Dashとは何か？

PoWとPoSeのハイブリッドを採用し、予算編成システムを持つ暗号通貨の全体像

DashJapan.com管理人　とみ三

自己紹介

ハンドルネーム：とみ三

Dashの日本語情報サイトDashJapan.comを運営。

Twitterでの情報発信

本業があり、フルタイムでの活動はしていません。

Dashのホワイトペーパーの一部を翻訳したりしていますが、英語力は低いです。

エンジニアではありません。

Dashの概要

【リリース】 2014年1月18日

【創始者】 エヴァン・ダフィールド（2011年からビットコインの開発に携わっていた）

【時価総額】 約1800億円（2018年9月27日現在。CoinMarketCapのランキングで11位。）

【コードベースと名称の変遷】 リリース時はXCoinという名称でLitecoinのコードベースフォークとしてスタート。リリース翌月にDarkcoinに改称(Lite=Light⇔Dark?)。リリース翌年3月にBitcoinのコードベースフォークとなり、Dashに改称。

【受け入れ事業者数】 DiscoverDashによると全世界で3,100以上（うち1,590がベネズエラ。日本は1。）

ビットコインとDashの比較（1）

	ビットコイン	Dash
リリース日	2009年1月3日	2014年1月18日
創始者	サトシ・ナカモト	エヴァン・ダフィールド
ハッシュアルゴリズム	SHA-256	X11
ブロック生成間隔	10分	2.5分
採掘難易度調整	2週間ごと	1ブロックごと
ティッカーシンボル	BTC / XBT	DASH
総供給量	2100万BTC	1774万～1892万DASH
ブロック報酬の削減	4年ごとに半減	1年ごとに7.14%削減
取引の認証方式	Proof of Work（PoW）	Proof of Work / Proof of Service（PoW / PoSe）

ビットコインとDashの比較（2）

	ビットコイン	Dash
公式クライアント	Bitcoin Core	Dash Core（Bitcoin Coreがベース）
ネットワーク構造	1層	2層（第2層はマスターノードネットワーク）
自己資金調達	なし	あり（ブロック報酬の10%）
ブロック報酬の内訳	マイナーに100%	マイナー45%、マスターノード45%、自己資金10%
意思決定方法	ハッシュパワー	マスターノードによる投票
プライバシー（送金履歴難読化）機能	なし	あり
送金の即時承認機能	なし	あり（2秒以内）
スケーリング手法	スモールブロック・オフチェーン	ウルトララージブロック・オンチェーン
開発中のソリューション	Lightning Network	Evolution

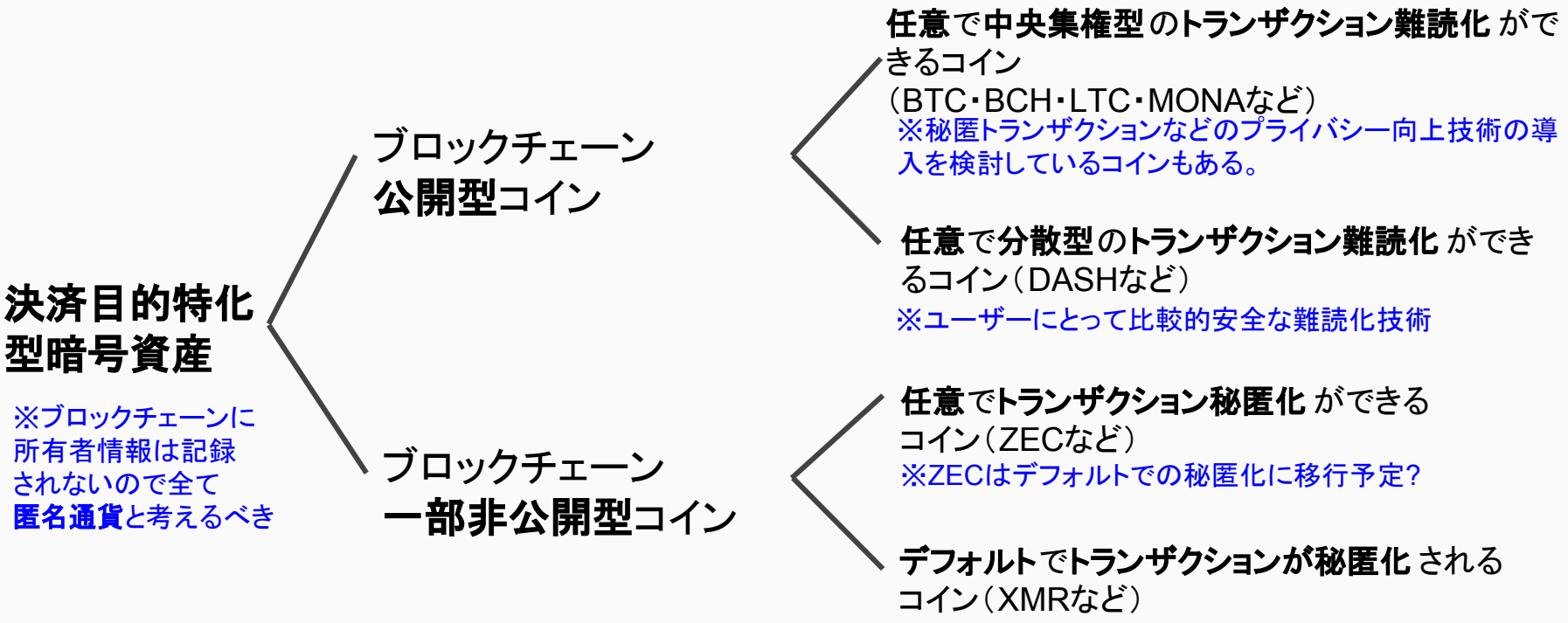
Dashに関するイメージ・誤解

「匿名通貨」、「匿名性仮想通貨」？

悪いことをするための暗号通貨？

ビットコインコピー？

決済目的特化型（通貨型）暗号資産の分類案



ビットコインのプライバシーとファンジビリティは低い

アドレスの所有者は基本的にわからない

しかし、取引の当事者は取引相手のアドレスがわかるので、そこから取引相手の保有量、使用状況などが推測できる

ネット上に晒されるリスクもある

ファンジビリティ（代替性、等価性）
通貨に必要不可欠な特性

犯罪に使われたコインは価値が低い

マイニングされたばかりのコインは価値が高い

ビットコインのプライバシーとファンジビリティを向上させるには

- 買い物用ウォレットを貯蓄用ウォレットと完全に分離する
- 取引所への入出金（取引所のホットウォレットで他のユーザーのコインとごちゃ混ぜになる）
- ミキシングサービス

現状では取引所の果たしている役割が大きい。しかし中央集権型で信用が必要になる（ビットコインを預ける必要がある）

Dashはマスターノードがミキシングの場となる（ミキサーとなること）で信用不要（トラストレス）で分散型のミキシングを提供している

ビットコインのフルノードとDashのマスターノード

Dashのマスターノードはビットコインのフルノードにあたる

フルノードの役割—**ダウンロード、検証、伝播**

マスターノードはその役割に加えて、

守秘送金（プライベートセンド）のミキサー

即時送金（インスタントセンド）の承認

の役割を担う

マスターノード稼働に必要な要件と権利

- 1つのマスターノードを稼働するには、1,000DASHの所有を証明する必要がある。
- マスターノード所有者は1,000DASHをいつでも動かすことができる（マスターノードを解消することができる）。
- 1,000DASHをどこかに預ける必要はなく、没収されることもない。また、オンラインウォレットに保管しておく必要はなく、ハードウェアウォレットでの保管が推奨されている。
- マスターノードには予算提案（バジェットプロポーザル）と重要事項の決定への議決権が与えられる。1マスターノードにつき1票。
- マスターノードにはブロック報酬の一部が与えられる。

現在のマスターノード情報

マスターノード数	4861
マスターノードへの報酬支払間隔	平均8.86日ごと
マスターノードへのブロック報酬	1.67DASH（約35,513円）
1 DASHの価格	21,265円
1,000 DASHの価格	21,265,000円
1日あたりの報酬	約4,008円
1年間の価格平均が21,265円だった場合の1年あたりの報酬	約1,462,920円
1年間の価格平均が21,265円だった場合の投資利益率（ROI）	約6.87%

Dash Masternode Information をもとに作成（2018年9月26日15時現在）

プライベートセンド（守秘送金）の仕組み

ビットコインの取引履歴難読化技術としてG・マクスウェルによって開発されたCoinJoinを発展させたもの

Dash Core ウォレットに入っているDashを4つの金種（**10・1・0.1・0.01** DASH）に分割する（ミキシングは金種ごとに行われる）

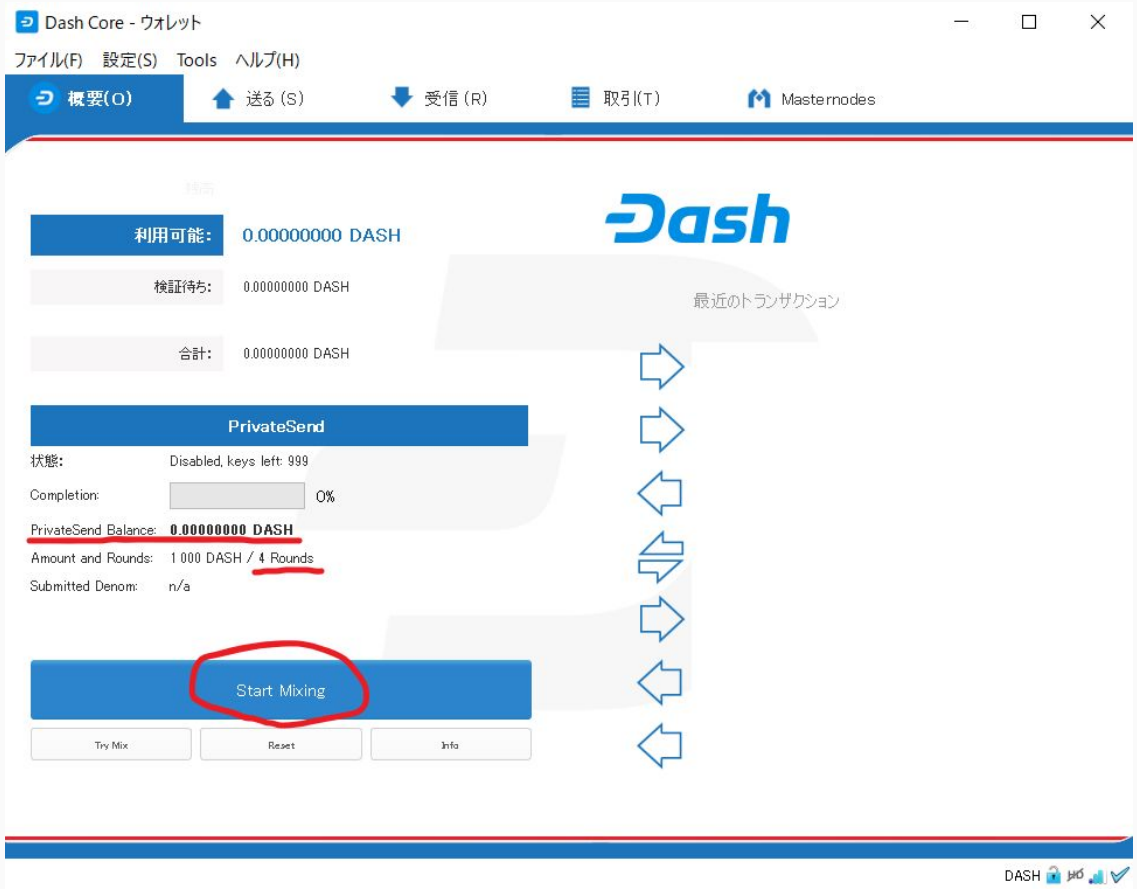
⬇

マスターノードにミキシングを要求。他に2人のユーザーが集まるとミキシング開始。ミックスされたDashがウォレットの新しいアドレスに返ってくる【1ラウンド】（4ラウンド以上が推奨。ラウンドを重ねるごとに指数関数的に追跡が難しくなる）※ミキシングはバックグラウンドで実行される

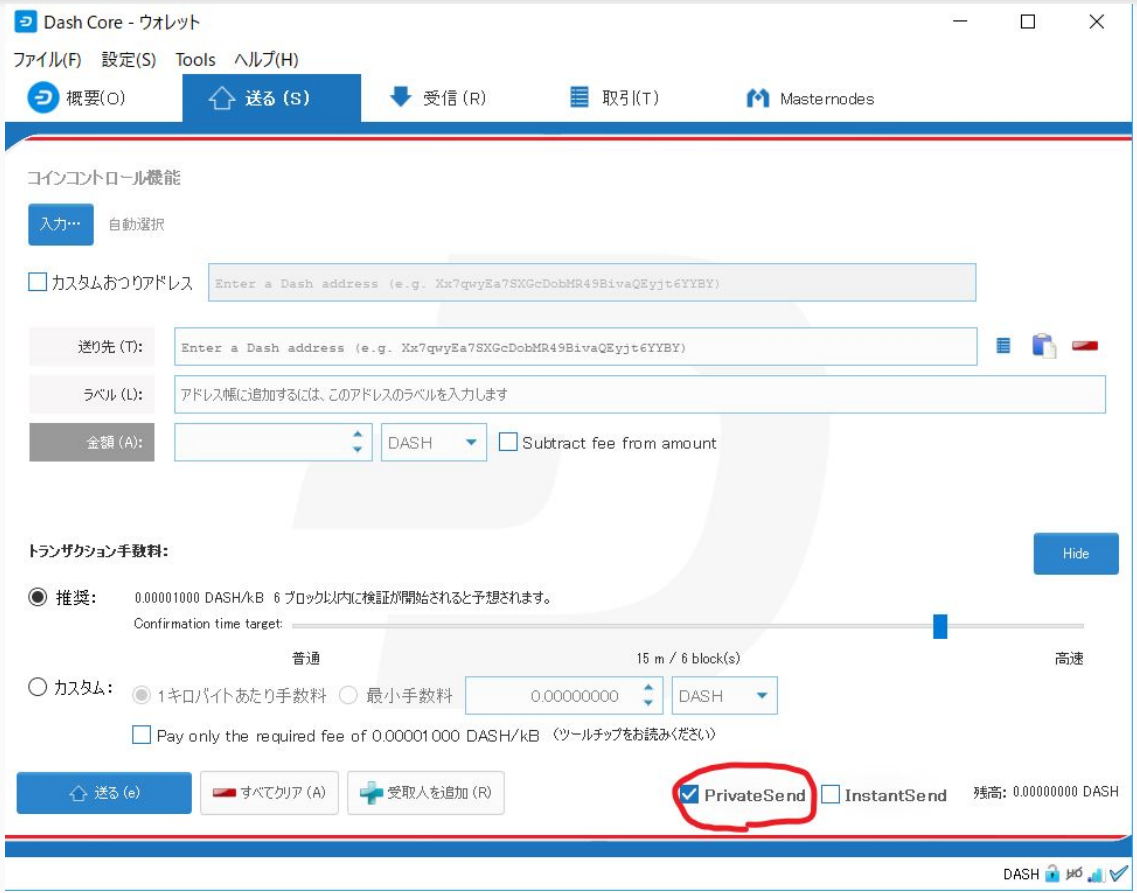
⬇

プライベートセンドを選択して取引相手のアドレスに送信をする

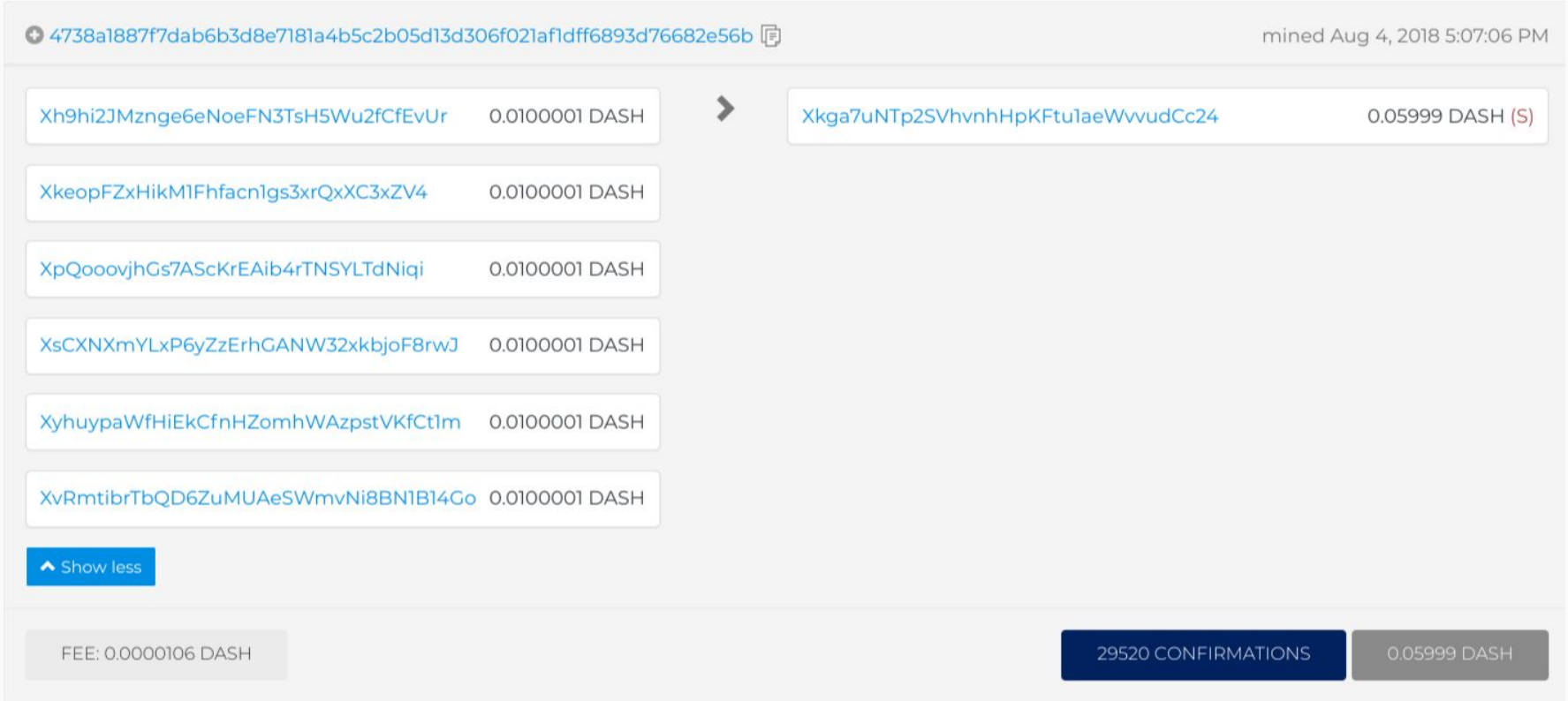
Dash Core ウォレットでのプライベートセンドの操作（1）



Dash Core ウォレットでのプライベートセンドの操作（2）



プライベートセンドのトランザクションの一例



インスタントセンド（即時送金）の仕組み

ビットコインは承認に時間がかかるという問題がある。ゼロ承認で即時に決済完了とするのはリスクがある。

Dashはマイナー（採掘者）の承認ではなく、マスターノードにインスタントセンドの承認を任せている。

インスタントセンドを選択して取引相手にDashを送信

⬇

ランダムに選抜された10のマスターノードのうち6つが承認して決済完了

⬇

マスターノードがトランザクションをロックし、ブロードキャスト

⬇

該当トランザクションは必ずブロックに取り込まれ、競合するトランザクションは拒否される

Proof of Service

マスターノードがプライベートセンドのミキサーとなり、インスタントセンドの承認をすることでブロック報酬を得る仕組みを**Proof of Service（PoSe）**という。決済に使われる際の問題をマスターノードを使って解決したと言える。

その他にも**ガバナンス・意思決定機能**。

大口所有者が売買を繰り返さなくても利益を得ることができるので、**価格変動性を低くする効果**も期待されている。

Dashは現在2MBのブロックサイズを拡張していく予定。**分散型の状態でビッグブロックに対応できる**仕組みでもある。

現在マスターノードのランニングコストはそれほどかからないが、将来ブロックサイズが拡張すると専用のハードウェアを購入する必要がある。

DAO（自律分散型組織）としてのDash

ブロック報酬の10%はコミュニティ内で自由に使える自己資金となる

使い途はマスターノードによる投票で決める。予算提案は5DASHを支払うことで誰でもできる。

財団のようなものがあって蓄えるのではない（内部留保やキャリーオーバーはない。）

予算は毎月1回生成されるスーパーブロックから予算獲得者のアドレスに直接支払われる

2018年10月2日のスーパーブロック…使用可能な予算は最大6,177 DASH（日本円で約1億2763万円）

現在の投票状況

賛成票から反対票を除いた数がマスターノードの総数の10%以上（現在486票）に達することで提案は可決される

Dashの予算の使用例

・Dashコアグループ（開発請負業者。スタッフ数39名。米国アリゾナ州にオフィス）の報酬

・アリゾナ州立大学との提携

・ベネズエラのコミュニティ（Dashカンファレンス、Dash Help、Dash Textなど）

・Alt36社

・Dash大使館

・Dash Force 独自メディア

等々、多岐にわたる

投票は重要事項の決定にも使われる

一例…2MBブロックへの拡張

24時間以内に可決された

Dash Evolution

ユーザーネームを登録、ログインして利用

「あなたのおばあちゃんでも理解できる」を合言葉に開発されているUI、UXを重視した公式ウォレット

開発はクローズドソース。リリース時にオープンソースになる予定。
特許取得予定

世界初の分散型API（DAPI）によりサードパーティのDash統合が容易になる

自動引き落とし機能、トラストレスマスターノードシェアの構想も

ネットバンキング、メッセンジャーアプリ、マーケットプレイスを融合したようなものになるのか？年内にリリース予定

結論　Dashとは何か？

1. Dashはビットコインのプライバシーを向上させることを目指して始まった

2. Dashはマスターノードの仕組みを導入したことで、Proof of WorkとProof of Serviceのハイブリッドを採用する暗号通貨となり、高機能となった

3. Dashは、ブロック報酬の10%を自己資金とし、マスターノードの投票による予算編成システムを持ったことで世界最大のDAO（自律分散型組織）となった

Dashに関心のある方へ

日本語翻訳チームが活動中

Dash Forum

Discord　Dash Nation

参考文献

- アンドレアス・M・アントノプロス著（2016年）『ビットコインとブロックチェーン』NTT出版.
- A・ナラヤナンほか著（2016年）『仮想通貨の教科書』日経BP社.
- Dash Core Group, Inc.（2018年）「Dash Documentation」, <https://docs.dash.org/en/latest/index.html>2018年9月25日アクセス.

ありがとうございました

とみ三

www.DashJapan.com

Twitter: @samurai3311

ご意見、ご質問などがありましたら
お気軽にどうぞ

著作権について

https://creativecommons.org/licenses/by/4.0/

この資料は、クレジットを表示したうえで、ご自由に複製・再配布していただいて結構です。商用利用も可能です。資料を改変した場合はその旨を明記して下さい。

ご利用にあたっては，下記のクレジットを必ず表示してください．

© 2018 DashJapan.com クリエイティブ・コモンズ・ライセンス（表示4.0 国際）