NISHIMURA & ASAHI

2020年8月24日（月） / BG2C - FIN/SUM BB

西村あさひ法律事務所

ブロックチェーンとデータプロテクション

セッション概要

NISHIMURA & ASAHI

ブロックチェーンとデータプロテクション

ブロックチェーンの利用におけるデータプロテクション（個人情報保護法制）に関して、欧州GDPRにおける議論の紹介と共に、ブロックチェーンを利用する際の個人情報保護法上の論点及び金融実務への示唆について検討を行う。

- 日本、EU、米国における議論

  スピーカー：山本俊之・津田麻紀子

- 金融機関と個人情報・顧客情報

  スピーカー：本柳祐介

モデレーター：有吉尚哉

NISHIMURA
& ASAHI

ブロックチェーンとデータプロテクション
～日本、EU、米国における議論～

山本俊之・津田麻紀子

1　概要

NISHIMURA & ASAHI

- ブロックチェーンの特徴として、①改ざんが困難で、かつ、②非常に可用性の高いデータベースであることが挙げられる
  - 金融取引の記録、契約の記録等、個人情報を格納することが期待される
  - 特にグローバルにノードをつなぐ場合において個人情報の保護が問題

  ⇒　ブロックチェーンに記録された情報に個人情報保護法制の適用はあるか？
- 欧州ではオフィシャルな会議体等で議論が進んでいるが、日本や米国ではあまりされていない（法令との関係での緊張関係の度合いによるもの？）

1　概要～ブロックチェーンの分類（一例）

NISHIMURA & ASAHI

	パブリック型	コンソシーアム型	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 不特定、悪意のある参加者を含む	許可制 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	
台帳閲覧	制限なし	制限可能	
コンセンサス方式（合意形成方式）	PoW等 ブロック確定しない 電力消費が多い	PBFT等 ブロック確定する 軽量、高速、低消費電力	
マイニング報酬	必要	任意	
トランザクション処理時間	長い（10分等）	短い（数秒等）	
ユースケース・実装例	暗号資産（ビットコイン）等	銀行間送金、証券取引等ビジネスネットワーク等	

出所：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」等より作成

1　概要～個人情報保護法制との衝突

NISHIMURA & ASAHI

■ パブリック型ブロックチェーンの特徴

① 管理者が存在せず、

② ノードは国境をまたいで存在し、

③ その取引記録が共有、公開され、

④ 取引記録の改ざん等が（事実上）不可能である

■ ビットコインの仕組みとしては有益なものであるが、個人情報保護法制との関係では不整合・衝突が生じることに

2　日本での議論

NISHIMURA & ASAHI

- 個人情報保護法：中央集権的に個人情報を収集・利用する事業者を想定し、そのような事業者の行為を規律する法律
  - ブロックチェーンの分散・分権の技術思想と相反する

    ⇒　そのまま個人情報保護法を適用すると法令違反の疑いあり？
  - そもそも個人情報該当性、個人情報取扱事業者該当性がブロックチェーンの仕組みによりけり、定説もない（詳細はスライド7頁）
  - その他、以下の個人情報保護法の規定との関係で議論あり（詳細はスライド8頁）
    - ✓利用目的
    - ✓正確性の確保等
    - ✓安全管理措置、委託先の監督
    - ✓第三者提供の制限
    - ✓記録義務
    - ✓訂正権、利用停止
    - ✓域外適用

2　日本での議論

NISHIMURA & ASAHI

- 個人情報：生存する個人に関する情報であって、①氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む）、又は②個人識別符号が含まれるもの（2条1項）
  - 暗号化等によって秘匿化されているかどうかを問わない（ガイドライン通則編2-1）＝暗号化されても個人情報に該当
    - それでも、ハッシュ化によりブロックチェーンに記録された情報は、単なる記号等が羅列された情報に不可逆的に変換されたものであり、特定の個人の識別不可と解釈することは可能か？　という議論あり
- 個人情報取扱事業者：個人情報をデータベース化して事業の用に供している者（2条5項）
  - 非営利でも「事業」には該当し得るが（ガイドライン通則編2-5）、純粋な技術的関心や学術目的の場合は非該当と考えるべきとの議論
  - 全てのノードが個人情報取扱事業者に該当する可能性もあるが、特にパブリック型においては各ノードが個人情報保護法上の義務の自覚がないおそれ、エンフォースメントも困難
  - 他方、各ノードは、分散型台帳の一構成要素として個人情報を保有し、個人情報保護法が前提とする中央集権型データベースがないことから、（責任者・主導者を除き）個人情報取扱事業者に該当しないとの議論もある

2　日本での議論

NISHIMURA & ASAHI

- 個人情報保護法が適用される場合、例えば、以下の論点がある
  - 利用目的の特定・利用目的による制限（15条・16条）：ブロックチェーンの情報は無期限に消去されず、不特定多数又は特定複数のノードに共有

    ⇒　利用目的の達成に必要な範囲に留まらず（必要最小限の原則と緊張関係）、利用目的の特定が困難、仮に特定して同意を得たとしても、その同意の撤回があった場合の処理
  - 正確性の確保等（19条）：ブロックチェーン上の情報は削除・訂正が事実上不可
  - 安全管理措置・委託先の監督（20条・22条）：ブロックチェーンの分権・分散構造と相反、また、委託先の選定・把握が困難
  - 第三者提供の制限（23条・24条）：ノードへの情報提供には本人の同意が必要（同意の例外への依拠は困難かどうか？［次頁参照］）、海外のノードとの関係では越境移転規制あり
  - 第三者提供に係る記録作成・確認等（25条・26条）：パブリック型のブロックチェーンでは、情報の提供先を特定できない、ノードの全員がこれらの義務を負うか
  - 訂正権・利用停止（29条・30条）：記録された情報の訂正・削除を予定しないブロックチェーンの技術思想と相反
  - 域外適用（75条）：国内にある者を本人とする個人情報を（直接）「取得した」か

2　日本での議論～第三者提供の制限の論点

NISHIMURA & ASAHI

手法	論点
本人同意（法23条1項）	①　そもそも同意を取得できるか ②　本人が同意を取り消した場合・撤回した場合にどうなるか ③　新規にノードが追加された場合どうなるか
オプトアウト（法23条2～4項）	④　「個人データの第三者への提供を停止」することを本人より求められた場合（法23条2項）の処理をどうするか ⑤　（実際の利用は想定しづらいかもしれないが）法令上は要配慮個人情報は対象外であることとの関係はどうか（法23条2項）
委託（法23条5項1号）	⑥　ブロックチェーン上の他の参加者らに対して委託を観念できるか ⑦　委託先の監督義務（法22条）は果たせるか
共同利用（法23条5項3号）	⑧　共同して利用する者の範囲の明確化が可能か。とりわけ、個人データの管理について責任を有する者の氏名又は名称を特定可能か ⑨　「共同して利用される個人データの項目」及び「共同して利用する者の範囲」についての変更は原則として認められないが（法23条6項、ガイドライン通則編3-4-3(3)）、それはビジネス上許容できるか

3 EUでの議論

NISHIMURA & ASAHI

- 主に以下の議論が参照される
  - Article 29 Working Party（第29条作業部会）
    - GDPRの前身にあたる1995年EUデータ保護指令に基づいて設置された、加盟国各国のデータ保護機関の代表、欧州委員会司法総局データ保護課の代表、欧州データ保護監察機関の代表により構成
  - European Union Blockchain Obsservatory（EUBOF）
    - EUにおけるブロックチェーンイノベーションの加速とブロックチェーンエコシステムの発展を目的として、欧州委員会の支援によって設立
  - Commission Nationale de l'Informatique Libertés（CNIL：仏個人情報当局）
  - Michéle Finck（マックス・プランク研究所）
  - 直近では、欧州委員会の2020年戦略（"A European strategy for data"）においてもブロックチェーンに関する言及あり

3　EUでの議論

NISHIMURA & ASAHI

GDPRの適用可能性

- 2018年5月25日より適用開始されたデータ保護法
- EU域内に拠点を有さない管理者や処理者に対しても域外適用あり
  - ①EEA域内にいる個人に対する商品・サービスの提供に関連して個人データを処理する場合、②EEA域内で行われる個人の行動の監視に関連して個人データを処理する場合
  - 世界中に散在するノードのネットワークに媒介されてデータのやり取りを行うブロックチェーンでは、GDPRへの対応が必要となる
- 一般に、ブロックチェーンに記録された情報は「個人データ」に該当するとされる
- ブロックチェーンに参加するノードは「管理者」に該当しうる
- GDPRとの緊張関係だけではなく、ブロックチェーンによるGDPR遵守の側面も指摘されている

3　EUでの議論

NISHIMURA & ASAHI

- 個人データ：識別された自然人又は識別可能な自然人に関するあらゆる情報を意味する（GDPR4条(1)号）
  - 個人情報をブロックチェーン上に、①プレーンテキスト（平文）、②暗号化、③ハッシュ化といった形式で書き込んだ場合、何れの場合も全て個人データに該当（29条作業部会）
  - ただし、ハッシュ値の個人データ該当性についてはグレーゾーン（EUBOF）
  - ハッシュ化のリバーサルリスク対応としては鍵付きのハッシュタグがCNILにより推奨されている
  - GDPRの適用除外となる匿名化（前文26条）を満たすかどうかも論点
  - 個人データに該当しないような設計とすることを推奨する論調も存在

3　EUでの議論

NISHIMURA & ASAHI

- データ管理者（Controller）：個人データの取扱いの目的及び方法を決定する者（GDPR4条7号）
  - 開発者、ノード、マイナーそれぞれの関与があるため、中央集権的なControllerの概念と親和的ではない
  - パブリック型のブロックチェーンにおいて問題が顕著
  - そもそも誰が管理者となり得るのか？という論点
  - 開発者、コア開発集団は管理者に該当しない（EUBOF）：個人データの取扱いの手段は提供するが、目的を定めるものではない
  - ノードの管理者該当性の議論は定まっていない
    - CNIL：私的又は家庭内活動目的（GDPR2条2項(c)）を根拠に管理者に非該当との見解
    - EUBOF：多くのケースでノードは管理者に該当しないとするが議論はあり得るとの立場
    - Finck：各ノードが管理者に該当する可能性を示唆するが、権限等の限界故に管理者としての責務を果たすことが困難と分析
  - マイナーは管理者に該当しないとされている（CNIL）：マイニングを行うだけであるため個人データの取扱いの目的や方法を定めるものではない

3　EUでの議論

NISHIMURA & ASAHI

- 個人からの訂正・消去等の請求（GDPR16条、17条）との関係：過去のブロックを構成するデータを消去できないという問題
  - CNIL：復号用の鍵の破壊等が消去権に適合し得るとの見解
  - Finck：ブロックチェーンへの個人データの記録を可能な限り避ける対応を提唱（オフチェーン（ブロックチェーン以外の媒体でのデータ処理、ブロックチェーンの技術思想は後退する可能性あり）に保存する等）
- 保存期間（GDPR5条(e)）との関係
  - データが永久に保存されることは許容されないのではないかという問題意識
- データ保護影響評価（GDPR35条）との関係
  - データ保護影響評価（DPIA：特にリスクの高い個人データの取扱いについてリスクを分析・測定等すること）を実施することでデータ主体の権利に及ぼす影響を懸念

4　米国での議論

NISHIMURA & ASAHI

- 連邦法レベルでは、ブロックチェーンに係る規制は特段存在しない
  - 仮想通貨に関する州法間の整合性を図るため、仮想通貨事業法に関する統一規則が発表されている
- ブロックチェーンや仮想通貨に関する規制は各州で対応
  - ニューヨーク州では、仮想通貨関連企業を対象とする営業許認可制度により、サイバーセキュリティ、プライバシー・個人情報保護などを含む厳しい水準を要求している
- 米国において、ブロックチェーンの課題として、個人情報や機密データを保存できるセキュリティ機能は強固かという問題が挙げられている

５　まとめ

NISHIMURA & ASAHI

- サービス設計上、各参加者が適用対象となることを前提に対応すべき
  - 個人情報保護法、GDPRとも、いかなる範囲の参加者に適用されるか不明
  - 法令違反の疑いを避けるため、①プライベート型の採用、②オフチェーンの採用、③過去の取引情報を削除できる設計の採用などの対応が考えられる
    - ただし、ブロックチェーンの技術思想と相反し、イノベーションの進展を阻害するおそれ
- ブロックチェーンを提供する企業にとって、ハッシュ化その他の技術を踏まえ、プライバシーの水準等について配慮する形でのサービス設計が重要
  - Privacy by Designの考え方を取り入れた設計とする必要

NISHIMURA
& ASAHI

ブロックチェーンとデータプロテクション
～金融機関と個人情報・顧客情報～

本柳祐介

1　金融機関と個人情報・顧客情報

- ブロックチェーン技術の金融機関での利用に対する期待は大きい
  - 「ブロックチェーン技術は、特に金融の仕組みそのものを変革するゲームチェンジャーとなる可能性が高いため、我が国金融ビジネスの競争力を確保する観点から、金融分野における実用化に向けた取組を先取的に進める。」（未来投資戦略2017—Society 5.0 の実現に向けた改革—（平成29年６月９日））
- しかし、個人情報・顧客情報について金融機関に対しては厳格な規制があるため、その規制との整合性が重要な問題
  - 銀行法等の法令、監督指針
  - 金融分野における個人情報保護に関するガイドライン
  - 金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針
  - 金融機関における個人情報保護に関するQ&A

２　個人情報･顧客情報に関する規制内容

NISHIMURA & ASAHI

- 銀行法12条の2第2項

  取得した顧客に関する情報の適正な取扱い･･･その他の健全かつ適切な運営を確保するための措置を講じなければならない。

- 主要行等監督指針　Ⅲ－３－３－３　顧客等に関する情報管理態勢

  顧客に関する情報は金融取引の基礎をなすものである。したがって、その適切な管理が確保されることが極めて重要

- ブロックチェーンとの関係で特に問題になるのが金融分野における個人情報保護に関するガイドライン9条

  事業者は、預金者又は保険契約者等の個人データの保存期間については契約終了後一定期間内とする等、保有する個人データの利用目的に応じ保存期間を定め、当該期間を経過した個人データを消去することとする。

３　外部委託

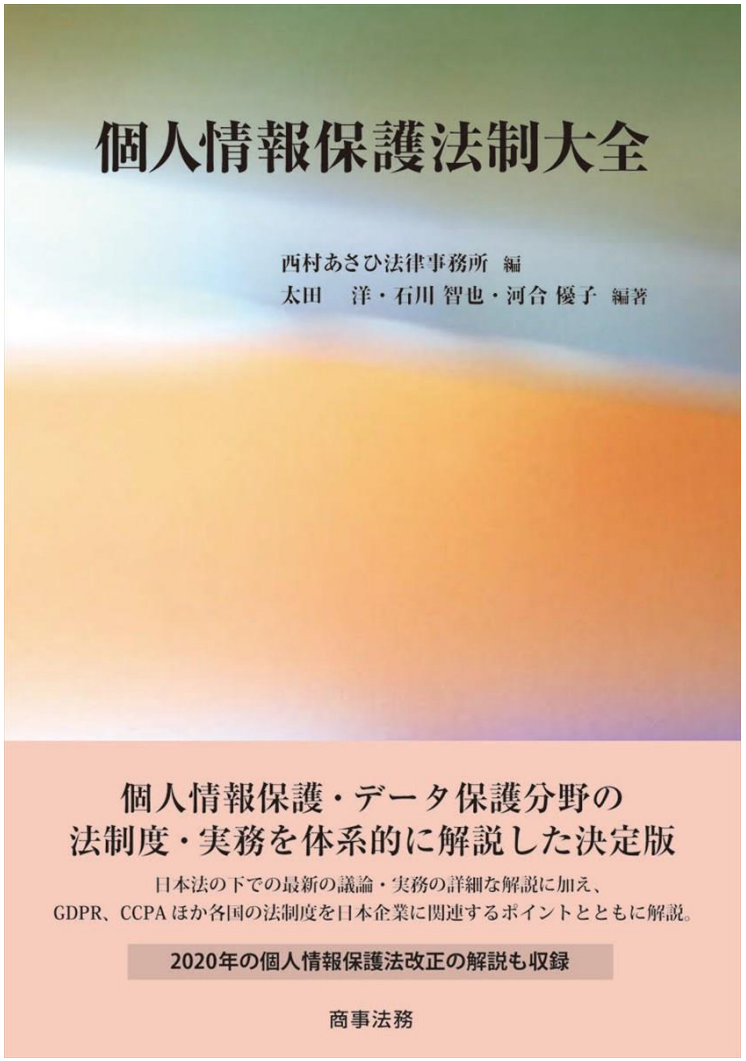
NISHIMURA & ASAHI

- 外部委託に関する整理が課題
  - 銀行法12条の2第2項は、「その業務を第三者に委託する場合における当該業務の的確な遂行その他の健全かつ適切な運営を確保するための措置を講じなければならない。」とする
  - 銀行法施行規則13条の6の5は「銀行は、その取り扱う個人である顧客に関する情報の安全管理、従業者の監督及び当該情報の取扱いを委託する場合にはその委託先の監督について、当該情報の漏えい、滅失又は毀損の防止を図るために必要かつ適切な措置を講じなければならない。」とする。
  - 主要行等監督指針　Ⅲ－３－３－４－２
  - 金融分野における個人情報保護に関するガイドライン12条3項
- ハッシュ化により、各ノードについて外部委託がないとの整理が可能かを検討

4　FISC安全基準とブロックチェーン

NISHIMURA & ASAHI

- 公益財団法人　金融情報システムセンター（ The Center for Financial Industry Information Systems 、FISC）が作成している「金融機関等コンピュータシステムの安全対策基準・解説書」（FISC安全基準）等の基準との関係も課題
- 金融機関においてもクラウドサービスの利用は進んでおり、その延長線上でブロックチェーン技術を使うことが想定される
- セキュリティの確保が重要なものについてはオンプレミスとの併用又は使い分けが想定される



西村あさひ法律事務所編、太田洋・石川智也・河合優子編著『個人情報保護法制大全』（商事法務）

- 第Ⅲ編第7章「ブロックチェーンと個人情報保護法制」