経済産業省

ブロックチェーン技術を活用したシステムの評価軸 ver. 1.0

平成28年度 我が国におけるデータ駆動型社会に係る基盤整備事業

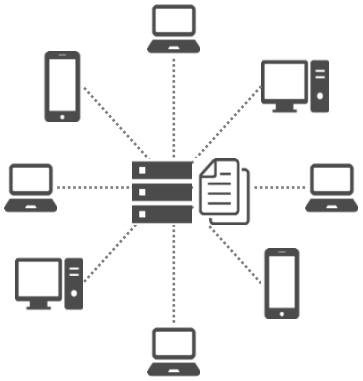
平成29年3月29日

商務情報政策局　情報経済課

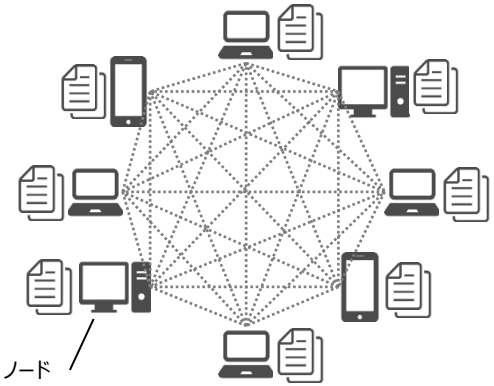
ブロックチェーン技術を活用したシステムの評価軸策定の背景

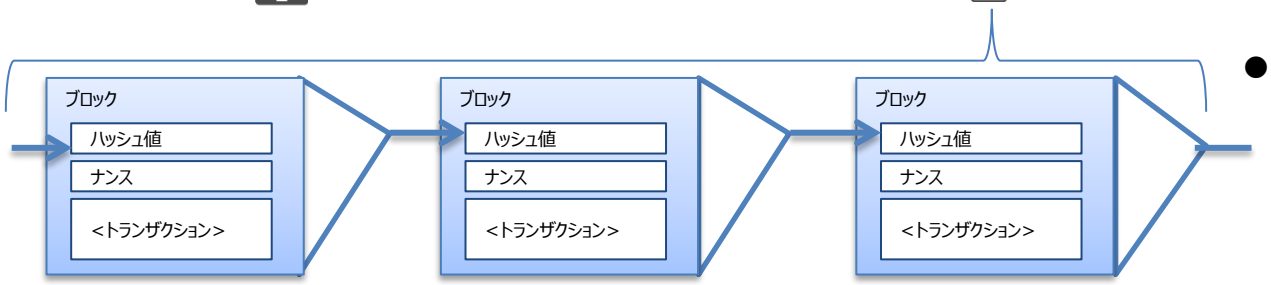
- ブロックチェーン技術は、従来システムに比べ、『改ざんが極めて困難』であり、『実質ゼロ・ダウンタイム』のシステムを『安価』に構築可能であるという特性から、幅広い分野への応用が期待されている
- 一方、当該技術の特性を正しく評価し、既存のシステムとの比較を可能とする基準等が整備されていない状況
- そのため、当該技術に対する不安感や過度な期待や誤解が生じ、結果として適切な導入が進まない恐れもある

中央集権型システム（従来システム）



ブロックチェーン技術を活用したシステム





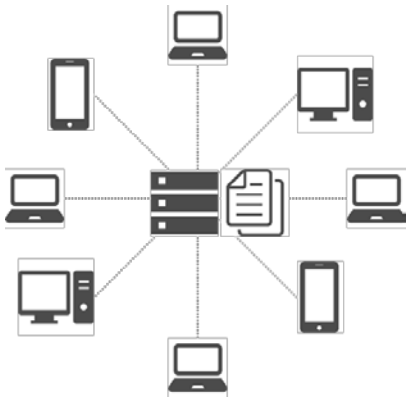
ブロックチェーン技術の特性（一例）

- 各ノードがトランザクション履歴を共有するため、システムの単一障害点がなく、**『実質ゼロ・ダウンタイム』**を実現可能
- さらに、トランザクション履歴は順番にブロックに格納され、各ブロックが直前のブロックとつながっているため**『改ざんが極めて困難』**
- ノードへの分散やコンセンサス方式などの要素を組み合わせることにより、同程度の堅牢性を持つシステムを、従来システムに比較して**『安価』**な構成で達成することが可能

ブロックチェーン技術を活用したシステムの評価軸策定の意義

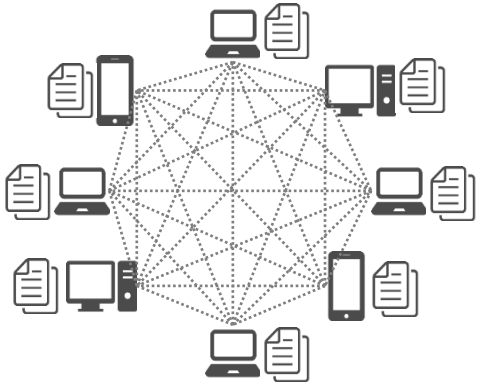
- 企業や組織がITシステムを導入検討する際に必要となる性能等の品質評価方法はISO/IECにおいて策定されている
- ブロックチェーン技術を活用したシステムでは複数ノードによるコンセンサス形成などブロックチェーン技術の仕組みに由来する特有のトレードオフ関係が存在することから、従来システムと同様の評価ができない

中央集権型システム（従来システム）



- 一般的に、処理能力はコンピュータのハードウェア性能・台数に依存する部分が大きいため、単一設備の性能値による評価が可能
- システム・ソフトウェアの品質に関する議論が行われており、ISO/IEC 25000(SQuaRE)シリーズとして国際規格化

ブロックチェーン技術を活用したシステム



- 複数ノード間のコンセンサス方式をはじめ、ネットワーク帯域やノード数など特有のトレードオフ関係のある複数の要因に依存するため、単一の性能値による評価が困難
- 国内外において、品質に関する議論は未着手

従来システムとの比較可能性・網羅性を考慮し、評価項目間のトレードオフを整理した
世界初の「ブロックチェーン技術を活用したシステムの評価軸」を策定

評価軸策定上の方針

ブロックチェーン技術を活用したシステムの評価に関する国内外の文献や事例、有識者委員会による議論を踏まえ、以下の通り、評価軸策定上の方針を決定、これに基づき評価軸を策定した*

*平成28年度 我が国におけるデータ駆動型社会に係る基盤整備（ブロックチェーン技術を活用したシステムの評価軸整備等に係る調査）として実施

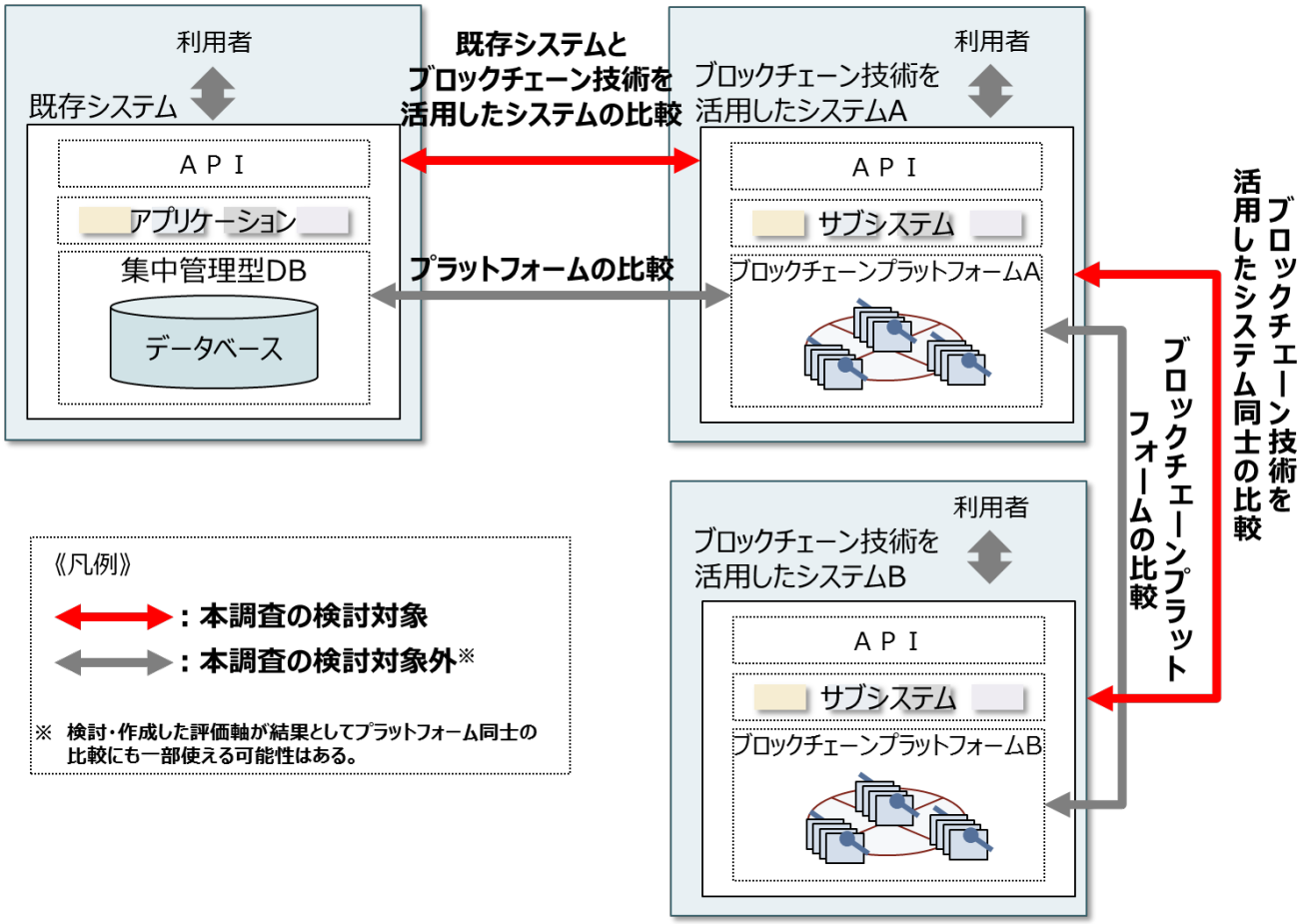
検討項目		評価軸策定上の方針
評価軸の目的		■ ブロックチェーン技術を活用したシステムの特性を適切に表現すること ■ 想定される利用シーン※において、必要十分な評価項目を極力網羅すること ※ 主に、既存システムをブロックチェーン技術を活用したシステムに置き換える場合に、既存システムと比較する目的でシステムベンダーが評価を実施する場合を想定
評価の対象	比較対象	■ 既存システムとブロックチェーン技術を活用したシステムの比較 ■ ブロックチェーンを活用したシステム同士の比較
	対象範囲（詳細①）	ブロックチェーン技術を活用したシステム（ブロックチェーンプラットフォーム＋周辺サブシステム）
	業務変革への対応	■ ブロックチェーンの特性を生かすことで既存の業務要件が変わる場合も、業務フローが変わる程度であれば対象 ■ 今までにないサービスを実現するようなシステムについては、比較対象が存在しないため対象外
	ﾌﾟﾗｯﾄﾌｫｰﾑの分類（詳細②）	■ プラットフォームの分類の違い（パブリック型／コンソーシアム型・プライベート型）やコンセンサス方式等に拠らず、すべてのパターンを対象 ■ これらの違いによる評価上の留意点を評価項目ごとに記載
	ﾕｰｽｹｰｽの網羅	■ ユースケースによる要件の違いを想定し、網羅性のある評価軸を作成
評価軸の構成要素 評価項目 評価指標 評価方法 （詳細③）		■ 品質はISO/IEC25010、保守・運用はIPAのリファレンスモデルより、ブロックチェーン技術を活用したシステムに特に関係性の深い項目を評価項目として抽出 ■ コストに関する評価軸はシステムベンダーが認識するコスト（≒顧客に請求する費用）ベースで構成 ■ 一律の評価指標や評価方法は設定せず、実際評価する際の留意点などの記載を充実

＜留意点＞ 原則として、2016年11月時点で主要なプラットフォームであったBitcoin、Ethereum、Hyperledger Fabric 等のブロックチェーン技術を念頭に置き、システムの評価軸を検討した。今後の技術的進歩や新たに生じうるユースケースについては有識者検討委員会の委員の見識をベースに極力検討対象としたものの、限界がある点については留意が必要

評価軸の検討①（対象範囲）

- 本評価軸ではシステム全体（ブロックチェーンプラットフォーム＋周辺サブシステム）を評価対象とした
- 本評価軸を活用する場面として想定した、主にシステムベンダーが評価を実施し、導入検討者が投資判断を行う場面においては、全体としての機能や性能に対するニーズが高いと考えられること等から判断した

対象範囲のイメージ



評価軸の検討②（プラットフォームの分類）

- 下表のように管理主体や参加者等に違いがあり、特性が異なるが、パブリック型、コンソーシアム型、プライベート型のすべてのパターンを網羅するものとした
- これらの違いにより生じる評価上の留意点については、評価項目ごとに記載した

管理主体による一般的なブロックチェーンプラットフォームの分類

出所）IBM公開資料を一部加工

	パブリック型	コンソーシアム型	プライベート型
管理主体	なし	複数組織	単一組織
参加者	自由	許可制	
	不特定、悪意のある参加者を含む	参加者の身元が判明しており、信頼できる者で構成される	
コンセンサス方式（合意形成方式）	Proof of Work(注1)型等	PBFT(注2)型等	
	ブロック確定(注3)しない 電力消費が多い	ブロック確定する 軽量、高速、低消費電力	
トランザクション処理時間	長い（10分など）	短い（数秒など）	
ユースケース	仮想通貨等	銀行間送金、証券取引等ビジネスネットワーク　等	
実装例	Bitcoin、Ethereum　等	Ripple、Hyperledger Fabric　等	

（注1）Proof of Work：一般的に「単純だが手間がかかる、ただし本当にそれを行ったことの検証は簡単な、特定の作業 をあえて行わせることにより、悪意のないことを確認する（不正を行う動機を低減させる）」という仕組みのこと。ビットコインにおいては、ネットワーク参加者が与えられた条件に合致する値が得られるまで計算を続け、求める値を得られた参加者がブロックの生成権限を得る、という仕組みによって、参加者間の合意を形成する方式

（注2）PBFT（＝プラクティカル・ビザンチン・フォールト・トレラント）：コアノードにブロックの生成権限を集中させ、コアノードによる合議制において、トランザクションの承認を行う方式

（注3）ブロック確定：ブロック生成においてフォーク（分岐）等が生じることで、生成されたブロックが後に否認される可能性がある状態となることがあるが、そのような可能性が無くなった状態。実際のビットコインの取引では、6回程度の後続ブロック生成が行われたことをもって、「取引が正当なものと認められた」（＝ファイナリティが得られた）とみなしている。厳密には、どれだけブロックが連なったとしても、フォークする確率がゼロにはならないため、トランザクションが取り消されるリスクも非常に小さな確率で残る。

5

評価軸の検討③（評価軸の構成要素）

- 品質はISO/IEC25010（システム及びソフトウェア品質モデル）よりブロックチェーン技術・特性と関係性の強い評価項目を抽出
- 保守・運用については、IPAの検討（システム・リファレンス・マニュアル、第4章保守・運用、2005年）を参考とし、同様に評価項目を抜粋
- コストについては、システムベンダーが費用認識するコスト（≒顧客に請求する費用）項目を整理

評価軸の構成

システム・ソフトウェアの品質モデル
出所）ISO/IEC25010

システム保守・運用の評価指標
出所）IPA

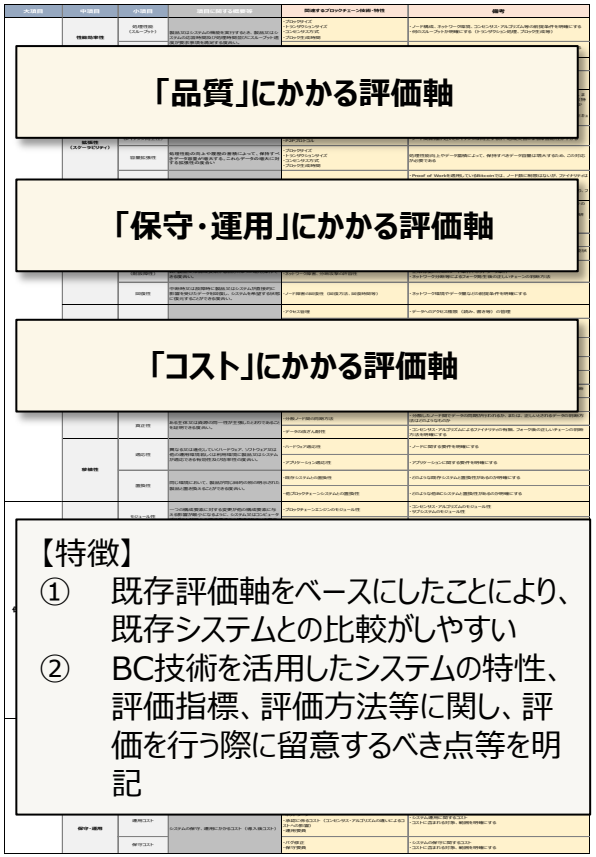
コストの観点
- 研究開発コスト
- 実装コスト
- 保守・運用コスト

BC技術を活用したシステムの特性
- 有識者検討委員会における意見・議論
- 有識者ヒアリング調査
- 文献調査

既存の評価軸をベースに
- 既存システムとの比較しやすさ
- 網羅性を担保

BC技術を活用したシステムの特性に着目した評価軸の抽出・追加
- BC技術・特性の評価軸
- 備考・留意点を充実

ブロックチェーン技術を活用したシステムの評価軸



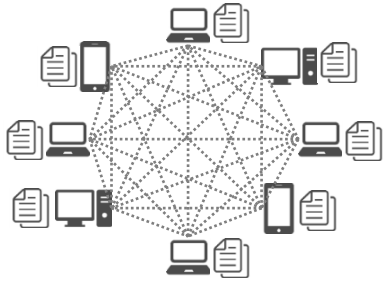
【特徴】
① 既存評価軸をベースにしたことにより、既存システムとの比較がしやすい
② BC技術を活用したシステムの特性、評価指標、評価方法等に関し、評価を行う際に留意するべき点等を明記

評価軸の検討④（ブロックチェーン技術の特性の反映）

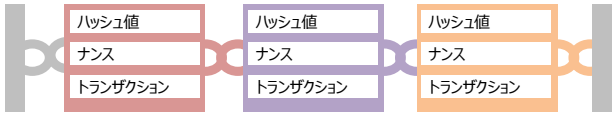
- ブロックチェーン技術の技術的な特徴より生じる特性を、それが関係する複数の評価項目に織り込むことで評価軸を構成した
- 多くの評価項目や特性が互いにトレードオフの関係となっている

ブロックチェーン技術の特徴　例

- **分散型であり複数のノードが同一のトランザクション履歴を持つ**



- **ブロック内に多くのレコードが記録され、それぞれのブロックが、暗号学的な署名により次のブロックに繋がっていく構造**



（フォークのイメージ）
フォークが生じた場合、ブロックが後から否認される可能性がある

関連性の強い評価項目の一例

- 一般に可用性や耐故障性が高いという特性につながる
- ノードの構成やノード間のネットワーク環境、適用するノード間でのコンセンサス方式等が、多くの特性に影響しあいトレードオフの関係になる

＜品質に関する評価項目＞
可用性、障害許容性、ネットワーク性能（向上性）、参照性能・・・等
＜保守・運用に関する評価項目例＞　解析性等
＜コストに関する評価項目例＞　各実装コスト等

- 一般に改ざんが困難という特性につながるが、ブロックサイズやブロック生成に要する時間等が、処理性能向上性など、多くの特性に影響しあい、トレードオフの関係になる
  *「ブロックサイズを大きくする」又は「ブロック生成に要する時間を短くする」ことがスループットの向上に有効。一方でブロックサイズを大きくすると処理できるトランザクション数が増えるが、データの転送時間が増し、応答性能は低下するなど、トレードオフとなる
- 適用するコンセンサス方式によって、ブロックの分岐（フォーク）等により生成されたブロックが後に否認される可能性が残ることも特性のひとつ。
  *ブロック確定が可能なコンセンサス方式では、参加できるノード数が限られ可用性も下がるなど、トレードオフが存在する

＜品質に関する評価項目例＞
処理性能（向上性）、容量拡張性、ブロック確定性能、否認防止性、真正性・・等
＜保守・運用に関する評価項目例＞　修正性等

ブロックチェーン技術を活用したシステムの評価軸 評価項目の概要

- ブロックチェーン技術の特性と特に関係性の強い32項目より構成されている

大項目	中項目	小項目
品質	性能効率性	処理性能（スループット）
		ネットワーク性能
		ブロック確定性能
		参照性能
	相互運用性	既存システムとの相互運用性
		他ブロックチェーン技術を活用したシステムとの相互運用性
	拡張性（スケーラビリティ）	処理性能向上性（スループット向上性）
		ネットワーク性能向上性
		容量拡張性
		ノード数拡張性
	信頼性	成熟性
		可用性
		障害許容性（耐故障性）
		回復性
	セキュリティ	機密性
		インテグリティ
		否認防止性
		真正性
	移植性	適応性
		置換性

大項目	中項目	小項目
保守・運用	保守・運用性	モジュール性
		再利用性
		解析性
		修正性
		試験性

大項目	中項目	小項目
コスト	研究開発	ブロックチェーンエンジン技術要素の研究開発
		サブシステムの研究開発
	実装（製品化）	ハードウェアコスト
		ソフトウェアコスト
		システム実装コスト
	保守・運用	運用コスト
		保守コスト

ブロックチェーン技術を活用したシステムの評価軸 ver. 1.0
- 品質に関する評価項目　1/4

大項目	中項目	小項目	項目に関する概要等	関連するブロックチェーン技術・特性	本評価軸を活用する際の留意点、備考等
品質	性能効率性	処理性能（スループット）	製品又はシステムの機能を実行するとき、製品又はシステムの応答時間及び処理時間並びにスループット速度が要求事項を満足する度合い。	・ブロックサイズ ・トランザクションサイズ ・コンセンサス方式 ・ブロック生成時間	・ノード構成、ネットワーク環境、コンセンサス方式等の前提条件を明確にする。 ・スループットの定義を明確にする。たとえば、「対象とする処理は、トランザクション処理で理論性能など。」。 ・他評価項目等とのトレードオフの関係に留意し、明確に示す。 ※トレードオフの内容については、「処理性能向上性（スループット向上性）」の項目に詳述。
		ネットワーク性能		・ネットワーク環境 ・ノード分散	・ノード構成、ネットワーク環境等の前提条件を明確にする。 ・処理時間の定義を明確にする。たとえば「ランダムに2つのノードを選択して、そのノード間で〇kBのデータ送信にかかる時間を測定する。これを〇回実施した平均値。」など。
		ブロック確定性能		・コンセンサス方式 ・ネットワーク環境 ・ノード分散	・ブロックが確定するまでの時間。処理時間の定義を明確にする（たとえば「トランザクションを投げてからブロック確定まで」など）。 ・ブロックが確定する場合には、確定を得られるまでの時間、確定しない場合には、〇〇%の確定度合いを得られるまでの時間等、用いているコンセンサス方式の特徴・トレードオフ関係を明確にする。たとえば、「PoWを用いており、ブロック確定はできないが、後続に6ブロック生成されれば、確定度合いが〇%となる。また、ノード数に特別な制限はない。」など。 ・他評価項目等とのトレードオフの関係に留意し、明確に示す。 ※トレードオフの内容については、「処理性能向上性（スループット向上性）」の項目に詳述。
		参照性能		・ノード分散 ・ネットワーク環境 ・ブロック構造	・特定のブロックおよびトランザクションを参照する際の性能。ノード構成、ネットワーク環境等の前提条件を明確にする。
	相互運用性	既存システムとの相互運用性	二つ以上のシステム、製品又は構成要素が情報を交換し、既に交換された情報を使用することができる度合い。	・データ構造 ・API仕様	・相互運用のための前提条件を明確にする。 ・連携実績のある既存システムおよびどのような連携なのか明示する。
		他ブロックチェーン技術を活用したシステムとの相互運用性		・データ構造 ・コンセンサス方式 ・API仕様	・相互運用のための前提条件を明確にする。 ・連携実績のある他のブロックチェーン技術を活用したシステム、およびどのような連携なのか明示する。

- 品質に関する評価項目　2/4

大項目	中項目	小項目	項目に関する概要等	関連するブロックチェーン技術・特性	本評価軸を活用する際の留意点、備考等
品質	拡張性（スケーラビリティ）	処理性能向上性（スループット向上性）	性能を向上させられる度合い	・ブロックサイズ ・トランザクションサイズ ・コンセンサス方式 ・ブロック生成時間	・ スループット向上のために取りうる方法と、その方法により生じうるトレードオフにつき明確にする。 【明確にすべきトレードオフ関係】 ・ 信頼性にかかるトレードオフ関係：たとえば、「処理性能を上げることでデータ容量が増大することにつながり、ノードの負担（特に全データを保持するフルノードの負担）が大きくなり、フルノードを担えるサイトが減少し、信頼性が下がる。フルノードが〇ノード以下になるとリクワイアメントを満たすことが困難となる。」など。 ・ 適用するコンセンサス方式により生じるトレードオフ関係：たとえば、「高速な●●コンセンサス方式を適用してスループットを向上させている。この方式では、特定の管理された承認ノードが必要に なり、承認ノード数は実運用的に30台程度が上限である。これらのうち1/3が不通となるとシステム機能を維持できなくなるため、可用性は低下し、〇となる。」など。
		ネットワーク性能向上性		・ノード分散 ・ネットワーク環境 ・P2Pプロトコル	・ 分散環境であることから、ネットワーク環境に強く依存するため、ネットワーク性能向上のボトルネックになっている部分を示し、性能向上のポイントの所在を明確にする。
		容量拡張性	処理性能の向上や履歴の蓄積によって、保持すべきデータ容量が増大する。これらデータの増大に対する拡張性の度合い	・ブロックサイズ ・トランザクションサイズ ・コンセンサス方式 ・ブロック生成時間	・ データ蓄積によって、保持すべきデータ容量は増大する。ある一定期間後のデータ容量を見積り、取りうる対応につき明確にする。
		ノード数拡張性	分散システムのためどの程度のノード数に対応可能かの度合い	・データ容量 ・コンセンサス方式	・ 各種別のノード（フルノードやライトノード等）について拡張の上限を明確にする。 ノード数が増大すると、処理性能を超過するトランザクションが発生する可能性がある。このため、処理性能に見合ったノード数の想定を明確にする。 ・ 他評価項目等とのトレードオフの関係に留意し、明確に示す。 ※トレードオフの内容については、「処理性能向上性（スループット向上性）」の項目に詳述。

- 品質に関する評価項目　3/4

大項目	中項目	小項目	項目に関する概要等	関連するブロックチェーン技術・特性	本評価軸を活用する際の留意点、備考等
品質	信頼性	成熟性	通常の運用操作の下で、システム、製品又は構成要素が信頼性に対するニーズに合致している度合い。	・既存の実用技術（暗号技術等） ・研究開発した新規の技術（コンセンサス方式等） ・ブロックチェーン技術を活用した実用システムとしての成熟性、稼動実績	・ システムの成熟性については、通常導入実績などで評価するが、ブロックチェーン技術の導入実績は、策定時点においてほとんどなく、端的に評価することが難しい。そこで、ブロックチェーン技術を活用したシステムは、暗号技術等の既存技術とコンセンサス方式やスループット等性能・機能向上のために研究開発された新しい技術を組み合わせて実現されていることから、個々の要素技術の実用実績、類似システムの稼動実績、テスト環境における稼動実績等によりシステムとしての成熟性を示す。
		可用性	使用することを要求されたとき、システム、製品又は構成要素が運用操作可能及びアクセス可能な度合い。	・単一障害点の有無	・ 単一障害点となるノードの有無について明確にする。 ・ 単一障害点がない場合においては、どの程度のノードが不通等により機能しなくなるとシステムとしての信頼性が得られなくなるか明確にする。
				・コンセンサス方式	・ 正しいコンセンサスを得るための条件（ノード数等）を明確にする。 ・ コンセンサス方式に起因する不正状態（51%攻撃）、コンセンサス不能状態（PBFTにおける1/3以上のノードとの不通）等のコンセンサスが機能しなくなる条件を明確にする。
		障害許容性（耐故障性）	ハードウェア又はソフトウェア障害にもかかわらず、システム、製品又は構成要素が意図したように運用操作できる度合い。	・ノード障害の許容性 ・ネットワーク障害、分断攻撃の許容性	・ 正常稼動の定義を明確にする。 ・ 正常稼動のためのノード条件、ネットワーク条件を明確にする。 ・ ネットワーク分断等によるフォーク発生後のメインチェーンの決定方法を明確にする。
		回復性	中断時又は故障時に製品又はシステムが直接的に影響を受けたデータを回復し、システムを希望する状態に復元することができる度合い。	・ノード障害の回復性（回復方法、回復時間等）	・ ネットワーク環境やデータ量などの前提条件を明確にする。

- 品質に関する評価項目　4/4

大項目	中項目	小項目	項目に関する概要等	関連するブロックチェーン技術・特性	本評価軸を活用する際の留意点、備考等
品質	セキュリティ	機密性	製品又はシステムがアクセスすることを認められたデータだけにアクセスすることができることを確実にする度合い。	・アクセス管理	・ データへのアクセス権限（読み、書き等）の管理方法、設定レベル等を明確にする。
				・データ秘匿化	・ データを秘匿する機能の有無を明確にする。 ・ 秘匿化の対象、範囲を明確にする。 ・ 秘匿化されたデータの第3者による検証方法を明確にする。
				・トランザクション秘匿化	・ トランザクションを秘匿する機能の有無を明確にする。 ・ 秘匿化の対象、範囲を明確にする。 ・ 第3者による検証方法を明確にする。
		インテグリティ	コンピュータプログラム又はデータに権限をもたないでアクセスすること又は修正することを、システム、製品又は構成要素が防止する度合い。	・メンバー管理	・ メンバーシップ管理機能の有無等を明確にする。
				・アクセス管理	・ データへのアクセス権限（読み、書き等）の管理方法、設定レベル等を明確にする。
		否認防止性	事象又は行為が後になって否認されることがないように、行為又は事象が引き起こされたことを証明することができる度合い。	・コンセンサス方式	・ コンセンサス方式によるブロック確定の有無を明確にする。フォーク後のメインチェーンの決定方法を明確にする。
				・ハードフォークポリシー	・ ブロック巻き戻しに関するルール、方法、影響範囲を明確にする。
		真正性	ある主体又は資源の同一性が主張したとおりであることを証明できる度合い。	・分散ノード間の同期方法	・ 分散したノード間でデータの同期が行われるかを明確にする。また、同期する際に正しいとするデータの決定方法を明確にする。
				・コンセンサス方式	・ コンセンサス方式によるブロック確定の有無を明確にする。また。フォーク後のメインチェーンの決定方法を明確にする。
	移植性	適応性	異なる又は進化していくハードウェア、ソフトウェア又は他の運用環境若しくは利用環境に製品又はシステムが適応できる有効性及び効率性の度合い。	・ハードウェア適応性	・ ノードに関する要件を明確にする。
				・アプリケーション適応性	・ アプリケーションに関する要件を明確にする。
		置換性	同じ環境において、製品が同じ目的の別の明示された製品と置き換えることができる度合い。	・既存システムとの置換性	・ どのような既存システムと置換性があるのか明確にする。
				・他のブロックチェーン技術を活用したシステムとの置換性	・ どのような他のブロックチェーン技術を活用したシステムと置換性があるのか明確にする。

ブロックチェーン技術を活用したシステムの評価軸 ver. 1.0
- 保守・運用に関する評価軸　1/2

大項目	中項目	小項目	項目に関する概要等	関連するブロックチェーン技術・特性	本評価軸を活用する際の留意点、備考等
保守・運用	保守・運用性	モジュール性	一つの構成要素に対する変更が他の構成要素に与える影響が最小になるように、システム又はコンピュータプログラムが別々の構成要素から構成されている度合い。	・ブロックチェーンプラットフォーム	・ブロックチェーンプラットフォームの構成要素、技術要素のモジュール性について明確にする。たとえば、「コンセンサス方式は、モジュール性の高い実装としているので、他の方式への変更は容易である。」など。
				・サブシステム	・サブシステムの構成要素、技術要素のモジュール性について明確にする。たとえば、「サブシステムの●●機能について、高機能化することを考慮したモジュール設計としているため、●●機能の高度化は容易である。」など。
				・コントラクト・コード	・コントラクト・コードの仕様（記述言語等）を明確にする。
		再利用性	一つ以上のシステムに、又は他の資産作りに資産を使用することができる度合い。	・ブロックチェーンプラットフォーム	・コンセンサス方式の再利用性を明確にする。たとえば、「ブロックチェーンプラットフォーム●●に実装したコンセンサス方式は、ブロックチェーンプラットフォーム▲▲にも実装できるようになっている。」など。
				・サブシステム	・サブシステムの再利用性を明確にする。たとえば、「サブシステム●●は、▲▲システムでも利用できるようになっている。」など。
				・コントラクト・コード	・コントラクト・コードの仕様（記述言語等）を明確にする。
		解析性	製品若しくはシステムの一つ以上の部分への意図した変更が製品若しくはシステムに与える影響を総合評価すること、欠陥若しくは故障の原因を診断すること、又は修正しなければならない部分を識別することが可能であることについての有効性及び効率性の度合い。	・障害検知	・障害が発生しているかどうかの検知機能の有無を明確にする。 ・障害がどこで発生しているかの特定（ノード障害、ネット障害等）機能の有無を明確にする。 ・障害の影響範囲の特定機能の有無を明確にする。
				・パフォーマンス解析	・スループット、ネットワーク性能、スケーラビリティ等のパフォーマンス・モニタリング機能の有無を明確にする。
		修正性	欠陥の取込みも既存の製品品質の低下もなく、有効的にかつ効率的に製品又はシステムを修正することができる度合い。	・バグ対応	・バグの修正対応の方法、責任所在等を明確にする。
				・コントラクト・コード	・ブロックチェーン技術を活用したシステムでは、書き込まれたものは修正（改ざん）できないが、コントラクト・コードにバグが発見された場合の対応はどうするのか明確にする。
				・ハードフォーク	・ブロックチェーン技術を活用したシステムでは、書き込まれたものは修正（改ざん）できないが、バグや不正アクセスによる不正データが発見された場合のブロックの巻き戻し対応について明確にする。

- 保守・運用に関する評価軸　2/2

大項目	中項目	小項目	項目に関する概要等	関連するブロックチェーン技術・特性	本評価軸を活用する際の留意点、備考等
保守・運用	保守・運用性	試験性	システム、製品又は構成要素について試験基準を確立することができ、その基準が満たされているかどうかを決定するために試験を実行することができる有効性及び効率性の度合い。	・ブロックチェーンプラットフォーム	・ ノード構成、ネットワーク構成によって、試験結果は影響を受けるため、どのような環境でどのような機能、性能試験ができるのか、環境が変わったときにどのような影響を受けるのか明確にする。
				・ノード障害、ネットワーク障害の耐性 ・スケーラビリティ ・コンセンサス方式	・ 分散環境では、ノードやネットワークの障害への耐性試験、容量やノードの拡張性試験、コンセンサス方式の試験が重要であるため、これらについてどのような試験ができるのか明確にする。
				・コントラクト・コード	・ ブロックチェーンでは、書き込まれたものは修正（改ざん）できないため、コントラクト・コードは十分な試験が必要であるため、どのような試験ができるのか明確にする。

ブロックチェーン技術を活用したシステムの評価軸 ver. 1.0
- コストに関する評価軸

大項目	中項目	小項目	項目に関する概要等	関連するブロックチェーン技術・特性	本評価軸を活用する際の留意点、備考等
コスト	研究開発	ブロックチェーンエンジン技術要素の研究開発	研究開発に係るコスト（導入前コスト）	・新しいコンセンサス方式 ・高速なP2Pプロトコルの開発	・ 処理性能向上等にためのブロックチェーンプラットフォームの技術要素の研究開発コストを見積る。 ・ 既存技術の機能・性能レベルを整理し、目指す機能・性能を明確にして見積る。
		サブシステムの研究開発		・アプリケーション開発 ・コントラクト開発環境	・ 適用分野等を広げるためのサブシステムの研究開発コストを見積もる。 ・ 機能・性能を明確にして見積もる。
	実装（製品化）	ハードウェアコスト	システムの実装に係るコスト（導入時コスト）	・ノード ・ネットワーク ・サブシステム	・ コストに含まれる対象、範囲を明確にする。 ・ プラットフォームの分類の違い（パブリック型/コンソーシアム型・プライベート型等）で見積り対象、範囲が異なることを明確にする。たとえば、「パブリック型の場合は、不特定の参加者の資材をコストとして見積もらない（見積もることができない）。」、「プライベート型では、ノード数や参加者が明確であり、また、サーバ的役割を担う機器等も想定されるためこれらのコストを見積もる。」など。
		ソフトウェアコスト		・OS ・ミドルウェア ・アプリケーション	・ コストに含まれる対象、範囲を明確にする。 ※明確化の例示については、「ハードウェアコスト」の項目に記述
		システム実装コスト		・組み立て、実装、試験	・ コストに含まれる対象、範囲を明確にする。 ※明確化の例示については、「ハードウェアコスト」の項目に記述
	保守・運用	運用コスト	システムの保守、運用にかかるコスト（導入後コスト）	・ノード ・ネットワーク ・コンセンサスに係るコスト（コンセンサス方式の違いによるコストへの影響）	・ コストに含まれる対象、範囲を明確にする。
		保守コスト		・バグ修正	・ コストに含まれる対象、範囲を明確にする。 ・ 新技術のため、修正頻度の高さや対応に必要となる技術的レベルを明確にする。

本評価軸の活用　①既存システムとの比較評価

本評価軸は、主にシステムベンダー等が、システム導入者に対する提案の中で、既存システムをブロックチェーン技術を活用したシステムに置き換える場合の比較評価を行う際に活用されることを想定

- 既存のシステム評価の枠組み（ISO/IEC25010やIPAのシステム・リファレンス・マニュアル）によりシステム全体を評価
- ブロックチェーン技術に関連性が高い品質や保守・運用、コストの各評価項目については今回の評価軸に沿って評価
- 結果を併せてシステム導入検討者に対して提示

システムベンダーによる活用のイメージ

本評価軸			既存 Aシステム ・システム構成：・・・	ブロックチェーン技術を活用したXシステム ・システム構成：ノード数○○、・・・
品質	性能効率性	処理性能	・時間当たりの処理件数　●●件/sec ・レイテンシ　●msec 測定条件：・・・・・・・	・時間当たりの処理件数　○○件/sec ・レイテンシ　○msec 測定条件：・・・・・・・
		ネットワーク性能	●msec 測定条件：・・・・・・・	○msec 測定条件：・・・・・・・
		ブロック確定性能	-	・ブロック確定不可（コンセンサス方式PoW） ・○ブロック生成時点における確定度合○%
		参照性能	●msec 測定条件：・・・・・・・	○msec 測定条件：・・・・・・・
	相互運用性	既存システムとの相互運用性	Pシステムとの連携実績有・・・・・	連携実績なし・・・・
		他ブロックチェーン技術を活用したシステムとの相互運用性	-	ブロックチェーンプラットフォームYとの相互運用有・・・・
	・ ・	・ ・	・ ・	

本評価軸の活用　②実証実験等の評価

本評価軸をブロックチェーン技術を活用したシステムの実証試験結果等の評価に利用するケースも想定される

- 実証実験の目的やユースケースのリクワイアメントに応じて、着目する評価項目に関し評価
- 「本評価軸を活用する際の留意点、備考等」に基づいて評価を実施
- 複数の実証試験結果において着目する評価項目を合わせて評価することで、結果を横並びに比較することが可能

実証実験等の評価のイメージ

本評価軸			ブロックチェーン技術を活用したシステムの実証実験　A ・システム構成：ノード数○○ ・ブロックチェーンプラットフォーム：X	ブロックチェーン技術を活用したシステムの実証実験　B ・システム構成：ノード数○○、・・・ ・ブロックチェーンプラットフォーム：Y
品質	性能効率性	処理性能	・時間当たりの処理件数　●●件/sec ・レイテンシ　●msec 測定条件：・・・・・・・	・時間当たりの処理件数　○○件/sec ・レイテンシ　○msec 測定条件：・・・・・・・
		ネットワーク性能	●msec 測定条件：・・・・・・・	○msec 測定条件：・・・・・・・
		ブロック確定性能	・ブロック確定可能（コンセンサス方式PBFT）	・ブロック確定不可（コンセンサス方式PoW） ・○ブロック生成時点における確定度合○%
		参照性能	●msec 測定条件：・・・・・・・	○msec 測定条件：・・・・・・・
	相互運用性	既存システムとの相互運用性	－（着目しない）	－（着目しない）
		他ブロックチェーン技術を活用したシステムとの相互運用性	－（着目しない）	－（着目しない）
	・ ・	・ ・	・ ・	

今後期待される取組とブロックチェーン技術の社会実装に向けた課題

- ブロックチェーン技術の活用進展に寄与していくために、今回の検討に加えて評価軸に関する以下の取り組みや検討が必要

評価軸に関し期待される取組

- **実際のシステムにおける評価の実施とその蓄積**
  - ・評価指標・評価方法に関する指針・ガイドラインの整備も必要
- **ユースケースの蓄積に応じた評価軸の網羅性の検証／技術の進展に合わせた評価軸のメンテナンス**
  - ・評価軸の管理の主体の決定も必要（公的機関やコンソーシアムによるオープンソース的な更新）
- **評価軸の国際標準化**
  - ・イノベーションの阻害とならないよう留意しつつも、我が国が国際標準化を主導する期待もある

- ブロックチェーン技術の特性が生かされるような、新たなサービス・仕組みの社会実装を進めるために、以下が課題であると認識

新たなサービス・仕組みの社会実装に向けた課題

- **ブロックチェーン技術の特性の把握と周知を行うこと**
  - ・今回の評価軸整備のような観点での継続的議論
  - ・ユースケースを増やし、ブロックチェーン技術に対する理解を深める
- **課題解決に関するステイクホルダーによるコンソーシアムの構築**
  - ・ブロックチェーン技術の特性を活用することで解決可能な社会課題を抽出
- **ブロックチェーン技術を活用したシステムを構築する際の要素技術の整理**
  - ・リクワイアメントと実現されていることとのギャップとそれを満たす技術の抽出
  - ・処理性能、信頼性、情報の秘匿化、セキュリティに関連する技術など
- **社会実装のための環境整備（規制・制度の見直し等）**
  - ・監査・認証・証明制度等にブロックチェーン技術を活用するための法制度見直し
  - ・ブロックチェーン技術を活用したシステム上に記録されているデータの法的証拠力の明確化

（参考）ブロックチェーン技術を活用したシステムの評価軸検討委員会

- 「ブロックチェーン技術を活用したシステムの評価軸検討委員会」は、国際大学グローバル・コミュニケーション・センターの高木聡一郎研究部長を委員長に迎え、学識経験者、ブロックチェーン関連事業者、国内システムベンダー、国際的コンソーシアム参画事業者等により構成（下表参照）
- 2016年11月～2017年3月にかけて5回にわたり開催（事務局：株式会社三菱総合研究所）

《委員名簿》 50音順、敬称略

氏名	所属・役職等
■委員長	
高木　聡一郎	国際大学グローバル・コミュニケーション・センター　研究部長
■委員	
エドムンド・エドガー	株式会社ソーシャル・マインズ CEO
大岩　寛	国立研究開発法人産業技術総合研究所　情報技術研究部門 サイバーフィジカルウェア研究グループ長
加納　裕三	株式会社bitFlyer 代表取締役
楠　正憲	ヤフー株式会社 CISO Board
柴田　巧一	株式会社SKEED IoT事業開発室室長
杉井　靖典	カレンシーポート株式会社 代表取締役/CEO
高城　勝信	日本IBM株式会社 ブロックチェーン・アーキテクト
長　稔也	株式会社日立製作所 金融システム営業統括本部 事業企画本部　金融イノベーション推進センタ センタ長
鳥山　慎一	日本電気株式会社 事業イノベーション戦略本部　Fintech事業開発室 マネージャー
八田　真行	駿河台大学 専任講師
廣瀬　一海	日本マイクロソフト株式会社 クラウドソリューションアーキテクト
山崎　重一郎	近畿大学 産業理工学部 情報学科 教授