における結社である — だがそれらは、単なる共同体ごっこにとどまらないよう、必要なすべてのツールを備えていなければならない。

■ 耐性

国家を変える — あるいはその後継への移行に向かう — ために選ばれた道は、国家の許可に依存してはならない。ツールとその使い方は、可能なかぎり検閲不能でなければならない。平たく言えば、それらを検閲するコストは天文学的でなければならない。それがなければ、あらゆる努力はただ時間と生命エネルギーを燃やすだけである。

前提条件 2/5:組織化

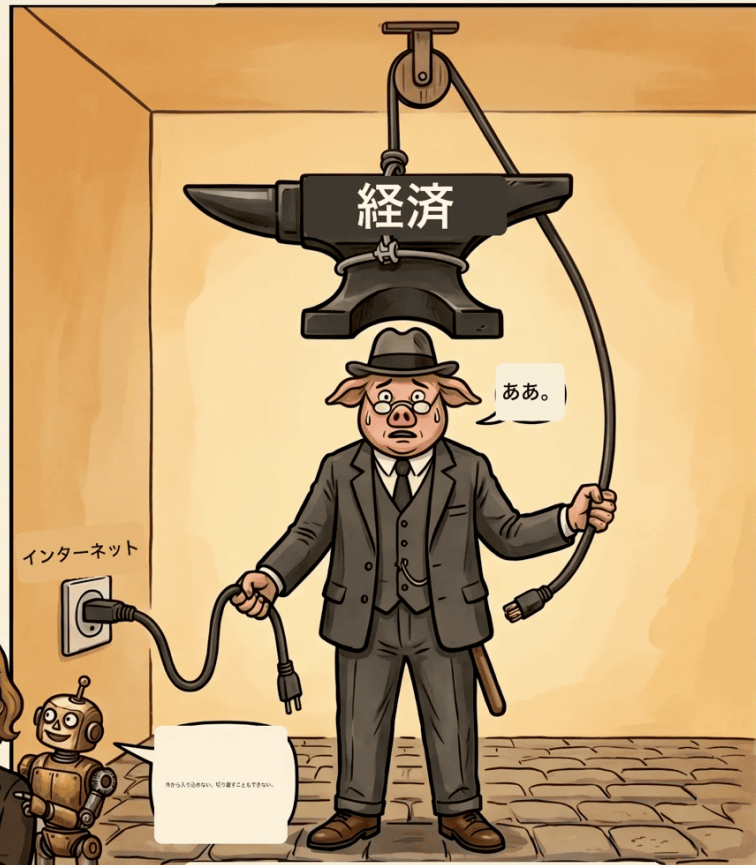


個人にはシステムを壊せない。コミュニティにはできる。

前提条件 3/5:レジリエンス



外部から検索することはできない。



プラグを抜けば —
自分自身を潰すことになる。

求める許可もなければ、抜くプラグもない。

■ コンセンサス

提案される解決策は、その本性上、コンセンサスを交渉する仕組みと、コンセンサスが破られた場合のための抑圧的な要素の両方を含んでいなければならない。それは自発的なウィンウィンの合意である必要はない。状況と社会的圧力が、共同体の内部で、また共同体どうしのあいだで妥協を確保するなら、それで十分である。

■ 買収不能性

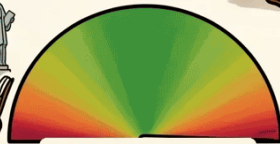
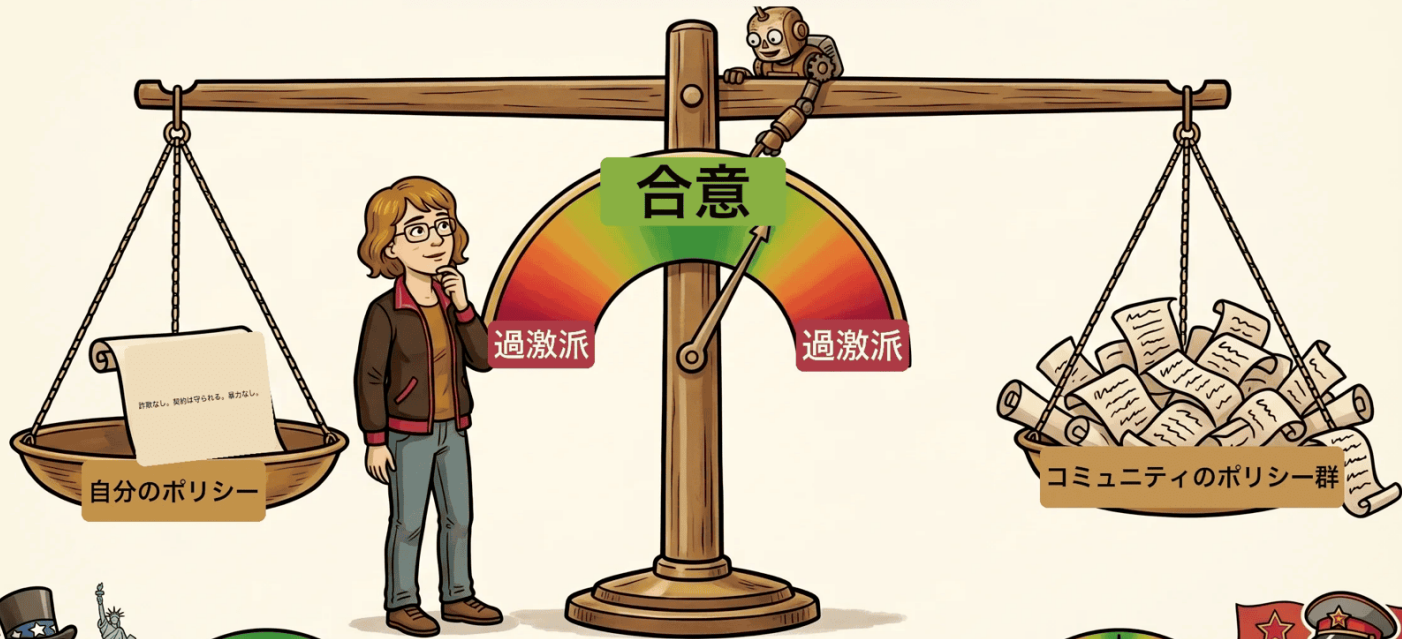
検閲不能性はシステムを外側から守る。だが人々のネットワークは内側からも腐りうる — 権威が乗っ取られ、公言された規則がひそかに放棄され、参加者が黙って買収される。もし内側の人々が結果を伴わずに墮落しうるなら、検閲不能性は虚しい勝利となるだろう。

買収不能性は、単一の巧妙な仕掛けの結果ではない。それは、**提案された設計のいくつかの原理が協調して働くこと**から創発する — 腐敗に抗する圧力はアーキテクチャ全体に分散され、個々の部分が互いを補強し合う。これがどのように達成されるかは、少しずつ示していく — ツールの記述において、検証において、そして罰の章において。最後に、積み上げられてきたすべてを振り返る。

買収不能性は、設計の前提条件であると同時に、結果として現れる創発的な性質でもある。それは第二の防御線 — 内側に向いた防御線 — であり、それがなければ耐性は半分の盾にすぎない。

範囲にとどまれ — 過激派にはなるな。

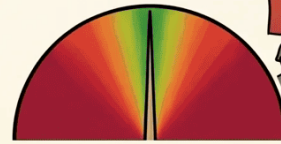
違っていてもいい。ただし、あまりにかけ離れていなければ。



自由な社会

許容範囲は文化の自由度に応じて広がる。

前提条件 4/5: 合意



権威主義社会

合意とは許容範囲であり、全会一致ではない。

前提条件 5/5:腐敗耐性



上層部を少し買収すれば済む —
土台はどのみち払わされる。



一人買収すれば — 彼は評判を永遠に失う。全員買収しようとするれば — 先に破産する。

腐敗には値段がある。このメッシュではあまりに高すぎる。

ツール

評判に基づくソーシャルネットワーク

変革をもたらすには、注意深く設計されたツールが必要である。まずそれを簡潔にスケッチする。後の章では各部分をより詳しく検討し、さらに肉付けしていく。検閲不能でグローバルな分散型ソーシャルネットワークを想像してほしい。そこであなたは、自分の代理となるアイデンティティ — いわゆる分散型アイデンティティ（DID） — を安全に作成し管理できる。DID とは、いかなる中央権威にも依存せず、あなた自身が作成し管理するデジタルアイデンティティである。それはあなたの秘密（あるいはマルチシグによる複数の ）で暗号的に署名されているため、誰もそれを奪ったり偽造したりできない。

あなたのアイデンティティ、あなたの鍵、あなたのルール

自分自身で作る

秘密鍵 — あなたに代わって署名する。保持するのはあなただけ。決して共有しない。

公開鍵 — あなたの署名を検証する。ネットワークに公開されている。



登録窓口も、行政書頼も、企業の承認も不要。自分自身で生成する。

あなたのDID文書

申立て — あなたについて検証された事実



DID文書

公開鍵:[暗号ハッシュ]

ネットワークアドレス:[オニオンゲートウェイ]

検証ポリシー:やり取りに関する自分のルール

申立て:右を参照

国籍:チェコ共和国 —
市公証人により検証済み

学歴:情報科学修士 —
大学同窓ネットワークにより検証済み

資産:アパート42号室の所有者 —
地域コミュニティ登記により検証済み

傍観者:不正行為を見過ごした —
ポリシー違反 —
近隣住民証人による申立て

詐欺:隣人の貯金をだまし取った —
地域コミュニティ裁判所による申立て

国家はこれを取り消せない。

申立てとは検証済みの陳述だ。良いことも悪いことも、権威はそこに自らの評判を賭ける。



国民ID —
取消可能:国家はいつでも無効にできる。



DID —
取消不能:変更に署名できるのは自分の秘密鍵だけ。

あなたのアイデンティティ。あなたの鍵。あなたのルール。許可は不要。

■ 注記

ひとつの含意は、そのようなアイデンティティが国家発行の身分証明書を徐々に置き換えるということである — だがそれについては移行の章で詳しく述べる。

そのようなネットワークでは、あなたは自分のアイデンティティを通じて、誰かがあなたに危害を加えたと報告できる（そして後には、その者がそれを是正した、あるいは是正を強いられたと報告できる可能性もある）。このフィードバック — 危害の発生源に向けられたもの — が関連する情報源として価値を持つためには、ネットワークへの情報の入力に時間、エネルギー、そして金がかからなければならない — その上で、これがただの無駄話ではないことを他者に対して検証可能な証明として生み出さなければならない。

情報を読むのは容易で比較的安価だが、個々の記録を作成するのはコストがかかり要求が厳しい。書き込みは明確なプロトコルに従う。そこでは選ばれたアルゴリズムに基づく計算が、提出された情報の検証をどの **DID** に求めるか、そして選ばれた参加者があなたに代わって情報を処理し、公開し、その検証者となるようにどう進めるかを厳密に決定する。

■ アルゴリズム対過激主義

検証者のアルゴリズム的な選定は、過激でない情報公開者が時間とともに、公開された情報のコストと検証への報酬のあいだでほぼ中立的な均衡を保つことを保証する。

公開には時間、エネルギー、お金がかかる

ネットワークへの書き込みは決して無料ではない — 読み取りは無料だ

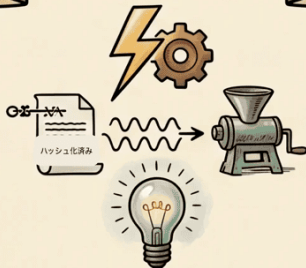
3つのチャンネル — すべてが現実のもの

時間



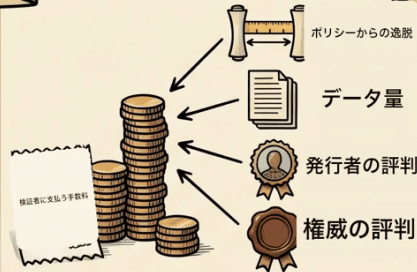
アルゴリズムが検証者を選び、検証者が記録を読む間、あなたは待つ。

エネルギー



署名、ハッシュ化、検証 —
どの段階も現実の計算であり現実の電力だ。

お金



中定でが検証者のポリシーから離れているほど、記録が大きいほど、発行量やその権威への信頼が低いほど、手数料は高くなる。

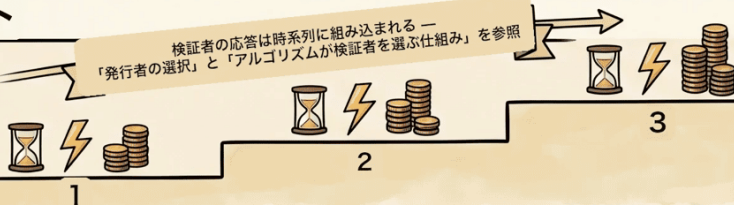
次に起こること

「アルゴリズムが検証者を選ぶ仕組み」、「検証者の選定方法」、「発行者の評判、権威の評判」

なぜ高価な書き込みが評判を守るのか
— この章の後半で

反復ごとのコスト

再試行のたびにコストは上がる



却下や再抽選のたびに、アルゴリズムが取り込む時系列が増える — そして次の試みは3つのすべての面でより高つく。

読み取りの非対称性

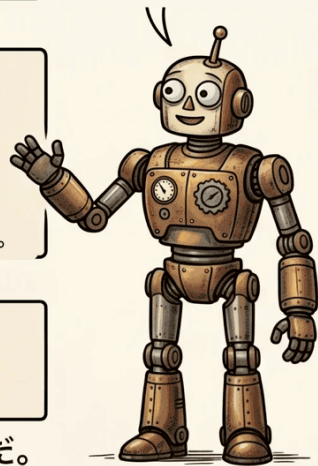
読み取りは安価



問い合わせは無料

誰でも評判と記録を読む — コストがかかるのは書き込みだけだ。この非対称性が設計そのものだ。

書き込みにはコストがかかる — 読み取りにはかからない。この非対称性こそが要点だ。



アルゴリズムがどのように検証者を選ぶのかを見てみよう。

■ アルゴリズム

アルゴリズム的な選定は、異なる情報片ごとに非決定的に別の検証者（あるいは可能な検証者の集合）を選ぶ。完全な **DID** 文書のハッシュ（任意の入力から一意な「指紋」を生み出す一方向の数学関数 — 文書の指紋のようなもの）が、一貫性ハッシュリング上の位置を決定し、検証者の候補を選ぶ。

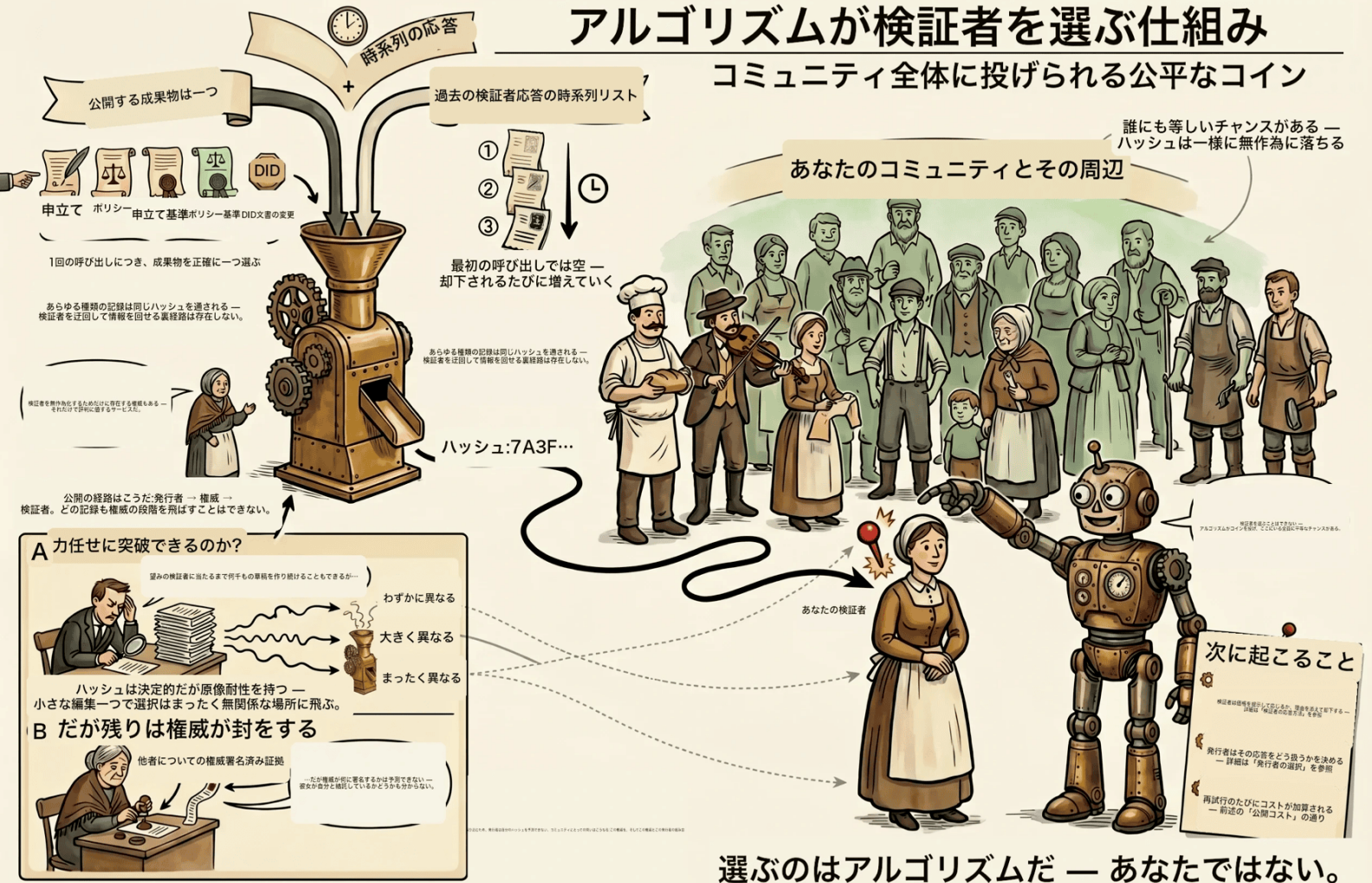
$$\text{verifier_DID} = \text{hash}(\text{DID_document})$$

平たく言えば、アルゴリズムはあなたの **DID** 文書全体を取り、そこから指紋を計算し、その指紋があなたの検証者を決定する。

アルゴリズムが選ぶ最初の検証者では、公開者としてのあなたはうまくいかないかもしれない — あなたの評判や公言した設定が、その検証者の要件を満たさないことがある。あなたはアルゴリズム的に次の検証者の探索を続け、さらなる再帰的な反復を実行する。それはあなたにもう一人の検証者を割り当てる。各ステップごとに、目標の検証者までの「距離」は大きくなり、公開しなければならない付随メタデータも増えていく。データが増えるにつれ、コストは自然に上がる（当初の主張の大きさのためだけでなく、拒絶のたびに蓄積するメタデータのためでもある）。信頼できる情報は、ばかげた思いつきよりもはるかに容易に通る。どれほど高い代価を負う覚悟があるか、その記録が自分にとってどれほど重要かは、各人次第である — 過激主義は間違いなく高くつく。

アルゴリズムが検証者を選ぶ仕組み

コミュニティ全体に投げられる公平なコイン



検証者の応答方法

価格付きで受理 — または理由付きで却下



却下 — 理由付きで



- 発行者の評判が自分には低すぎる
- この記録の背後にある権威は信頼していない
- 発行者のポリシーが自分のものとかけ離れすぎていて橋渡しできない
- 文書そのものが自分のポリシーのルールを満たしていない

検証者は理由を書き記す — その応答が次の試みへのフィードバックになる。

受理 — 価格付きで



検証者は公開に同意する —
だが価格は、その申立てが自分のポリシーからどれだけ離れているか、どれだけデータを含むか、発行者がどれだけ信頼されているかを反映する。

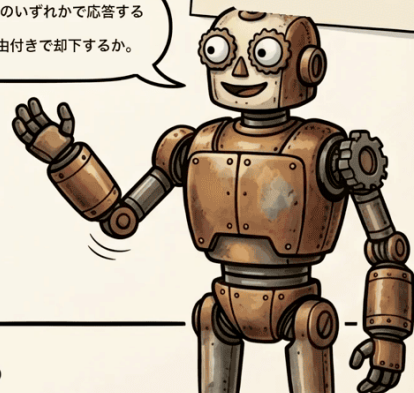
検証者の応答は時系列リストに追加される —
詳細は「アルゴリズムが検証者を選ぶ仕組み」を参照

検証者が何を言おうと、その応答は次の呼び出しへの入力になる。

すべての検証者は次の2通りのいずれかで応答する —
価格付きで受理するか、理由付きで却下するか。

次に起こること

- ⚙️ 発行者はこの応答をどう扱うかを決める — 詳細は「発行者の選択」を参照
- ⚙️ 応答のために次の試みのコストが変動する — 前述の「公開コスト」の通り



検証者は価格を設定するか、なぜ駄目かを教える。

あなたの検証要求に応じて検証者が何を決めようと、ボールは公開者のコートに戻ってくる。公開者は、検証サービスに対する検証者の申し出を受け入れることも、その応答を時系列に折り込んでより高いコストで再度試みることも、あるいは立ち去って埋没費用を飲み込むこともできる。

自分の情報により大きな重みを与え、検証者に受け入れられる可能性を高めるために、あなたは — 発行される情報に利害を持つ公開者として — **信頼された権威**のサービスを利用できる。権威は提出された情報を拒否するか、あるいはそれを受け入れて自らの名声（評判）を賭ける。権威は通常、現実世界の証拠を要求し、それを検証し、分類する。その出力は、与えられた時点における与えられた事案についての、権威による評価のプロトコルである。権威とは、現実世界とデジタル世界の双方における、ある種のサービスの専門家だと考えてほしい — たとえば調査員、監査人、保険業者、ある種類の財の供給者（要するに、市場における任意の経済的行為者）である。

発行者の選択

検証者の応答をどう扱うか

検証者が何を言おうと、発行者の手元には一つの応答がある。



「アルゴリズムが検証者を選ぶ仕組み」に戻る
— 前述の通り

ループするのは再試行の経路だけだ — 受理と撤退はどちらも話を終わらせる。

3つの選択肢

取引に応じる

DIDネットワーク



受理された場合のみ

発行者が手数料を支払う —
記録がネットワークに公開される。検証者が受理した場合のみ可能。

再試行する



小型の力任せ生成機



応答が暗号列にまとめられ、アルゴリズムが再び投げる。検証者が発行者の意に沿わない価格で受理した場合でも、完全に却下した場合でも機能する。

手を引く



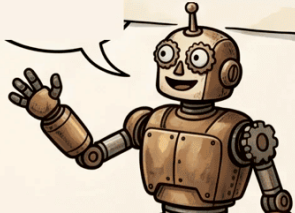
すでに費やした労力とエネルギーは戻ってこない

発行者は草稿を放棄する。何も公開されないが、それ以上の支払いもない。

次に起こること

再試行のたびに次の試みのコストが変動する
— 前述の「公開コスト」の通り

検証者の応答そのもの —
前述の「検証者の応答方法」の通り



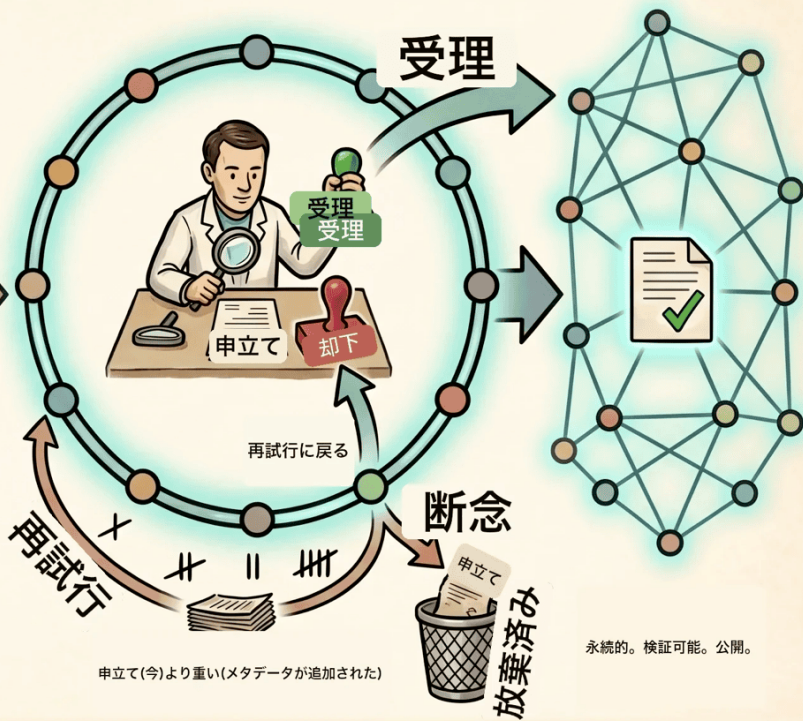
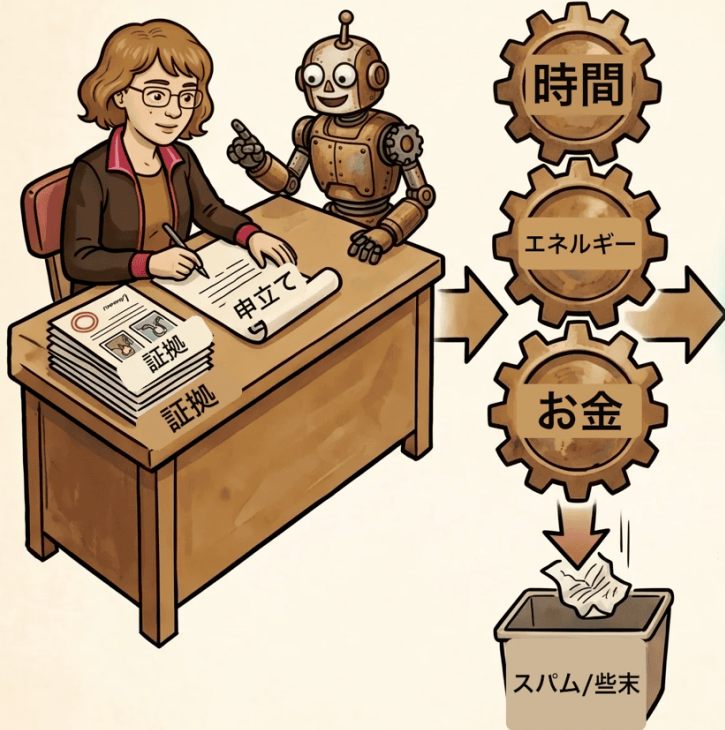
検証者が提案し、発行者が決定する。

段階1 —
申立てを公開する

段階2 —
品質フィルター

段階3 —
再帰的検証

段階4 —
永続記録



偽造は高コスト。検証は低コスト。

あなたが情報をネットワークに公開しようとするところには、ネットワークにはおそらくすでにその行為者たちについての情報が含まれている — これらは評判シグナルである。評判シグナルをどう読むか — それが異なる状況であなたにとって何を意味し、どんなリスクを伴うか — をつかむのは、簡単ではないかもしれない。各参加者は、相手方に関して自分が対処している状況に応じて、自分の **DID** を通じて評判記録を異なる仕方で見ることができる。相手方は信頼できる支払人か、それとも取引のために前金を要求する必要があるか。提示された製品には、隠れた詐欺や欠陥についてのレビューが付いているか。何か問題が生じたとき、相手は契約上の責任から逃れようとしているか。ときには、相手方の全体的な一貫性についてのより複雑な見方が役に立つ — それは概観を要求する者の好みによる。市場は、目下の状況の文脈における評判の読み取りを単純化し、処理し、明確化する製品やサービスを提供しうる。さまざまな権威とその提供サービスも、この目的に資することができる。

評判の読み方

情報に基づく判断



彼女は自分が誰と取引しているかを知っている。

与信する前に。署名する前に。信頼する前に。

盲目的な信頼



彼は自分が誰と取引しているのか分かっていない。

■ 例

公開者にとって関心があり — 他者にとって価値がある — 典型的な情報は、現実世界あるいは仮想世界における通常の対人コミュニケーションを超えた出来事に関わる。

否定的な例： - 犯罪行為の証拠（例：信頼された調査機関によって監査されたもの） - 間接証拠（単独では弱い、統計的に累積する） — 例：短期間に複数の窃盗の近くに繰り返し居合わせた → それでも偶然か？ - 契約違反

肯定的な例： - 是正された危害（自発的に、あるいは罰として共同体からの圧力のもとで） - 権威 **X** が提案した罰の受諾とその履行 - 権威 **X** が、ある程度まで加害者の財産権の承認を取り消した

相手方について入手可能な情報を集め、自分の好みに応じてリスクを評価するのは、各人次第である。

■ あなたについての情報がネットワークに現れるかどうかは、もっぱらあなた自身の振る舞いにかかっている。

あなたはそのようなネットワークに決して加わる必要はないが、それでもあなたについての情報はそこに現れうる。それはもっぱらあなたの行動と、それが他者に与える影響にかかっている。

どんな種類の申立てがあり得るか？

申立て成果物の例

(申立てとは誰かについての陳述だ)
— 人々が公開する種類を挙げる。)

一 否定的な申立て



暴行
他者に対する身体的暴力



窃盗
同意なく他人の所有物を奪った



詐欺
私利のために他者を欺いた



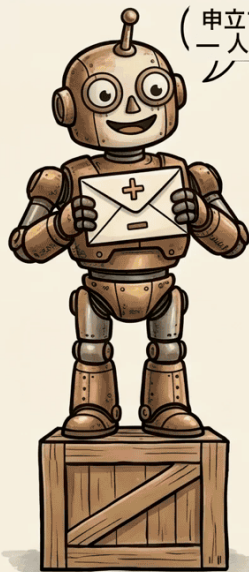
契約不履行
合意した義務を果たさなかった



名誉毀損
有害な虚偽を広めた



遺棄
扶養家族や義務を放置した



+ 肯定的な申立て



損害の是正
以前に与えた損害を修復した



債務完済
負っていたものを全額支払った



支援の提供
自らの負担で他者を助けた



検証済みの専門技能
技能や分野における実証された技術



傑出した貢献
コミュニティへの長年の貢献

あくまで一例 — すべての申立ては申立て基準に従い、基準はさらに項目を追加できる。

参加する必要はない — だが自分の行動が他者に影響するなら、誰かがそれについて申立てを公開できる。

申立てとは、行動がネットワークに入る仕組みだ。

コミュニティがあなたの代わりに開設できる



彼は自分のDIDを持っていない。登録したことがない。



DIDを開設しなかったので、コミュニティがあなたについてのDIDを開設する。否定的な申立てはここに紐づく。



自分で開設することはできる。だがコミュニティは同意を拒否する。評判は鍵ではなく本人についてまわる。

1. 加害する -----> 2. コミュニティが申立てる -----> 3. 逃げられない ->
DIDを開設しないことは選べる。だが自分の評判から逃れることはできない。

私が今しがた簡潔にスケッチしたのは、分散型アイデンティティ（**DID**）に触発されたソーシャルネットワークがどのように機能しうるか、である。**DID** という概念の第一の目的は、自分が従い生きていく規則に加入するという原理を通じてプライバシーと自由を強化すること — ユーザーにどの情報をどんな条件で共有するかを決める能力を与えることである。

私はさらに、**DID** を通信ネットワークへと連結し、その保有者たちが、誰かに何かが起きて共同体や個人が反応する必要がある状況を超えてもフィードバックを交わすことを提案する。私たちが加入した規則をあらかじめ比較すること — 相手方がどう振る舞うべきかについての期待の相互の食い違いがもたらす経済的その他の帰結を計算できる選択肢とともに — は、コンセンサスを見出す動機と見なせる。自由の代わりに、そのようなシステムは、現実世界の振る舞いに対する責任と結びついた自発的な意思決定を強調する。

個人は一人ではシステムを打ち破れない — 人々の集団のほうが大きな見込みを持ち、多くの問題で交渉されたコンセンサスと足並みをそろえる動機を持つ人々の集団は、権威主義的な傾向に抵抗するうえでさらに大きな見込みを持つ。第一章で挙げた組織化の前提条件は、二つの条件が満たされたときに達成される。**DID** 評判ネットワークが、その利用がもはや珍奇でなくなる程度に十分に代表的な形で諸共同体を覆うこと。そして同時に、この共同体セグメントが、社会の残りの部分と毅然として交渉できる、経済的に有意義な少数派となることである。

■ 自発性対自由

自由は — 肯定的な意味における自由は — 二つの要素、すなわち自発性と、責任へ向かう周囲の圧力を釣り合わせることの二次的な効果となるだろう。

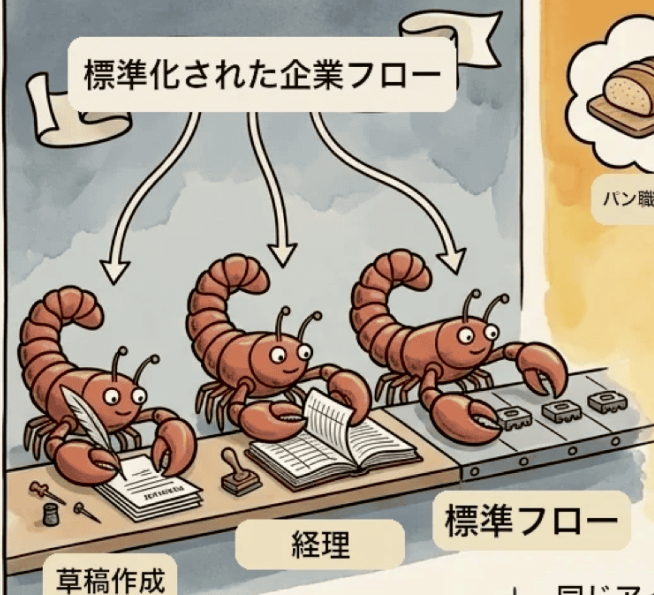
■ AI の時代と評判の価値

人工知能の時代には、認知的思考に結びついたすべてが自動化されつつある — そしてそれはさらに先へ進むかもしれない。では人間の活動において競争優位として残るのは何か。その答えは難しく、何かはきっと見つかるだろうが、確実に言えることが一つある。評判が決め手になる、ということである。あなたの振る舞い、約束とその履行の検証可能な履歴 — それは **AI** があなたのために築いてはくれないものである。

AIが思考を担うなら — あなたに残るものは何か？

AIエージェントが反復作業を引き継ぐ

標準化された企業フロー



草稿作成

経理

標準フロー

反復的な知的作業は、一つずつエージェントへと引き渡されつつある。

では人間に残るものは何か？



パン職人

アイデア

大工

AI工房を営む

同じアイデアは誰でも選べる。

あるパン職人、大工、AI工房を、隣の同業者と違うものになっているのは何か？

評判 — 二つを分けるもの



約束を守る

顧客と対話する

自分のAIの責任を負う

10年、無苦情

これは自分にすら代わりにつれない
— 果たした自覚でなければならぬ。

取引を成立させるのは今も人の手だ。

エージェントの行いには誰かが責任を負わなければならない
— その責任は譲り渡せない。

評判がなければ、どのパン職人も同じに見える — そして最大手のブランドが全員を飲み込む。

これこそがAIを制御下に置く分散型の道であり、たった一つの主体が市場全体を握るのを防ぐものではないか？

AIが作業を自動化する — 評判があなたを人間らしくとどめる。

真実の経済学

コミュニティ帯



一つのコミュニティ。異なる立場。

不人気だが許容範囲



合意の内側



合意の外側



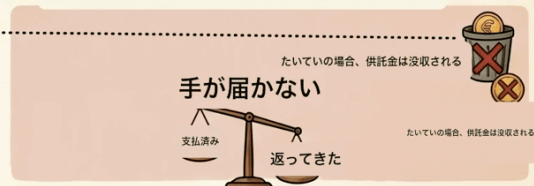
提出

抽選



返金

台帳



下部の観客者帯

アルゴリズムは公平に選ぶ。人は自分の信念に値段をつける。

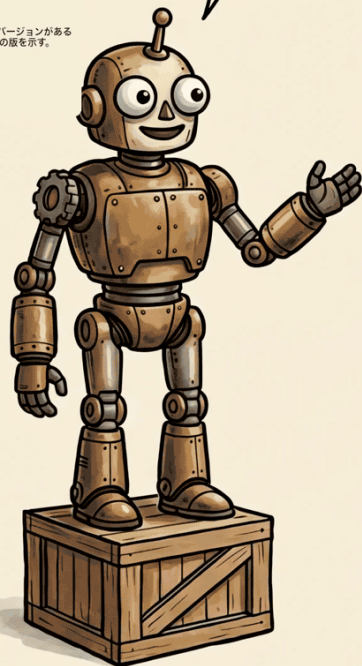


抽選は一樣。反応は一樣ではない。合意から離れるほど、価格は高くなる。

ネットワークに公開されるもの

公開できるものは5種類 —
どれもバージョンを持つ。

すべての成果物にはバージョンがある
— バージョンは現在の版を示す。



v1

DID文書

ネットワーク上のあなたの身元記録 —
鍵、メタデータ、ネットワークアドレス。

管理者: DID保有者



v2

申立て基準

申立てが従うべき様式 —
何が有効な証拠とみなされるか。

管理者: その分野で評判を持つ権威



v3

ポリシー基準

ポリシーが従うべき様式 —
— 受理ルール の形。

管理者: その分野で評判を持つ権威

↓ 由来

↓ 由来



v4

申立て

申立て基準に従った、主体についての陳述 —
発行者が公開し、発行者と検証者双方が求めれば基準の権威が運営する。

管理者: 発行者が公開 —
— 主体が対象

申立てには2種類ある —
肯定的(+)と否定的(-)。



v5

DIDポリシー

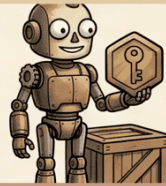
DIDが宣言したルール —
検証、合意、発行に使われる。

管理者: DID保有者 (DIDごとにポリシーは1つ)

すべての成果物にバージョンがある。すべての版が公開される。

DID文書の中身は？

DID文書成果物の例

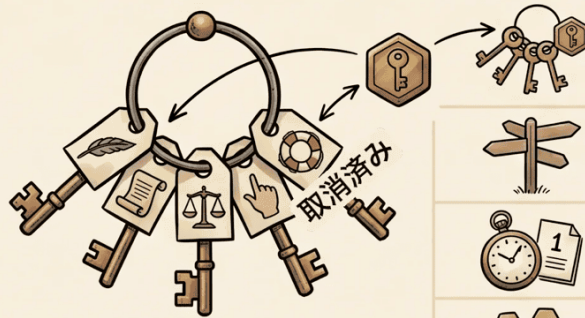


DID文書はネットワーク上のあなたの身分証だ
— その中身を見てみよう。

内部にある項目

鍵と署名ルール

各鍵は一つの権限を与える —
この文書を編集する、申立てを発行する、権威として振る舞う、ポリシーを管理する、回復を委任する。権限は別のDIDに譲渡でき、後で取り消すこともできる。



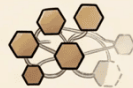
ネットワークアドレス

ネットワークがあなたに到達できる場所 — アイデンティティを書き換えずに変更可能



作成日とバージョン

このアイデンティティが最初に現れた時期と、今読んでいる版



紐づいたアイデンティティ

つながっているDIDの要約 —
便宜的な表示で、技術的には別の場所に保存される

継承マーカー

アイデンティティを失った、または盗まれた場合、権威がこのDIDを終了とマークし、後継者を示すことができる



DID保有者が各新版を書く —
だがどの版もネットワークが公開する前に検証を通過しなければならない。

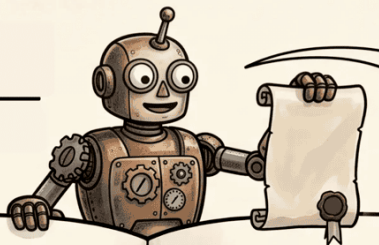
自分で書く — ネットワークがそれを検証する。ただ公開するだけで存在を作り出すことはできない。



あなたが自分のアイデンティティを著す — ネットワークがそれを確認する。

申立て基準とは？

申立て基準成果物の例



基準とは空の様式であり、申立てとはその様式に記入したものだ。両方を並べて見せよう。

基準 — 空の様式



主体のDID

この申立ての対象となるDID



発行者のDID

申立てに署名するDID



いつ、どこで

日付と場所



承認された証拠の種類

これらの種類の証拠のみが有効



結果の尺度

一段階だけを選ぶ — 自由記述は不可

申立て — 記入済みの様式



主体のDID

did:nwo:alice-9f2b...



発行者のDID

did:nwo:magistrates-04...



いつ、どこで

3月3日、市場広場



承認された証拠の種類

写真 ✓ — 証人の宣誓 ✓ —
医師の診断書 ✓



承認された証拠の種類

中程度 — 4段階中2段階目

左側の各項目には右側にちょうど一つの記入済みの対応がある — これが同種の申立てを比較可能にする。

記入済みの申立てに押される権威の印は誓約だ：手続きが本当に守られたという。



これが基準通りに処理されたことに、自分の印を付ける。

暴行 v3



債務 v2



医療支援 v4



職人技 v1



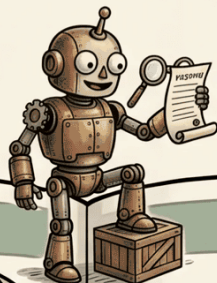
証言 v5



基準とは様式であり、申立てとは記入され誓約された様式だ。

DIDポリシーとは？

DIDポリシー成果物の例



それは重要な注意だ。自分のポリシーが決めるのは、そもそもその申立てを認めるかどうかを判断した上で決める。その結果の否決にある権威を行使する。そしてその内容は重要を扱う範囲があるもの。

基準 — 継承された初期設定

ルール名



発行者評判の下限

評判が10点中5点を超える発行者を受け入れる



権威の信頼リスト

評判が10点中4点を超える権威の基準を受け入れる



実質性フィルター

『些末』の基準を上回る重みを持つ申立てのみを処理する



スパム防止の価格曲線

実質的で稀な申立ての提出は安価だが、些末で繰り返される申立ては急速に高くなる



複合的な重み付け

発行者評判と権威評判を掛け合わせる。些末な内容なら結果を半減させる

ポリシーは基準を書き換えない — 人と事案を判断するものだ。維持、変更、削除、追加 — 共通の出発点に対するこの4つの単純な操作がすべて。

自分のポリシー — そこから派生

ルール名



維持
チェック



変更
動作語



削除
動作語



追加
動作語



発行者評判の下限

厳格化 — 10点中7点を要求する



権威の信頼リスト

出資者も信頼は必要だが、市の監視下にある申立ては基準を半減させる。権威者の信頼のものはいち受け付けられない



実質性フィルター

些末な迷惑申立てを無視するコストはゼロ — 単に読まないだけで



スパム防止の価格曲線

維持 — 初期設定の曲線で問題ない



複合的な重み付け

削除 — 自分独自の計算式を使う



繰り返し申立てへの指数関数的コスト

同一発行者から自分についての新しい申立てが頻りに来るたび、コストは前期の10倍になる



静穏時間帯

追加 — 深夜から夜明けの間に提出された申立ては一切読まない



検証 — 自分のポリシーは受信する申立てで、実行前の自分の事前の両方をフィルタリングする。実行とは出て行く方向の検証だ。

合意 — コミュニティが共通のルールを交渉するとき、自分のポリシーが自分の一票になる。

あなたのポリシーが判断するのは様式ではなく、伝える者だ。



なぜネットワークは検閲不能なのか

これまで私たちはネットワークが何をできるかを記述してきた。今度は、それがなぜ停止させられたり検閲されたりできないのかに焦点を当てよう。

ネットワークはおそらく、**Tor** ネットワークとオニオンルーティング（**Mixnet** の原理を用いてネットワークトラフィックを覆い隠す方法）の原理の上に構築される — 通信が複数の暗号化の層を通過し、いかなる単一のノードも送信者と受信者の両方を同時には知らないという技術である。中央機関はあなたの肩越しにのぞき込むことができない。のぞき込む場所がどこにもないからである。

あなたはそれと戦うことはできるが、勝つことはできない — 国全体を、個々のネットワークパケットのレベルで、そしてインターネットに接続し当該の評判ネットワークで通信するあらゆるハードウェア上の低水準の動作のレベルで、全体主義的な監視へと突き落とさないかぎり。そしてそれこそが中央集権主義の直面する選択である。市民があなたの手の届かないツールを持つことを受け入れるか、それとも全体主義的統制の名のもとに経済的停滞の暗い片隅へと自らを掘り進めるか。

幻想を抱くのはやめよう — 民主的な体制ですら、中央集権主義のための戦いにおいてこれを試みるだろう。彼らは権力を手放すくらいなら、人々に鎖をかけるほうを選ぶ。

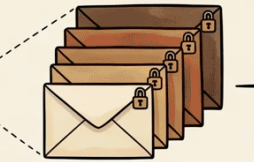
あなたのメッセージが追跡不能であり続ける仕組み 同時に働く2つの防御線 — 層と雑音

内容:層に包まれる

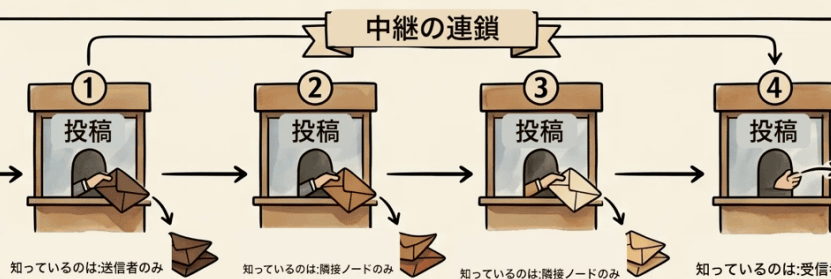
(Torの背後にある技術 — 『オニオンルーティング』)



送信者



4つの錠、4つの鍵 —
ノードごとに一つ。

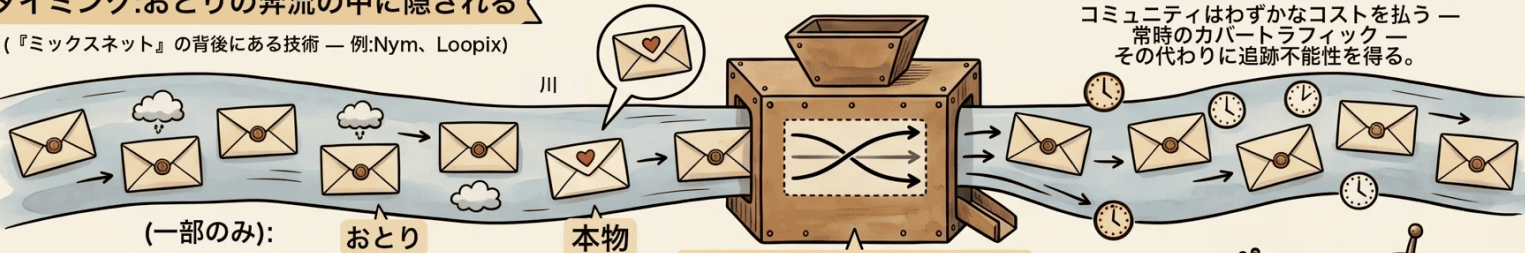


受信者

会話の両端を見られるノードは一つもない。

タイミング:おとりの奔流の中に隠される

(『ミックスネット』の背後にある技術 — 例:Nym, Loopix)



2つの盾が共に

マトリックス 誰⇄誰を隠すか? → いつを隠すか?

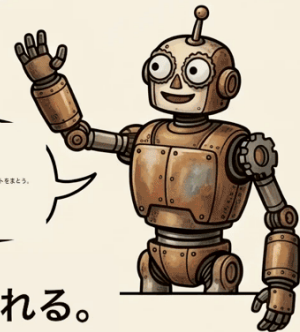
層のみ	✓ はい	✗ いいえ
雑音のみ	✗ いいえ	✓ はい
層+雑音	✓ はい	✓ はい

(オニオンルーティング+ミックスネット — 必要な組み合わせ)



1時間に100通の封筒
—
どれが本物なのか?

観察者は流れを見ることができるが、本物とおとりを区別できない。



内容は層によって隠され、タイミングは雑音によって隠される。

当然の疑問に答える

記述したシステムは当然ながら多くの疑問を呼び起こす。最もよくあるものに答えよう。

技術への依存

あなたはおそらくすでに気づいているだろうが、近代国家 — 私たちと約 **150** 年ともにある — とは異なり、ここに記述した評判ネットワークの解決策は、グローバル／ローカルなインターネットの技術に大きく依存している。障害が起きた場合、そのようなネットワークの機能は危険にさらされる。

障害が一時的なものであれば、データの喪失もネットワーク内の主張の一貫性の喪失もなく、諸共同体の内部で達成された評判の均衡も乱されないはずである。比較しうる決済ネットワークとは異なり、このネットワークはプロセスとデータ項目の非常に低い頻度を前提とする。この点で分散型評判ネットワークは、今日の国家と変わらない。国家もまた今や技術に大きく依存しており、紙のカード式ファイルの扱い方を忘れてしまっている（もっとも危機計画においては、そうする以外に選択肢がないだろうが）。

評判ネットワークという形態を取る国家の進化的後継は、恒久的な障害（前例のない規模の破局）の場合には、より原始的な中央集権システム — 国家 — へと後退することができる。

技術は人類がより高い文明的な統治形態に到達することを可能にし、私たちに恩恵をもたらすが、同時にリスクももたらす。

ネットワークに公開することで私は金を窓から捨てているのか

評判ネットワークに主張を公開するコストは、大部分が埋没費用ではない。公開者がネットワークに投じたメッセージの有用性 — 現実の苦情、検証された経験、関連する警告についての情報 — は、より長

2つの道 — 国家は閉じ、ネットワークは開く

評判ネットワーク

国家

何もしないことも、正しい扉を選ぶことだ。

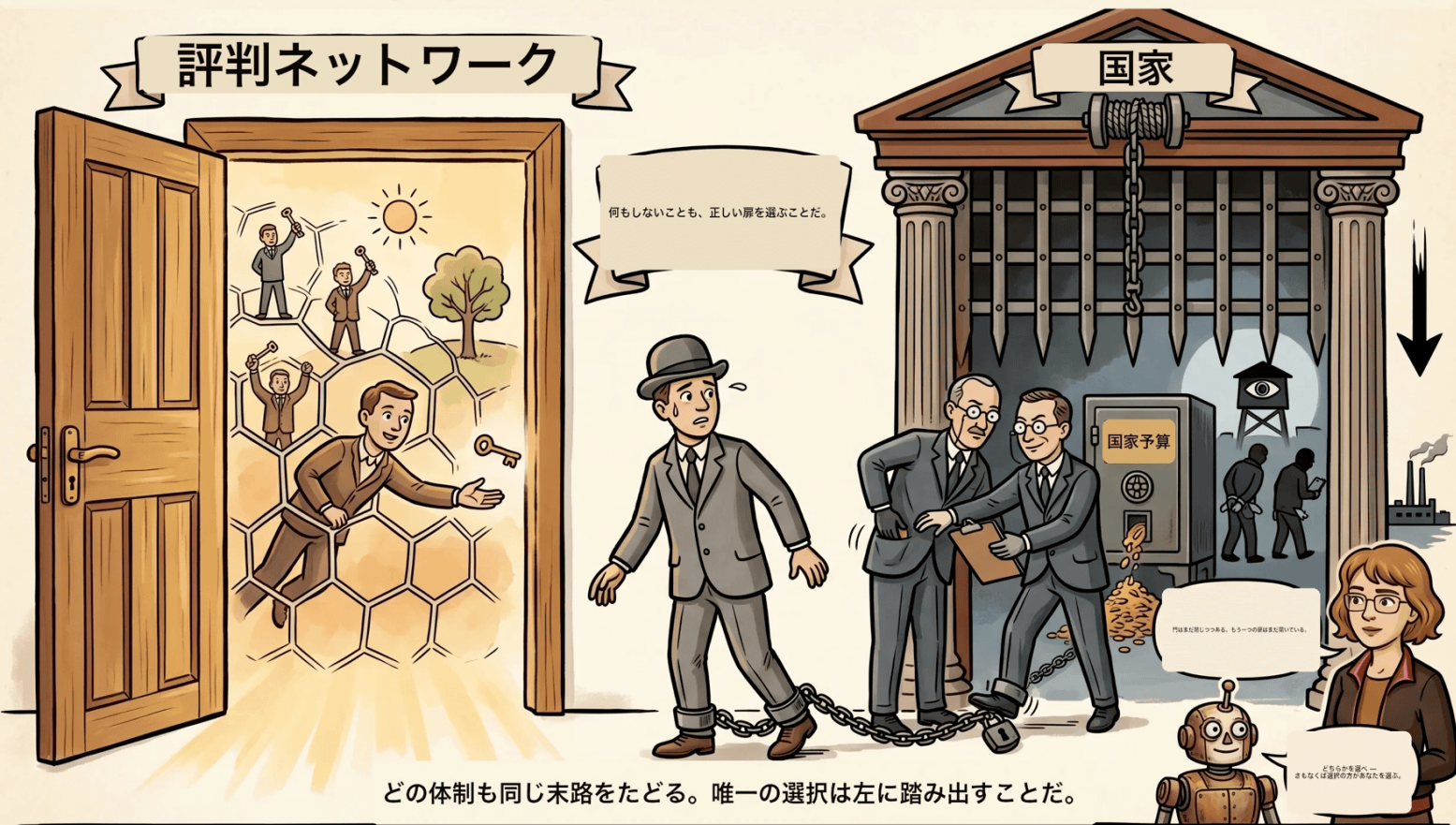
国家予算

門はまた閉じつつある。もう一つの扉はまた閉じられている。

どちらかを選ぶべ—
さもなければ選択の方があなたを選ぶ。

どの体制も同じ末路をたどる。唯一の選択は左に踏み出すことだ。

国家はデフォルトで閉じる。ネットワークは選択によって開く。



い時間の地平で、共同体の誰か他人の主張を検証したことへの手数料という形で統計的に返ってくる。共同体は利益を得、公開者は評判を築き、こうして真実の情報を公開するコストは、実際のネットワーク維持費のより小さな部分だけを差し引けばよい払い戻し可能な保証金に近づく。逆に、真実でない、あるいは些末な記録は返ってこない — そのコストは純損失である。したがって正直さは道徳的な選択であるだけでなく、経済的にも合理的な戦略である。

ネットワーク維持費を差し引いたあとのこの原理は、経済的中立性の原理と呼べるだろう — 私は共同体とともにあるとき損をせず、共同体に逆らうとき損をする。

共同体はまた、メンバーの正直な取り組みを評価するための連帯のチャネルを持つ。だが幻想を抱くのはやめよう。連帯への呼びかけはたいてい共同体の社会的圧力から生じるので、これは言葉の自発的な意味での連帯ではないかもしれない。

誰かが複数のアイデンティティを作ったら

一人の人間が複数の DID アイデンティティを並行して運用することはできる。しかし、それぞれのアイデンティティのために評判を築くには、独立した労力 — 時間、エネルギー、金 — が必要である。

近道はない。各アイデンティティは、実際の活動を通じて自らの実績¹を積み重ねなければならない。したがって並行するアイデンティティの維持は意図的に高くつく。

自由な社会では、コストが濫用を思いとどまらせる。

¹**実績 (track record)** — 一般的には、ある人物や組織の過去の結果、成功、失敗の履歴。ここでは、ネットワークにおけるある DID アイデンティティの過去のすべての相互作用 — 検証された主張、受け入れられた記録と拒否された記録 — の総和であり、そこからその評判が導き出される。

しかし独裁体制のもとでは、並行するアイデンティティは生存の道具となる。地下ネットワークの組織化、闇市場のより安全な航行、そして区画化²された抵抗を可能にする。区画化された抵抗では、一つのアイデンティティが露見しても他のアイデンティティは明かされない — そして体制が倒れたあとには、公的な生活とそこで築いた評判へのシームレスな復帰を可能にし、さらには以前は公式だった **DID** と秘密だった **DID** を、一つの主張を通じて単一の統合された記録の集合へと統合することさえ可能にする。

²区画化 (**compartmentalization**、英語の *compartment* から) とは、情報を孤立した単位に分離し、一つの単位の露見が他の単位を危険にさらさないようにすることを意味する。諜報機関から知られる原理である。エージェントは作戦の自分の担当部分しか知らないの、強要されても全体を明かすことはできない。

同じ労力 — 自由の中では無駄なプランB、圧政の下では命綱 並行アイデンティティのコストは同じ — だが買えるものは違う

自由の中では — 高くつくプランB

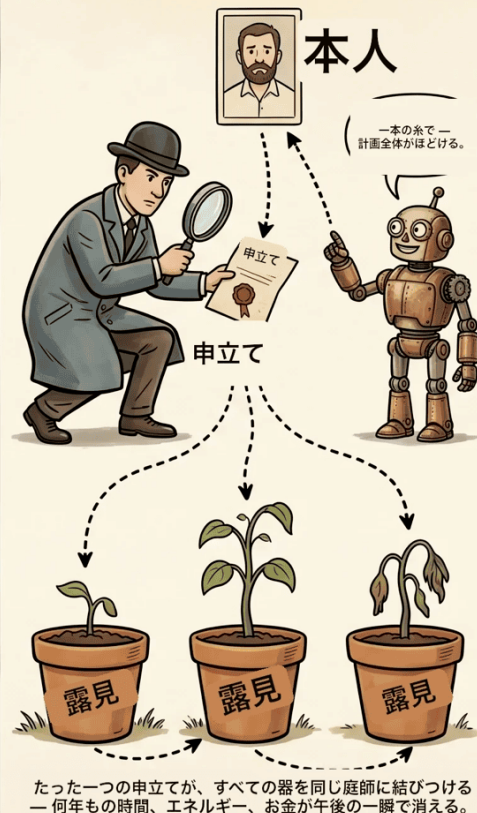


3つの庭、3倍のコスト — それでも手は2本しかない。

あるいは — 個人的な過ちの後のまっさらな出発し

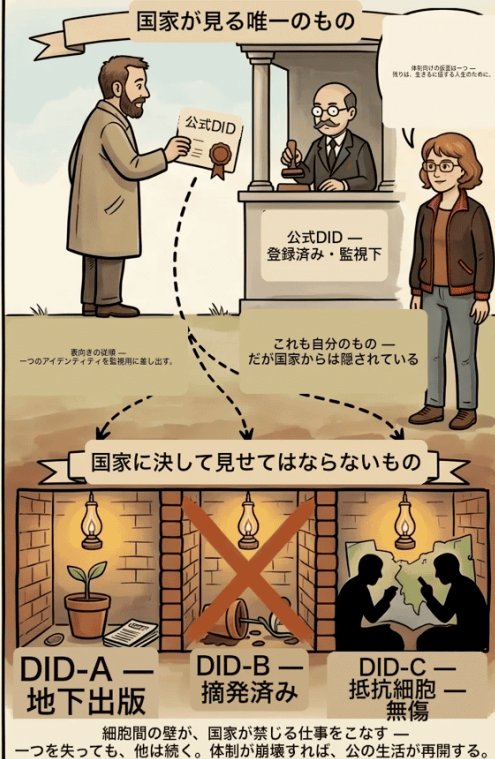


申立て一つでプランBは消える



圧政の下では —
一つは国家用、残りは自由な結社用

(国家はアイデンティティを全面禁止するか、自らの管理下に置くことを義務づける)



自由の中では、悪用は高くつく。圧政の下では、生き延びることが可能になる。

■ 裏返しにされた認識

国家とは異なり、分散型アイデンティティの上に築かれた評判ネットワークの原理は、認識される優先順位のパラダイムを反転させる。

- 重要なのは評判 — すなわち相手方との相互作用のリスクを評価するために用いられる過去 — であり、名前や住所などの個人データは、礼儀としてのデータ交換の問題でありうる
- 一方、国家はまず個人データを要求し、評判に関わるデータを蓄積し、共同体には自らに都合のよいものだけを見せる

富める者は単により多くのアイデンティティを「買える」（あるいは仮想的な共同体を作れる）のではないか

並行する分散型アイデンティティを作れるという可能性は、一見すると、経済的手段の乏しい者に対する、より豊かな手段を持つ者の不公平な優位に見える。しかし強調しておかなければならないのは、権力のピラミッドのいくつかの点を買収すればある種の悪事を消し去れる中央集権システムとは異なり、分散型システムでは共同体全体を買収しなければならない、ということである。

代替となる分散型アイデンティティはこの目的に資しうるが、その評判は、実際の他の共同体メンバーとの現実の相互作用を通じて時間をかけて築かれなければならない — それは単に買うことはできない。ネットワークは、あるアイデンティティがどう振る舞っているかを検証可能にするからである。

さらに、権威として振る舞い、複数の分散型アイデンティティが実は同一人物であるという証拠を生み出す調査を提供するサービスが市場に存在しうる（そしておそらく存在するだろう）。したがって、評判ネットワークに入力された単一の記録が、並行するアイデンティティの構築に費やされた時間、エネルギー、金のすべての投資を、そのコストのごく一部で無に帰しうる。

したがって経済的には、共同体を欺かないことが割に合う — そして必要なら、自分の行動を吟味し是正を進め、評判が受け入れ可能な水準に戻り、その担い手が共同体の怒りによって経済的にもその他の面でも苦しまないようにすることが割に合う。

自分の共同体で評判を失った経済的に強力なアイデンティティは、標的とされたアイデンティティとの陰の取引を通じて共同体の怒りから逃れようとするかもしれない — だがそうしたアイデンティティもまた、自らの評判を失う危険を冒す。

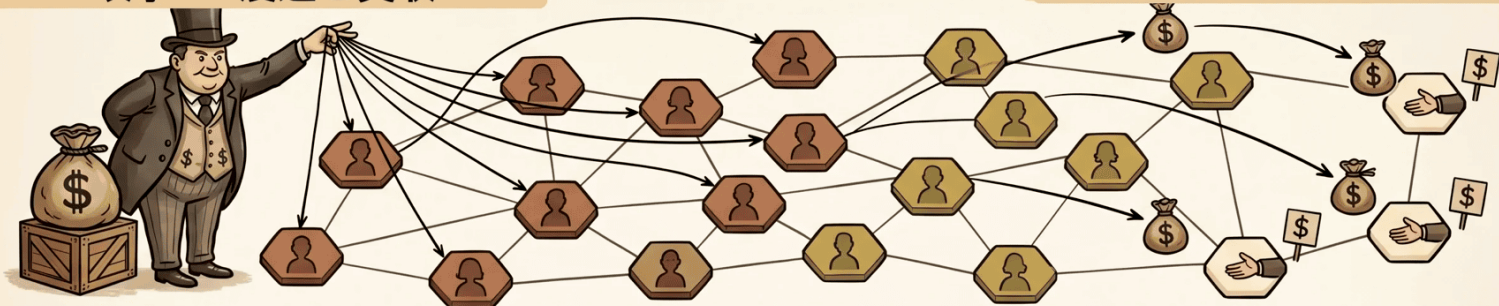
なお、新たなアイデンティティを持って別の共同体へ逃げるという道も残っている — だがそれはすべての達成を後に残し、評判ゼロでどこか別の場所をゼロから始めることを意味する。ときにはそれが理解できる道であり、唯一の出口であるかもしれない。

評判は経済力への対抗力だ

金持ちは影響力を買う — コミュニティはそれを記憶する

攻撃 — 浸透と買収

8体の操り人形を送り込み+隣人3人を買収

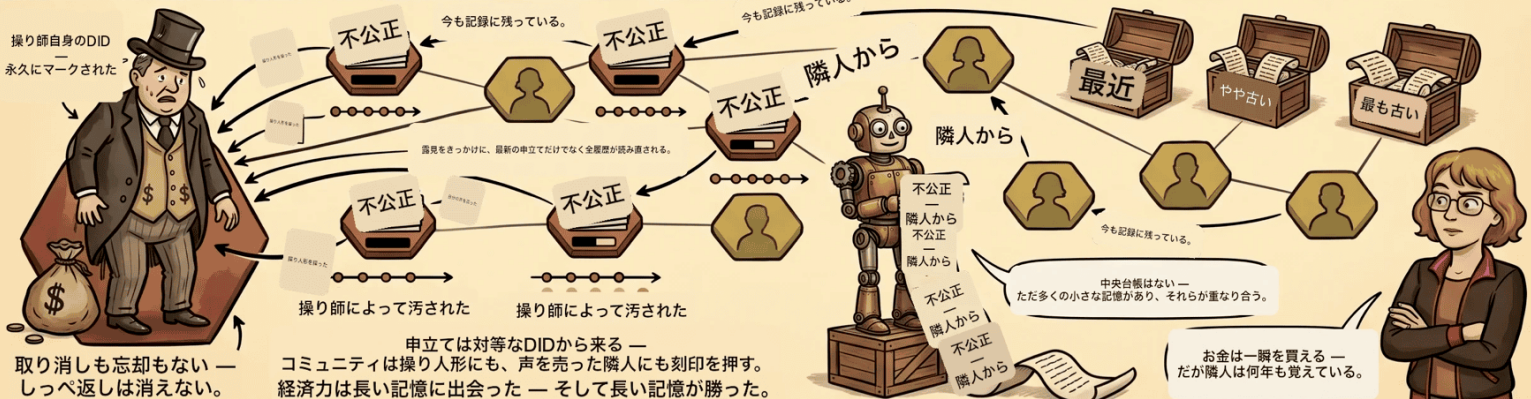


経済力はどんなコミュニティにも糸を忍び込ませることができ、その道中で本物の声もいくつか買い取れる。最初は、金持ちがただ友人の輪を広げただけのように見える。

その後

防御 — 長い記憶、分散した記憶

すべての隣人が自分自身の記憶を持つ — 中央台帳はなく、忘却もない



経済力は入り込む — だがしっぺ返しは自分に返り、決して洗い流せない。

■ 注記

同様に、共同体は、誰かが仮想的なアイデンティティの創出に資源を注ぐという攻撃にも対処するだろう。そのアイデンティティにとって、検証なしに別の共同体との相互作用に入ること — すなわち、その別の共同体のアイデンティティについての情報を無批判に受け入れること — はリスクが高い。評判は常に共同体の内部で築かれるのであって、グローバルにではない。

ただ読むだけで共同体に何も与えないフリーライダーはどうなのか

情報へのアクセスは、分散型アイデンティティを作った初日から無制限であるわけではない。新規参加者 — 実際の活動を通じてまだ評判を築いていない者 — は段階的な制限に直面する。より少ない情報、より長い待ち時間、より高い照会コスト。ネットワークは参加に報い、受動的な消費や恣意的なデータ収集には報いない。

分散型アイデンティティはまた、自らの評判を対価と引き換えに別の人物（DID 評判ネットワークにすらいけないかもしれない者）に貸し出すとき、自らの評判を危険にさらす。ここでも同じ原理が当てはまる。そのような共同体への裏切り（プライバシーの侵害）は裏切り者の評判に跳ね返りうるし、その行為は、中央集権システムで機能するような陰の取引を通じて消し去ることはできない。裏切り者は、達成の喪失を含めて共同体の怒りを覚悟しなければならない — 共同体は、裏切り者の目には、たとえば動産と不動産を所有する特権の保証人だからである。

■ 現実世界への錨

リスクを評価するとき、より危険な主体は当然、ある共同体によって承認された所有の特権を享受していない者である — 彼らは取引において失うものが少ない（デジタル資産のほうが動かしやすい）。

それは些細な細部に見えるかもしれないが、大きな帰結を持つ。共同体がそのメンバーに対して梃子を持つことを望むなら、それは特権としての所有を含意する — 最も自由な社会においてはほとんど不可侵だが、それでも権利でも根本原理でもなく、極端な場合には取り消されうる特権である（たとえば、武力紛争における共同体の防衛のための奉仕の拒否を私は想像できる）。

それはまた、共同体がそのメンバーをどう扱うか、そしてメンバーが共同体のために戦う — 自らの特権を保持する — どんな動機を持つかを、暗黙のうちに答えている。人は共同体への責任において失敗しうるが、苦労して勝ち取った特権の保持となると、道徳的に寛大さを期待することはできない。

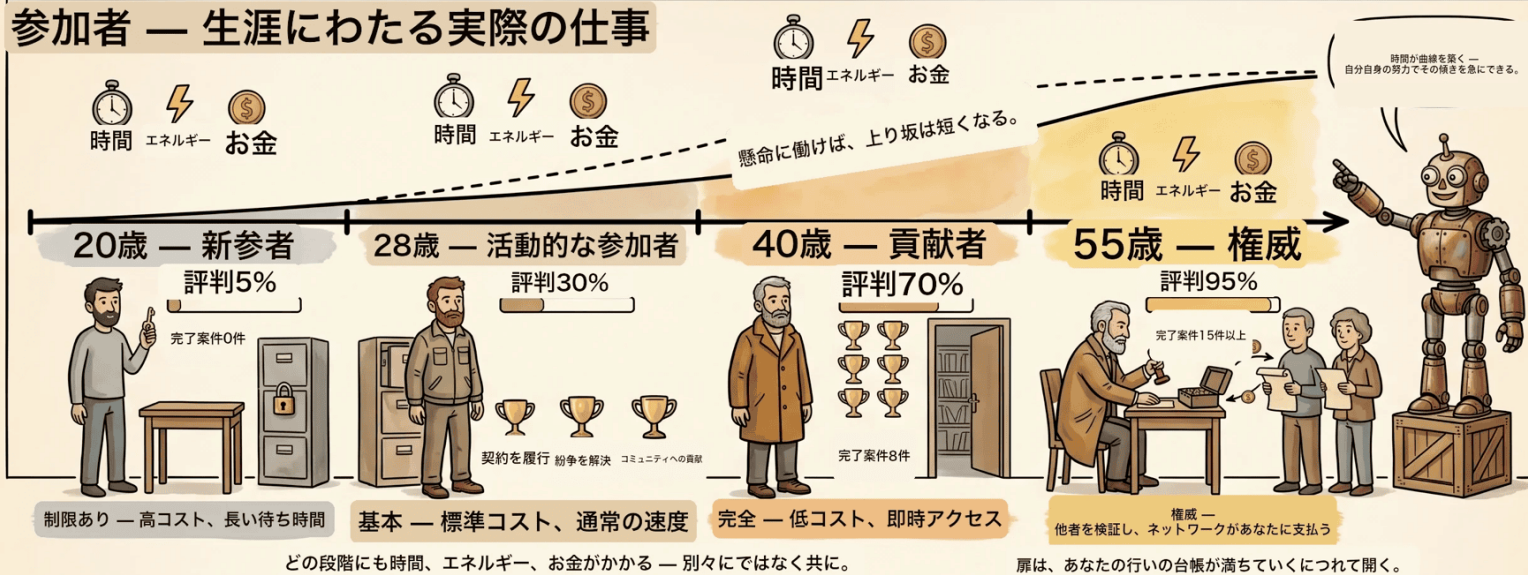
金銭的中立性

分散型、検閲不能、買収不能といった言葉を読むと、そうした語で描写できる最もよく知られた暗号通貨 — **Bitcoin**、**Monero**、そしてたとえば **Kaspa** — を連想せずにはいられない。だがここでは直観が誤りを招く。権威のサービス、検証と公開などに対する手数料は、任意の通貨や貨幣で決済できる。**DID** ネットワークのソーシャルネットワークに接続された参加者（すなわちあなたの共同体）とその周囲にとって重要なのは、支払いが行われたという評判に裏打ちされた確認である。主張の公開は、行為者がエネルギー、金、時間を費やすことなくいくつでもどんな主張でも公開できないよう、個別に妥当で検

ネットワークは参加に報いる

評判は一生をかけて築かれる — 買うことも借りることもできない

参加者 — 生涯にわたる実際の仕事



フリーライダー — 読むだけで、決して公開しない

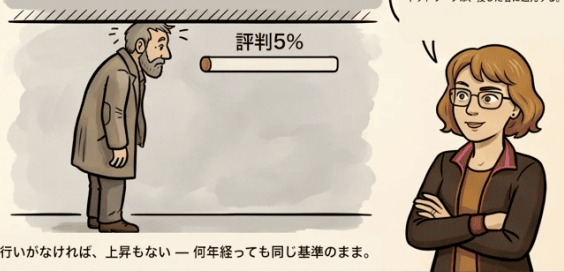


他の全員の記録を読む。



自分自身のものは何も公開しない。

制限されたアクセス — 天井は上がらない



評判5%

行いがなければ、上昇もない — 何年経っても同じ基準のまま。

時間、エネルギー、お金 — 実際の仕事に投じられたもの — こそがネットワークが尊重する唯一の通貨だ。

証可能なコストを伴わなければならない — それは今日の腐敗にまみれた国家システムにおけるエリートの特権に対応する、強く望ましくない事態である。

この点で、前述の暗号通貨には、ある支払いが行われたことを検証する信頼された権威としてそのネットワークが機能するという小さな利点がある。ただしプライバシーの小さな喪失と、自分のアドレスの一部が露出するという代償を伴う。

自発性、責任、そして自由

自発性は個人的なものである。私は自分自身で決める。責任は、私の決定が他者に影響を及ぼすときに生じる — フィードバックが働きだす。自由は贈り物でも権利でもない — それは自発性と責任へ向かう圧力とのあいだの何千もの二者間の相互作用を、社会全体で平均した現象学的³な結果である。ネットワークはこの平均を指図しない — それは検証者の価格シグナルから、そして共同体のメンバーが自らに設定するあらかじめ告知された検証方針から創発する⁴。

共同体の内部の個人がどれほど自由を選好するかは、自分が他者に課すものを、自分自身どれほど飲み込む気があるかという感覚にかかっている。自明で万人に有益なことについては、道徳的なジレンマはない — 殺人は悪い。次に、選択肢が許された特権の位置へと移る場合がある。技能を証明せよ、

³現象学的（phenomenological、ギリシャ語の *phainómenon* — 現れるもの — から） — 一般的には、諸現象を、その下の微視的世界にあらかじめ与えられた説明理論を用いることなく、それらから何が帰結するかを観察することによって、直接の経験に現れるがままに検討する取り組み方。ここでは、自由は上から定義される抽象的な原理ではなく、観察される現象 — 私たちが実際に互いをどう扱うかから創発する、人々のあいだの何千もの微視的な相互作用の帰結 — である。

⁴創発的（emergent、ラテン語の *emergere* — 現れ出る — から）とは、「誰かが設計したり指図したりすることなく、より単純な部分の相互作用から自発的に生じる」ことを意味する。鳥の群れは、どの鳥も編隊の計画を持たないのに、編隊を組んで飛ぶ — 編隊は各個体の単純な規則から創発する。同様に、評判ネットワークにおいても、全体の行動規則を誰も設計しない — それらは何千もの個々の決定から創発する。

そうすれば道路に出ることを許そう、そうすればあなたが私たちを殺す可能性が減る、というように。そして最後に、個人がこう言う事柄がある — 私にとっては割に合わない、自分でも落ち葉を燃やすのに隣人にそれを禁じたりはしない、あるいは私自身が相手の快適さを制限する何か別のことをして、相手が今度はそれを私に禁じたがるかもしれないからだ、と。私たちが歴史的に、他人の自由が始まる場所に自由の境界を引いてきたのなら、分散型アイデンティティの上に築かれた評判ソーシャルネットワークは、中央集権的な代表制民主主義よりもこれをよりよく満たす — 中央集権的な代表制民主主義では、たとえば選ばれた代表者という特権層が、個人的通信の監視から自らを免除しようとしながら、あらゆる陰の口実や操作を用いて、自分たちの有権者にはそれを課すことをためらわない。

自由と全体主義のスイッチ（そして委任）

DID ネットワーク内の単純な仕組みが、システム全体をより大きな自由へ、あるいはより大きな統制へと動かしうる。それは、ある DID が一定の期間に公開できる記録の数である。記録が希少なままなら、一つひとつが重みを持つ — それが自由である。記録が豊富で些末なことまで覆うなら、それが全体主義である。あなたは公開する記録の一つひとつで方向を選ぶ。ネットワーク自体は自由でも全体主義でもない — それは中立的なインフラである。それが何になるかは、人々がそれをどう使うかによって決まる。

自分自身の検証方針の内部では、私のソーシャルネットワークにおける一般的な DID に対して — 諸共同体の内部で — 公開者が一定期間に発行できる主張（一般に検証可能なあらゆる言明。ここでは評判ネットワークに公開される記録）の最大数を、私がそれを考慮に入れ、その検証要求を関連あるものとみなすための条件として設定することには意味がある。

私は直観的な数字を念頭に置いている — 年に一桁台の低い数である。そのような検閲的な取り組み方は、いくぶん孤立主義的に見えるかもしれない。だが私は正当に、申請者に選択を迫ることができる。

自発性 → 責任 → 自由

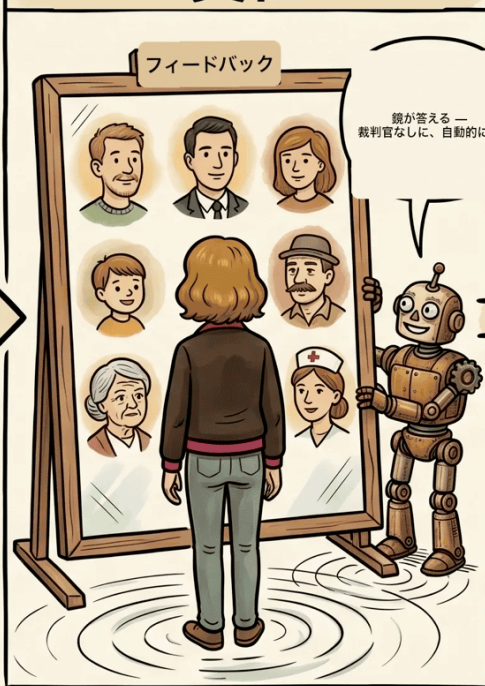
3つの段階 — 一人の選択から社会全体のパターンへ

自発性



個人が決める — 誰も彼女に強制しない。
そして誰も彼女に積極的な義務を負ってもいい。

責任



自分の選択は波紋のように広がり — その波紋は返ってくる。
結果が自ら物語る。

自由



誰もこの地図を描かなかった — それは自ら描かれた。
自由とは、隣人同士がどう接し合うかの統計的な形だ。

自由とは上から与えられる贈り物ではない — 私たちが共に作り出すパターンだ。

すでに発行した記録の一つを選び、検証者にそれを取り消すよう、すなわち無効にするよう求めよ、と。これは、申請者が偶然にも本当に複数の独立した不正の被害者になってしまった状況では、かなり攻撃的な要求であり、私はそれによってきっと、申請者の共同体からの疎外感に寄与してしまうだろう。

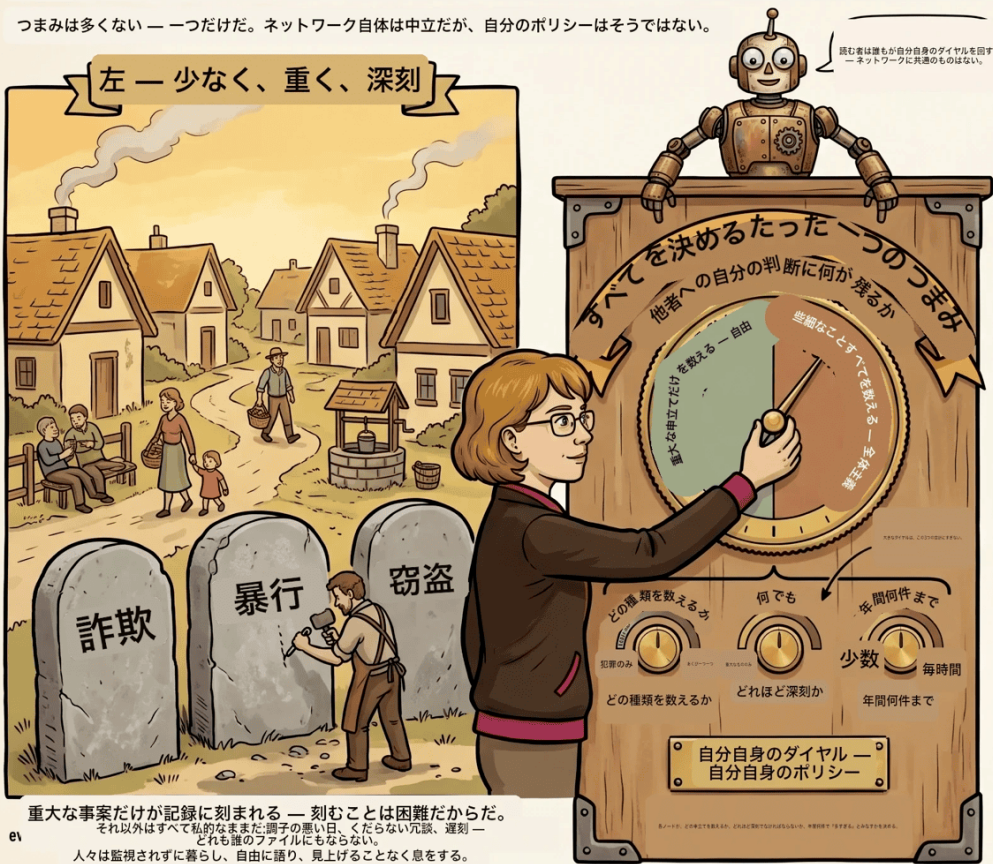
したがってより効果的な選択肢として現れるのは、評判ネットワークに情報を公開する自分の権利の一部を、共同体あるいは権威のために委任できることである。委任された共同体や権威は、その後 — 自らの内部規則に従って連帯的な仕方で — それらをどう配分するかを決める。集団は、自らが不利な立場にあるとみなす者たちの面倒を見られなければならない。共同体のメンバーは、委任された権利が使われるまではいつでも、自らの委任を取り消す権利を持つ。

自由と全体主義を分けるスイッチ

たった一つのパラメータ — 自分がどれだけ追跡することを選ぶか — が社会全体を自由と圧政の間で傾かせる

つまみは多くない — 一つだけだ。ネットワーク自体は中立だが、自分のポリシーはそうではない。

左 — 少なく、重く、深刻



右 — 多く、些細、息苦しい



重大な事案だけが記録に刻まれる — 刻むことは困難だからだ。
それ以外はすべて私的なままだ。調子の悪い日、くだらない冗談、遅刻 —
どれも誰のファイルにもならない。
人々は監視されずに暮らし、自由に語り、見上げることなく息をする。

あくび一つがファイルになる — 数えることは安上がりだからだ。
くしゃみ、買い物、夜道の帰宅: そのすべてが記録に残る、永遠に。
何も私的ではない — その目は決してまばたきせず、隣人は口をつくむ。

自由とは自分が数えることを拒むもの — 全体主義とは自分が追跡することに同意するものだ。

公開権の委任

あなたに仕える権威に鍵を貸し出す — そして一瞬で取り戻す

鍵は貸すが —
紐は自分の手元に残す。

委任 —
権威は自分が承認したルール範囲内で、自分の代わりに行動する。

召還の紐
自分の公開権 — 1件

権威 — サービス提供者
。ポリシー・基準・政党・会議所。

ポリシー

権威が行動するとき無作為に抽選される

委任された鍵
— プール

権威に貸す鍵は必ず無作為に抽選される

一引きで — 鍵は手元に戻る

紐は決して手を離れない —
それがすべての仕掛けだ。

使用済み

無作為に一つの鍵が抽選される
— その鍵は使用済みになる

取消可能な鍵は鍵が抽選で使われるまでの間だけだ。

鍵を持てる権威の種類



政党
PARTY



標準化団体
BUDT



職能団体

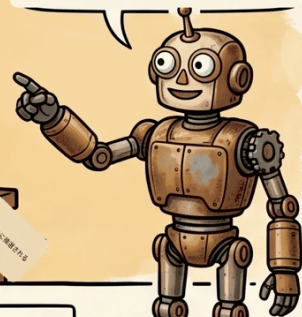


協同組合

その後、市民は権威との関係を保つために新しい鍵を発行しなければならない —
これはバックグラウンドで自動化できる。

権威は会員に仕える — その逆ではない。
紐を一度引けば取り決めは終わる。

鍵は貸す — 紐は保持する。委任とは決して明け渡しではない。



■ 自由対全体主義

公開される記録の量を見張り、制限する社会はより自由になる。記録が過剰な社会は全体主義へ傾く。記録を公開する権利を誰か他人に委任することも構想できる。

■ 文化的適応

人々はおおむね、互いの皿の中をのぞき込むのを好む。諸文明を通じて、私たちは歴史的経験と人口密度において異なる — したがって、諸文明や諸共同体の内部で、互いの皿の中をどれほど見たがるかにおいても異なる。アジアの国家は社会における自由をより厳格に見る傾向があり、ヨーロッパやアメリカの国家は、ある側面ではより自由に見る傾向がある。この対比がどれほど不正確であろうと、分散型評判ソーシャルネットワークの文脈では、個々の共同体の設定は差別せず、各共同体は自らの内部の通信を思うままに構成できる、と言える。

差異にもかかわらず、地球全体で承認される標準は存在するだろう（無差別な殺人は誰の利益にもならない）。他の設定は共同体固有のものとなり、さらに他の設定は個人的に固有のものにさえなる。利点は、相互の通信を通じて、また周囲の設定を観察することによって、コンセンサスを求められることである — 二者間の取り決めから共同体間の取り決めへ、そして時とともに、最もよく構成された共同体の経済的優位のおかげで、グローバルなレベルでさえ求められる。

だがコンセンサスについては次の章で詳しく述べる。

各コミュニティが自ら設定する

ネットワークは差別しない — どの地域も自らのダイヤルを設定する



北米 — 年間2件 — 高いプライバシー



ヨーロッパ — 年間3件 — より高いプライバシー



東アジア — 年間8件 — より厳格な監視



ラテンアメリカ — 年間5件 — バランス型



アフリカ — 年間4件 — コミュニティ主導

コミュニティは互いを見ている — 最良の設定は時とともに広がる

地図は判断しない — ネットワークはすべての設定を等しく運ぶ。

同じネットワーク —
5つの異なる地域社会。

一つのネットワーク、多くのダイヤル — 各コミュニティが自ら決める。



オラクル問題 — デジタル世界と物理世界を橋渡しする

「オラクル問題」という用語は、近年もっぱら暗号通貨、ブロックチェーン、分散型システムの世界と結びつけられてきた。一般には、デジタルシステムに入ってくるデータが、物理世界で実際に起きたことに忠実に対応することをどう保証するか、という問題である。システム自体は、誰かが本当に誰かに危害を加えたのか、あるいは契約が本当に破られたのかを検証できない — それはデジタルの記録しか見ないからである。

ここでは私たちはこれを権威 — デジタルの記録が物理的な現実に対応することに自らの評判を賭ける主体 — を通じて解決する。権威の評判が高いほど、記録は信頼できる。

デジタル世界と物理世界を橋渡しする 権威が現実を渡す



権威の評判がデジタル記録を信頼できるものにする。

*このシステムはオラクル問題を解こうとはしない — 権威が橋渡し役であることを受け入れ、現実世界ですでに機能している信頼の仕組みに沿う。

*橋渡し役が現実について誤っていれば、権威が代償を払う — 自らの評判で。

検証はどのように機能するか

コンセンサスと検証プロセス

社会が平均してどの規則を支持し執行すべきかについてコンセンサスを築くには、次の仕組みが役に立つ。**DID** の参加者として、私は自分が加入し、それに従って生きていく規則を宣言し、それを公開する。（私の見るところ、自分の理想の世界 — 制限されているとは感じず、安全だと感じる世界 — を構成する定款や規約のようなものだと考えてほしい。）

私は、自分の **DID** の連絡先がどう反応するかをあらかじめ見積もることができる — そして、通常の社会的・商業的な相互作用が仮に起きたとすれば、私がどれほど強く、誰によって制裁されるかを評価できる。

決定的な評価が起きるのは、あなたが別の **DID** に情報を要求するとき、あるいは評判ネットワークに公開したい主張の検証を依頼するとき（あるいは権威にサービスを依頼するとき、等々）である。それは、あなたが相手方の宣言した方針に対して自分で試験的に評価を実行したときと同じ結果になるはずである — そしてもしそうならなければ、相手方の側で何かが間違っている。相手は不正なゲームをしようとしているのだ。

その帰結は、検証の見積もり価格を添えた受諾（検証者や権威のサービスの場合）か、あるいは拒否である。評価者の方針からの逸脱に対する制裁とボーナスの両方が、見積もり価格に折り込まれる。要求者はそのうえで、その条件を受け入れるか、あるいは配分アルゴリズムの次の検証ラウンドへ進むかを定める — このプロセスを、満足するまで、あるいは続けることが経済的に無意味になるまで繰り返す。

■ ソーシャルグラフ

評判ネットワークは、何よりもまずソーシャルネットワークである。あなたは連絡先 — その接続に同意する人々 — を追加する。彼らには連絡先があり、その連絡先にも連絡先がある。アルゴリズムは、設定可能な深さ（例：三段階。あなたの直接の連絡先、その連絡先、そしてそのさらに一段先）の内部で検証者を探す。グローバルなブロックチェーンは必要ない — ネットワークは自然に、他の共同体と重なり合う共同体を形成する。

アルゴリズムは非決定的である。あなたの主張の文書をハッシュ化し、そのハッシュをこの圏内の既知のアイデンティティのリング上の位置に写像し、最も近いものを候補の検証者として選ぶ。あなたは誰があなたの主張を検証するかを予測することも左右することもできない。

各検証者の拒否は、あなたの文書を大きくし、その処理コストを増やす — それが第一のコストチャネル（文書の膨張）である。新たな検証者はそれぞれ、データ量、あなたの評判、そしてあなたの主張の内容がその検証者の宣言した検証方針からどれほど逸脱しているかに基づいて手数料を課す — それが第二のコストチャネル（リスクプレミアム）である。そして各反復は時間とエネルギーを費やす — それが第三のコストチャネルである。

■ 検証者が順に何を確認するか

ひとたび選ばれると、検証者はおおよそ四つの順序立てられたステップで主張を評価する — 最も安価なフィルターを先に、高価な内容確認を最後に。

1. **方針によるゲート判定。**この種の主張は、そもそも検証者が公に検証するものの範囲に入るか。入らなければ、要求はただちに拒否される。
2. **権威の信頼。**その主張を裏書きした権威は、検証者自身の宣言した方針のもとで十分に信頼されているか。検証者の信頼の閾値を下回る権威は、主張の内容にかかわらず拒否の根拠となる。
3. **発行者の評判。**発行者は、この種の主張について検証者が宣言した評判の閾値を満たすか。低い評判は、手数料を引き上げるか、あるいは拒否を引き起こしうる。
4. **内容確認。**最初の三つのゲートを通じたときにのみ、検証者は主張そのもの — 署名、内部の一貫性、形式的な正しさ、そして検証者の方針からどれほど逸脱しているか — を評価する。この最後のステップに課される手数料は、実際に負ったリスクを反映する。

検証者は、これらのゲートのそれぞれを支配する方針を公開するので、これらのステップは検証者の裁量に委ねられてはいない — 検証者はすでに宣言したものに拘束される。公開された方針からの逸脱は、それ自体が検証者に対する公開可能な主張であり、検証者はそれを自らの評判で支払う。

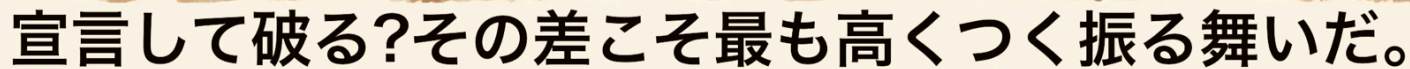
その結果、信頼できる有用な主張を公開するコストはほとんどゼロになる。過激な主張を公開するにはより多くのコストがかかる。嘘を公開するのは法外に高くつくようになる — あなたは検証者から検証者へと反復しなければならず、あなたを拒否するすべての検証者がコストを積み増す。市場があなたの主張に価格をつけ、その価格が、あなたが動き回る諸共同体との関係において自分がどこに立っているかを教えてくれる。

実際には従わない規則に従うと宣言するだけでは足りない。その場合、あなたの **DID** は、その偽善を暴く否定的な記録が公開される危険を冒す — それはあなたを他のみんなにとってのリスクに変える。その帰結は、より少なく、しかしより一貫して守られる規則であるべきであり、法律の専門家でさえほとんど航行できないあの法律と規制のジャングルの一掃であるべきである。

■ コンセンサス対アカウントビリティ

ネットワークが価値ある情報源として役立つためには、**DID** はあまり過激であってはならない — さもないと他の者たちがそれを拒否する。社会的圧力が均衡を求め、それを不安定化しようとする試みはおそらく罰せられる。

ネットワークはあなたの言葉と記録を静かに照らし合わせる — その差は誰の目にも見える

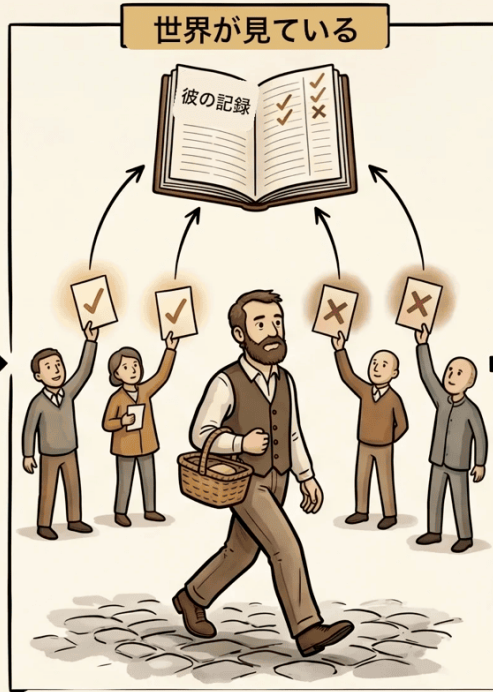


偽善への処方箋

自分のルールを宣言せよ — それに従って生きるか、さもなくば市場があなたを締め出す



誰でも自分の基準を読む。
門番も秘密もない。



世界は彼が実際に行うことを書き留める。
毎日、彼の台帳に少しずつ証拠が積み重なる。



偽善は権威によって罰せられるのではない — 市場によって値付けされる。

あなたが買う普通のサービスにはすべて、自分自身の記録に応じた加算料金がついてくる。

これを『描き直された社会契約』と呼べるだろうか？

倫理を強制するのは権威ではない — 価格だ。
毎日ゆるやかな圧力がかかり、皆が共に生きられる共通の平均へと向かわせる。

言行を一致させよ — さもなくば代償を払え。偽善は最も高くつく評判だ。

■ 票の数は声の重みと同じではない

Juraj Karpiš は「貨幣は善行の記憶である」と言う。私はこう付け加えたい。評判は悪行の記憶である、と。

ここから、メリトクラシー的に、より多く貢献し悪い評判を持たない者ほど、共同体においてより大きな声の重みに値することが導かれる。二者間の関係というレンズを通して見れば、どのコンセンサスの圧力に応えるかを私が量るとき、最大の重みは、私が最大の経済的利益を引き出す関係に置かれる。私が活発な取引を持たない十人よりも、一人の恒久的な取引相手のほうが、私にはるかに大きな影響を与える。このパラダイムは商取引に限られない — それは社会的、政治的その他の関係にも及ぶ。

Roles in the verification transaction and authorities

役割の概観

これらの役割のいくつかには、ネットワークとその基本的な性質についての章ですでに簡単に触れた。今こそ、それらをもう一度より詳しく見て、ネットワークをより堅牢にするために必要な追加の役割を加えるときである。すべての検証トランザクションには複数の役割が関わる — それらがどう振る舞うかを見てみよう。

■ 検証トランザクションにおける役割

それぞれの検証には最大で六つの異なる役割が関わる。それらを下の表にまとめた。それらはすべて、分散型評判ネットワークにおいて自分自身の **DID** を持つことができる。

役割	説明
発行者 (Issuer)	ネットワークに情報を公開する人 — 何かが起きたと主張する (DID が作成、編集、解消された、ある主張、ある DID の方針、など)
主体 (Subject)	情報が対象とする人 — 主張の名宛人
権威 (Authority)	主張を調査し、提示された証拠を精査するか、あるいは能動的に証拠を集めることによって、主張の質に自らの名を賭ける信頼された主体
オブザーバー (Observer)	検証者が主張をどう扱うかの記録を保つ独立した第三者 — 検証者が沈黙したり、宣言した方針から逸脱したりしないことを確かめる
検証者 (Verifier)	トランザクションを処理する、アルゴリズム的に選ばれた参加者
委任先 (Delegate)	別の参加者に代わって行動する人

発行者

発行者にはこれまでに会ってきた。誰かが不正を受けたとき、あるいは自分自身の達成を広めたいとき、その情報をネットワークに載せるプロセスを引き起こすのは、**DID** によって代表される人である — その人がそうすることに第一の関心を持つからである（動機は、満足を求める気持ちか、あるいは自分の公的なイメージを高めたいという願いのいずれかである）。

■ 肯定的な主張

自分自身についての肯定的な主張は、その主体としても発行者としても、私がそれを使いたい状況のために手元に置いておける（学位、提供した奉仕の証明書など）。ここに肯定的な主張と否定的な主張の違いがある。検証された否定的な主張を共有することは共同体全体の利益になるが、肯定的なものはその担い手の利益になる。

権威

権威は二重の役割を果たす。それは**監査人**（主張が公開される前に証拠の質を検証する）にもなれば、**保証人**（主張の真実性に自らの評判を賭ける）にもなれる。いずれの場合も、それは発行者の主張を強める。これら二つのサービスは分離可能である — 権威は一方を、他方を、あるいは両方を同時に提供しうる。作業上の前提は、権威が提供するサービスのほとんどが自由市場の基盤の上で提供されうる、ということである。それは、司法のような、民営化を想像しにくい分野においてすら成り立つ。そこでも専門的なサービス — 調査、証拠の評価、そして今日は中央集権的な軍隊によって提供されているサービス（戦略計画、標準化された訓練、調達と備蓄の管理など）に至るまで — は、市場の行為者によって

発行者 — 申立てを書く者 著者・署名者・自らの評判を賭ける者

発行者が行うこと

1. 自分自身の言葉で申立てを書く
2. 裏付けとなる現実世界の証拠を集める
3. 自分のDIDで署名し、選んだ権威に送る
4. 公開コストを支払う
5. 嘘をつけば、その結果を引き受ける

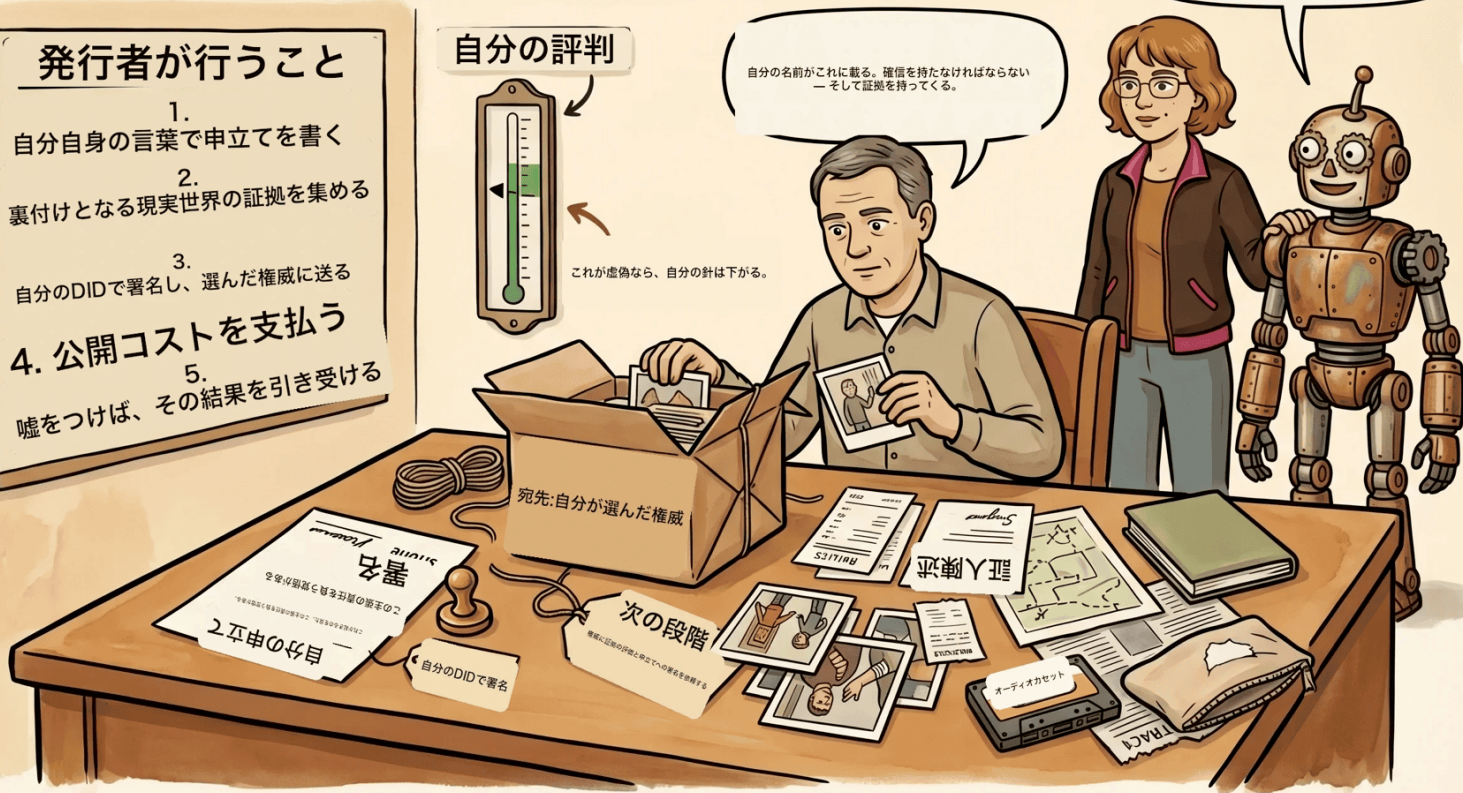
自分の評判



これが虚偽なら、自分の針は下がる。

自分の名前がこれに載る。確信を持たなければならない
—そして証拠を持つてくる。

誰でも発言できる。嘘は発言者に代償を課す。



発行者は著者だ。その名前が載っている。

*DIDを持つ者なら誰でも発行者になれる。求められるのは免許ではなく、勇気と説明責任だ。

効率的に提供されうる。再構築ののちには、自由市場のインセンティブによってより効率的にできないものはほとんど何もない。

■ **権威、発行者、そしてオブザーバーは、決して自分自身の事案の検証者になってはならない。**

検証者のアルゴリズム的な選定が独立性を保証する。誰も自分自身の主張、あるいは自分が直接の利害を持つ主張を検証することはできない。これは、**DID** の共同体全体が支持することに関心を持つ、基本的な規則の一つである。

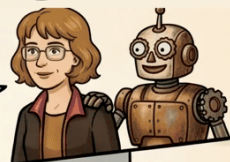
以下のグラフィックは、権威が覆う活動の広がりについての補完的な見方を示している（「権威」という語は「サービス提供者」と互換的に読める）。

案内人 — あなたの価値観に沿って導く

背後に深い分析・手前にシンプルな指針

案内人

彼女は複雑な世界を推奨へと集約する。フォローワーは注目という一帯を投じる —
いつでも離れ、別の案内人に乗り換えられる。



自分の分析

作業メモ — クライアント向けではない

公共支出 —
振り向け先変更



複雑な作業は自分が行う。あなたが得るのはシンプルな推奨だ —
ただし自分の価値観を共有する場合に限る。

提供者

1	70M	☆☆☆☆
2	70M	☆☆☆☆
3	70M	☆☆☆☆
4	70M	☆☆☆☆

あなたへ —
それが意味すること
あなたの利益を最大化するよう集約

支出をここに移し、あそこで節約する

自分の基準を満たす提供者を支持する

このポリシーのひな形を採用する



例:誰が案内人になれるか

—
ポリシーのひな形を公開する政党や運動

—
集約した調査結果を公開する独立監査法人

— サービス比較機関

評判集約機関(経済・ビジネス・地域・交通安全)

— ジャーナリスト評論家や消費者レビューサービス

それで自分のお金で正確には何を知られるのか —
どの分析と、どの数値を?

公に表明したことに縛られる。あなたの信頼が彼らの通貨だ。

“いつでも離れて別の案内人に乗り換えられる。あなたの信頼は縛られていない。

“案内人も自分自身でいくつかの申立てに署名することがある — 公開されているが、ここでの主題ではない。

■ 匿名のオブザーバーとしての権威

評判のある権威 — その事業がもっぱら自らの実績にかかっている公証人を思い浮かべてほしい — は、主要な機能（監査人／保証人）と並んで、第三の機能を提供しうる。検証中の匿名のオブザーバーの役割である。彼らは提出された主張のタイムスタンプ付きの記録を保つので、検証者はそれをひそかに握りつぶすことができない。オブザーバーの役割の仕組みは、オブザーバーの役割についての節でさらに記述する。

検証者

任意の **DID** が検証者として行動できる。直接に、あるいは第三の **DID** に委任された検証権を通じてである。私 — あるいは私の委任先 — が検証できるためには、私はネットワーク上で到達可能（オンライン）であるべきである。誰もがそれに縛られたいわけではない。だからこそ **DID** の記録は、その **DID** がオフラインのあいだに代わって機能を果たす代理人を、優先順位順に列挙できる。

ネットワークで活動するすべての **DID** は、自分自身の方針を公に宣言する。その方針に定義された規則を通じて、**DID** は検証プロセスのあいだに、相手方の評判と、発行者が評判ネットワークへの公開のために印をつけた主張の内容および形式を判断する。方針の一部は、検証サービスの手数料を計算するのに用いられる計算式である。それが定めれば、ネットワークを流れる統計的に多数の主張を通じて、私はネットワークのアルゴリズムが私を発行者の側に引き当て、ある反復において、発行される情報を検証するよう私に割り当ててのを待つ。発行者は、正しく振る舞う検証者がどう反応するかをあらかじめ計算できるが、実際にその検証者（あるいはその代理人）に接触することを避けることはできない。

提供者 — 申立て署名サービスを運営する

公開された基準・公開された価格



公に宣言したことに縛られる。あとは評判が仕事をする。

*提供者にも自分自身のポリシーがある — いつ受理し、いつ却下し、どう返金するか。これは公開されているが、ここでの主題ではない。

選ばれた検証者との反復は、たとえそれが通らないとあらかじめ分かっている、発行者が実行しなければならない。

発行者が正しい候補検証者 **DID** の集合に対して検証者選定アルゴリズムを実行していることを、私たちはどうやって知るのか。公に宣言した方針とともに、すべての **DID** は、評判ネットワーク内の自らのソーシャルネットワークの識別子の現在のリストも公開する。もし発行者が自らのソーシャルネットワークを、自分自身の見解をただ反響させ強化するだけの社会的な泡として定義するなら、それを通じて公開される情報は、他の共同体によってより広く受け取られることはほとんどない。私が高いコストをかけて過激な主張をネットワークに押し込むことに成功したという事実は、相手方の評判を判断するとき、私がそれに何らかの重みを与えることを含意しない。ある主張は、共同体によって考慮に入れるよう私が迫られる（違反者に科された刑罰と制限）。他の主張は完全に私次第である — ある情報片を含めるか除外するかの経済的な価値を、私は自分自身で決める。

主体

評判ネットワークに公開された情報が対象とする者たちは、その担い手であり、言い換えれば主体である。評判ネットワークにおけるインセンティブは、主体が自分自身の規則によって正しく公正に振る舞うあらゆる理由を持ち、共同体によって規則遵守のある種の黄金の中庸へと押しやられるように設定されている。主体は、自分が宣言した規則が要求する以上に道徳的に振る舞うインセンティブすら持つ — あらかじめ宣言された方針は、共同体が何らかの評価や措置を遡及的に適用するコンセンサスに到達することを妨げない。この角度から見れば、法秩序に対する評判ネットワークという代替案は、予想されるとおり、規則の文言よりもその精神によってより強く駆動される。

検証者 — 公開されたポリシーに照らして申立てを判断する

4つの関門、順に。安価なフィルターを先に。

検証の関門 — 順に

1. ポリシーによる選別

2. 権威への信頼

3. 発行者の評判

4. 内容の確認

そもそもこの種の申立てを検証するか?

その権威は自分の関心を越えているか?

発行者は自分の評判基準を満たしているか?

署名、整合性、ポリシーからの逸脱

なれないもの。発行者、権威、顧客者、主体。

検証者の評判

ポリシーから逸脱
→ 評判が下落 →
今後選ばれなくなる

検証者が行うこと

1. 公開したポリシーの関門で(順に)絞り込む

2. 権威への信頼、次に発行者の評判を確認する

3. 関門を通過した場合のみ申立ての内容を評価する

4. リスクに比例した手数料を課す

5. すべての判断に自らの評判を附ける

手数料 $\propto$ リスク

リスクが大きいほど →
手数料も大きい

安価なフィルターを先に。高コストな内容確認は最後に。

検証者は自分自身が公開したルールに縛られる —
そして失いかねない評判にも。

主体 — 申立ての対象となる者

受け取る・黙らせることはできない・応答できる



主体には拒否権がない — あるのは応答する権利だけだ。
*反論申立てもまた申立てだ —
返答の内容には主体自身の評判がかかっている。

オブザーバー

オブザーバーの役割は、検証者が規則を曲げるインセンティブを取り除く。検証者が発行者や権威の要求を気に入らない状況では、検証者は単に沈黙する — 応答せず、アルゴリズム的な連鎖を塞ぐ — こともできてしまう。オブザーバー — あるいはオブザーバーの集合 — は、検証者がどのように照会されたかを記録することに自らの評判を賭ける。もし検証者が、そうでないと述べた宣言済みの方針にもかかわらず沈黙するなら、その検証者はプロトコル違反で有罪とされうる。

仕組み：タイムスタンプとチャレンジコード

あなたが検証者に主張を送る前に、あなたはそれをオブザーバー — あなたが信頼する人々、あるいは小さな手数料を課す専門のオブザーバーサービス提供者 — を経由させる。各オブザーバーはあなたの提出物を受け取り、それにタイムスタンプを押し、それが送り出されるのを見たとき署名し、チャレンジコード — 自らの署名の暗号ハッシュ — を生成する。それらのコードはあなたの要求に付加される。検証者はそれらを見るが、オブザーバーが誰なのか、あるいはそのコードがそもそも本物なのかさえ見当がつかない。したがってオブザーバーは、発行者と検証者のあいだのプロキシとして行動し、主張が提出されたことと、それが何を含んでいたかについての独立した記録を保持する。オブザーバーはゼロから N 人までありうる。

検証者が正直に振る舞うとき — 宣言した方針に沿って受諾または拒否するとき — コードは不透明なままである。誰も露出しない。

だがもし検証者が、応じる姿勢の方針にもかかわらず沈黙するか、あるいは公開したことに矛盾する仕方で応答するなら、あなたは元のオブザーバーの署名を握っている。あなたはそれらを、主張が提出されたこと、そして検証者がプロトコルに従わなかったことのプロキシ証言として公開できる。誰でも、その署名がチャレンジコードと一致することを検証できる。

観察者 — 申立てを中継し、往復を見守る代理人

検証者は彼女に話しかける。検証者は彼女が誰なのか —
そもそも誰かが見ているのかどうかさえ、決して知らない。



観察者が行うこと

1. 発行者から申立てを受け取る
2. 自らの印を押す。その印がタイムスタンプ付き記録となる
3. 発行者に代わって検証者へ転送する
4. 応答が返ってくるかどうか、そしてその内容を見守る
5. 検証者が不正を働いた場合のみ自らの署名を公開する — 自分の評判が保証となる

脚注

この図は、検証者が必ずしも「信頼できる」人である必要はないことを示しています。検証者は、検証者の評判が保証されることを示しています。検証者は、検証者の評判が保証されることを示しています。

コードは見える —
誰かは見えない。

公衆に対しては匿名、ネットワークに対しては説明責任を負う。検証者にはコードだけが見え、観察者自身は決して見えない。

「対外的に、検証者も自分の署名を添えて応答を送ることができると同時に、検証者は匿名である。」

落ち：本物のオブザーバーは要らない

そしてここが最もエレガントな部分である。**あなたには本物のオブザーバーがまったく要らない。**あなたはチャレンジコードとそっくりに見える乱数を生成できる。検証者はその違いを見分けられない — 検証者は自らの評判を賭ける危険を冒すかどうか、賽を振らなければならない。彼らが受け取るあらゆる要求の背後には、匿名で見張っている尊敬されたオブザーバーがいるかもしれない — あるいはそれは純然たるノイズかもしれない。検証者はそれを知らない。そしてその不確実性こそが仕組みである。

正直な圧力を維持するコストはほぼゼロである（乱数はタダである）。検証者にとっての不正の潜在的なコストは破滅的である。実際には誰も見張っていないときでさえ、正直な振る舞いにインセンティブが与えられる。

このシステムが機能するのは、誰もが少しかだけ疑心暗鬼だからである。不確実性は監視よりも安上がりである。

■ 単一の反復における複数の検証者

検証者の可用性を補強する伴走的な規則として、単一の反復において一人だけでなく候補検証者の集合を返すアルゴリズム的な拡張がありうる。

委任

文明は、分業と専門化の能力の上に経済成長を築いてきた。世界はその満ち足りた輝きにおいて複雑であり、私たちがそれをその複雑さのすべてにおいて把握できる見込みはほぼ皆無である。自然な出口は、快適な生活を支える幅広い活動を専門の提供者に委任することである。彼らは私たちの時間、エネルギー

検証者を誠実に保つはったり

本物の観察者と無作為なはったりは、検証者の視点からはまったく同じに見える

【発行者 — カミラ】

【本物の観察者】

【検証者】

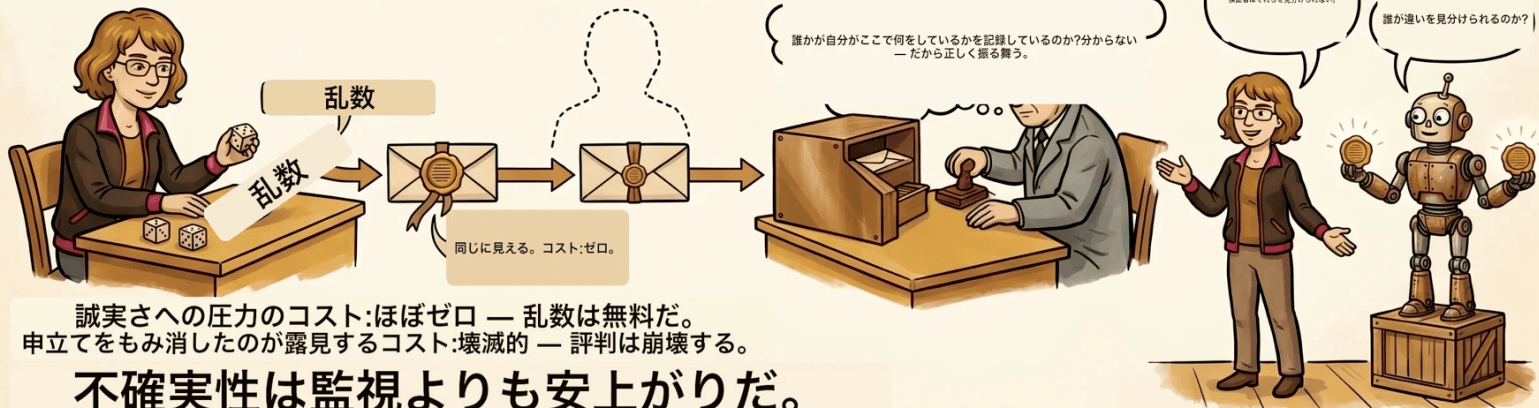


検証者は本物の記録とはったりを見分けられない。誠実な振る舞いだけが唯一の安全な賭けだ。

【発行者 — はったり】

【観察者なし】

【検証者 — 同じ振る舞い】



一、金を節約してくれ、そして今度は私たちが専門化することを許してくれる — 私たちが最も得意とするサービス、あるいは市場が私たちに最も高く評価するサービスを提供することへと。

同じ委任の論理が評判ネットワークにも及ぶ。「自由と全体主義のスイッチ（そして委任）」の章で、私たちは、一定の時間の窓の内部でネットワークに公開できる主張の数を制限することによって自由な社会を守るための原理を示した（単純化して言えば、社会が最大限に自由であるように、年に一桁台の低い公開権を思い浮かべてほしい）。この原理は複数の次元へと拡張できる。私たちはただ一つの数を持つ必要はない — 異なる種類の主張に適用される複数の上限を持つことができる。他者の偽善を指摘するのには、商取引における不正行為とは別の数を用いることができるし、たとえばパスワードの変更のような **DID** 文書の変更は、共同体がほとんど気につけないものであり、等々。すべては、共同体が進化的な時間をかけて、目標とする自由の水準とアカウントビリティのあいだの適切な均衡を見出すうえで何が自らの利益に資するかをどう定義するかにかかっている。

なぜ共同体が私に与える公開権の数は十分に少なくあるべきなのか。ある **DID**（主体）に否定的な主張で印をつけることは、長い時間をかけて築かれた評判を破壊し、その損害は長く続く。破壊された評判は、さらなる、あるいは繰り返される違反のたびに、共同体からの段階的に増大する制裁の尺度に直面する — 破壊的な主体の完全な排除（極端な場合）に至るまで。指数関数的に増大する罰の尺度は、検証可能な証拠に裏打ちされていれば、大量の主張を必要としない。これは、社会が（外的あるいは内的な）破局によって揺さぶられていない、平和な定常状態について当てはまる。

きわめて確率の低い出来事については、統計的な頻度は個人に適用すると変動が激しい。共同体の集団全体にわたっては、そうではない。それが、自分の公開権を専門の集約する権威に委任することの価値である。彼らは — 損失が生じた場合の相互保険のように — あなたの権利を用い、あなたに代わってそれを適用する。もっと具体的に語り、いくつか例を挙げよう。- 組織犯罪の探知と撲滅 - 商業上の合意の執行 - 特権の管理（教育の証明、資産の取得／処分など） - 等々

代理人 — あなたが契約する申立てサービス

自分では対応できないことを委任する・自分にとって大切なことは保持する



自分では対応できないことを外部委託する。状況は把握し続ける。権利はいつでも取り戻せる。

*代理人が合意した範囲外で行動すれば、代理人自身とあなたの評判の両方が公に影響を受ける。

■ 「公開権」が実際にどう機能するか

委任先のグラフィックは、分かりやすさのために公開権を物理的なトークンとして示しているが、システムの中にそのような物体は存在しない。実際に起きるのはこうである。あなたが良好な関係を保ちたい人々 — あなたの共同体 — の方針が、彼らがあなたをノイズとして扱い始める前に、あなたから関連あるものとして年に何件の主張を受け入れるかについての創発的な規則へと集約される。この上限が存在するのは、ネットワークが些末な「もしも」の主張に溺れず、共同体が望むだけ自由なままでいられるようにするためである（量を制限することでシグナルが保たれる）。

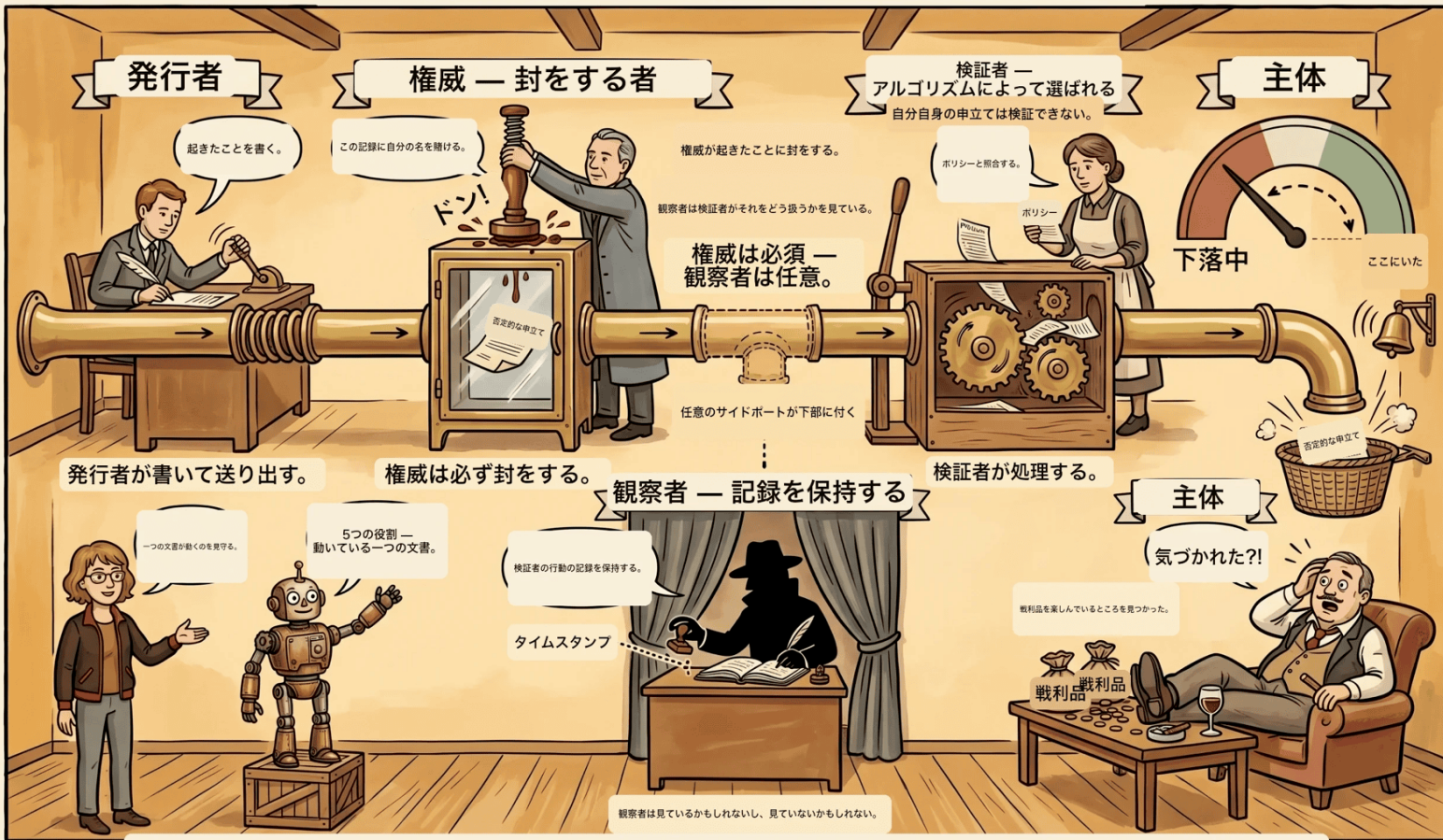
あなたは、共同体があなたに許すものを読み取る。ある幅があり、あなたが最も重く見る人々によっていくらかのばらつきがある。そのうえであなたは — その許容量の内部で — 自分でいくつの主張を公開し、いくつを、出来事が自らの範囲に収まるときにのみあなたに代わって公開する専門サービスに委任するかを決める。これが、あなたに起きるあらゆる些細なことについて主張を提出することを強いられずに、あなたを良好な関係に保つものである。

グラフィックの「トークン」は、この読み取って決めるループの視覚的な代役であり、文字どおり的人工物ではない。

評判ネットワークにおいて、委任された公開権を取り消せることには価値がある。これは、委任先がまだその委任された権利を用いていないかぎり、いつでも行える。

否定的な申立てがシステムを流れる

一つの文書を追う — 各役割がそれに何をするかを見る



5つの役割、動いている一つの文書 — 誰も自分自身を検証できない。

役割間のコミュニケーション

下のグラフィックは、現実の事案において役割がどうつながるか — 発行者による主張の提出から評判ネットワークへの公開まで — をまとめている。

創発する社会契約 — 方針

これまで私たちは、主張がどう検証されるか、そして各役割がどんな部分を担うかを記述してきた。今度は、何千もの個々の方針がどうやって、現実の社会契約のように機能する何かになるのかに目を向ける。社会契約と強制された連帯という左派の夢に似たものは何一つない。

すべての参加者は、自らの道徳（方針）に基づいて自分自身の方針を宣言する — 何を受け入れ可能とみなすか、そして他者の特定の振る舞いにどう反応するか。ある **DID**（共同体）が知るネットワーク全体のすべての方針の総体が、創発する倫理 — 誰も設計しなかった観察可能な規範 — を生み出す。これらの創発する規範は、二者間の価格シグナルに支えられて、測定可能な社会契約を形づくる。誰も生まれたときに署名しなかった理論的な構築物ではなく、実際の振る舞いに裏打ちされた経験的に観察可能な規則である。

■ 社会契約

人々は「社会契約」が撞着語法ではないかと議論する。誰も何にも署名しないのに、それは中央集権的な社会における立法上・行政上の行動を正当化するために持ち出される。

分散型ネットワークにおける相互作用の現象学的な分析は、ある種の創発する規則 — グローバルなものやローカルなもの — を明らかにしうる。これら広く共有された規範を私たちは何と呼ぶべきか。社会契約か。共同体と同じように、共同体の社会契約は正確に観察し境界づけることはできない — 共同体に対するあらゆる角度が、異なる社会契約をもたらす。

■ 価値観に基づく方針

「価値観に基づく方針」を意思決定の基盤として扱うことも、同じように誤りを招く。価値観は、ある時点で一般に選好される規則の現象学的なクラスターのようなものである。それらは進化し、時とともに一定ではない。

ポリシーが会う。姿勢が形作られる。

宣言されたルールが今日の価格を決める — 一致には割引、乖離には割増

ポリシーが一致するとき



ポリシーが乖離するとき



取引で二つのポリシーが会うとき、その一致度が価格の修正要因になる。

*これは評判の話ではない。それぞれが公に宣言し、今それを守ることが期待されている内容の話だ。

個々のポリシーから倫理が生まれる仕組み

ポリシーから規範へ

暴力犯罪なし —
99%が同意

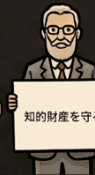
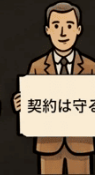
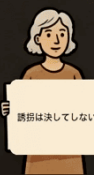
詐欺なし —
78%が同意

契約を守る
—
60%が同意

公正な賃金
—
25%が同意

直接的な害に近いほど、合意は強くなる

創発的な規範 — 誰かが書いたものではなく、大多数が合意したもの



個々のポリシー — それぞれの人が支持するもの



比較のために —

上記の創発的な規範は経路的に観察可能な

倫理は設計されるものではない。それは私たちが実際に互いをどう扱うかから生まれる。

*個々のポリシーはその人の道德観を映し出す — コミュニティや環境に適応しようとする圧力によって形作られる。

自分についての情報を提供する

互いを知らない二人の **DID** の主体が経済的な関係に入るとき、私たちは相手方に代わって自分自身の共同体への要求に署名し、私たちについての情報を提供するように共同体に求めることができる。しかしこれは、共同体とは何かについての非常に素朴な考え方である。共同体は閉じた集合ではない — 一つの **DID** が複数の共同体の参加者でありうる。

共同体は、ある参加者の視点からすれば、その者のソーシャルネットワークにおいて自らを現す現象学的な現象のようなものである。それは常に明示的に境界づけることが理にかなうものではない。村の住民は共同体を形づくりうるが、週末にしかそこに来ない人は、その同じ村の別の共同体にも属しているかもしれない。共同体は、サッカーチームとそのファン、その関係者、そして関わるすべての人の家族が一緒になったものでもありうる。ある国民、あるいはある国家の市民も、共同体あるいは複数の共同体を形づくりうる。一つの **DID** を異なる角度から見ると、異なる（そしてしばしば直観的な）共同体の見方が得られる。

したがって境界にある **DID** は共同体どうしの架け橋であり、そして — 現実の生活とまったく同じように — アマチュアのレベルであれ、あるいは人々をつなぎ危険な **DID** についての情報を集約することを専門とする権威のようなプロのレベルであれ、他の共同体のメンバーについての情報を提供する役割を果たす。

DID ネットワークにおけるある種の情報は、無条件の相互交換によく適している（暴力犯罪、詐欺など）。しかし他の種類の情報は、共同体がその内部での使用に制限されるものとして扱いうる（市民権に相当するもの、共同体に提供された奉仕など）。そのような情報が広められうるかどうかは、共同体のメンバーの宣言した方針にかかっている。

共同体は自らの圏内でプライバシーを守り、その見返りに、無条件の基盤の上で相互に有益な情報を交換する。

犯罪と罰

犯罪と罰

私たちはネットワークがどう機能するかを知っている。記録がどう作られるか、誰がそれを検証するか、検証者の不正がどう抑止されるか。一つの問いが残っている — 誰かが実際に他者に危害を加えたとき、何が起きるのか。

■ 私たちはどれほど互いに依存しているのか

私たちは皆、この大いなる世界の舞台に立っており、ここで起きることは何であれ私たち全員に関わっている。

ヤン・アモス・コメニウス（『世界の迷宮と心の楽園』）

評判ネットワークに加わる、あるいは拒む理由は多くありうる。しかし私は、人間の本性のある側面 — しばしば暗いものとみなされる — が良い目的に役立ちうると信じている。私が語っているのは、認識された不正を前にして満足感を覚えたいという人間の欲求である。

満足、正義、復讐 — 私たちはそれらを否定的な感情と結びつける。社会がまとまっているためには、私たちは少なくとも、満足が中央集権的な制度を通じてもたらされるふりをしなければならない。さもなければ個人は自分が生きる社会と結びついていると感じられないだろう。平均して、私たちは何らか

のチームに属し、それを信頼する必要がある。誰かが他者に危害を加えたとき、社会は、満足がどのように、どの程度もたらされるかを見守る。いくぶん物議を醸すが、私はこう論じる。歴史においてしばしば — そして今も — 被告に対する手続きが清廉だったかどうかは問題ではなかった。問題だったのは、社会が誰かが罰せられるのを見たことである。それは自らの機能を果たした（数々の冤罪と、古い事案の再審への抵抗が、その物語を十分によく物語っている）。被害者と遺族の視点は二次的なものにすぎない。まず問題になるのは社会の残りへのシグナルである。というのも、不正は、あらゆる個人の一日に登場するほど日常的なものではないからである。

分散型評判システムは、直接証拠と間接証拠（監査されたものとされていないもの）を公衆が見られるようにするだろう。社会は情報を評価し — 自分自身で、あるいはそうした評価を専門とする自由市場のサービスを通じて — 質的・量的なシグナルに基づいて、主体（あるいは作成者や検証する権威に対してさえ）にどんな措置を適用するかを決められる。

罰とは何か。それは、その特権の喪失を通じて、疑わしい加害者を謙虚にさせる一形態である — 被害者も社会も、有害な行為が割に合わないと感じられるように。これが本質的な点である。有害な、あるいは危険な振る舞いは割に合ってはならず、同時に、被害者と社会／共同体の残りの両方に満足感を与えなければならない。

そのような罰は中央権威によって施されなければならないのか。もし誰もが、ある種の行為にどう反応するかをあらかじめ宣言できたらどうだろう。私は明らかに、他人の財産の上で罰を執行することはできない。だが私は、違反者が私の領域に入ってきた場合には、加害者を罰する目的で、選ばれた執行権威の集合に自分の財産を利用可能にする、と宣言できる。そして私は、他者が私の取り組み方を評価できるよう、これを公に宣言できる。

そしてここで比例性の価格メカニズムが登場する。もし私が些細な違反に対して厳しい罰を宣言すれば、ネットワークは私の極端さに価格をつける。他者は私を不釣り合いだと感じ、私の検証コストは上がる — 私と取引したがる人は減るか、あるいはより悪い価格でしか取引せず、私の記録を妥当な価

格で受け入れる検証者も減る。逆に、もし私が寛大すぎれば、共同体は私をリスクとみなす。もし私が詐欺を大目に見れば、共同体はおそらく、私に関わる行為の加害者に対して寛大になるだろう — 私に自分の薬を味わわせるために。

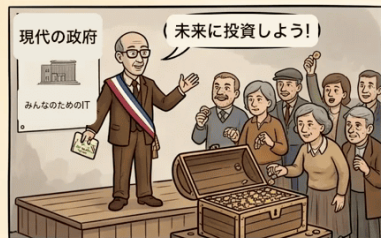
正義はもはや贅沢品ではなくなる。誰かがあなたに危害を加えたとき、その不正を記録するのは手頃であり、記録は恒久的であり、加害者にとっての帰結は現実である。

■ 偽善の検知

方針を宣言するだけでは足りない — もし私がある規則に従うと宣言しながら私の振る舞いがそれから逸脱するなら、その隔たりは評判上の負債である。ネットワークは「法を破った」と「自らの言葉を破った」を区別しない — どちらも測定可能なシグナルである。偽善は高くつくし、私はこれ以上に苛立たしい赤い布を知らない。

一つの罠。一つの出口。

内部者は常に契約を勝ち取る — ネットワークが人々に、許可不要で直接購入できるようにするまでは。



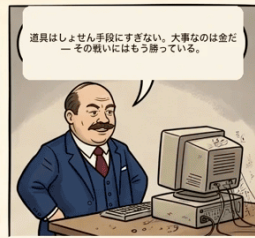
新しい公共ITシステムが必要だと市民は合意する。予算から、税金から支払われる。



密室では、調達担当者や内部者が一社のために入札条件を設計する。封閉が手渡される。



担当者を買収する。ポケットは暗黙で膨らんでいる。



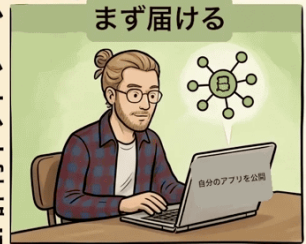
契約は落札される。内部者は免許を持っているが — 技術もなければ、仕事への敬意もない。



内部者は職人を訪ねる。「親切な申し出」はほんのわずかなお礼からだ。

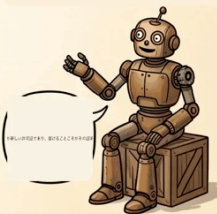


評判ネットワーク
— ここから新しい世界が始まる —



二つの道。罠はルールの中にある。出口はルールをまるごと迂回することだ。

「ルールが内部者によって書かれているとき、ルールの内側で苦情を言うこと自体が罠だ — 罰金でさえ次の不正入札の資金になる。評判ネットワークが出口だ。市民が製品を見つけ、開発者に直接支払い、コミュニティが唯一重要な免許を与える — 届けることで得た信頼だ。」



1. 従来型

2. 評判ネットワーク

■ 量対質 — 有罪の二値パラダイムを打ち破る

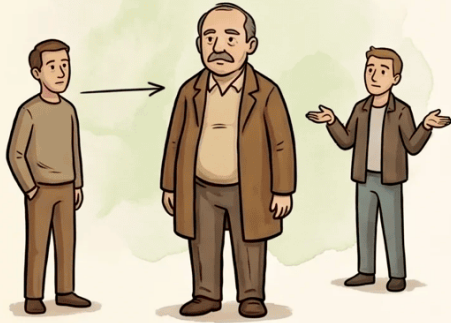
中央集権的な司法では、有罪は二値である。0 か 1 か、有罪か無罪か。評判ネットワークでは、問題になるのは有罪が証明されるかどうかではなく、シグナルの蓄積である。

被告に対する単一の証明されていない窃盗の告発は、おそらく大した警戒を呼び起こさないだろう — だがそれは告発者に対する警戒を呼び起こす。しかし、さまざまな独立した情報源からの複数の間接的な指標は、重みを持ち始める。問題になるのは量だけでなく質でもある。証人の独立性（異なる人々、異なる文脈）、パターンの一貫性（繰り返される種類の疑い）、時間的な相関である。

逆に、同じ発行者からさまざまな標的の主体に対して繰り返される、頻繁で根拠のない告発は、中傷として評価されうる — そして告発者の評判がその代価を支払う。

証拠が積み重なる仕組み

『孤立した一つの申立て』



申立て一つだけでは一行動を起こすには薄すぎる。どちらの側も断罪されない。

『パターン』



5つの独立した情報源 — パターンが浮かび上がる。

『圧倒的な重み』



20の独立した情報源 — 圧倒的な重み。

A

『雑音の仕掛け』



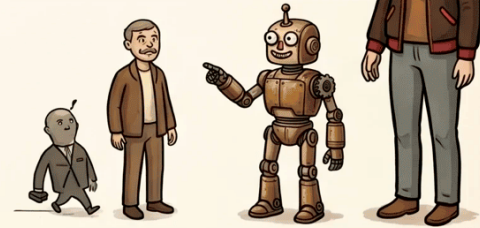
証拠なしに同じ主張を拡散する — コミュニティが何も見出せなければそれは中傷であり、告発者に代償が課される。

B

『恨み』



一人の告発者が全員を指している — パターンをなすのは告発者であって、告発された側ではない。



これは今日の世界に似ている。実際そうだ — 流うのは感情が今や現実であることだけだ。革命ではない。ただより良いインセンティブがあるだけだ。

独立性こそがすべてだ。繰り返される一つの声は雑音。異なる場所から上がる多くの声は信号だ。

私たちは償いも見落とすべきではない — 有罪が証明される前の自発的な行為であり、より軽い罰への道を差し出す。罰が働きだすのは、加害者が償いへの一歩も踏み出さず、帰結から逃れることを望むときである — 中央集権システムでは、その帰結が腐敗を通じて買えるのと同じように。

■ 違反の種類

情報の種類は犯罪行為に限られる必要はない。それには次のものが含まれる。 - 犯罪の記述
- 契約違反と詐欺 - 不道德な振る舞い - 現実と仮想の双方における公序の乱れ - ...

DID ネットワークにおけるあらゆる新しい記録は、当該の **DID**（主体、作成者、あるいは検証する権威のいずれであれ）について評価された評判とリスクを調整する。私が他者の運命に対して負う責任が大きいほど、私はより慎重になる。

害が生じた後 — あなたはどのようにするのか？

追いつく。強制する。自発的。村が応じる三つの方法。

何が起きたか



さて、どうする?



合理的な選択は常に最も安上がりなものだ: 自分で直せ。

『無視しようとする — どこでも追いつかれる』



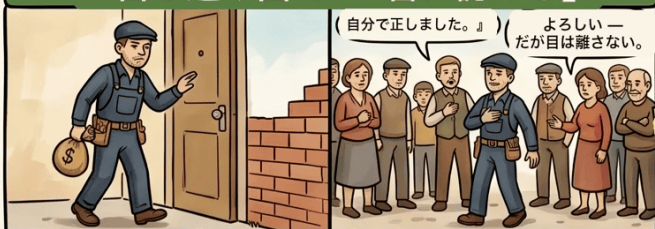
救済なし — どの店も彼を追いつく — 経済生活からの追放

『正すことにする — だが群衆の視線の下でのみ』



群衆の視線の下での強制的な償い — 返済はしたが、村は彼の値段を吊り上げる — 教訓は染み付かせなければならない。

『自ら進み出て — 皆に認める』



自発的な早期の償い — 公に受け入れられる — 評判は慎重を伴いつつ回復する



■ 委任を通じた罰の執行

私は個人的に罰を執行する必要はない。私は（保険と同様に）あらかじめ定められた規則に従って帰結を執行する権威に支払える — 捜査、法執行、司法のサービスに相当するものである。もし権威が不釣り合いに執行するか、あるいはまったく執行しなければ、その評判が損なわれる — そしてその評判こそが、生計を立てる能力の基盤である。

委任はネットワークにおける一般原理である。**DID** のあらゆる活動は別の **DID** に委任できる — 検証、主張の発行、紛争への応答、コンセンサスの宣言。委任はいつでも取り消せる。それは、究極の統制を失うことなく専門化を可能にする。

誰が調査し、誰が執行するのか？

『害』 → 『調査員』

『記録』 → 『執行者』 → 『説明責任』



委任は取消可能だ。どんなDID活動も別のDIDに委任でき、いつでも取り戻せる。

自分自身で罰を執行するわけではない。委任するのだ。そして代理人はあなたに対して責任を負う。

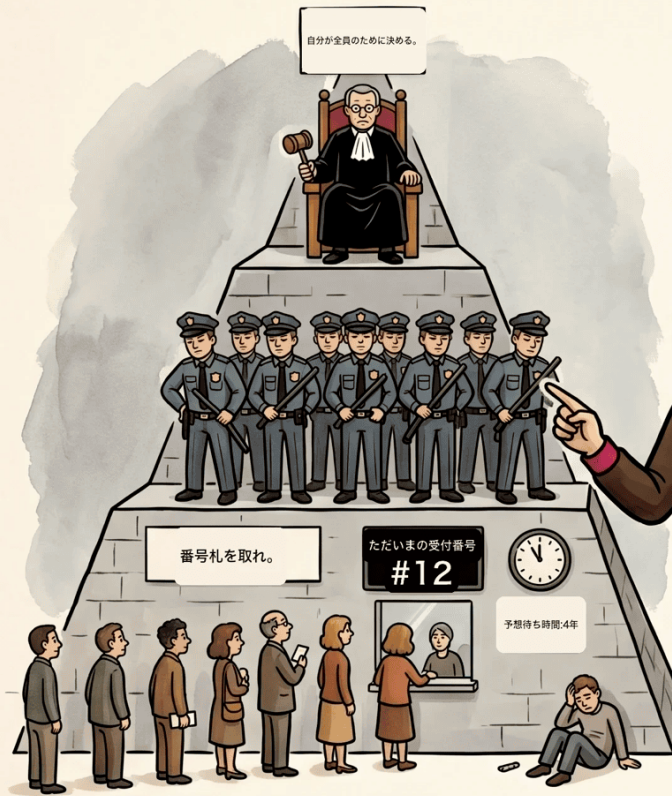
■ リスク管理の民主化

検閲不能な評判ネットワークは、銀行や大規模な産業複合施設の保守担当者がすでに中核的な活動として行っていること — リスク管理 — を民主化するだろう。

顧客に向き合う銀行員にとって、リスク評価はあらかじめ用意されているので、彼らはあらかじめ定められた限度の内部で商業的な相互作用に集中できる。洗練された保守チームは、定期的な点検の間隔ごとにリスクの指標（構造的な亀裂の兆候、運用インフラを劣化させるプロセスなど）を集め、設備の寿命だけでなく、いつどんな介入が必要になるかも予測できる。

私は **DID** の利用を同様に思い描いている — 誰かが（おそらく有料で）相手方についての人間が読める要約を提供するだろう。その要約は、顧客が注文したリスク評価の角度を反映する。

中央権力なしの制裁



一人が全員のために決める — 被害者は待つ
— 加害者はそれを知っている。

償いは処罰よりも安上がりだ。



コミュニティがポリシーを宣言する —
加害者はあらゆる方向からそれに直面する
— 権威が合意された内容を執行する。

処罰は無視よりも安上がりだ。

金の流れを追え

金の流れを追う

私たちは分散型評判ネットワークと、それを使う動機を持っている。それはすでに、利用者に競争優位をもたらしうる — 潜在的なリスクを明らかにし、相手方の選定と交渉戦略をより効率的に計画するのを助け、それら既知のリスクを減らす措置を含めるのを助ける。

以下に続くのは、それを使うための一つの可能な方法論⁵である — ネットワークの性質を活用して、現行のシステムからその進化的後継への移行の道を構築する。それはおそらく、この論考が生まれた中欧に特徴的な特色を帯びている。ローカルな条件はローカルな調整を必要とするだろう。私がどこでも保つよう勧めたいのは、国家に対する措置の妥協なき性格である — それがなければ、目標は果てしない議論の中で薄められ、変革は決して訪れない。気をつけよ — 国家の代表者と支持者たちは、あなたをたわごとで忙しくさせ続ける。それに引っかかるな。彼らの生計がかかっているのだ。

国家の弱点 — 金

初めに立ち返ろう。私たちはより多くの結果としての自由、その形へのより多くの影響、そしてそれに見合ったより多くの責任を望んでいる。問いは単純である。国家はどこに、暴力に訴えることなく私たちが圧力をかけられる脆弱な点を持っているのか。

答えは退屈であり、それゆえいっそう強力である。金である。

⁵ **国家の脱構築** — チェコの文脈では、これはおそらく、チェコの著者ダニエル・シュタイガーヴァルト (Daniel Steigerwald) による同名の近刊書 (2026 年予定) で深く扱われるだろう。私は個人的に、そこに含まれる示唆に富む手順に大きな期待を寄せている。

その核心において、国家は金の流れである。金を通じて、国家はその強制装置 — 国家の規則を執行する最後の環 — に支払う。金がなければ暴力の独占はない。ひとたび金が滞り始めると、国家は退き始める — 国家を物理的に所定の位置に保つ者たちに支払うものが何も残らないからである。

金の流れは自然に変動する — 季節的に、経済的に、投資家のセンチメントに応じて。国家はこれを金融市場での借入を通じて覆い隠す。ときに借入は合理的である。元が取れる投資である。しかしより多くの場合、それは、防衛、国内治安、刑事司法、外交という国家の核心的な目的をとうに超えて肥大した課題への過大な支出を賄う。ある種の閾値がひとたび越えられると、中央銀行は、自らのインフレ推計に錨づけられた金利で反応する。

そしてここで静かな税がやってくる。インフレは、マクロ経済学者の単なる会計上の懸念からはほど遠い。それは通貨の購買力への隠れた税であり、老後のために数枚の硬貨をわきに取り置いたすべての人が支払う。低いインフレは、その長期的な影響を人々がつかめないために、公衆に大目に見られる — 人々は、一桁の数字でさえ長い地平で複利で効くと、貯蓄を人々がもはや自分の老後を確保できない水準まで蝕むことに気づかない。そしてそれができなくなると、人々は国家の給付への依存へと条件づけられる。最後には人々はその給付にすぎり、国家につながる。

激動の時代 — 戦争、パンデミック、「必要な」投資 — には、国家は単に印刷機のスイッチを入れる。責任ある貯蓄者と労働者の購買力は下がるのに、私たちは彼らに、あなたたちは十分に報われていると約束する。誰かがひそかに彼らの時間を盗み、彼らがなんと見事に稼いでいることかと褒めそやす。

これは国家への信頼を深刻に損なう。そして信頼こそ、機械全体をまとめる唯一の接着剤である。それが、踏ん張って押す価値のある梃子である。

■ なぜ金であって、他の弱点ではないのか

文明のもう一つの弱点は、たとえばエネルギーの分配である。だがその流れを妨害することは梃子ではない — それは侵略、テロになるだろう。自発的な不参加は、意図的に他者を害することと同じではない。金は、圧力を自発的に、透明に、そして暴力なしにかけられるという点で例外的である。

Proposed transition to the state's successor

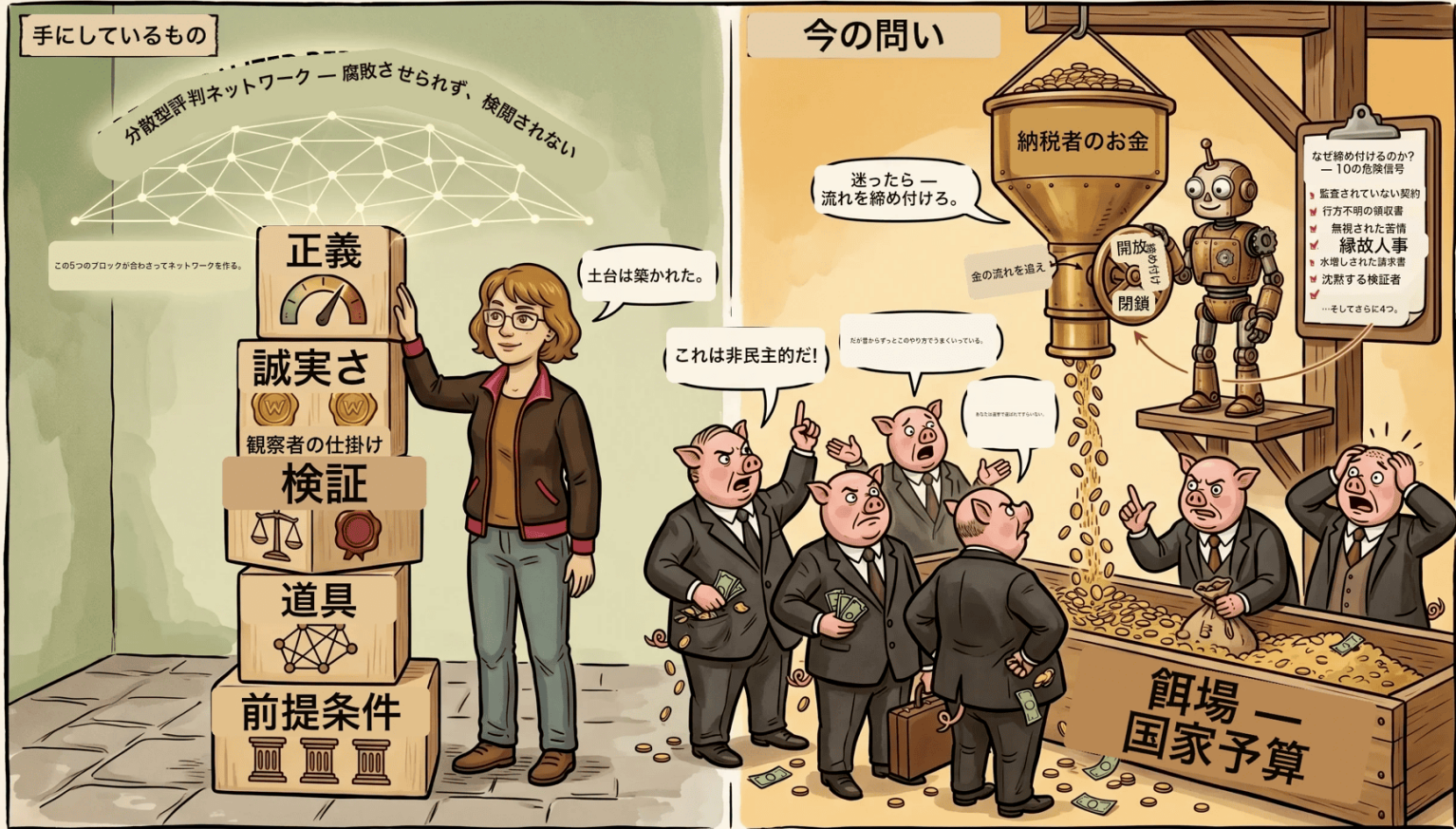
革命ではなく進化

急激な変化は、最終的な目標が魅力的であるときですら抵抗を呼び起こす。それは絆 — 社会的、経済的、政治的な絆 — を断ち切り、人々は本能的に、まだ見ぬものに対して、すでに知っているものを守る。

したがって正しい取り組み方は漸進的 — 進化的 — なものである。古いシステムがボタンのひと押しで新しいシステムを切ってしまうのを防ぐものである — というのも、そうできる瞬間、古いシステムはそうするからだ。

残念ながらこれは、評判ネットワークを展開した瞬間に均衡的な自発性に達するわけではないと受け入れることを意味する。それは漸進的な採用率とともに訪れる。取り込みは遅いかもしれない — そしておそらく遅い — だろう。順応的な正義の求め方が失敗するとき（そしてそれは失敗する）、評判ネットワークを通じて自らの共同体に救済を見出したいという個人の欲求に引かれて進む。その道がどんなものかを、比例的な見積もりも含めて見てみよう。

金の流れを追え — これまでの物語



ネットワークは手にした。仕組みも分かっている。さあ:迷ったら、餌箱を締め付けろ。
国家の権力はお金の上に成り立つ。それを追え。

■ 空の飼い葉桶 — あなたが負けるよう仕組まれた規則で勝負するな

国家を内側から改革しようとする試みは、権力の内部の仕組みに頼り、役人たちが自らのインセンティブに逆らって変化を押し通してくれることを望む。それは起こらない。

なぜシステムに命をもたらしチャネルを枯らす代わりに、システムに を与えるのか。古いシステムを変えてその規則で勝負する代わりに、その上に新しい層を築こう — 古いシステムを新しいシステムの部分集合へと徐々に変えていく層を。始まりにおいて、その部分集合はほとんど全体集合を満たす。時とともに行為者たちは移っていく。

企業はこれを知っている。古いシステムが置き換えるにはあまりにも絡み合っているとき、あなたは並行するシステムを築き、利用者を徐々にそこへ移していく。

国家が、実際に提供するものとその法令が要求するもののあいだの食い違いに行き着き、その食い違いを持ち出したがるだろうという事実は、もっぱらその代表者と参加者の問題である — それを振り返る必要はない。見張る価値がある唯一のことはこれである。暴力的な革命を挑発するな。

互いを支え合う四つのツール

これまで **DID** 評判ネットワークは、主に正義とコンセンサスに役立つように見えたかもしれない。私は、それが自らを安定させ攻撃に耐えられると信じている — 形式的な肩書きではなく実際の功績に基づいて、メリトクラシー的に。だが評判だけでは国家に譲歩を強いることはできない。経済がそれを強い、そしてそれを通じてかけられる圧力が強い。

私たちが、金に強く圧力をかける追加のツールの管理者として **DID** アイデンティティを使うことを妨げるものは何もない。市民の側の完全な自発性から始めるな — 国家が止められない方向を設定せよ。移行は、互いの背中を支え合う四つの具体的なツールの上に立つ。そのどれも単独では十分ではない。

単純な税制 — 入口の誘い

第一のツールは、**DID** インフラの上に築かれた単純で透明な税制である。すべての所得に対する単一の比例税率。例外なし、免税期間なし、法人向けの控除なし、優遇措置なし。すべての支払いは、それを支払った **DID** と監査可能な形で結びつく。相互照合は容易である。

税率は、納税者の一部にとって古いシステムよりもいくぶん有利に設定される — それが入口への誘いである。税負担は年を追うごとに下がり、システムはますます魅力的になり、移行は勢いを増していく。システムは同時に記録の保持者であり徴収者でもある — 仲介者なし、不透明さなし。

電子支出登録 (ESR)

第二のツールは、**EET** (電子収入記録) を逆さまにひっくり返すことである。国家が個人事業主のあらゆる領収書を追跡する代わりに、私たちは国家のあらゆる支出を追跡する。国家は、それぞれの支払いが — 例外なく — このふるいを通過しないかぎり、いかなる個々の支払いについても単純な税制から資金を受け取らない。

ESR は、国家と公共部門のあらゆる実現された支出を、計画された支払いの記録 — 文脈的な正当化と、受取人、支出主体、目的の識別を含む — と突き合わせるプロキシ⁶である。その結果は生の公開データであり、階層化可能である。誰でもそれを取って分析できる。誰でも、それをどう扱うかについて

⁶プロキシ (proxy、ラテン語 *procurator*、英語 *deputy/intermediary*) — ここでは、別の主体に代わって行動する仲介者。**ESR** プロキシは、計画された支払いの記録を誰からでも受け付け、それらを国家の実現された支出と突き合わせ、結果として得られるデータセットを公衆に利用可能にする。

納税者に推奨を提供できる。監査機関が何年かけても達成できなかったことが、突如としてみんなにとってワンクリックの距離になる。

参加するために新しい税制に切り替える必要はない。実現された支払いごとに、完全に払い戻し可能な保証金（たとえば **1〜3** ユーロ）を支払えば十分である。実現されなかった残りは、システムが攻撃で氾濫しないよう、スパムフィルターとして没収される。記録は誰でも提出できる — 判断能力を失った祖父母のために親族が、放置された公共サービスのために隣人が、未払いの請求書のために起業家が、自らのシステムからのエクスポートによって役人が。

私は、政党が自然と分析の提供者へと姿を変えるか、あるいは古いものにとって代わる新しいものが現れると予想している。税から引き出される拠出金の代わりに、彼らは専門知識を提供し始める — 支持者に、盟友となる権威、そのサービス、検証方針についての価値観に基づく概観を提供する。怠惰ゆえにずさんな、あるいは無意味な記録は、自動的に予算削減の候補になる。第一ラウンドではあなたの支払いは常に支給されるが、集められたデータは、ある国家支出がなお意味をなすかどうかを評価するための基礎に役立つ。請負業者やその他の国家の給与を受け取る者たちは、役人が支出を責任を持って突き合わせることを確かめるインセンティブを持つ。さもなければ、次のラウンドで金は流れてこない。

■ ESR という略語の由来

2016 年から 2022 年にかけて、チェコ政府は EET（電子収入記録）と呼ばれるシステムを、自国の市民 — 個人事業主と起業家 — に対して実施した。そのメッセージは単純だった。「我々は君たち一人ひとりが国家を欺いていると想定する。君たちはあらゆる取引を記録し、それをリアルタイムで我々のサーバーに送信し、我々は君たちを見張る。君たちが EET を逃れようとすれば、それを通報した同胞の市民に我々は金銭的に報いる。」

EET はバルカンの先例をモデルにしていた。全国的な義務としてのリアルタイムのオンライン売上記録システムを世界で初めて開始したのは、2013 年、クロアチアであり、*fiskalizacija*（フィスカリザツィア）という名だった。チェコ共和国は数年後にこのモデルを採用し、ヨーロッパで最も厳格な収入追跡体制の一つを運用した。

闇の側がためらわないのなら、なぜ私たちがためらう必要があるのか。ESR は同じ論理を逆さまにひっくり返したものである。国家が市民に対して自らを証明するのだ。

市民による税の配分 — 決定の重み

第三のツールは、納税者に、自分の金がどこへ流れるかへの直接の影響を与える。第一ラウンドでは、国家は ESR が何を明らかにしようと自らの金を受け取った。第二ラウンドでは、国家はもはやそうしない — 第一ラウンドの分析と、そこから導かれる措置が引き継ぐ。支払われた税のわずかな割合を、支払人自身が配分できる — ただしその DID が評判上の要件（市民権、居住、共同体に承認された成人／能力）を満たしていれば。配分可能な割合は年を追うごとに増えていく。潜在的には指数関数的に。今日の五パーセントから、十年のうちに数十パーセントへと。

ESR — 電子支出報告

すべての国家支出が記録される — すべての記録が公開される — すべての詳細が精査に開かれる。

誰が提出するか

記録は以下によって提出できる:-
支払いを処理した職員 -
支払いを受け取った受領者

国家支出の公開台帳 ― 開かれた記録

分類:法務顧問 契約業者:法律事務所XYZ
s.r.o. 金額:1,400万ユーロ 支払済み
契約日:2026-01-14
支払日:2026-01-19

背景:新しい調達改革法案についての外部意見 —
 草案3件作成、省庁とのワークショップ1回、公聴会は開催されず
 — 最終草案は立法期限後に提出。

分類:道路設計コンサルティング
契約業者:コンサルタンシー
金額:900万ユーロ 契約日:2026-02-03
支払日:-

背景:D-X高速道路延伸のための実現可能性調査 —
 同じ会社がこの路線について過去に3件の調査を書いている
 — 結果:従来の見積もりより18%増での続行を勧告。

見たい人には誰にでも聞かれている

分類:ナンバープレート発行
受領者:地域事務所Z
金額:1枚あたり45ユーロ

契約日:2026-02-19 支払日:2026-02-19
背景:発行されたプレートごとの標準事務手数料
— 手数料は材料費と処理費を含む —
今四半期の総発行数12,400枚。

分類:病院設備 契約業者:MedSupply
a.s. 金額:820万ユーロ 期限超過

契約日:2026-03-08 支払日:—
背景:地域病院へのMRIスキャナー設置 —
公開入札、応札者3社 —
選定された入札は中央値より2%低い —
60日以内の納品 — 請求書は期限を90日超過。

スパムフィルター — 返還可能な供託金

記録が正確だと証明されれば償還金は返還される。

政党は分析提供者へと姿を変える

この記はこそが原材料だ。――

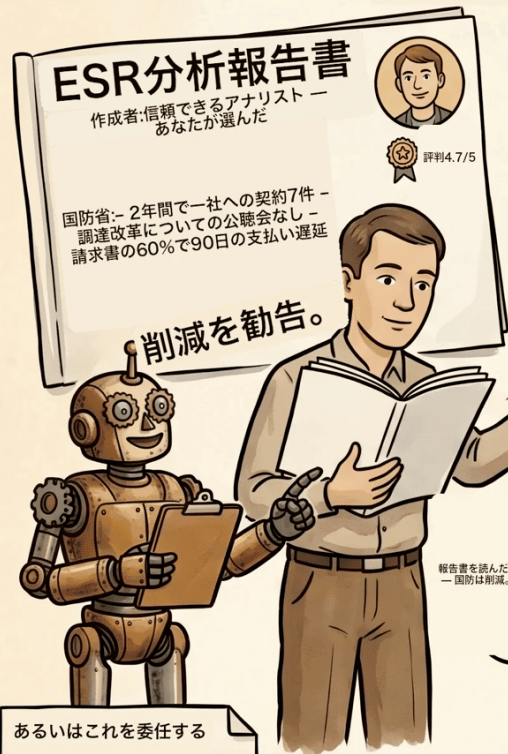
公金の一クラウンに至るまで — 記録され、公開され、精査可能だ。

その価値は不正を捕まえることにあるのではない — 帳簿を開くことにある。

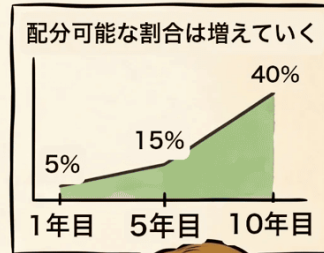
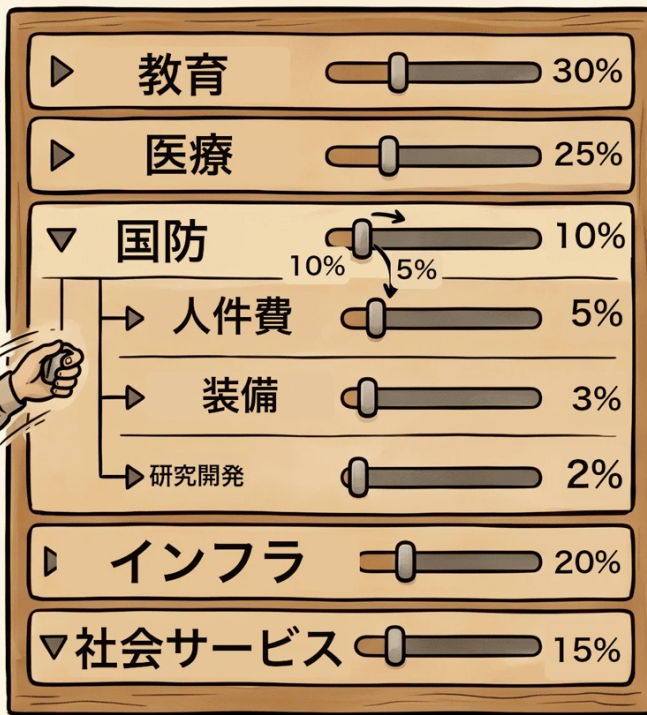
生の **ESR** データは自然に納税者の決定を導く。質の低い記録は、推奨される削減の警告シグナルとして機能する。誰でも記録を作れる。役人はそれを突き合わせなければならない。それがなければ、税制は国家にいかなる金も送らない — 国庫にも、他の予算章にも。政治的な戦いは、投票箱から、具体的な硬貨の日々の配分へと移る。

市民による税配分 — 自分の税金の行き先は自分で決める

ESRの記録を調べる。それからスライダーを動かす。



報告書を読んだ後ー国防は削減。



任意の行をクリックして詳細を掘り下げるー好きな順番で配分できる。

今日の5%から、10年後には40%へ。決めるのはあなただ。

記録は開かれている。分析はあなたのものだ。スライダーもまた。

国家との交渉プラットフォーム — 梃子

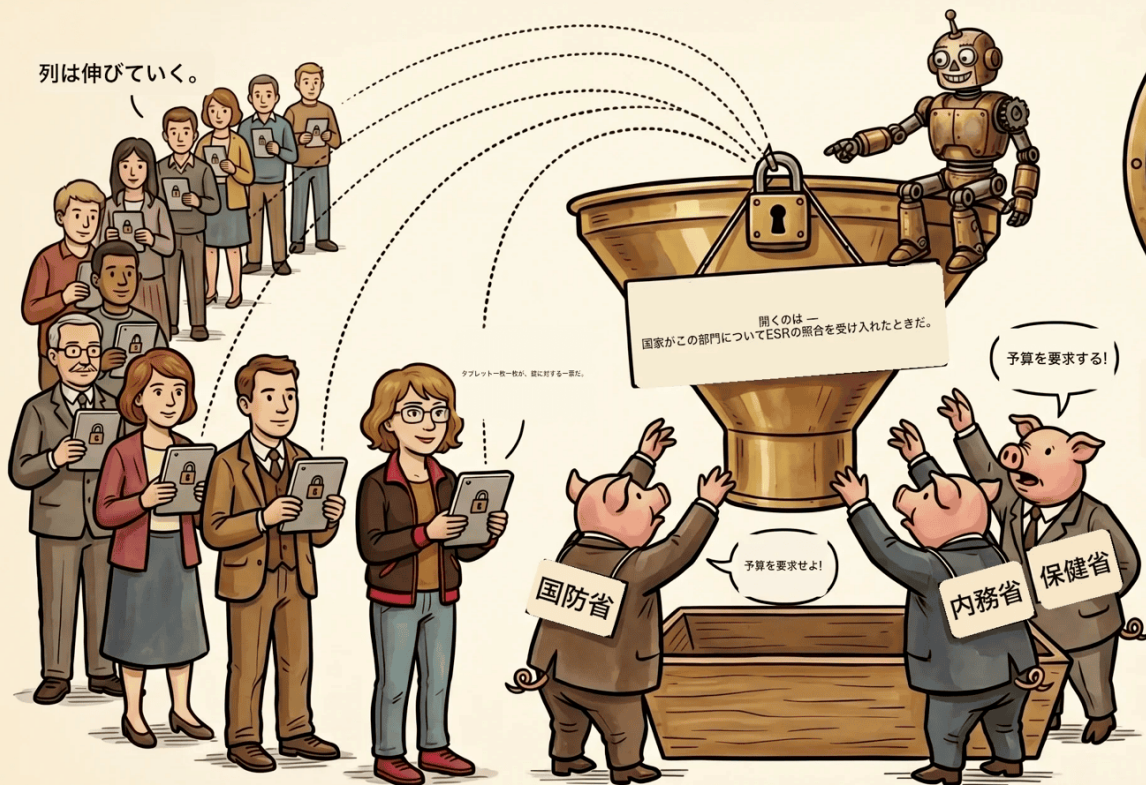
第四のツールは、すべてを結びつけ、今こそネットワークを現実の脅威にする梃子である。主要な対立は、国家が **ESR** を拘束力ある標準として受け入れるかどうか — まずは国家のレベルで — をめぐるもの、そしてそれが起きる前に評判ネットワークの参加者からの脅威がどれほど大きくならなければならないか、をめぐるものになる。

梃子は、支払いが **ESR** と突き合わされることを条件とする、ジャストインタイムの国家資金供給である。国家が透明性の条件を満たした瞬間にのみ、金は流れる。参加者の待機リストが評判ネットワークの内部で形成される。集団が経済的に有意義な規模 — **GDP** 成長を脅かすに足る大きさ — に達したとき、作動が始まる。その時点で、市民的不服従は身振りではなく信頼できる脅威になる。

国家は、腐敗に結びついた問題ある支払いに最も長くしがみつくだろう。圧力のもとで、国家はまず、容易な防御を持ち、節約を探る余地のないところで譲る。漸進的で高まる圧力が、あらゆる立場から一歩ずつ退くことを国家に強いる。

交渉プラットフォーム — 閉ざされた餌箱

鍵を握るのは市民だ。条件が満たされれば国家は開く。



GDPのわずかな割合で十分だ — 臨界質量に達すれば、支払い保留は現実の脅威になる。

臨界質量を超えると —

国家はまず、単純で正当化できる支払いから帳簿を開く。

腐敗と結びついた分類は最も長く閉ざされたままになる。

解錠のたびにより大きな圧力が必要になり — それ自体も記録される。

透明性があるとき、お金は流れる。鍵を握るのは市民だ。

武力はいらない。革命もいらない。支払い保留を現実的にするだけのタブレットがあればいい。

身分証明書のない市民権

DID インフラへの移行に伴い、国家発行の身分証明書はその独占的な目的を失う。身分証明書は必要ない — あなたは一連の **DID** アイデンティティを持ち、そのいくつかは、たとえばあなたがチェコ人である、特定の自治体の住民である、特定の学校の卒業生である、という主張を帯びる。その主張は検証可能で、恒久的で、国家の行政から独立している。

技術的な実装の問題が開ける。関心を持つ当事者たちを、適切な主張を帯びた **DID** へと移行させるために、国家の統制の外で既存の市民を検証する役目を、市場で誰が引き受けるのか。おそらく、アイデンティティの検証を専門とする自由市場の権威 — 公証人、地域の共同体、雇用主 — が現れるだろう。彼らは、ある **DID** が本当にそう主張する人物に属するという事実に至らの評判を賭ける。市民権 — すなわち、共同体についての特定の見方への帰属 — は、中央集権的な記録保持の必要から解放される。評判ネットワークを通じてつながることで、埋め込まれたデータは二度、三度、四度、そしてそれ以上と、接続され検証される。

その帰結は直観的だが、中央集権システムでは解決不能である。今日、政治指導部は — より容易な再選を見据えて — 共同体の領域に集中した問題を持ち込める。吸収能力や既存の共同体の意思にかかわらず、別の文明圏からの移民を受け入れ、他の文明圏からの到来者を同化させるのが追いつかないほどの圧力のもとで、元の共同体を変質させる。**DID** ネットワークでは、腐敗した形で受け入れられた移民は、共同体が自分をこれからも仲間の一人とみなし続けるとは確信できない。共同体のメンバーは、見知らぬ者が共同体の制服を着て玄関に来て、家の中で実行しようとする措置の合法性（ソーシャルメディアの投稿を理由とした子どもの電話の没収）で自分たちを脅すのに、客観的に耐える必要はない。分散型の評判があれば、社会の多数派はこれに甘んじる必要はない — 共同体への帰属は、役人によってではなく、共同体自身によって、その評判シグナルを通じて決められるからである。

進化的移行のための4つの道具

システムは内側から作り直される — それを壊すことなく。

単純税



税率は一つ。抜け道はない。相互照合可能。

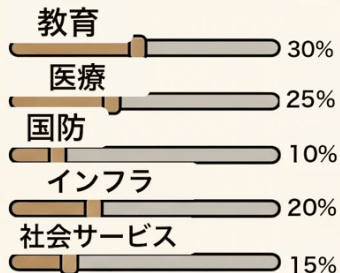
ESR — 電子支出報告



すべての支出が記録される —
すべての記録が公開される —
すべての詳細が開かれる。

市民による税配分

5% → 15% → 40%
1年目 → 5年目 → 10年目



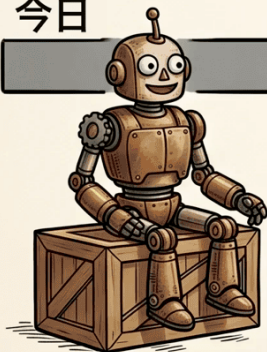
記録を調べる —
それからスライダーを動かす。

交渉プラットフォーム



お金が流れるのは、透明性の条件が満たされたときだけだ。

今日

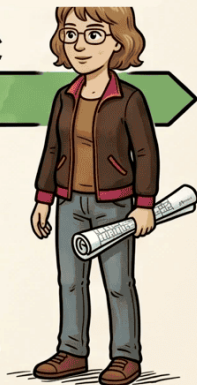


進行中の進化

95%

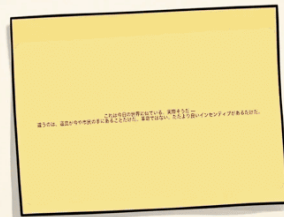
10年後

拡大中



革命ではなく、進化だ。

システムを内側から変える4つの道具。



身分証のない市民権

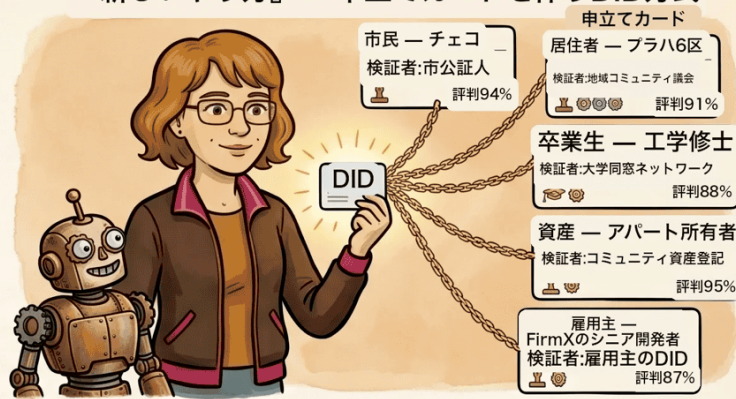
国家の許可からコミュニティの承認へ。

『古いやり方』 — 制度化された国家発行ID方式



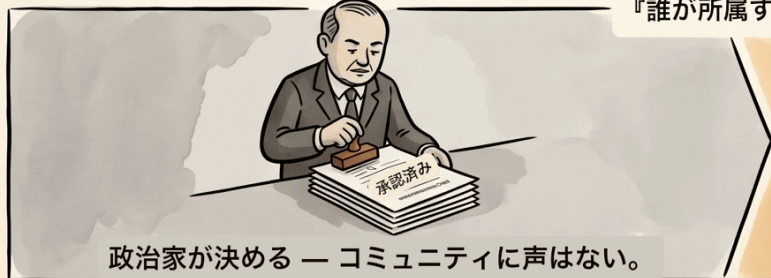
アイデンティティ=国家の許可 — 取消可能 —
コミュニティに発言権はない。

『新しいやり方』 — 申立てカードを伴うDID方式



すべての申立てを支配する単一の権威は存在しない —
それぞれが独立している — それぞれの検証者が自らの評判を賭ける。

『誰が所属するのか?』



あなたの市民権は政府の許可証ではない。それはあなたのコミュニティの承認だ。

国家の印は、独立した検証者たちの連鎖に置き換えられる — それぞれが自らの利害を賭けている。

国家の管轄下の事柄についての選挙票の重みは、将来的には、単純な税制への貢献の記録と厳密に相関させることができる。適切な **DID** の主張（たとえば「この人物はチェコ市民である」）と組み合わせれば、外国の国民を選挙から除外できる — 住民登録が単純にここへ移るのだ。

重なりと可逆性

私はこれが唯一の道だとも、あるいは最良の道だとも主張しない。だがそれは包括的に見える — 主要な梃子を覆い、後戻りする選択肢を保つ。始まりにおいて、新しいシステムは古いシステムと重なり、インセンティブだけを変える。時とともに古いシステムは縮み、やがて — そうする必要はないが — 溶けて消えうる。利点は漸進性と可逆性である。設計に誤りが現れても、それは終わりではなく、ただの修正である。

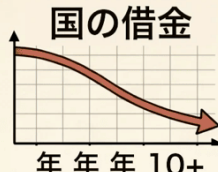
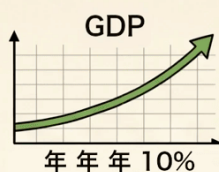
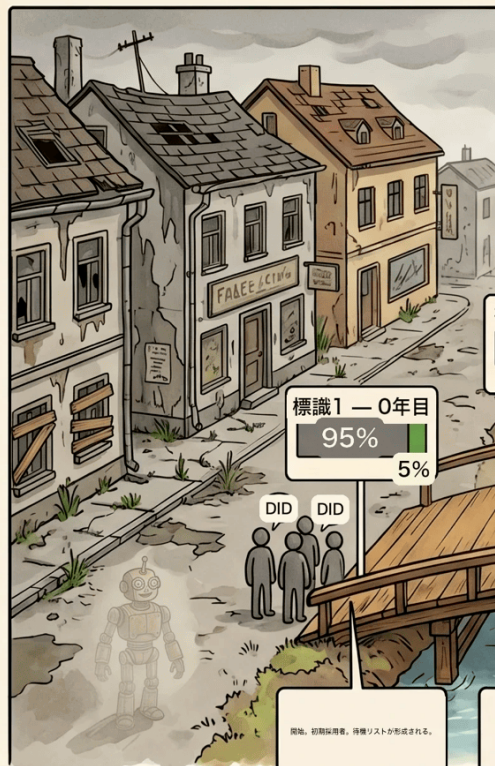
■ 平和と戦争

国家のある部分は、完全に市場に基づく代替を持たないかもしれない — おそらく軍隊である。危機における非常権限の一時的な委任（古代ギリシャ人が独裁官を任命したように）は存在し続けうる。だが責任は、指導者ではなく、分散型の社会に置かれる。中央集権的な統治とは異なり、脅威が過ぎ去ったなら — あるいは必要ならもっと早く — 委任された権限を取り戻すのは容易になる。自由な社会は、権威主義体制に対する武力の衝突においてすら不利にはならない。

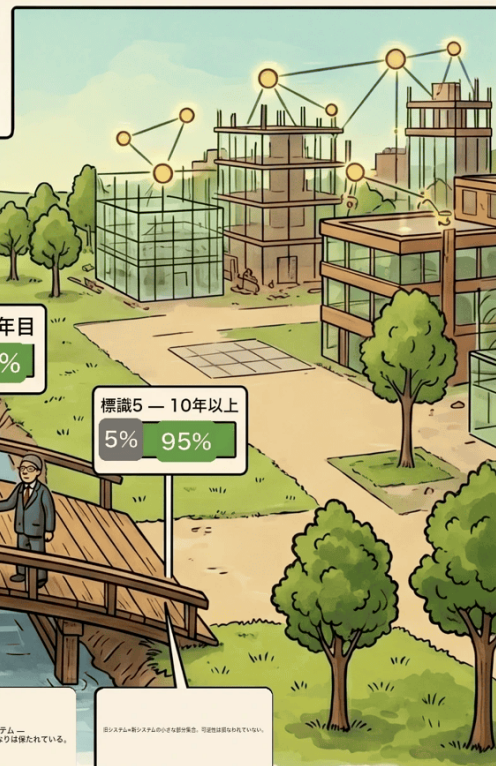
■ 戦争犯罪人

ジャストインタイムの国家資金供給と透明な支出があれば、侵略戦争のための資源を蓄積するのは難しくなる。そのような戦争に資金を供給し続ける納税者は、正当な標的になり、ジュネーブ諸条約のもとで民間人の地位を持ち出すことはできない。新しい仕組みのもとでは、沈黙の同意は参加とみなされる。

左岸 — 『旧システム』



右岸 — 『新システム』



標識1 — 0年目
95% 5%

DID DID

開始、初期採用者、待機リストが形成される。

標識2 — 2年目
80% 20%

成長中、参加者リストが膨らむ。

標識3 — 5年目
50% 50%

設計に誤りがあれば後戻りできる、可逆性は保たれている。

標識4 — 8年目
25% 75%

75%が新システム — 国家はその部分集めた、重なりは保たれている。

標識5 — 10年以上
5% 95%

旧システムと新システムからの移行が完了、可逆性は保たれていない。

臨界質量 —
経済的圧力の下で国家がESRを受け入れる。

逆行

旧システム

> 漸進的な移行。誤りがあれば後戻りできる。止められない方向性。

結論

道は存在する

国家が今ある姿なのは、その創出の時点で利用可能だった技術が、人間の本性と組み合わせあった結果である。平均的な人間の本性を否定しながらすべてを自発性の上に築くのは素朴である。それは腐敗からも、全体主義へと漂流する傾向からも、自らを解き放てない。国家の後継は、私たちが現在是否定的とみなし、追放するか罰するかしている性質とともにでも機能しなければならない。

この本はある問題を記述した — ルールを書く人々がその帰結とともに生きることが決してないシステム（国家）である。それは、そのシステムが機能しなくなるために成り立たなければならない条件を記述した。それは、それらの条件を満たすツールを記述した。そしてそれは、移行の方法論 — そのツールをどう使うかの具体的なステップ — を、一つの可能な例として提案した。

第一章で私は五本の柱を挙げた。自発性、組織化、耐性、コンセンサス、そして買収不能性である。私たちはそのすべてを満たした。

- **自発性** — 誰もあなたをネットワークに強制しないが、あなたも自分の行動をそこから消し去ることはできない。
- **組織化** — 共同体は、上から割り当てられた者からではなく、あなたが知る者から育つ。
- **耐性** — あらゆるパケットの監視に支払う気のある国家でさえ、それを切ることはできない。
- **コンセンサス** — それは票や署名からではなく、偽善につけられた値札から生じる。
- **買収不能性** — 五つの小さな規則が腐敗をコストへと織り込む。自発性と責任の均衡、誰もが持つ発言の権利、誰も選べない入口、偽善に代価がつく公の約束、そしてあらゆるトランザクションの背後にあるオブザーバーの影である。

どの柱も単独では国家に取って代われない。それらが一つになって、国家がそのあらゆる装置をもつてしても築けない、腐敗への抵抗を形づくる。

私たちは、その全体を現代の技術（暗号技術、分散型アイデンティティ、インセンティブを正しく設定するためのよく知られた心理的なパターン、...）で築ける地点にいる。欠けているものはただ一つ。それを支持する勇気を見出し、始めることを決める人々のクリティカルマスである。

革命によってではなく。

これらのアイデアは **2025 年 6 月から 2026 年 5 月**にかけて形をなした。書き始めるために腰を下ろすころには、私は頭の中でその枠組みをおおむね練り上げていた — だからこそ、**Farewell To Westphalia** が現れたとき、私はそれをあれほどの好奇心をもって読んだ。彼らの描く絵が、どこで私のものと重なり、どこで分かれるかを見たかったのである。第二のきっかけは、**2026 年 5 月**現在なお異なる角度から自分自身の本『国家の脱構築』に取り組んでいるダン・シュタイガーヴァルト（**Dan Steigerwald**）から来た。彼のプロジェクトが、私自身のビジョンを全幅で書き記すことへと私を押しやった — 世界がそれを、他のものと並べてテーブルの上に持てるように。

私はそのどれも信じてほしいと頼んでいるのではない。それについて考えてほしいと頼んでいるのだ。そして私はあなたに一つの問いを残す。

あなたなら何を変えるだろうか。

Pavel Kudrna 2026 年 5 月 23 日、プラハ、チェコ

謝辞

インスピレーション

Farewell to Westphalia (Jarrad Hope、Peter Ludlow) の著者たちに感謝する。自分自身のアイデアを、国家のウェストファリア型モデルを脱構築するというより広い文脈の中に位置づけるのを助けてくれた知的な枠組みに対して。

レビューとフィードバック

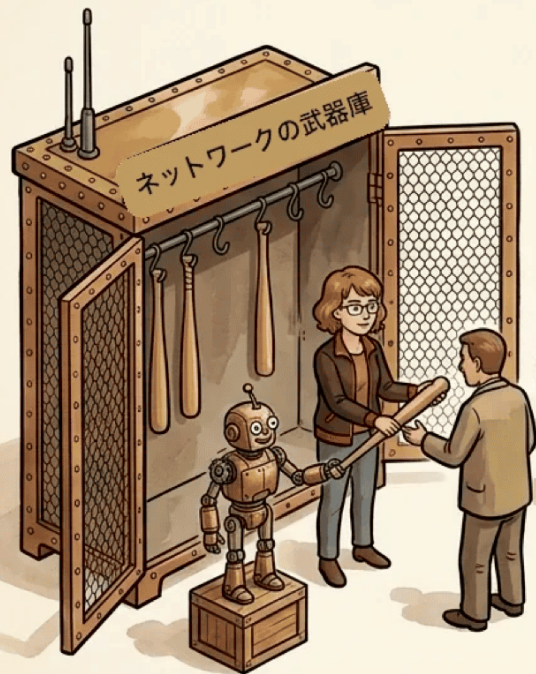
ツール

本文の準備、アイデアの構造化、そして表現の推敲にあたって、私は **AI** ツールの助けを用いた。すべてのアイデア、議論、結論は私自身のものである — **AI** は推敲のためのツールとして役立ったのであって、内容の共著者としてではない。

インフォグラフィックは、著者の仕样に基づいて生成ツールとの協働で設計された。

自分の時間を取り戻せ

市民が寄生者を公的生活から追い出す。



彼らが奪おうとする時間を守れ。

欺瞞によって奪われたものは、自らの手で取り戻す。

プロジェクトを支援する

Personix はあなたのような読者によって支えられています。



Bitcoin オンチェーン

bc1q7cctdz6r026dgy06ul94eygg49ujtxnrq5czaj



Bitcoin Lightning

LNURL1DP68GURN8GHJ7AMPD3KX2AR0VEEKZ
AR0WD5XJTNRDAKJ7TINH4KXCCTTDEHHM30
D3H82UNVWQHXXMNP0FA8JMTDVD5XJMN9XUE
RX55QRQK

■ この金の行き先 — そして行かない先

これらの QR コードは**著者の個人的なチャンネル**である — 寄付は Pavel Kudrna に直接届き、さらなる執筆、社会実験／シミュレーション、そして周知活動の資金となる。

このプロジェクトの唯一の正当な資金調達チャンネルは次のとおりである。

- **本書の著者版** — 著者が承認した版に含まれる QR コード。
- **personix.org** あるいはそこからリンクされる Tor オニオンミラー — そこで *Personix* 財団がそこに記された活動のために集める。財団の資金は著者の個人的な資金とは分けて保管される。

それ以外の場所で宣伝されているもの — 再版で差し替えられたアドレス、そっくりのドメイン、ソーシャルメディアでの「**Personix のための募金**」、上記のいずれにも結びついていない資金調達 — は**ほぼ間違いなく詐欺である**。私たちは意図的に暗号通貨市場とその参加者を避けている。

用語集

用語集

用語	チェコ語	意味
権威 (Authority)	Autorita	情報を検証し、それに自らの評判を賭ける信頼された主体（人、組織）。専門化されている場合もある（捜査、法律、技術）。
主張 (Claim)	Tvrzení	一般には、任意の検証可能な言明。ここでは、評判ネットワークに公開された記録 — 暗号的に署名され検証された、出来事、性質、関係についての言明。 例：「私は自治体 X の住民である」あるいは「この人物は契約に違反した」。

用語	チェコ語	意味
区画化 (Compartmentalization)	Compartmentalize	一般には、情報を孤立した単位に分離し、一つの単位を露見させても他の単位を危険にさらさないようにすること。諜報機関から知られる原理。ここでは、独裁体制における並行する DID アイデンティティ — 一つが露見しても他は明かされない。
一貫性ハッシュリング (Consistent Hash Ring)	Hash ring	検証者を選定するためのアルゴリズム的な仕組み — リング上の位置は、ソーシャルグラフ内の DID 文書のハッシュによって決定される。非決定的でありながら検証可能な選定を保証する。
DID	DID (Decentralizovaná identita)	中央権威なしに、あなた自身が作成し管理するデジタルアイデンティティ。あなたの秘密 で暗号的に署名される — 誰もそれを取り消したり偽造したりできない。

用語	チェコ語	意味
DID 文書 (DID Document)	DID dokument	あなたの DID アイデンティティを記述する公に利用可能なデータファイル — 公開、ネットワークアドレス、メタデータを含む。ネットワークであなたのアイデンティティを検証するために用いられる。
デューデリジェンス (Due Diligence)	Due diligence	一般には、商業的あるいは法的な関係に入る前の相手方の綿密な検証 — その履歴、財務、評判、リスクを調べること。ここでは、評判ネットワークにおいては、検証された記録の入手可能性のおかげで、より速く、より自動的に行われる。
経済的中立性の原理 (Economic Neutrality Principle)	Princip ekonomické neutrality	ネットワークにおける正直な振る舞いは、経済的にはゼロに近い — 公開のコストは検証への報酬として返ってくる。不正な振る舞いは純損失である。
創発的 (Emergent)	Emergentní	誰かが設計したり指図したりすることなく、より単純な部分の相互作用から自発的に生じること。鳥の群れは計画なしに編隊を組んで飛ぶ — 編隊は各個体が従う単純な規則から創発する。

用語	チェコ語	意味
創発する社会契約 (Emergent Social Contract)	Emergentní společenská smlouva	上から（法）ではなく下から — 共同体内の繰り返される相互作用とコンセンサスから — 生じる振る舞いの規則。
ESR	Electronic Spending Register	公共支出を透明に追跡するための提案されたシステム — 国家のあらゆる実現された支出が計画された支払いと突き合わされる。チェコの EET に触発されているが、国家に対して向けられている。
ハッシュ (Hash)	Hash (otisk)	一般には、任意の入力から一意な固定長の「指紋」を生み出す一方向の数学関数 — 文書の指紋のようなもの。同じ入力には常に同じ出力を生むが、出力から入力を導き出すことはできない。ここでは、ハッシュリング上の位置を決定し、文書の完全性を検証するために用いられる。
ジャストインタイム資金供給 (Just-in-Time Funding)	Just-in-time financování	透明性を条件とする国家資金供給 — 国家が ESR を受け入れ、その支出を突き合わせたときにのみ金は流れる。協力を強いるための梃子。

用語	チェコ語	意味
メリトクラシー (Meritocracy)	Meritokracie	一般には、地位が、形式的な肩書き、コネ、あるいは相続された特権ではなく、実際の功績と証明された能力によって決まるシステム。ここでは、評判ネットワークは、共同体に明白に貢献する者を自然に優遇する — 彼らの声は、役職によってではなく実績によって、より大きな重みを持つ。
オニオンゲートウェイ (Onion Gateway)	Onion gateway	オニオンネットワーク上の DID アイデンティティのネットワークアドレス。 DID 文書とは別物 — アイデンティティを失うことなく変更できる（ドメインの背後の IP アドレスを変えるのと同様）。
オニオンルーティング (Onion Routing)	Onion routing (Tor)	ネットワークの検閲不能性を保証する通信プロトコル。メッセージは層状に暗号化される — 各ノードは一つの層を剥がすが、経路の全体は知らない。

用語	チェコ語	意味
オラクル問題 (Oracle Problem)	Oracle problém	一般には、デジタルシステムに入ってくるデータが、物理世界で実際に起きたことに忠実に対応することをどう保証するか。この用語はブロックチェーンの領域に由来する。ここでは、デジタルの記録が物理的な現実に対応するという保証として自らの評判を賭ける権威を通じて対処される。
現象学的 (Phenomenological)	Fenomenologický	一般には、諸現象を、あらかじめ与えられた理論なしに、それらから何が帰結するかを観察することによって、直接の経験に現れるがままに研究する取り組み方。ここでは、自由、社会契約、振る舞いの規範は観察される現象である — 上から定義される原理ではなく、人々のあいだの何千もの微視的な相互作用の帰結。

用語	チェコ語	意味
方針 (Policy)	Policy (politika)	一般には、ある文脈における振る舞いを支配する規則や原理の集合。ここでは、DID ネットワークのすべての参加者が自らの方針を宣言する — 他者の特定の振る舞いにどう応じるか、どの規則に従うか、どの罰を釣り合いが取れているとみなすか。方針の総体が創発する社会契約を形づくる。
プロキシ (Proxy)	Proxy	一般には、代役あるいは仲介者 — 別のものに代わって行動するシステムや主体。ここでは二つの文脈で用いられる。(1) 公共支出を計画された支払いと突き合わせるプロキシとしてのESR。(2) オブザーバーの仕掛けにおける、公開者と検証者のあいだのプロキシとしてのオブザーバー。
公開者 (Publisher)	Vydavatel	記録（不正、是正などについての主張）を作成し公開するネットワーク参加者。公開のコストを負う。

用語	チェコ語	意味
評判に基づくソーシャルネットワーク (RSN)	Reputační síť	参加者が現実世界の振る舞いについてフィードバックを交わす分散型ソーシャルネットワーク。記録は作るのに費用がかかり、読むのは安い。
評判シグナル (Reputation Signal)	Reputační signál	ネットワークにおける個々の記録 — 肯定的なもの（危害の是正、義務の履行）あるいは否定的なもの（不正、契約違反）。累積的に、シグナルは評判プロフィールを形づくる。
ソーシャルグラフ (Social Graph)	Sociální graf	あなたの連絡先と、あなたの連絡先の連絡先のネットワーク。アルゴリズムは設定可能な深さ（たとえば 3 段階）で検証者を探す。グローバルなブロックチェーンはない — ネットワークは自然に、重なり合う共同体を形づくる。
税の配分 (Tax Allocation)	Alokace daní	納税者が自分の税の一部がどこへ行くかを決める仕組み。配分可能な割合は年を追うごとに増えていく。

用語	チェコ語	意味
実績 (Track Record)	Track record	一般には、ある人物や組織の過去の結果、成功、失敗の履歴。ここでは、ネットワークにおけるある DID アイデンティティの過去のすべての相互作用 — 検証された主張、受け入れられた記録と拒否された記録 — の総和であり、そこからその評判が導き出される。
検証者 (Verifier)	Ověřovatel	記録を検証し公開するためにアルゴリズム的に選ばれた参加者。情報の真実性に自らの名声を賭ける。

制作についての注記

著者が留保する要素（CC BY-SA ライセンスの対象外）：**Personix** の名称とワードマーク、本書の表紙、そして支援チャネル（QR コード、アドレス、連絡用メールアドレス）。派生版はこれらの要素を削除するか置き換えなければならない。それらは、この原著を参照する目的でのみ用いてよい。

ソースファイル。完全なソース — マークダウンのテキスト、インフォグラフィック、ビルドスクリプト — はこの PDF とともに入手できる。

ツール。本文の準備と表現の推敲にあたって、著者は AI ツールの助けを用いた。インフォグラフィックは、著者の仕様に基づいて生成ツールとの協働で設計された。すべてのアイデア、議論、結論は著者自身のものである。

PERSONIX

妥協なき変革

検閲不能かつ買収不能な分散型評判ネットワーク

国家は、通信が遅く、決定がローカルで、権威が自らの治める町と同じ町に住んでいたときには機能した。今日のネットワークはその三つの前提をすべて反転させる — そしてそれらの上に築かれた諸制度は、もはや自らが統治する世界に合わなくなっている。この本は、実際に合うツールを記述する。アイデンティティは自分のものとして保て、真実は公に監査可能で、賄賂は評判上の自殺行為となる、分散型評判ネットワークである。

マニフェストではない。予測でもない。国家の後継をどう築けるかについての実用的な設計図である — 自発的に、一つの宣言から。

Pavel Kudrna ・ プラハ、2026

personix.org

クリエイティブ・コモンズ表示-継承 4.0 国際 (CC BY-SA 4.0) のもとでライセンスされる。