特集
Special Feature

ブロックチェーン技術の最新動向

編集にあたって

吉濱佐知子 日本アイ・ビー・エム（株）

サトシ・ナカモトを名乗る人物がビットコインの論文を発表して10年が経過しました．現在世の中に流通している仮想通貨（暗号資産）は数百種類以上もあり，新技術の発表や取引所への攻撃など，さまざまな観点で連日ニュースを賑わせています．一方，企業間コンソーシアムなどのクローズドな環境でブロックチェーンを使う試みも多く，国内外の銀行間コンソーシアムや証券市場，貿易金融やサプライチェーンなど，多くの取り組みが発表されており，実証実験を超えた本格運用への移行もはじまっています．

このように注目を浴びているブロックチェーン技術ですが，技術的に正確な理解をするのが時として困難となっています．ひところのブロックチェーンブームのおかげで，ブロックチェーンの基本的な仕組みについて解説した記事は比較的多くなってきています．一方，ブロックチェーンの実装は非常に多くの種類がありますが，比較的未成熟な技術であるために，常に新しい方式が提案され，日進月歩の進化を遂げています．こういった「基本」を超えた一歩先の取り組みについては，まとまった技術情報がなかなか見つからないというのが実情です．

本特集は，ブロックチェーンに関連する技術の最新動向について解説を行い，今後の技術開発を促進するための基礎となるような情報を提供することを目指して企画いたしました．

なお，いわゆるブロック構造のデータを持たない実装もあることから，一部の記事ではブロックチェーンの代わりに分散台帳技術（DLT：Distributed Ledger Technology）という語を用いていますのでご了承ください．

佐古和恵氏，古川諒氏，中川紗菜美氏の共著による「**Bitcoin技術のその後の動向**」では，現在ビットコインの抱えるさまざまな課題を解決する取り組みについて，解説を行っています．特にビッ

トコインは単位時間あたりのトランザクション処理件数が少ないという課題があり，これを回避するためにブロックチェーンの外で処理を行う仕組みがいろいろと考案されています．また，新しい暗号アルゴリズムを用いて複雑な取引条件を実現する仕組みについても解説しています．

ブロックチェーンは分散台帳技術であるために，参加者すべてに台帳の情報が共有されるという性質があり，取引のプライバシが保護できないことが懸念されます．長沼健氏の**「分散台帳上での匿名送金とその監査について　ゼロ知識証明を利用したセキュアプロトコル」**では，zk-SNARK というゼロ知識証明プロトコルによる，取引のプライバシ保護の仕組みについて解説しています．

松尾真一郎氏の**「ブロックチェーンの安全性―攻撃や脆弱性とその対策―」**では，ブロックチェーンで満たすべきセキュリティ目標とはなにか，またそれを実現するために必要な技術はなにかということを，6 つのレイヤに分類して解説しています．また，現在知られている代表的な脆弱性を紹介するとともに，将来的な暗号の危殆化などの懸念に対する考察を行っています．

齋藤新氏の**「分散台帳技術におけるコンセンサス・メカニズム」**では，ブロックチェーンで使われる分散合意アルゴリズム（コンセンサス）の仕組みを中心に解説を行います．ビットコインを始めとする多くの仮想通貨では，Proof-of-Work（PoW）という参加者間の計算競争によってブロックを追加していく方式が取られていますが，エネルギーの無駄遣いや安全性などが問題となり，これに変わる新しいアルゴリズムが考案されています．この記事では，誰でも参加できるパブリック型と，参加許可制のプライベート型のそれぞれのタイプのブロックチェーンについて，代表的なアルゴリズムやその特徴を紹介しています．

（2019 年 11 月 18 日）