分散台帳を用いたソーシャルコミュニケーションチャネルの実装に向けて

宝田 一希[1]　新城 靖[1]　周 毅[1]　林 致遠[1]

1. はじめに

テキストチャットやビデオ通話などのコミュニケーションツールが広く普及しており，人々の生活に必要不可欠なものになっている．このようなツールは中央サーバに依存しているよるものが多く，管理者による検閲や過度な規制，および持続可能性に関する問題がある．

ユーザの端末同士が直接通信すれば中央サーバに起因する問題は解消する．しかし，中央サーバなしでコミュニケーションツールを実装する時に，通信相手の発見および認証において様々な問題がある．たとえば VPN (Virtual Private Network) で友人の PC と接続するためには，変化する友人の IP アドレスの取得においてしばしばなんらかの中央サーバを必要とする．

上記の問題を解決するため，本研究では分散台帳技術を用いたコミュニケーションチャネルを実現する．コミュニケーションチャネルとして具体的には，デスクトップ PC 間を接続するための VPN，および携帯端末間を接続する SIP (Session Initiation Protocol) を実現する．これらのコミュニケーションチャネルを用いるツールを使う時には，通信相手の IP アドレスが必要になる．本研究では分散台帳技術を用いることでこれを取得する．この時，通信相手は分散台帳技術により認証される．

2. ソーシャル VPN

ソーシャル VPN とは，インターネット越しの友人の PC との間で安全な通信路を提供する VPN である．これにより，友人との交流を既存の LAN 用アプリケーションを用いて容易かつ安全に行うことが可能になる．

ソーシャル VPN では接続確立時に変化する友人の IP アドレスの取得する必要がある．本研究では，分散台帳技術の 1 つである Ethereum を用いてこの問題を解決する [1]. Ethereum はスマートコントラクトと呼ばれる分散台帳上で動作するプログラム実行機能と，ウォレット機能を有する．本研究で実装するソーシャル VPN では，2 人のユーザが交流を開始する時，ウォレットアドレスと VPN 接続の認証に使う公開鍵を交換する．各ユーザの PC ではデータベースを持ち，これらの情報を友人の名前で取り出せるようにする．

本研究では，友人の IP アドレスを取得するためにスマートコントラクトを用いる．このスマートコントラクトは，**表 1** に示した関数を持つ．各ユーザの PC では自分自身の IP アドレスを調べ，それが変化すると関数 putIPv4() または putIPv6() を呼び出して公開する．これらの関数は，トランザクションを実行し，呼び出したユーザのウォレットアドレスをキーとして IP アドレスをスマートコントラクトのストレージに保存する．getIPv4() および getIPv6() は，スマートコントラクトのストレージに保存された IP アドレスを取得する関数である．これらの関数は，ブロックチェーン内に保存されたデータを参照するだけなので，トランザクションは行われない．よって，トランザクションの費用はかからず，また，ブロックチェーンを更新する間隔（Ethereum では約 16 秒）を待たずに完了する．

本研究では，strongSwan を用いてソーシャル VPN を実装している．本研究では strongSwanVPN を制御するプログラムであるコントローラを実装した．ユーザはこのコントローラを利用して，容易に VPN の接続，切断，コンタクトリスト管理などを行うことができる．たとえば友人の PC に VPN の接続を行う際，友人の名前を指定してコントローラのコマンドを実行する．このとき，コントローラは以下の処理を行う．

(1) データベースから友人の名前でウォレットアドレスと公開鍵を取得する．
(2) (1) で得られたウォレットアドレスを指定して，スマートコントラクトの getIPv4() または getIPv6() 関数を呼び出して IP アドレスを取得する．
(3) (2) 得られた IP アドレスと (1) で得られた友人の公開鍵を指定して strongSwan に接続を指示する．

strongSwan は指示を受け付けると，受け取った IP アドレ

表 1　IP アドレスの交換に用いるコントラクト関数

関数名	説明
putIPv4(v4) putIPv6(v6)	自分の IPv4 または v6 アドレスを公開する．
getIPv4(w) getIPv6(w)	ウォレットアドレス w を持つ 友人の IP アドレスを返す．

[1] 筑波大学

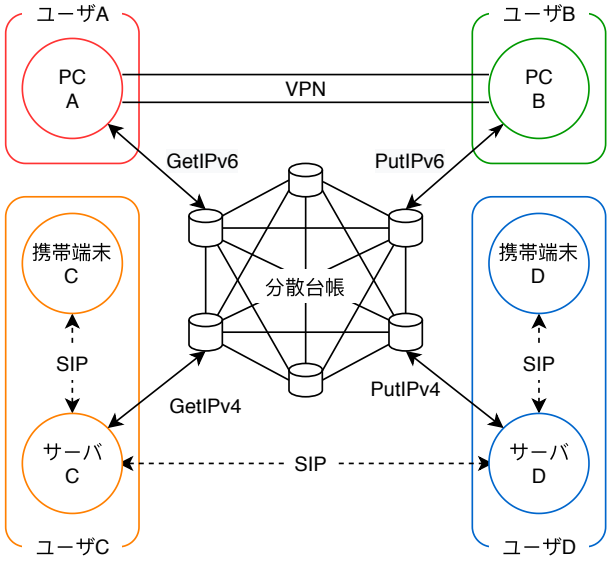

図 1 分散台帳技術を用いたソーシャル VPN とソーシャル SIP

スと公開鍵を使って友人の PC で動作している strongSwan に接続要求を送る．接続要求を受けた strongSwan は，接続相手を保存してある公開鍵のリストにより認証する．

本研究では，ユーザ名に基づくドメインを名前解決できる DNS サーバを各 PC で実行する．この DNS サーバは友人の名前を含むドメイン名（たとえば alice.socialvpn）の解決が要求されると，ドメイン名からユーザ名を抽出し，データベースからユーザ名に対応するウォレットアドレスを取得する．そして，ウォレットアドレスをもとに VPN セッションを特定し，接続先の IP アドレスを取得する．最後に，取得した IP アドレスを名前解決の結果として返す．

実験により，コントローラに友人の名前を与えてから VPN 接続が完了するまでの時間を測定した．その結果，論文 [1] の環境では，1 秒程度で VPN 接続の確立が完了することを確認した．

3. 携帯端末のためのソーシャル SIP

ソーシャル VPN では，PC で VPN サーバや DNS サーバを立ち上げておく必要がある．したがって，サーバ機能を有することが難しい携帯端末では利用が困難である．携帯端末では，コミュニケーションツールとしては，音声通話やビデオ通話に対する要求が高い．これらのツールでは，SIP を利用するものが多い．そこで本研究では，携帯端末における友人間のコミュニケーションチャネルを実装するために，SIP をサポートすることにした．この機能を本研究では，**ソーシャル SIP** と呼ぶことにする．

本研究で実装するソーシャル SIP では図 1 に示すように，各ユーザは自分の携帯端末で SIP のツールを実行し，自宅の SIP サーバと接続する．そして，SIP サーバ同士を分散台帳技術を用いて相互に接続する．

本研究では，SIP サーバである Asterisk を拡張し，ソーシャル SIP の実装する．拡張した Asterisk では以下のユーザ情報を管理する．

- Ethereum のウォレットアドレス．友人の Asterisk サーバの IP アドレスを取得するために利用する．
- 自分の携帯端末がログインするためのユーザ名とパスワード．
- 自分および友人の内線番号．ランダムに生成する．

交流したいユーザは友人と，ウォレットアドレスと内線番号を交換し，自分のサーバに登録する．各ユーザは携帯端末で SIP のツール，たとえば，Zoiper を実行し，それぞれ自身のログイン用のユーザ名とパスワードを使って，それぞれの自宅の SIP サーバにログインする．携帯端末の SIP ツールで通信を行いたい場合，友人の内線番号を指定して，発信の操作を行う．すると，以下のように SIP の通信を行えるようになる．

(1) 発信側の SIP サーバは，内線番号から友人の内線番号とウォレットアドレスを取り出す．
(2) 発信側の SIP サーバは友人のウォレットアドレスを用いて，2 章で述べたソーシャル VPN と同様に，友人の SIP サーバの IP アドレスを得る．
(3) 発信側の SIP サーバは，友人の SIP サーバの IP アドレスと内線番号を用いて着信側の SIP サーバに接続要求を送る．
(4) 着信側の SIP サーバは，接続要求を受け付け，携帯端末を呼び出す．

4. 関連研究

Klukovicr ら [2] は，携帯端末の利用も考慮したプライバシーを保護する分散型 SNS を提案している．この研究では外部のクラウドストレージサービスを必要としているが，本研究では必要としない．

5. おわりに

本研究では分散台帳技術に基づくソーシャル VPN，およびソーシャル SIP を実装している．現在，ソーシャル VPN は動作しており，ソーシャル SIP の実装を行っている．今後はこれらに留まらず XMPP (eXtensible Messaging and Presence Protocol) などに対して拡張を行う予定である．

参考文献

[1] Zhou, Y., Shinjo, Y., Takarada, K. and Lin, Z.: Towards Exchanging Connection Information by Using the Blockchain Technology for Decentralized Social Networking Services, *IPSJ Computer Symposium Poster Session* (2020).
[2] Klukovich, E., Erdin, E. and Gunes, M. H.: POSN: A privacy preserving decentralized social network app for mobile devices, *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 1426–1429 (2016).