2V-03

ブロックチェーンでの条件提示と同意に基づいた位置情報提供システムの提案

伊部友貴† 新井浩志†

千葉工業大学大学院工学研究科†

1. はじめに

通信キャリアなどが位置情報を第三者に提供する際には，ユーザの同意が必要である．そこで本提案では，位置情報を提供する条件とその条件に対するユーザの同意をブロックチェーン(以下 BC)に書き込むことで契約を行う手法を提案する。ユーザはその条件に基づいて位置情報を直接利用者に提供する．位置情報は暗号化するとともにデジタル署名を付加することで，本人確認とプライバシー保護を両立しつつ，従来よりも詳細な位置情報データを用いたサービスの提供が可能になる．

2. 位置情報提供システムの従来研究

位置情報提供システムでは BC を用いた研究が行われている．BC を用いることで，位置情報を提供するユーザがどのような位置情報を誰に提供しているのかを明確にすることができる．

Bulat 氏らによる CHAINMOB[1]では，モビリティ分析のためのシステムを提案している．このシステムは，位置情報を提供するユーザが位置情報などの個人情報を BC に書き込み，位置情報を取得したいユーザがインセンティブと引き換えに，データへのアクセス権を得る．

Onik 氏らは個人情報の共有と追跡のためのプライバシーを考慮した BC の研究[2]を行っている．BC はデータの削除ができない．このため Onik 氏らは BC に個人情報を書き込むことは，プライバシーの侵害に当たるとしており，個人情報はオフチェーンストレージで管理し，位置情報を提供した履歴を BC で管理する手法を提案している．

しかし，これらの研究では，位置情報を提供するユーザがどのような条件に対して，位置情報を提供するのかが明確になっていない．また位置情報を BC に書き込むことは BC の増大を招くとともに，BC へのデータの書き込みが完了するまでの時間を長くする．このため，ある程度リアルタイムに位置情報を取得し，利用するサービスには適さないと考えられる．そこで，本研究では BC を用いて，位置情報を取得するユーザが条件を提示し，提供するユーザがその条件に同意することで，位置情報を提供するシステムを提案する．

3. BC での条件提示と同意

3.1 提案するシステムの概要

以下では，EU における個人データ保護に関する法律 EU 一般データ保護規則(GDPR: General Data Protection Regulation)に基づき，データの提供者を User，データの管理者を Controller，データの処理者を Processor と定義する[3]．

提案するシステムでは，まず位置情報を提供するための条件を Processor が BC 上に書き込み，提示する．そして、この条件に対する User の同意を BC 上に書き込むことで契約を行う．この条件に基づいて User の位置情報を暗号化して Controller を介さず直接 Processor に提供する．提案するシステムの構成を図 1 に示す．本研究のシステムは P2P Node，Processor Node，User Node の 3 種類の Node で構成される．図 1 では Processor Node を保有する人物を P1，User

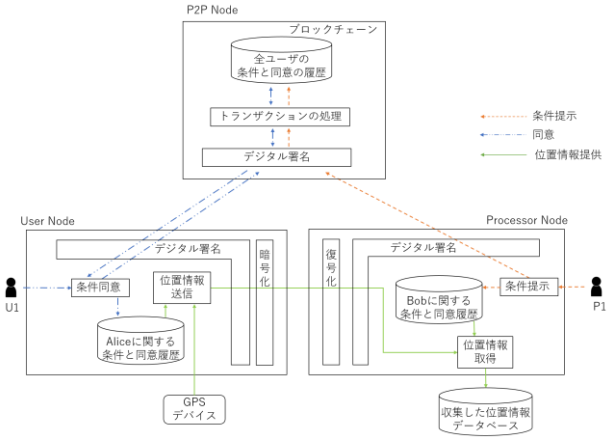

図 1 システム全体の構成

A Location Information Provision System based on Conditions and Consent Using Blockchain

†Tomoki Ibe, Chiba Institute of Technology, Graduate School of Engineering

†Hiroshi Arai, Chiba Institute of Technology, Graduate School of Engineering

Node を保有する人物を U1 としている．また，Processor は条件を提示する権限があり，User は Processor の条件を参照し，同意する権限を有する．

以下では本研究で提案するシステムの流れについて説明する．まず，P1 が条件提示を行う．この条件は位置情報を収集するエリア，頻度，契約の有効期間などを定義したトランザクションとして P2P Node へ送信し，BC に書き込む．また，P1 は BC に書き込むデータを自身の Processor Node に履歴として保存する．このデータは，U1 から P1 へ位置情報を送信するとき，U1 がどの条件に同意しているかを判断するために用いる．

次に，U1 は P1 によって BC に書き込まれた条件を参照し，この条件に同意するか否かを判断する．同意する場合は同意のトランザクションを生成し，P2P Node に送信する．P2P Node はこのトランザクションを BC に書き込むことで，U1 と P1 の契約が成立したことを保証する．このとき，U1 は自身が同意した条件を自身の Node に保存し，この条件に基づいて P1 に位置情報を送信する．

3.2 暗号化とデジタル署名

本研究では，User から Processor へ位置情報を送信する際に公開鍵暗号を用いる．まず，Processor と User はそれぞれ，秘密鍵と公開鍵のペアを生成し，自身の Node に保存する．Processor は条件を提示する際に，自身の公開鍵を P2P Node へ送信し，BC 上で公開する．User は条件に同意する際に，自身の公開鍵を P2P Node に送信し，BC 上に書き込む．このとき，User は自身の公開鍵を Processor の公開鍵を用いて，暗号化して書き込むことも可能である．これによって，User は契約を行う Processor のみに自身の公開鍵を渡すことができる．

User が位置情報を Processor に送信する際には，User が Processor に送信する位置情報のハッシュ値と自身の秘密鍵でデジタル署名を生成する．次に，Processor の公開鍵を用いて送信する位置情報の暗号化を行い，Processor へ送信する．暗号化された位置情報を受け取った Processor は，まず自身の秘密鍵を用いて，暗号化された位置情報を復号することによって，User の位置情報を得る．さらに，Processor は User の公開鍵を用いて，デジタル署名を検証することができる．このように，暗号化とデジタル署名を併用することで，第三者に位置情報を公開することなく，User は Processor に位置情報を送信することが可能である．

4. ブロックチェーンのデータ量の評価

提案したシステムにおいて，User と Processor の数が時間経過とともに増加した場合の 1 日当たりのデータ量の推移を特定の条件の下で推定した．この結果を図 2 に示す．ここで，関数 F(t)は同意，条件，位置情報のすべてを BC に書き込んだ場合のデータ量であり，G(t)は同意，条件のみを BC に書き込んだ場合のデータ量である．図 2 が示すように，本研究で提案したシステムは位置情報を BC に書き込まず，User から Processor へ直接送信することで，BC サイズの増大やスケーラビリティ問題を抑えることができ，長期的なシステムの運用が可能である．

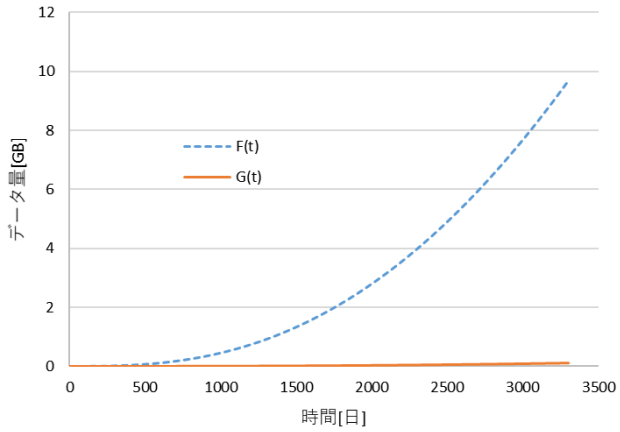

図 2　1 日当たりのデータ量の推移

5. まとめ

本報告では，BC を用いて条件提示と同意を行い，またこの条件と同意に基づいて，位置情報を暗号化して提供するシステムの提案を行った．しかし，今回提案した手法は User が Processor の提示した条件に対して同意するか否かしか考慮していない．さらにプライバシーを考慮したシステムにするためには，Processor が提示した条件に対して User 各自がエリアや時間に関する条件を加えた上で同意できるような仕組みを構築する必要がある．

参考文献

[1] Bulat Nasrulin, et al. “CHAINMOB: Mobility Analytics on Blockchain”, DOI 10.1109/MDM.2018.00056
[2] Md Mehedi Hassan Onik, et al. “Privacy-aware blockchain for personal data sharing and tracking”, DOI 10.1515/comp-2019-0005
[3] EUGDPR-Information Portal,https://eugdpr.org/, Accessed: 6-Jan-2021