DPF研究会

2022.5.20

DXとトラストと検証可能性

早稲田大学基幹理工学部情報理工学科

佐古和恵

自己紹介

佐古和恵　早稲田大学 基幹理工学部 情報理工学科　教授

- 京都大学理学部（数学）卒業後, NECに入社.
- 情報セキュリティ, プライバシ保護, 公平性保証の研究に従事.
- 例：電子投票システム、電子抽選システム、匿名認証技術
- 「暗号技術を使っていかに健全なIT社会に貢献できるか」 2020年より現職.
- 第26代日本応用数理学会会長、2017-8年度電子情報通信学会副会長、現情報処理学会理事
- 国際会議Asiacrypt, CT-RSA, FC, PKC, ESORICS, ACNS, AsiaCCS 等プログラム委員長.

自己紹介：現在関わっていること

佐古和恵　早稲田大学 基幹理工学部 情報理工学科　教授

- 日本学術会議連携会員、文科省 科学技術・学術審議会専門委員、
- 金融庁　金融審議会委員、デジタル・分散型金融への対応のあり方等に関する研究会
- 最高裁判所　裁判の迅速化に係る検証に関する検討会委員メンバー
- 内閣官房　TrustedWeb推進協議会TFメンバー、新技術等効果評価委員会 委員
- デジタル庁　トラストを確保したDX推進SWG構成員
- ISO/IEC JTC 1 SC27 WG5 エキスパート
- (社)MyDataJapan副理事長.

MyData.org

The purpose of MyData Global is to **empower individuals by improving their right to self-determination regarding their personal data**.

MyDataGlobal

私たちはパーソナルデータに対する**個人中心**の取り組みを推進しています。個人が自身のデータについて十分に理解し、**主体性と主導権**を持って、自らのためにパーソナルデータを活用できる世界を目指しています。

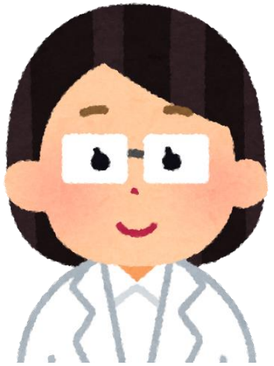
MyDataJapan

本日の内容

- DXとトラスト
- トラストと検証可能性
- 検証可能性と暗号技術
  - 公開鍵暗号、デジタル署名
  - ブロックチェーンとスマートコントラクト

Disclaimer

- セキュリティ研究者の職業病：疑り深い
- 悪い意図の人がはいってきても大丈夫なように設計したい
  - 基本的にすべての人を疑ってかかる
  - たとえ、100人中95人の人はいい人だとはわかっていても。。



DXと「トラスト」

トラストという言葉

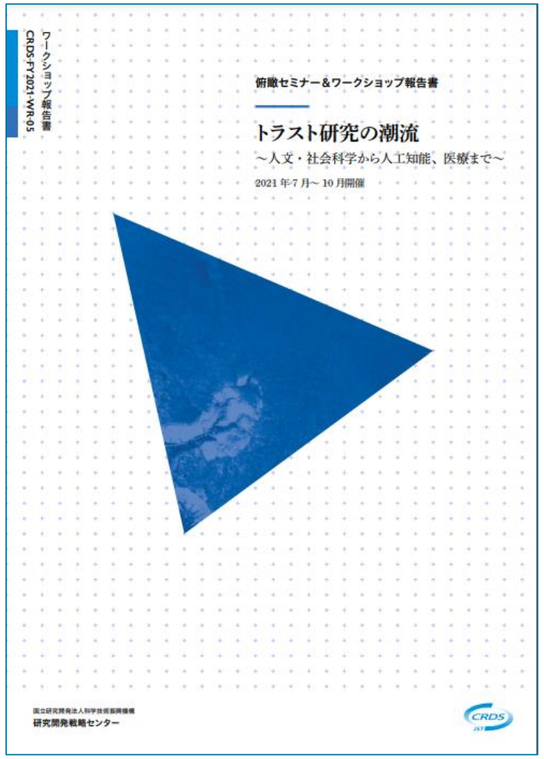
■ JST 俯瞰セミナー＆ワークショップ

「トラスト研究の潮流　～人文・社会科学から人工知能、医療まで～」

- 報告書

https://www.jst.go.jp/crds/report/CRDS-FY2021-WR-05.html
(2022.2月発行)

- セミナー 2021.7月-10月、計15回



JST 俯瞰セミナー：豪華な講師陣

1 **小山 虎** 「人文・社会系のトラスト研究の系譜」 (山口大学時間学研究所)

2 **上出 寛子** 「社会心理学におけるトラスト」 (名古屋大学 未来社会創造機構)

3 **犬飼 佳吾**「行動経済学・実験経済学とトラスト」(明治学院大学経済学部)

4 **大屋 雄裕** 「法制度とトラスト」 (慶應義塾大学法学部)

5 **神里 達博**「科学技術へのトラスト」 (千葉大学大学院国際学術研究院)

6 **村山 優子** 「情報科学におけるトラスト」 (津田塾大学)

7 **中島 震** 「ソフトウェア品質保証におけるトラスト」 (NII)

8 **松本 泰** 「ゼロトラストから考えるトラストアーキテクチャー ～トラストのメカニズムのパラダイムシフト～」 (セコム)

10 **山田 誠二** 「ヒューマンエージェントインタラクションと 信頼工学」 (NII)

11 **中川 裕志** 「AI のトラスト」 (理研)

12 **工藤 郁子**「公共政策とトラスト」(阪大社会技術共創研究センター)

13 **山口 真一** 「ソーシャルメディアにおけるトラスト問題」(GLOCOM)

14 **尾藤 誠司** 「医療におけるトラスト（1）」(東京医療センター)

15 **山本 ベバリーアン** 「医療におけるトラスト（2）」(阪大人間科学研究科)

トラストの定義の例

- ISO/IEC 25010:2011

‘degree to which a user or other stakeholder has confidence that a product or system will behave as intended

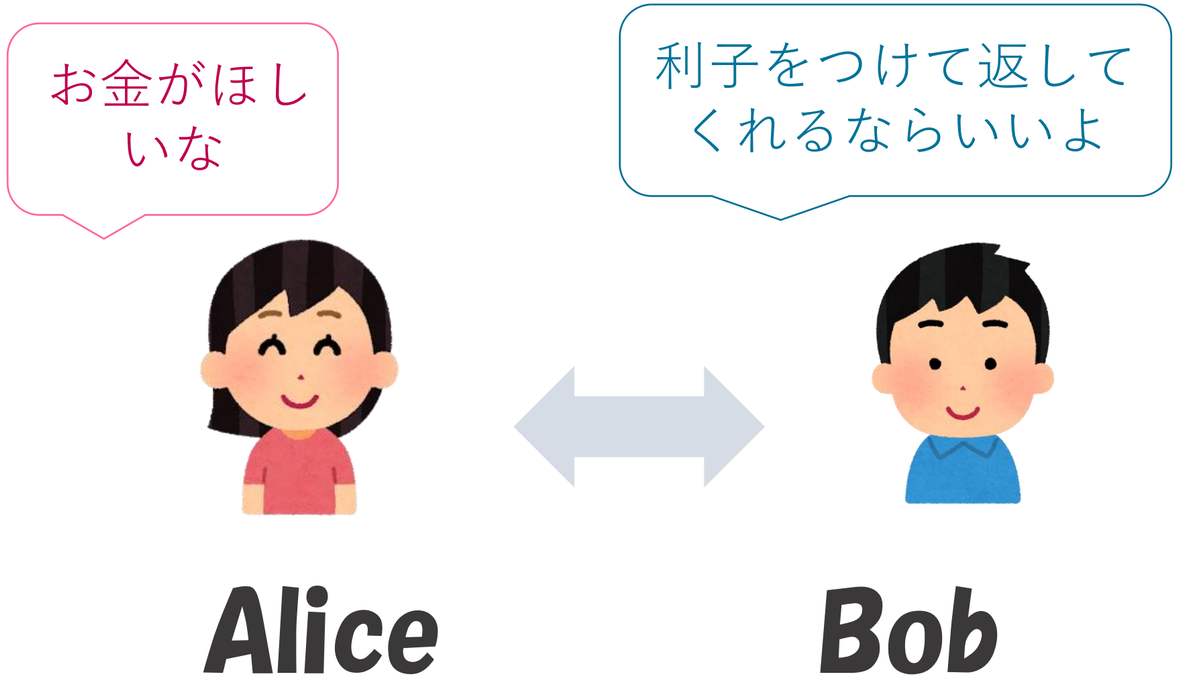
- TrustedWeb Whitepaper 1.0

「相手が期待したとおりに振る舞うと信じる度合い」

私の気づき

- 「トラスト」というのは、はやりの新しい言葉に聞こえるが、古来より人間が社会生活を営む上で必要不可欠な概念

例



リスク

お金がほしいな

利子をつけて返してくれるならいいよ

法外な利子を請求されないだろうか

ちゃんと返してくれるかな

Alice

Bob

不信

現在の社会のリスクの低減法

お金がほしいな

利子をつけて返してくれるならいいよ

Alice

Bob

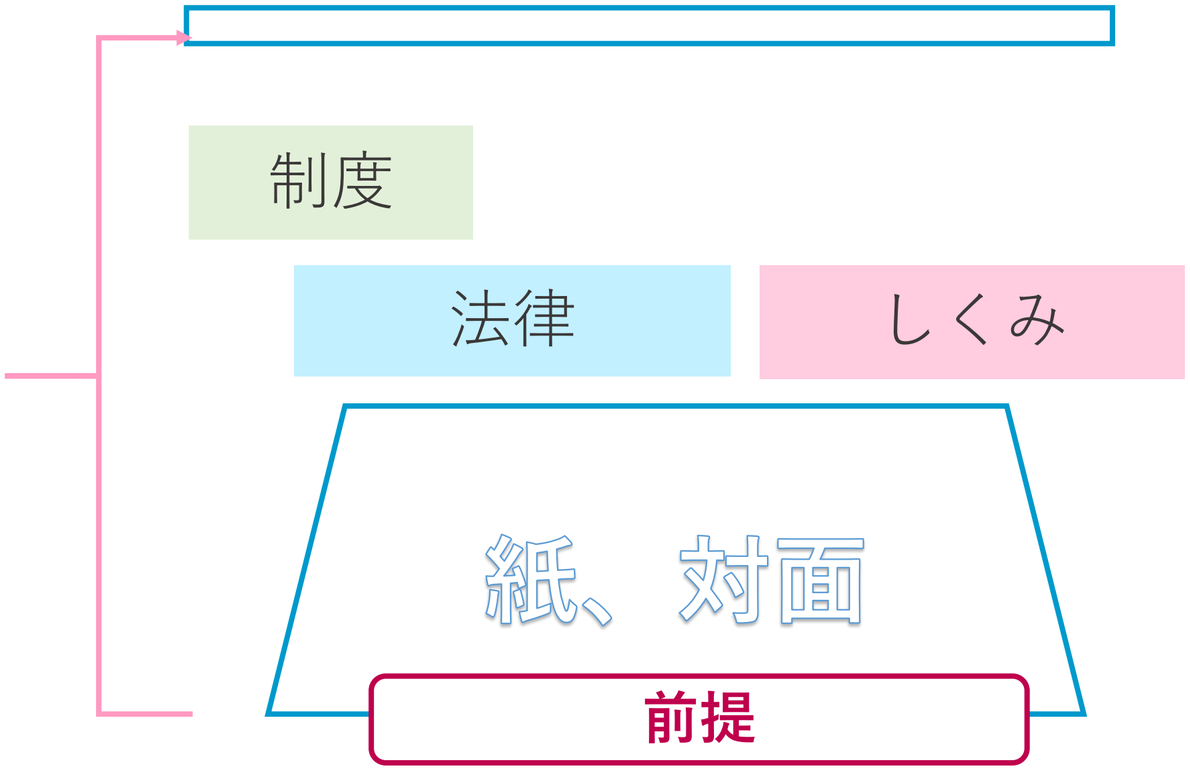
個人信用情報機関

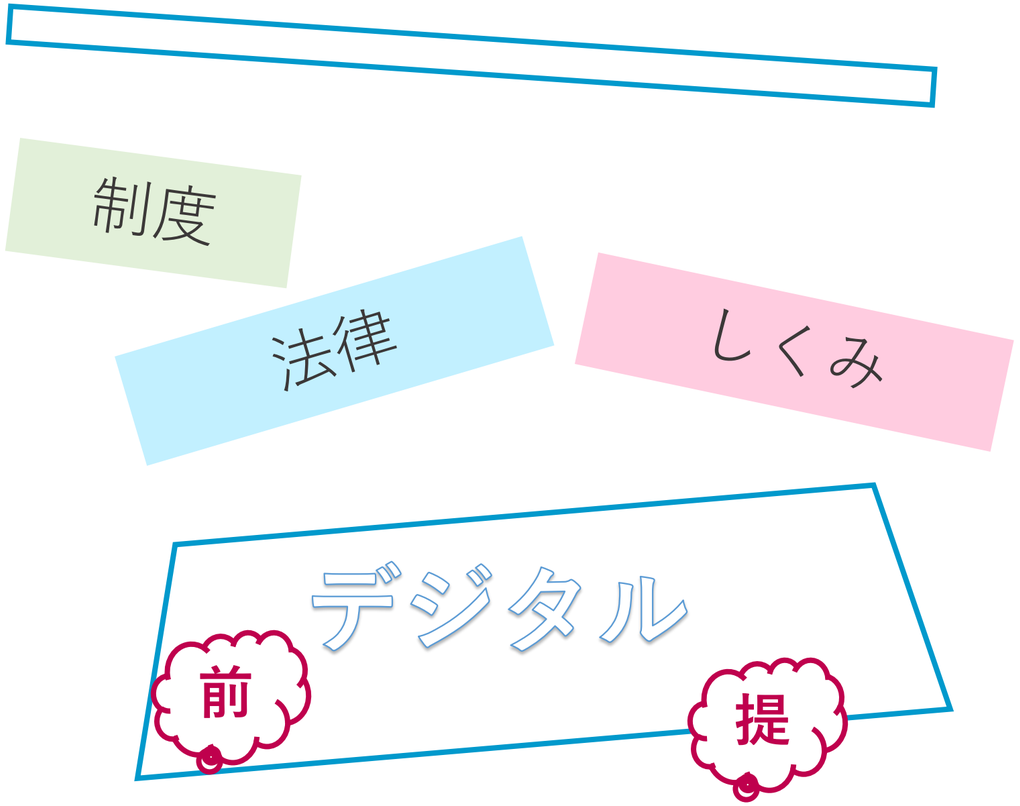
私の気づき

- 「トラスト」というのは、はやりの新しい言葉に聞こえるが、古来より人間が社会生活を営む上で必要不可欠な概念
- そもそも「トラスト」を~~確保~~なんとかする（リスクを減らす）ために数々の法律や制度がうみだされてきた
- 「紙」や「対面」でなんとかしてきた法律や制度がDXの波をうけてトラストにほころびが出てきたので、「トラスト」が（セキュリティに代わり）目新しくなってきたのでは

基本にたちかえって根本的な議論を

トラスト





私の気づき

- 「トラスト」というのは、はやりの新しい言葉に聞こえるが、古来より人間が社会生活を営む上で必要不可欠な概念
- そもそも「トラスト」を~~確保~~なんとかする（リスクを減らす）ために数々の法律や制度がうみだされてきた
- 「紙」や「対面」でなんとかしてきた法律や制度がDXの波をうけてトラストにほころびが出てきたので、「トラスト」が（セキュリティに代わり）目新しくなってきたのでは
- 解決すべき根本的な問題は変わっていないのでは
- **多くの人を巻き込んで、言葉や概念を共有し、少しでもベターな方法を地道に試行していくしかないのでは。**

デジタルデータとトラスト

- デジタルデータは変更が容易
  - 違うデータにすり替えられても気が付きにくい
- 他人のコンピュータでの処理は「ブラックボックス」
  - どのようなデータにどのような処理を施した結果が提示されているのか

トラストと検証可能性

- デジタル世界の取引リスクを軽減するために「検証」
- 相手は誰なのか（認証）
- 相手は約束を守っているのか（検証可能性）
  - 守ってくれなかったことの証拠（第三者検証性）

  - 暗号技術がささえてくれるのでは？
  - 公開鍵暗号、デジタル署名とスマートコントラクト

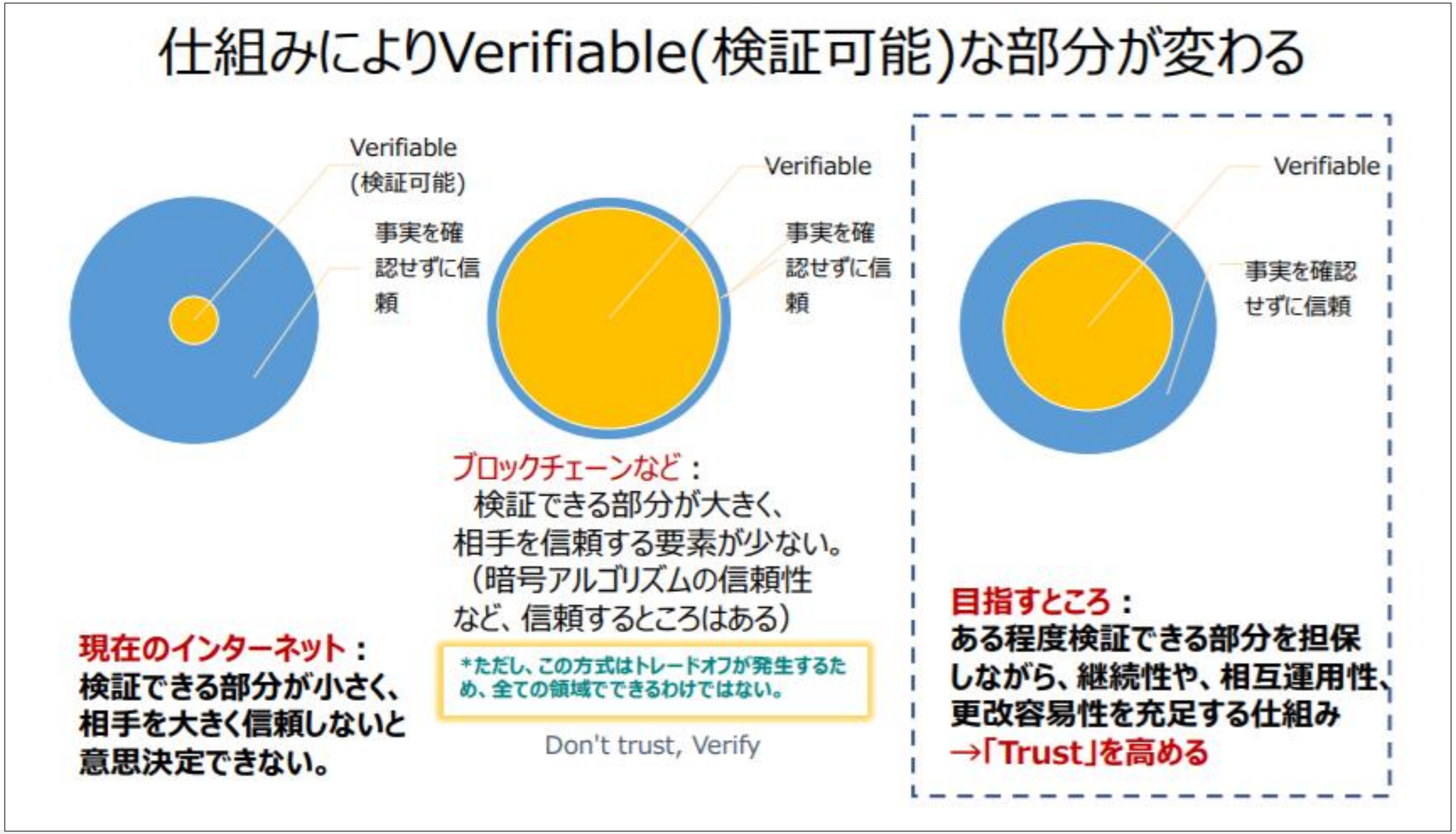
トラストと検証可能性

- デジタルデータは変更が容易
  - 違うデータにすり替えられても気が付きにくい
    →ある人から発出された時点から変わっていないことが検証可能
- 他人のコンピュータでの処理は「ブラックボックス」
  - どのようなデータにどのような処理を施した結果が提示されているのか

  →決められた処理を施した結果であることが検証可能

Trusted Web推進協議会のホワイトペーパー(p12)

https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/pdf/documents_210331-2.pdf



TrustedWeb 設計・運用における原則

支える仕組み

1.持続可能なエコシステム

ステークホルダーがそれぞれの責任を分担し、責任を果たすインセンティブがあること。

2.マルチステークホルダーによるガバナンス

マルチステークホルダーがガバナンスに関与し、ステークホルダーの責任が明確で、問題が発生したときに原因究明ができること。

3.オープンネスと透明性

アーキテクチャー設計、実装とそのプロセスがオープンであり、透明性が高く相互に検証可能であること。

TrustedWeb 設計・運用における原則

ユーザの観点

4.データ主体によるコントロール

データへのアクセスのコントロールは、データ主体（個人・法人）に帰属すること。

5.ユニバーサル性

誰も排除せず、弱い立場にある人を取り残さないこと。誰でも自由に参加できること。

6.ユーザ視点

ロックインフリーでユーザに選択肢があること。ユーザにとって分かりやすく安心して使えること

TrustedWeb 設計・運用における原則

システムの観点

7.継続性

既存インターネットアーキテクチャーを基礎として、上位に構築することとし、Transitionalな形で現行ウェブに付加されること。既存トラスト手段とのフェデレーションも考慮すること。

8.柔軟性

構成部品が疎結合で構成され、拡張可能なアーキテクチャであること。

9.相互運用性

技術のみだけでなく、法制度、ガバナンス、組織等の社会システム全体について異なるシステム間で連携可能であること。

10.更改容易性・拡張性

特定の技術に依存しすぎず、中長期での利用を意識して継続的に機能拡張が容易でスケーラブルであること

2022.3.15 イベント
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/kaigi_shiryo.html

首相官邸 Prime Minister of Japan and His Cabinet

政策会議 ▲トップページへ

トップ > 会議等一覧 > デジタル市場競争本部 > Trusted Web推進協議会 > Trusted Webイベント

Trusted Webイベント

信頼性を確保した新たなインターネットの実現に向けて、"Trusted Web"イベントを２０２２年３月１５日（火曜日）にオンライン形式で開催いたしました。

会議資料

第１部　講演（今Webに求められる信頼性のあり方）	
１１：００－１１：３０（３０分）	【特別講演】 村井純氏（慶應義塾大学　教授） ○ テーマ：「Web：デジタル社会のプラットフォーム」（PDF／1,839KB）
１１：３０－１２：００（３０分）	【基調講演】 浦川伸一氏（日本経済団体連合会 デジタルエコノミー推進委員会企画部会長） ○ テーマ：「Trusted Webへの産業界からの期待」（PDF／4,389KB）

今後の取り組み:公募

https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/pdf/20220315/shiryo11.pdf

デジタル庁　補正予算（令和３年度）

4

Trusted Web共同開発支援事業費

令和３年度補正予算額　2.7億円（新規）

事業の目的

○様々な社会活動のデジタル化が進む一方で、フェイクニュース等のデータそのものの信頼への懸念、先鋭化していくプライバシーリスク、データの取扱いへの懸念からくる産業界におけるデータ活用の停滞、勝者総取り等によるエコシステムのサステナビリティへの懸念など、信頼できる自由なデータ流通（DFFT）を妨げる、様々な歪みが生じている。

○これらの懸念は、データそのものが信頼できない、データのやり取りをする相手を信頼できない、相手方におけるデータの取扱いを信頼できないといった現状が主な原因と考えられる。

○こうした中で、インターネット上で、DFFTを確保する枠組みを構築すべく、特定のサービスに依存せずに、個人・法人によるデータのコントロールを強化する仕組み、やり取りするデータや相手方を検証できる仕組みなどの新たな信頼の枠組みを付加することを目指す「Trusted Web」構想を実現していくために実証を行う。

○本事業を通じて、Trusted Webによって具体的に解決される課題を「見える化」するとともに、さまざまな産業分野におけるユースケースを創出し、 Trusted Webの具現化及び国際標準化、ひいてはDFFTの実現につなげる。なお、本事業は、内閣官房等と連携して取り組む。

事業の概要・イメージ

○DFFTの実現に向けて、データのやりとりをめぐり「信頼」の確保に関する現実の課題を有する企業と、解決ツールを提供できる企業との共同開発プロジェクトを公募し、そのプロトタイプ／システム開発を支援する。

○Trusted Web の４つの機能のうち、少なくとも３つの機能に関する課題を有することを要件とする。

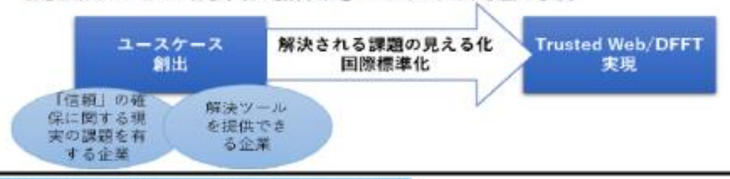
（参考）Trusted Webの４つの機能

①Identifier（識別子）管理機能
　データの主体（個人や法人）自らが識別子を発行・管理し、その識別子を自らの様々な属性情報と紐づけながら、自らの属性情報の開示範囲をコントロールでき、これにより、プライバシーや営業秘密の保護を実現する。

②Trustable Communication機能
　第三者によるお墨付きやレビュー等を受けた自らの属性情報（卒業証明、検査結果など）を自らが管理し、相手に対し必要な範囲で開示する。受け手は、発行者等に都度照会することなく、属性の確からしさを検証できる。

③Dynamic Consent機能
　データをやり取りする際に、双方で様々な条件設定をして合意を行うプロセスと結果を管理することができる。データのやり取りにおける条件をコントロールし、また、双方の意思を反映し、齟齬があれば動的に修正できる。

④Trace機能
　合意形成のプロセスや合意事項の履行状況をモニタリングし、検証できる。



スキーム図（資金の流れ）

期待される効果・成果イメージ

○データを提供する主体のプライバシーや営業秘密の保護が確保され、データ提供者の安心が向上する。
○データの信頼性が確保され、受け取る側の確認コストが低減し、処理スピードが向上する。
○これらにより、信頼性ある自由なデータのやりとりや活用が円滑化することで、DFFTが実現される。

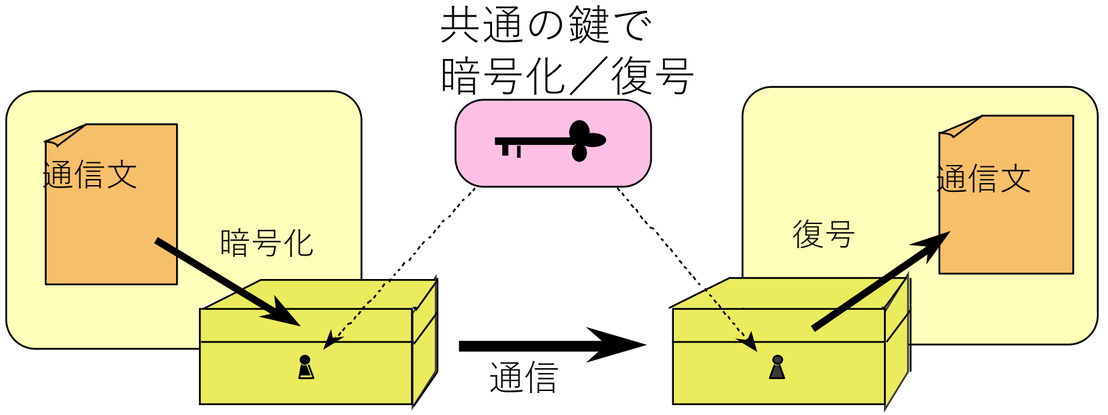
検証可能性と暗号技術

共通鍵暗号と公開鍵暗号

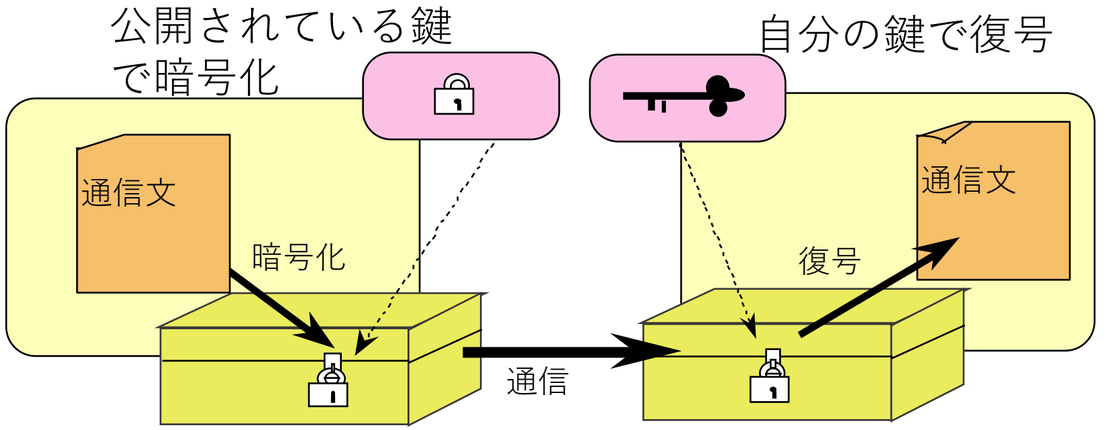
共通鍵暗号と公開鍵暗号

Encryption 敵に知られず味方にメッセージを送る方法

共通鍵暗号
（秘密鍵暗号）
単機能で高速
BC50くらい～



公開鍵暗号
高機能で低速
1970代～



公開鍵暗号とデジタル署名

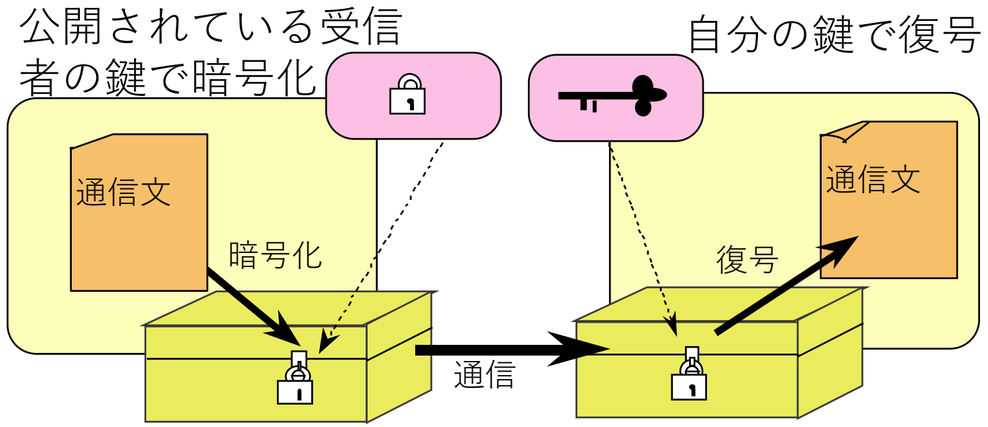
公開鍵暗号とデジタル署名

不正を防止のため

Cryptography: 一部秘匿しつつ目的を達成させる方法

公開鍵暗号

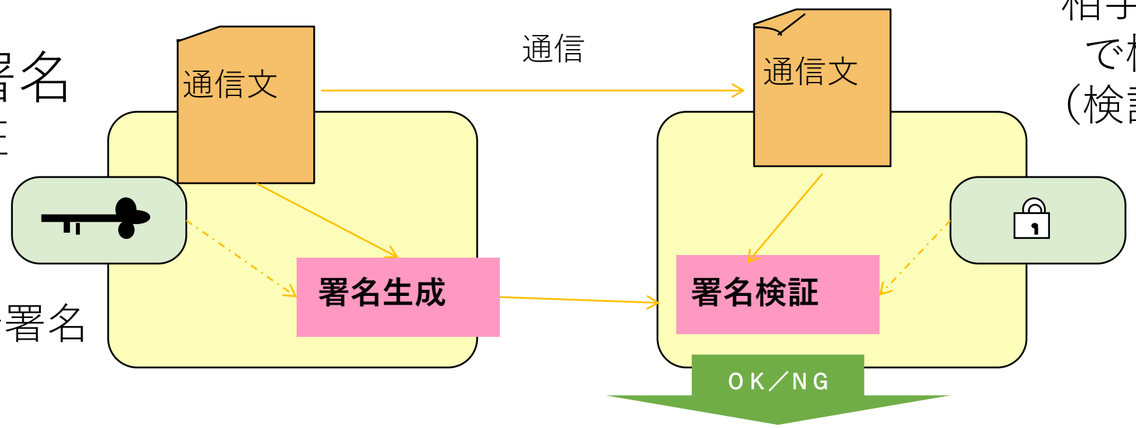
通信内容を秘匿



デジタル署名

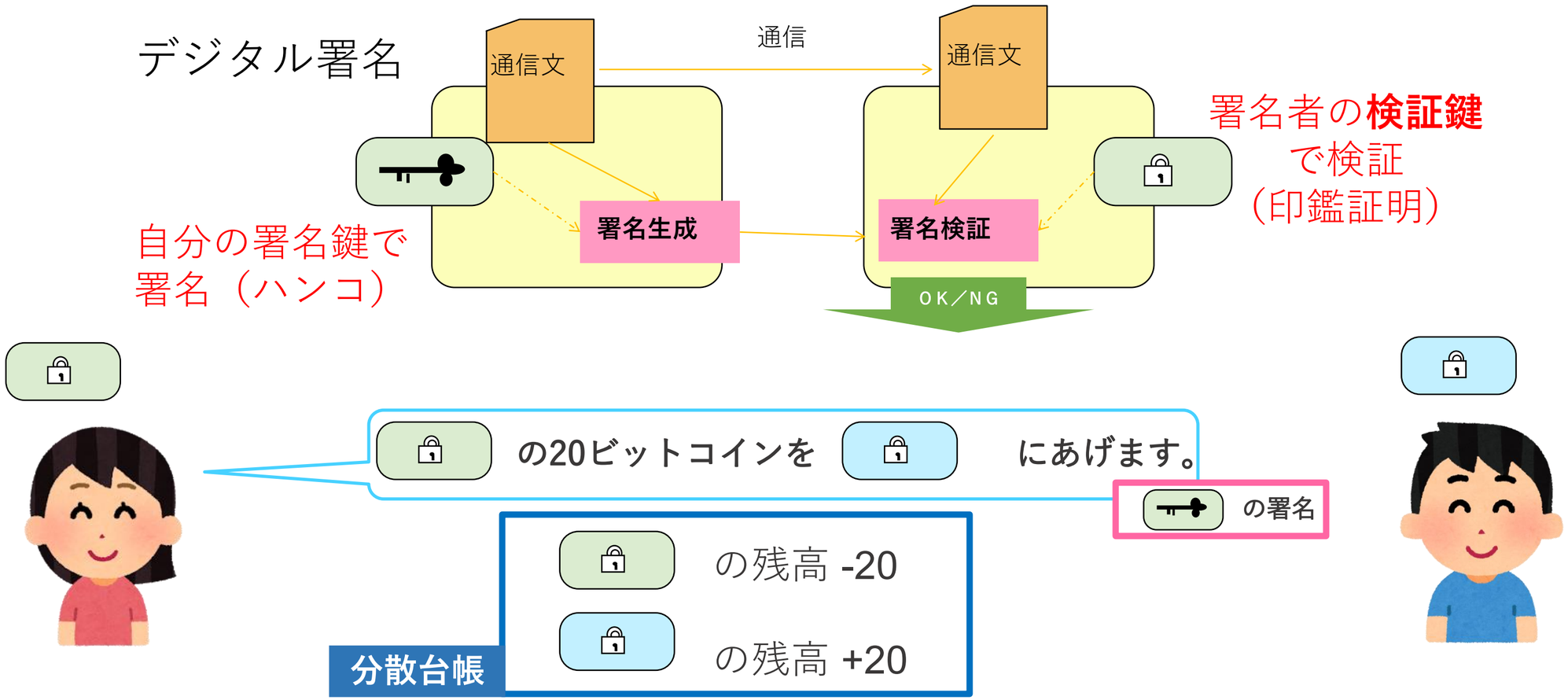
送り元保証
署名鍵を秘匿

自分の鍵で署名



ビットコインでは検証鍵をうまく使っている！

検証鍵が口座名（アドレス）になる！



暗号技術はIT上でルールをエンフォースする技術

権利が付与されている人しかデータを読み出せない（暗号化技術）
　　権利を持つ人に復号鍵を渡す

権利が付与されている人しかデータを書きこめない（認証技術、デジタル署名技術）

無作為に決定する（じゃんけんプロトコル）

無記名だけど一人一票（電子投票プロトコル）

正しく運営されていることを確認できる技術

正しい開票結果（電子入札プロトコル）

正しい通貨流通量増加（ビットコイン）

個人情報を秘匿しつつ開示

証拠隠滅の抑止

そのための要素技術：

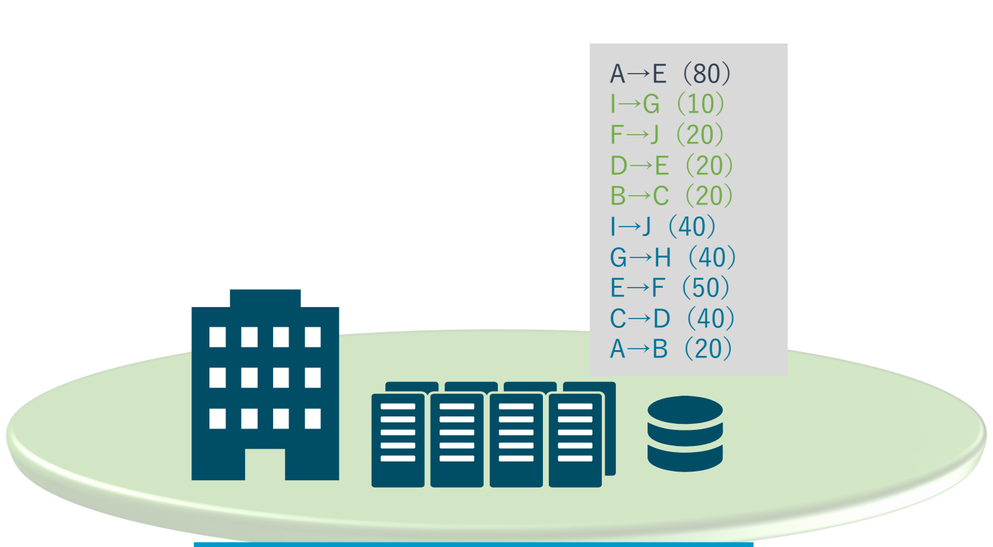
一方向性関数・
ゼロ知識証明・
ブロックチェーン

ブロックチェーンとスマートコントラクト

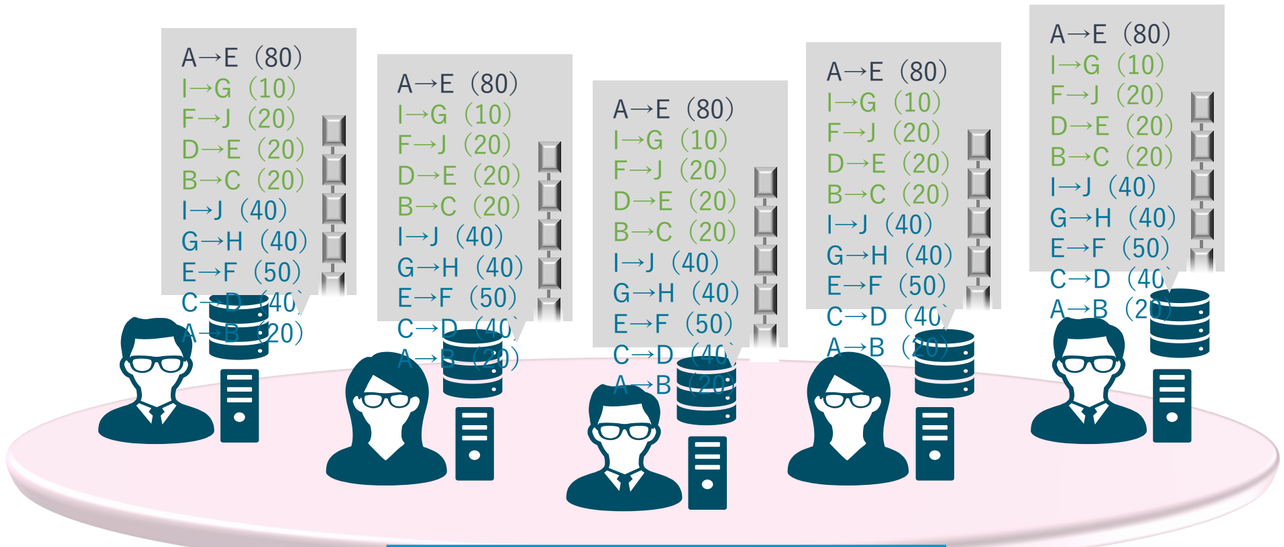
ブロックチェーンとは

学術的な定義はない。

ビットコインに使われている「みんなで台帳を管理する技術」を（ビットコイン）ブロックチェーンと呼んでいたが、その後、それぞれが独自の変更を加えたものをブロックチェーンと呼んでいる。



従来の台帳管理

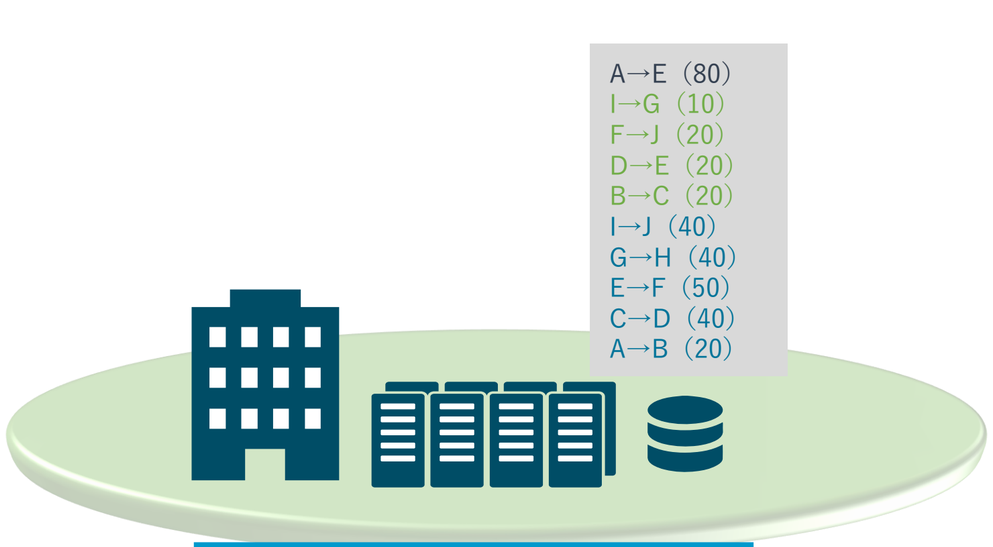


みんなで台帳管理

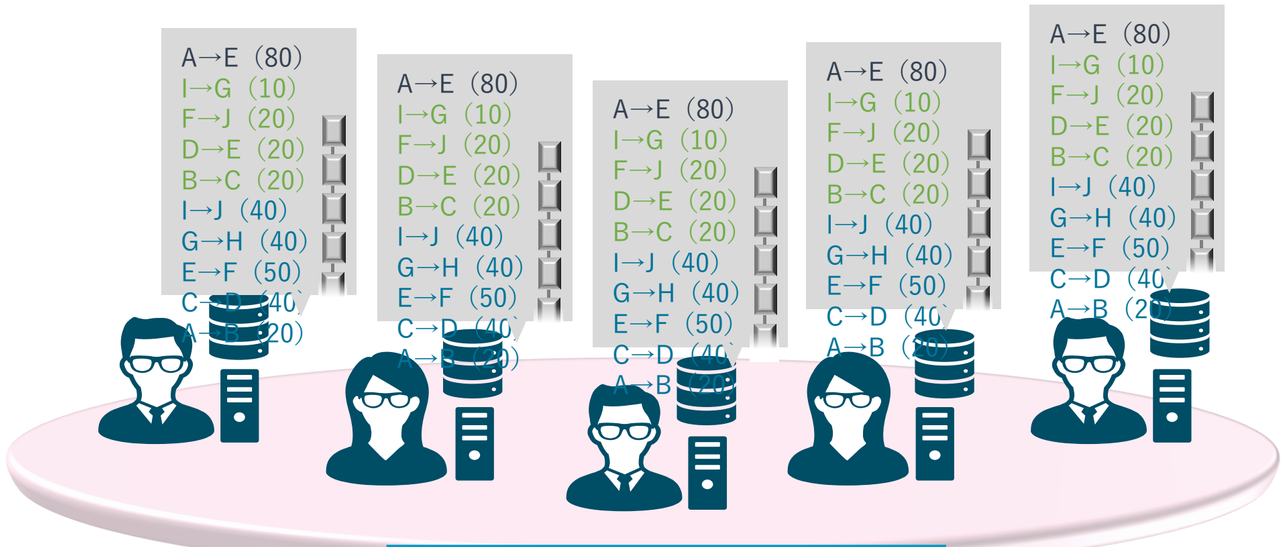
ブロックチェーンとは

暗号技術で改ざんを抑止可能な公開掲示板（台帳）

ビットコインに使われている「みんなで台帳を管理する技術」を（ビットコイン）ブロックチェーンと呼んでいたが、その後、それぞれが独自の変更を加えたものをブロックチェーンと呼んでいる。



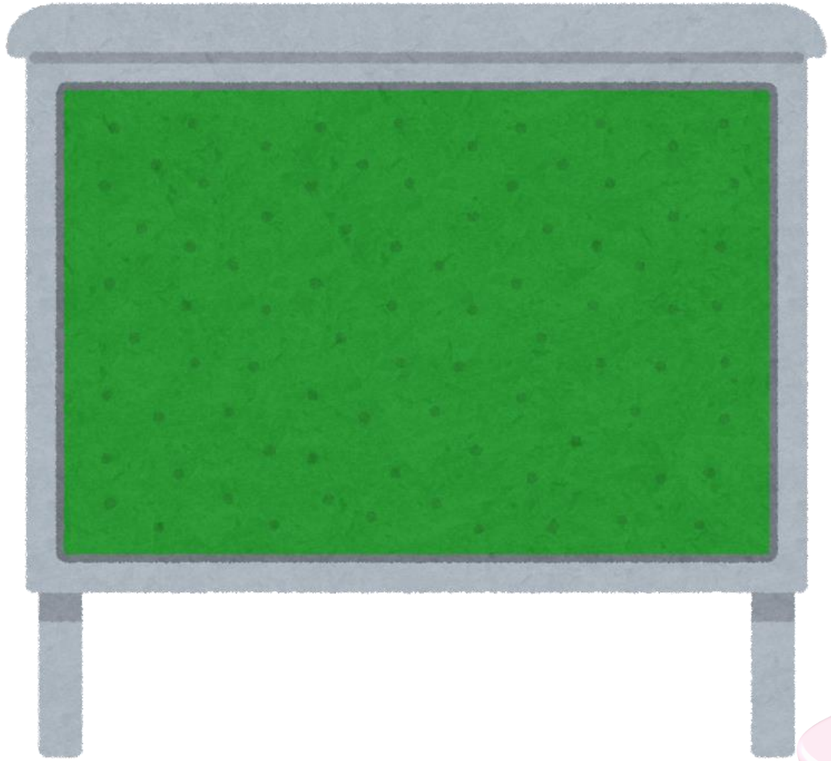
従来の台帳管理



みんなで台帳管理

ブロックチェーンとは

暗号技術で改ざんを抑止可能な追記式の公開掲示板（台帳）



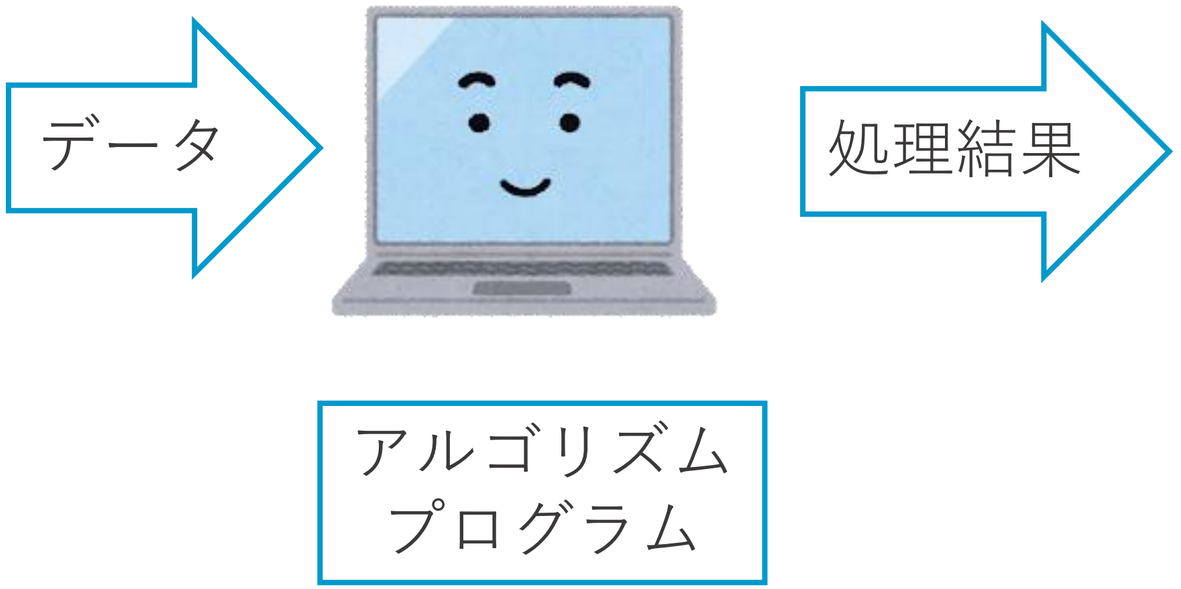
あらかじめ決められたルールに整合すればだれでも書き込める

一度書かれると消せない

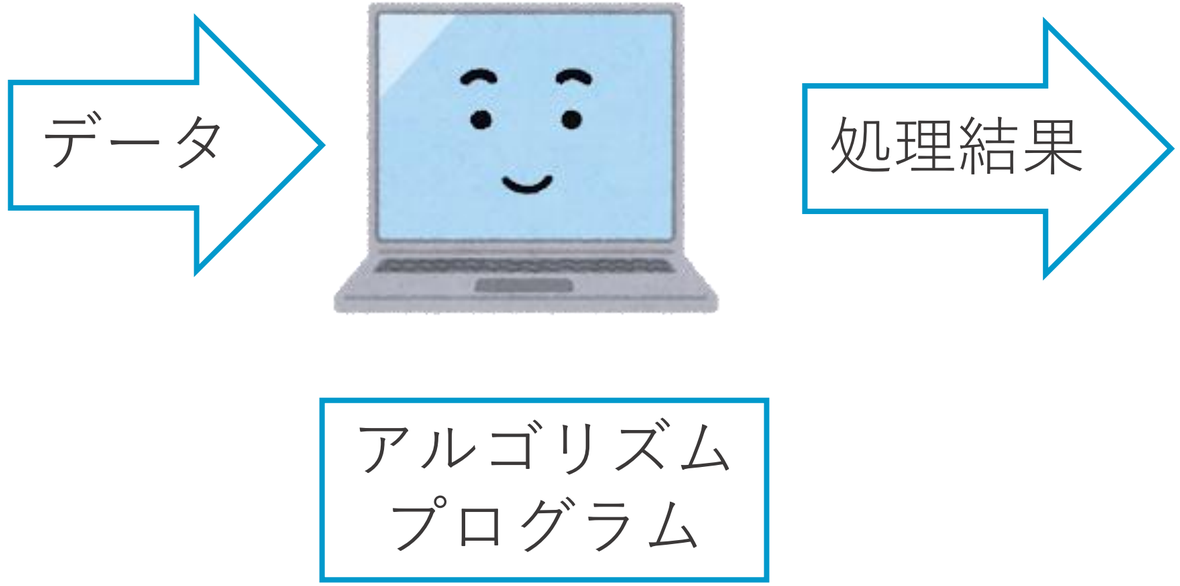
誰でも読める。

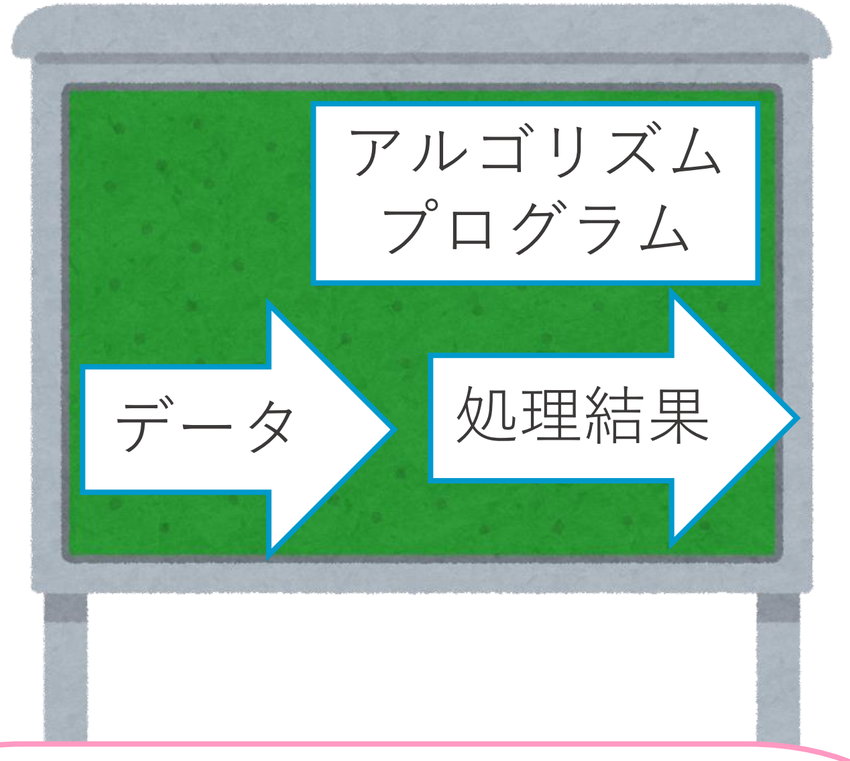
みんなで台帳管理

データ処理



ブロックチェーンとスマートコントラクト



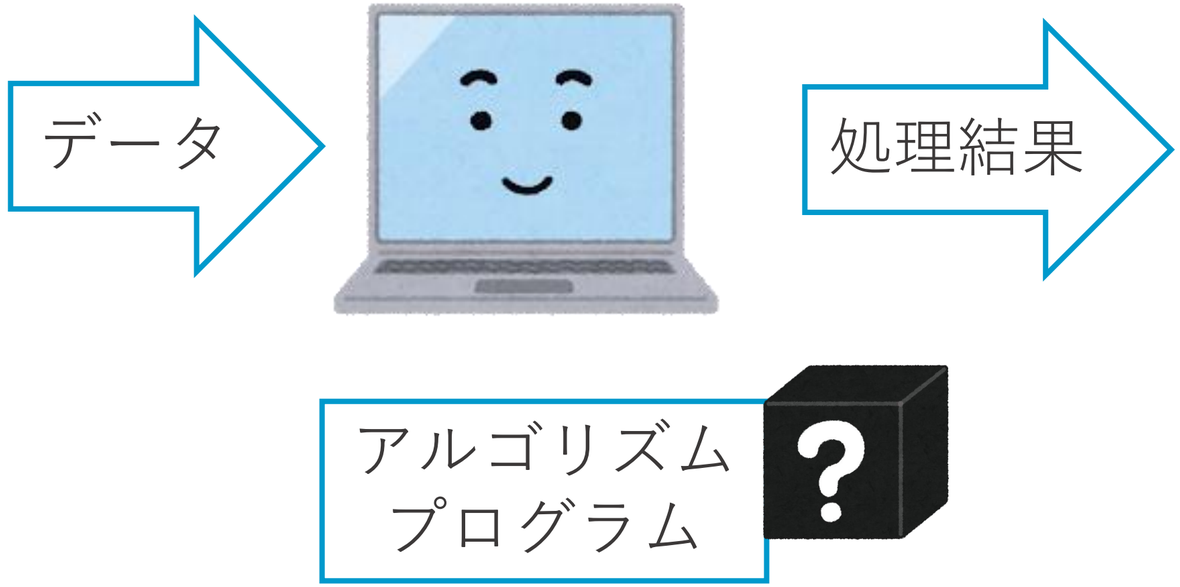


あらかじめ決められたルールに整合すればだれでも書き込める

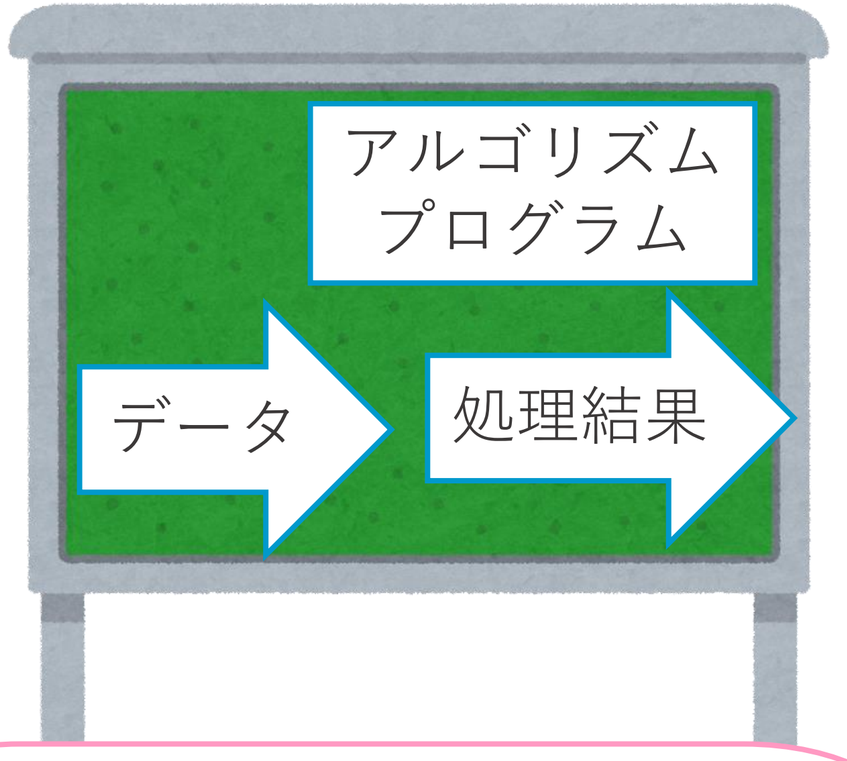
一度書かれると消せない

誰でも読める。

ブロックチェーンとスマートコントラクト



透明性



あらかじめ決められたルールに整合すればだれでも書き込める

一度書かれると消せない

誰でも読める。

本日の内容

- DXとトラスト
- トラストと検証可能性
- 検証可能性と暗号技術
  - 公開鍵暗号、デジタル署名
  - ブロックチェーンとスマートコントラクト