参考4

ブロックチェーン活用検討SWG
取りまとめ 概要

1．ブロックチェーン技術の基本的特徴

1．事実上落ちない（正しく動作）

- データを保管するノードを多数配置し、当該データをネットワーク全体で共有する分散処理構造を採っているため、仮にいずれかのノードが何らかの原因により動作しなくなったとしても、他のノードが動き続けることでデータベースとしての高可用性を実現。
- コンピュータネットワークに参加するノードが意図的に、またはソフトウェアのバグにより意図せずエラーが起きるような通信をする状況において、ネットワークを構成するノード全体でデータの同期を正しくとることができるかという問題（ビザンチン将軍問題）を、合意形成プロトコル（コンセンサスアルゴリズム）によって実用レベルで解消。

2．事実上改ざん不可能

- 取引データ等の電文を一定数とりまとめてブロックを形成し、当該ブロックごとに不可逆のハッシュを生成して「ダイジェスト」を作成し、この「ダイジェスト」をチェーンのように後続のブロックへと次々につなげていくことによって、あるブロック内のデータが改ざんされた場合には、その後続のブロックの「ダイジェスト」と整合しなくなるため、改ざんの検出が容易。

3．オープン性

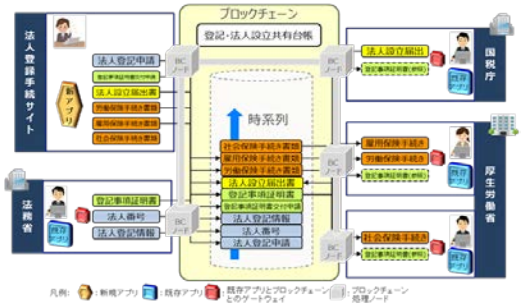
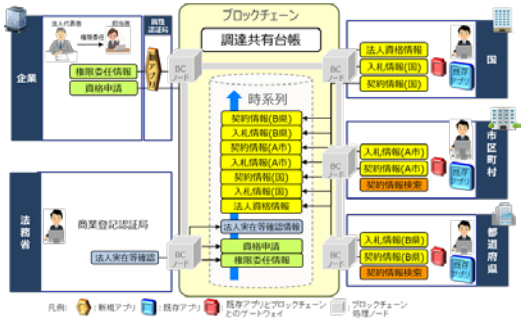
- 「落ちない」「消えない（事実上改ざん不可能）」データベースを、オープンプロトコルにより監査性を確保することで、オープンなネットワーク上のノード（サーバの集団）により実現。
（インターネット技術は「切れない通信」をオープンテクノロジー（TCP/IP、HTTP、WWW等）で実現）

4．スマートコントラクト

- データを自動処理するプログラム（スマートコントラクト）をブロックチェーン上で動かすことにより、人手を介さなくとも、手続や契約を履行。

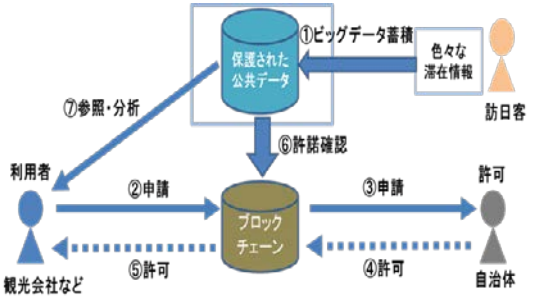
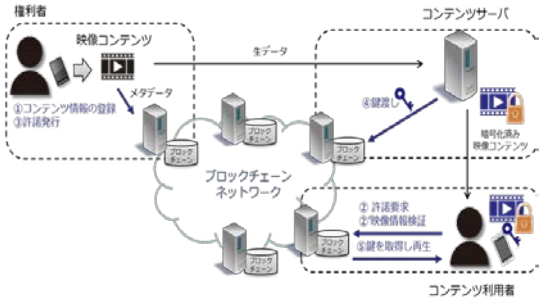
2．ブロックチェーン技術の活用ユースケース①

1．行政手続など公的分野での活用

	ユースケース	ユースケースの概要
(1)	法人設立手続	・法人の設立等に伴う手続にブロッチェーンを活用し、登記事項証明書を関係行政機関で共有することで、オンラインでの登記事項証明の真正性を確保するとともに、手続の負担・コスト軽減と迅速化を実現。  貝塚構成員プレゼン資料より
(2)	政府調達手続	・国と自治体の電子調達手続にブロックチェーンを活用し、入札参加資格申請の簡素化・共通化による官民の事務処理の効率化を図るとともに、国・自治体を通じた調達実績を共有することによって、国・自治体での調達コストの削減を実現。  貝塚構成員プレゼン資料より
(3)	電子自治体	・地域振興ポイント等の各種ポイントの運用管理、受注先との手形債権の管理、母子保健・学校検診・企業検診をカバーするPHRの管理等、安定的かつセキュアな環境の下で、多数当事者間でのデータ共有等が必要となる住民向けサービスをブロックチェーン上でリーズナブルに提供することで、効率的な電子自治体を構築。  中村構成員プレゼン資料より

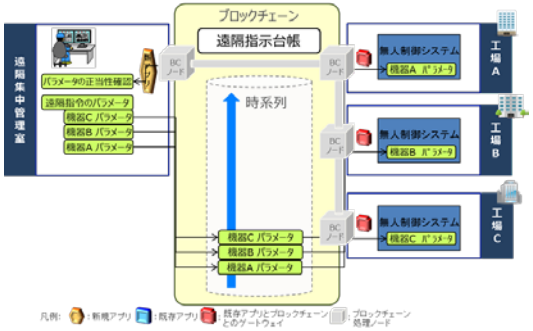
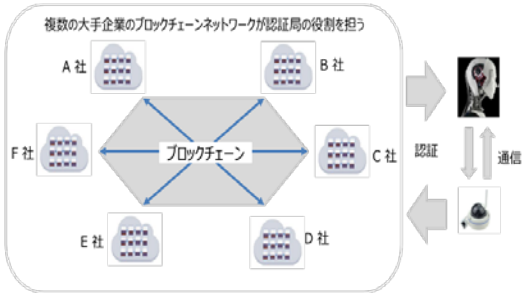
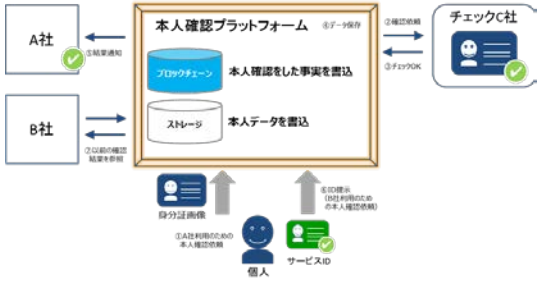
2．ブロックチェーン技術の活用ユースケース②

1．行政手続など公的分野での活用

	ユースケース	ユースケースの概要
(4)	公共データの利活用促進	・自治体等が保有する公共データについて、利用申請・許諾プロセスや有料の場合の課金処理などをブロックチェーンで効率的かつ適正に管理することで、公共データの利用許諾等の真正性を確保しつつ、その利用を促進。  岸上構成員プレゼン資料より
(5)	デジタルコンテンツ	・デジタルコンテンツの権利者情報、有効期間、価格など、コンテンツに付随するデータ（メタデータ）をブロックチェーン上に記録することで、第三者に委ねない形でコンテンツを管理するとともに、その権利関係についての真正性を保証。  岸上構成員プレゼン資料より

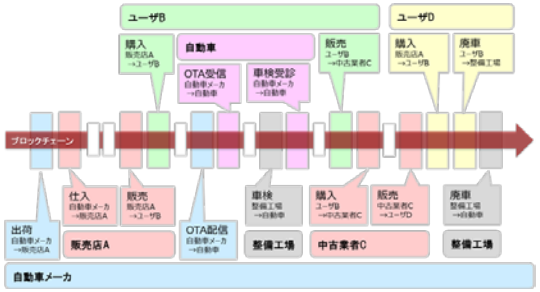
2．ブロックチェーン技術の活用ユースケース③

2．IoTなど民間サービスでの活用

	ユースケース	ユースケースの概要
(1)	遠隔制御システム等におけるソフトウェアのバージョン管理	・遠隔制御システム等の稼働パラメータ等のソフトウェアについて、ブロックチェーンの耐改ざん性を活かして管理し、その不正書き換えを防ぐとともに、脆弱性のある箇所にセキュリティ対策を緊急に施す等の措置により、サイバー攻撃に対処。  貝塚構成員プレゼン資料より
(2)	IoT機器の信頼性向上	・IoT機器の認証情報（どのIoT機器が通信したのか）をブロックチェーンで管理することで、認証情報の信頼性を向上するという直接の目的のほか、サイバー攻撃を探知してIoT機器のセキュリティ回復、IoT機器間の通信暗号化やIoT機器が生成するデータの真正性確保を通じたビッグデータの信頼性向上を実現。  合同会社Keychain 三島様 プレゼン資料より
(3)	シェアリングサービスにおける本人確認手続	・運転免許証やマイナンバーカード等により本人確認を行った結果をパブリックブロックチェーンに記録することにより、本人確認サービスの信頼性の向上を図るとともに、シェアリングサービスにおける本人確認を業界で共通化し、本人確認の煩雑さを解消。  北村構成員・肥後構成員プレゼン資料より

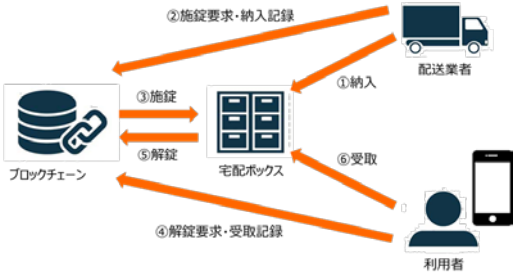
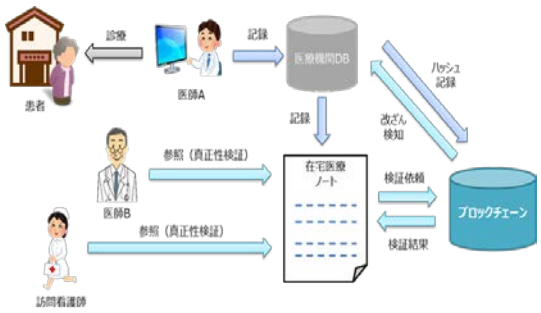
2．ブロックチェーン技術の活用ユースケース④

2．IoTなど民間サービスでの活用

	ユースケース	ユースケースの概要
(4)	顧客データの更新	・サービス提供事業者が保有する顧客データについて、本人がブロックチェーンに書き込んだ情報を、ブロックチェーンに参加する事業者間で共有することで、顧客データの一括更新手続を効率的に実現。  阿部構成員プレゼン資料より
(5)	電力取引の自動化・効率化	・電力会社から分散型電源（自治体などが保有する非常用電源や一般家庭の太陽光発電など）への発電要請、対価支払いといった電力取引の履歴管理について、スマートコントラクトを活用して自動で処理し、透明性ある電力シェアリングエコノミーを形成。  肥後構成員プレゼン資料より
(6)	自動車のトレーサビリティ	・Connected Carに関する多様な機器・サービスのうち「誰（どの機器）が、いつ、何を行ったか」をブロックチェーン上に記録することで、出荷から車検、中古車販売など、自動車のライフサイクルにおける正確なトレーサビリティを関係者間で確保。  北村構成員プレゼン資料より

2．ブロックチェーン技術の活用ユースケース⑤

2．IoTなど民間サービスでの活用

	ユースケース	ユースケースの概要
(7)	宅配ボックスの 配達・受取記録	・宅配ボックスを用いた配達・受取については、その利便性を確保しつつ、授受に伴うトラブル発生のリスクを可能な限り低減するため、宅配ボックスの開閉記録をブロックチェーンで管理することで、荷物の受け渡し・受け取りの事実を、改ざんのない形で客観的に把握可能。  山下構成員プレゼン資料より
(8)	医療データの 真正性確認	・在宅医療に携わる関係者（医師、看護師、救急隊員など）が、ブロックチェーン上で管理されている署名済みの在宅医療データの「ハッシュ」（アクセス可能な範囲でグルーピングされたもの）を検証することで、アクセスコントロールを効かせつつ、別のデータベースに格納されている患者のデータの真正性を確認。  慶應義塾大学 鈴木様プレゼン資料より

３．諸外国の動向

１．エストニア

- 各省庁や民間のデータベースをインターネット経由で相互参照可能とするプラットフォーム（X-ROAD）において、ブロックチェーン技術を採用。このプラットフォームとIDカードを用いた電子認証とを組み合わせることで、世界最先端レベルの電子政府を実現。

２．英国

- 政府がブロックチェーン技術を公共分野で活用する５つのユースケースを提案するなど、ブロックチェーン技術の活用について非常に積極的に取り組んでいる国の一つ。
- ユースケースとして、社会保障給付、国際援助といった金銭給付をはじめ、知的財産、特許等の登録データベースへの活用やソフトウェア改ざん検知による重要インフラ防御など、行政全般にわたってブロックチェーン技術を活用するアイデアを提案。

３．その他

- スウェーデン、米国、オランダなどの欧米諸国のみならず、ジョージア（グルジア）、ホンジュラス、ガーナといった途上国でも、不動産登記や取引の記録へのブロックチェーン技術の活用を検討されてきている。

４．今後の取組の方向性

（１）ブロックチェーン技術の社会実装に向けて

① ブロックチェーン技術の、不特定多数の者がオープンネットワーク上で参加しながら取引内容の透明性と耐改ざん性を確保するという特徴は、ブロックチェーン技術の革新的な点である。加えて、複数のノード間を確実に同期させ、データベース全体の強靭性を高める機能や、スマートコントラクトによって処理の自動化を容易にする機能についても、ブロックチェーンならではの重要な特徴と考えられる。

一方、本サブワーキンググループで報告された活用事例には、不特定多数の者が参加してオープンネットワーク上で耐改ざん性等の確保を図る「パブリック型」と、認証されたノードによるネットワークを前提とする「パーミッションド型」の双方が見られたところである。

以上にかんがみれば、ブロックチェーン技術の社会実装を進めていく上では、共通の特徴やそれぞれの相違点を踏まえた上で、ニーズに応じて「パブリック型」と「パーミッションド型」の双方の活用を視野に進めていくことが適当と考えられる。

② ブロックチェーン技術自体は、データの秘匿性や入力されるデータの真正性を保証するものではない。そのため、ブロックチェーン技術の活用に当たっては、データの秘匿性を確保するためのアクセス制御、参加者の本人性や入力されるデータの真正性を確保するための公的個人認証サービスなど、他のソリューションを適切に組み合わせることで、活用ニーズに応じたデータベースを設計・構築していくことが必要である。

③ ブロックチェーンはデータベースの代わり、仮想通貨やトークン機能、自律的サービス稼働の仕組みとして活用できるが、特定の信頼できる組織を前提として、単に既存のデータベースの代わりとしてデータを登録するためだけにブロックチェーン技術を活用するメリットは少ないと考えられる。他方、スマートコントラクトを活用した処理の自動化、前後の業務プロセスとの連携、多様なステークホルダーが連携する業務（特に、生産性向上の観点から、異なる業態の組織・団体が現状それぞれ行っている顧客データの確認・更新など競争の働かない業務）への適用、IoTとスマートコントラクトの活用や既存システムとのAPI連携による決済処理への組み込みなど、既存システムでは容易に実現できないメリットを見出せるようなユースケースに導入することによって、大きな改善効果が得られると考えられる。

（２）先行的な導入実証に向けて

① 世界に先駆けてブロックチェーン技術の社会実装を推進するため、まず、処理の自動化等による業務プロセスの改善や多数当事者間での共有などにより、具体的にどのような課題が解決されるのかを明確にした上で、ブロックチェーン技術のメリットがより発揮されうるユースケースとして、

ア）政府の情報システム（特に、多数の行政機関・事業者が関わり自動処理や情報共有のメリットが見込まれる政府調達システム）への適用や、

イ）異なる業態の組織・団体間の生産性向上に向け、

実証実験に早期に着手する。

② これらの実証実験において、電子委任状に係る制度やブロックチェーンに記録されるデータの真正性確保、アクセス権確認のための公的個人認証の活用の実現等に向け、運用面、ルール面の課題について検討する。その検討結果も踏まえ、ブロックチェーンなど新たな技術も盛り込んだ業務改革により、効率性や利便性の向上に資する革新的な電子行政の実現に向けた計画を、来年度を目処に策定する。

③ また、民間分野での活用を後押しするため、具体的な検証等を通じて、開発のノウハウや技術的課題のフィードバックとともに、ブロックチェーン上のデータの取扱いなどに関する運用面・ルール面での課題を抽出し、具体的な対応方策を検討する。

特に、スマートコントラクトに関しては、契約の成立・履行等に関する法解釈の整理や、プログラムにバグがあった場合やバグが生じた場合の紛争解決ルールの検討にも取り組む。

あわせて、インターネットのTCP/IPなどの先例も参照しつつ、ブロックチェーンを活用したシステムがサステナブルに運営されていくための工夫や、ブロックチェーン上のデータにアクセスするための鍵の管理のあり方などブロックチェーンが安心して利用されるために必要な方策について検討することも重要である。