ブロックチェーンを用いた不正ログイン対策の検討

藤 竜成[1]　臼崎 翔太郎[1]　油田 健太郎[1,a)]　朴 美娘[2]　白鳥 則郎[3]　岡崎 直宣[1]

概要：リスト攻撃による不正ログインが国内外で頻繁に確認されている．リスト攻撃とは，不正に入手した，あるサービス利用者のログイン ID とパスワードのリストをもとにログイン試行を行う攻撃である．リストは他の会員制サービスから漏洩したログイン ID とパスワードをもとに作成されており，ログイン ID とパスワードを使い回すユーザのアカウントに対しては，少ない試行回数での不正ログインが可能である．リスト攻撃に対して，IP アドレスのブラックリスト化やログイン試行回数による攻撃検知などが対策として取られているが，単一組織で行う対策には限界がある．そのため，複数組織間でリスト攻撃に関する情報（リスト攻撃情報）を迅速に共有し活用するためのシステムが必要である．本研究では，リスト攻撃情報を複数組織間で迅速に共有する，ブロックチェーン技術を応用した不正ログイン対策システムについて検討する．

キーワード：ブロックチェーン，不正ログイン対策

Investigation on Unauthorized Login Countermeasure Using Blockchain Technology

Ryusei Fuji[1]　Shotaro Usuzaki[1]　Kentaro Aburada[1,a)]　Mirang Park[2]　Norio Shiratori[3]
Naonobu Okazaki[1]

Abstract: Unauthorized logins due to list-based attacks have been confirmed frequently. List-based attacks perform the login attempts based on an illegally obtained list containing sets of a login ID and password. The list is created based on the sets of the login ID and password leaked from other membership services, and the unauthorized login with a small number of attempts is possible for the account of the user who recycles their login ID and password. As a countermeasure, a blacklist of IP addresses and an attack detection based on the number of login attempts are usually adopted, however, there is a limit to the measures taken in a single organization. Therefore, we need a system for rapidly sharing and utilizing information on the list-based attacks (list attack information) among multiple organizations. In this study, we investigate an unauthorized login countermeasure system using the blockchain technology which shares list attack information quickly.

Keywords: blockchain, unauthorized login countermeasure

1. はじめに

近年，リスト攻撃と呼ばれる不正アクセスを目的とした攻撃が流行している．リスト攻撃とは，不正アクセスを試みる際にログイン ID とパスワードを総当たりするのではなく，事前に入手しておいたログイン ID とパスワードの組を利用して不正アクセスの試行を実施する攻撃である．そのため，リスト攻撃はログイン ID とパスワードの組を異なる会員制サービス間で使いまわすユーザに対して，非常に有効な攻撃であり，総当たり攻撃や辞書型攻撃と比較し，不正ログインの成功率が高い．一般にリスト攻撃は，ボットを利用して実行される．リスト攻撃の概略図を図 1

[1] 宮崎大学工学部
Department of Computer Science and Systems Engineering, University of Miyazaki
[2] 神奈川工科大学情報学部
Kanagawa Institute of Technology
[3] 中央大学研究開発機構
Research and Development Initiative, Chuo University
[a)] aburada@cs.miyazaki-u.ac.jp

に示す．

リスト攻撃は国内でも頻繁に確認されている．例えば，2019 年 4 月から 5 月にかけて大手オンラインストアに対し，リスト攻撃による不正アクセスが確認されている [1]．不正アクセスが確認されたアカウントは 461,091 件であり，ユーザの氏名や住所，電話番号などの個人情報が閲覧された可能性がある．また，金銭的被害が確認された事例もある [2]．2019 年 5 月から 6 月にかけて，大手サイトにおいてリスト攻撃による不正アクセスが確認されている．この事例では，不正アクセスによる個人情報の閲覧だけでなく，708 アカウントに対し，総額約 2,200 万円の金銭的被害が発生した．2019 年 7 月に発生した不正アクセスの事例においても，リスト攻撃の可能性が高いとされている [3]．以上のように，リスト攻撃は頻繁に確認される攻撃であり，個人情報の流出や金銭的被害が発生しているため，早急な対策が必要である．

リスト攻撃による不正アクセス防止のため，ユーザ側と会員制サービスを提供している企業側の双方での対策が望まれる [4]．ユーザ側における対策として，例えば同じ ID とパスワードの組を複数の会員制サービス間で利用しないことが挙げられる．しかしながら，文献 [5] によると，パスワードを複数の会員制サービス間で利用しているユーザは 8 割以上であるとの報告もあることから，多くのユーザがパスワードを使いまわしているのが現状である．そのため，企業側におけるリスト攻撃に対する十分な対策が望まれる．企業側における対策としては，アカウントのロックアウトや二段階認証，IP アドレスのブラックリスト化などが挙げられる [6]．しかしながら，リスト攻撃は総当たり攻撃や辞書型攻撃と比較し，不正ログインの成功率が高い．文献 [7] における事例では，386 件のアカウントが 1 回のログイン試行で不正アクセスが成功した．そのため，上記対策だけではリスト攻撃に対する対策として不十分であると考えられる．

さらに，最近ではパスワードスプレー攻撃の被害も確認されている [8]．この攻撃は一般的に利用されるパスワードを用いて，同一または複数組織のアカウントに対して不正アクセスを試みる攻撃である [9]．アカウントを切り替えながらアクセス試行を行うため，個々のアカウントあるいは組織から見るとアカウントごとのログイン失敗回数が少なくなり，ロックアウトなどの上記の対策では検知が困難である．

そこで，我々は上記の対策に加えて，複数会員制サービス間でリスト攻撃に関する情報（リスト攻撃情報）を共有すれば，リスト攻撃による不正ログインが防止できるのではないかと考えた．すなわち，ある会員制サービスで検出したリスト攻撃を，リスト攻撃情報として複数会員制サービス間で共有すれば，不正ログインの成功率が高いリスト攻撃による不正アクセスを未然に防ぐことが可能ではないかと考える．

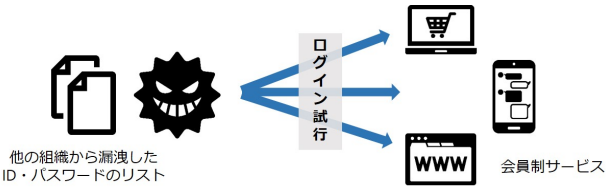

図 1　リスト攻撃の概略図
Fig. 1　Overview of list-based attacks

近年，データ共有の基盤としてブロックチェーン技術が注目されている．ブロックチェーン技術は，ビットコインをはじめとする様々な仮想通貨の根幹技術であり，様々な領域での応用が期待されている [10]．ブロックチェーン技術は，ビットコインを実現するための技術として，2008 年にサトシ・ナカモトによって提案された技術である [11]．この技術により，銀行などの第三者機関の仲介なしで，ユーザ間での迅速で低コストな取引が可能となった．本研究では，データ共有の基盤として，ブロックチェーン技術を利用した．複数会員制サービス間データ共有は，一般的なデータベースを利用しても実現可能である．しかしながら，誰がそのデータベースの管理を主体となって行うのかといった問題や，攻撃者によるデータベースの改ざんといった問題が発生する可能性がある．我々は，ブロックチェーン技術の採用により，上記問題を解決できると考えている．

本研究では，ブロックチェーンを用いたリスト攻撃による不正ログイン対策の検討を行う．本研究で提案するシステムにより，複数会員制サービス間でのリスト攻撃情報の共有が可能となる．そして共有されたリスト攻撃情報を活用することにより，リスト攻撃による不正アクセスを未然に防ぐことができると考える．

2. ブロックチェーン技術

本研究では，リスト攻撃情報の共有基盤としてブロックチェーン技術を採用した．本節では，最初にブロックチェーン技術の概要について説明する．次に，本研究で採用するブロックチェーンの形態について述べる．最後に，本研究で利用するブロックチェーンプラットフォームについて説明する．

2.1 ブロックチェーン技術の概要

ブロックチェーン技術は，2008 年にサトシ・ナカモトによって発表された論文 [11] において，ビットコインを実現するための根幹技術として提案された技術である．サトシ・ナカモトは，ブロックチェーン技術をはじめとする複数の技術を組み合わせることによって，従来，銀行が担っていた通貨発行や取引の仲介などの機能の分散化を実現した．この機能の分散化により，ビットコインは銀行などの第三者機関の仲介なしで，通貨の発行やユーザ間での取引

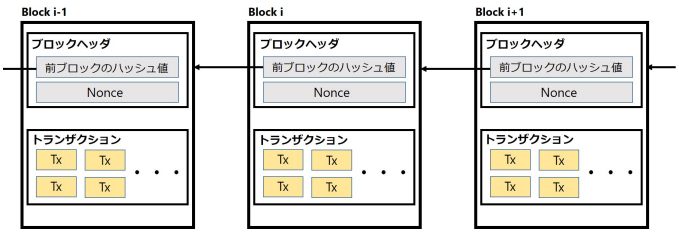

図 2　ブロックチェーンの一例
Fig. 2　Blockchain example

が可能となった．

ブロックチェーンの一例を図 2 に示す．ブロックチェーン上のブロックのヘッダは，前のブロックのハッシュ値を含んでいる．そのため，ブロックチェーンのあるブロックを改ざんしようとすると，それよりも時間的に後に生成された全てのブロックヘッダに含まれるハッシュ値を再計算する必要がある．この再計算は一般に非常に高い計算コストを要するため，ブロックの改ざんは難しい．

ユーザ間で送金を行う際，送金側のユーザは送金量や宛先のアドレス，自分自身のディジタル署名などを含む，価値の移転を記したトランザクションを発行する．発行されたトランザクションは，相互に接続されているノード間で送受信が行われる．トランザクションを受け取ったノードは，トランザクションの検証を行い，そのトランザクションが有効であれば，次のノードに送信する．このトランザクションの送受信により，発行されたトランザクションはブロックチェーンネットワーク全体に伝搬される．最終的には，マイナーによってブロックに含まれ，ブロックチェーンの一部になることにより送金処理が完了する．

ブロックチェーンの完全性を維持するために， Proof of Work (PoW) や Proof of Stake (PoS)，DPoS (Delegated Proof of Stake) などの合意形成アルゴリズムが利用される．ビットコインでは，合意形成アルゴリズムとして，PoW が利用される．PoW は，ブロックハッシュがある特定のハッシュ値を満たすように，Nonce を定め，次のブロックを生成する合意形成アルゴリズムである．PoW によって生成されたブロックは，ノード間のブロックの送受信によりビットコインネットワーク全体に伝搬され，独立に検証される．検証の結果，そのブロックがそれぞれのノードによって有効であると認められれば，ブロックチェーンネットワーク全体で受け入れられ，ブロックチェーンの一部となる．

2.2　ブロックチェーンの利用形態

ブロックチェーンには，Permissionless 型ブロックチェーンと Permissioned 型ブロックチェーンの 2 種類が存在する [12]．Permissionless 型ブロックチェーンは，不特定多数のユーザが参加可能なブロックチェーンであり，パブリックブロックチェーンとも呼ばれる．Permissionless 型ブロックチェーンは，完全に分散化されたブロックチェーンであり，ビットコインや Ethereum といったブロックチェーンが該当する．

Permissioned 型ブロックチェーンは，信頼できる特定多数のユーザや組織が参加可能なブロックチェーンである．Permissionless 型ブロックチェーンは，ブロックチェーンネットワークの管理主体が存在しないが，Permissioned 型ブロックチェーンは管理主体が存在する．管理主体が複数のブロックチェーンはコンソーシアムブロックチェーン，単独のブロックチェーンはプライベートブロックチェーンと呼ばれる．Permissionless 型ブロックチェーンと比較し，Permissioned 型ブロックチェーンは一般にトランザクションスループットが高く，合意形成にかかるコストが小さい [13] [14]．

コンソーシアムブロックチェーンは，複数の組織間におけるデータ共有の基盤として利用可能である．本研究では，データ共有の基盤として，コンソーシアムブロックチェーンを利用した．なぜならば，リスト攻撃情報は不特定多数のユーザに共有する必要はなく，会員制サービスを運営する特定多数の組織間で共有すればよいためである．複数の会員制サービス間でのデータ共有は，一般的なデータベースを利用しても実現可能である．しかしながら，誰がそのデータベースの管理を主体となって行うのかといった問題や，攻撃者によるデータベースの改ざんといった問題が発生する可能性がある．我々は，コンソーシアムブロックチェーンの採用により，上記問題を解決できると考えている．

2.3　ブロックチェーンプラットフォーム

ブロックチェーンプラットフォームには Ethereum[15] や Hyperledger Fabric[16] などの様々なプラットフォームが存在する．Ethereum は，スマートコントラクト利用する，Decentralized applications (Dapps) を構築するためのブロックチェーンプラットフォームであり，オープンソースで開発が進められている．Ethereum は一般にパブリックブロックチェーンに分類される．一方，Linux Foundation によってオープンソースで開発されてる，Hyperledger Fabric はコンソーシアムブロックチェーンに分類される．Hyperledger Fabric はコンソーシアムブロックチェーンを構築されるためのプラットフォームとして広く活用されていることから，本研究でも Hyperledger Fabric を採用する．

3.　提案システム

本節では，提案システムについて述べる．最初に，提案システムのモデルと概要について説明する．次に，各組織がリスト攻撃による不正ログインを防止する際に利用する，攻撃監視用リストについて説明する．その後，提案シ

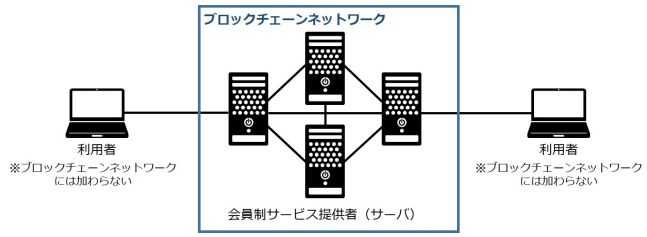

図 3　提案システムのモデル
Fig. 3　Model of the proposed system

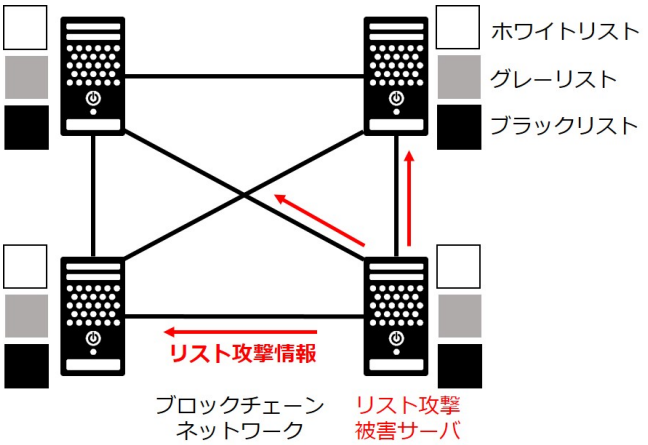

図 4　提案システムの概略図
Fig. 4　Overview of the proposed system

ステムにおける処理の流れについて述べ，ブロックチェーン上で共有するリスト攻撃情報について述べる．最後に，リスト攻撃を検知するためのシステムと，追加認証について説明する．

3.1　提案システムのモデル

提案システムのモデルを図 3 に示す．本研究では，ブロックチェーンネットワークの参加者は会員制サービスを提供する複数の組織とする．すなわち，会員制サービスのユーザはブロックチェーンネットワークには参加しない．これは，ブロックチェーンネットワーク上で共有されるリスト攻撃情報は，不特定多数のユーザに共有する必要はなく，会員制サービスを運営する複数組織間で共有すればよいためである．そのため本研究では，コンソーシアムブロックチェーンを採用する．

また，一般にブロックチェーンにおいては情報の送出元が記録される．そのため，各組織は虚偽のリスト攻撃情報など，不正な情報をブロックチェーンネットワーク上に送出しないとする．

3.2　提案システムの概要

提案システムの概略図を図 4 に示す．ブロックチェーンネットワークは，会員制サービスを提供する複数の組織のサーバによって構成される．各組織のサーバはそれぞれ，攻撃監視用リストを保有している．攻撃監視用リストは，ホワイトリスト，グレーリスト，ブラックリストの 3 種類のリストから構成される．また，リスト攻撃による不正ログインを検知するための，リスト攻撃検知システムを保有していると仮定する．リスト攻撃検知システムについては，3.7 で説明する．

ある組織のサーバがリスト攻撃による不正ログインを検知した際，そのサーバはブロックチェーンネットワーク上にリスト攻撃情報を送出する．ブロックチェーンには，そのリスト攻撃情報が記録される．他の組織のサーバは，共有されたリスト攻撃情報をもとに，攻撃監視用リストを作成する．そのため，既に観測されたリスト攻撃を受けた場合は，共有されたリスト攻撃情報をもとに，その不正ログインを防止することが可能である．

3.3　各組織が保有する攻撃監視用リスト

各組織は，リスト攻撃による不正ログイン防止のため攻撃監視用リストを保有する．攻撃監視用リストは，ホワイトリスト，グレーリスト，ブラックリストの 3 種類のリストから構成される．それぞれのリストは IP アドレスを含むリストである．

ホワイトリストは，ログインを試行するユーザが人間であるとみなすことができる，IP アドレスのリストである．会員制サービスを提供するサーバは，ホワイトリストに含まれる IP アドレスについては，追加認証がないログイン画面をユーザに返す．追加認証については，3.7 で説明する．また，3 種類のリストのいずれにも含まれていない IP アドレスについても，会員制サービスを提供するサーバは，追加認証がないログイン画面をユーザに返す．

グレーリストは，ログインを試行するユーザがボットの疑いがあるとみなされる，IP アドレスのリストである．会員制サービスを提供するサーバは，グレーリストに含まれる IP アドレスについては，追加認証を含むログイン画面をユーザに返す．

ブラックリストは，ログインを試行するユーザがボットとみなされる，IP アドレスのリストである．会員制サービスを提供するサーバは，ブラックリストに含まれる IP アドレスについては，そのサービスへの接続をブロックする．

また，本研究では，上記の 3 つのリストはブロックチェーンネットワークで共有されるリスト攻撃情報を利用して，各組織がそれぞれ独自の基準で作成するものとする．

3.4　リスト攻撃情報

ブロックチェーンネットワーク上に送出されるリスト攻撃情報について説明する．リスト攻撃情報は，2 つの要素から構成される．構成要素は以下の通りである．

- リスト攻撃の疑いのある IP アドレス

- 「悪性」または「良性」投票

リスト攻撃情報は会員制サービスのユーザがリスト攻撃検知システムに検知された時，または追加認証に成功した際にブロックチェーンネットワーク上に送出される．リスト攻撃情報は，ブロックチェーン上で集約されレコードとして表現される．

3.5 レコードの構成

ブロックチェーン上では，集約されたリスト攻撃情報はレコードとして表される．レコードは 3 つの要素から構成される．レコードの構成要素は以下の通りである．

- リスト攻撃の疑いのある IP アドレス
- 「悪性」の投票数
- 「良性」の投票数

以上のレコードをもとに，各組織はそれぞれ攻撃監視用リストを作成する．

3.6 各組織のサーバにおける処理

各組織における会員制サービスを提供するサーバの処理について説明する．各組織のサーバはそれぞれ，攻撃監視用リストを保有している．また，リスト攻撃による不正ログインを検知するための，リスト攻撃検知システムを保有していると仮定する．

サーバの処理は，ユーザのコンピュータからログインページを要求するリクエストを受信した際に開始される．ユーザのコンピュータの IP アドレスをもとに，ホワイトリスト，グレーリスト，ブラックリストにおける処理のいずれかを開始する．

リスト攻撃がブロックチェーンネットワークに参加しているいずれかの組織で検知できた場合，リスト攻撃情報がブロックチェーンに記録される．リスト攻撃情報を利用して，各組織はそれぞれの基準にもとづき攻撃監視用リストを作成する．攻撃監視用リストの作成の基準については，本論文では議論しない．リスト攻撃を実施したコンピュータは，追加認証が要求，もしくはその接続がブロックされる．そのため，リスト攻撃による不正ログインを未然に防ぐことが可能である．

3.6.1 ホワイトリストにおける処理

ホワイトリストにおける処理は，ホワイトリストに含まれている IP アドレスのほか，ホワイトリスト，グレーリスト，ブラックリストのいずれのリストにも含まれていない IP アドレスからのログインページのリクエストを受信した際に開始される．フローチャートを図 5 に示す．

ホワイトリストにおける処理は，人間とみなすことが出来る IP アドレス，もしくは 3 種類のリストのいずれにも含まれていない IP アドレスに対して実施される．これらのユーザのコンピュータから受信したリクエストに対しては，追加認証なしのログインページをレスポンスとして返す．ログイン試行の過程で，各組織のリスト攻撃検知システムに検知された場合は，ユーザがボットの疑いがあると判断しグレーリストに当該 IP アドレスを追加後，グレーリストにおける処理を実施する．

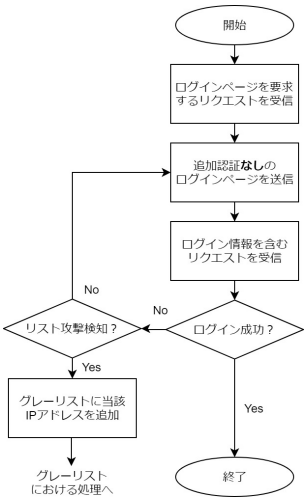

図 5 ホワイトリストにおける処理
Fig. 5 Flowchart for the whitelist

3.6.2 グレーリストにおける処理

グレーリストにおける処理は，グレーリストに含まれる IP アドレスからのログインページのリクエストを受信した際に開始される．フローチャートを図 6 に示す．

グレーリストにおける処理は，ボットの疑いがあるとみなされるユーザに対して実施される．これらのユーザのコンピュータから受信したリクエストに対しては，追加認証ありのログインページをレスポンスとして返す．追加認証は，ログイン試行を行う利用者がボットか人間かを判断するために実施される．そのため，追加認証が成功した場合は，ユーザが人間である可能性が高く，反対に失敗した場合はユーザがボットである可能性が高い．

以上から，追加認証を含むログインに成功した場合はユーザが人間であることを表す「良性」投票をブロックチェーンネットワーク上に送出する．その後，当該 IP アドレスをホワイトリストに追加する．反対に，追加認証もしくはログインを失敗し，リスト攻撃検知システムに検知された場合は，ユーザがボットであることを表す「悪性」投票をブロックチェーンネットワーク上に送出する．その後，当該 IP アドレスをブラックリスト追加し，ブラックリストにおける処理を実施する．これらの投票は，各組織の攻撃監視用リストが作成される際に利用される．

3.6.3 ブラックリストにおける処理

ブラックリストにおける処理は，ブラックリストに含まれる IP アドレスからのログインページのリクエストを受信した際に開始される．ブラックに含まれる IP アドレスについては，ログインを試行するユーザがボットとみなされる．そのため，会員制サービスを提供するサーバは，ブ

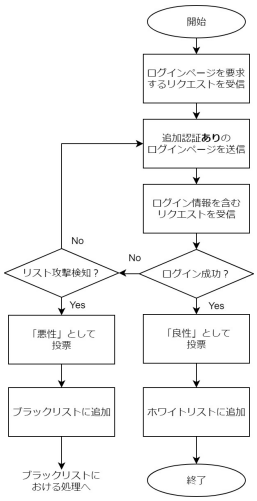

図 6 グレーリストにおける処理
Fig. 6 Flowchart for the grey list

ラックリストに含まれる IP アドレスについては，そのサービスへの接続をブロックする．

3.7 リスト攻撃検知システムと追加認証

本研究では，各組織のサーバはリスト攻撃による不正ログインを検知するための，リスト攻撃検知システムを保有していると仮定している．リスト攻撃の検知方法については，例えばログイン失敗率の監視や入力された ID とパスワードの組と既に知られているリストに含まれる ID とパスワードの組とのマッチングなどが考えられる．また，追加認証については，例えば CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) や二要素認証などが考えられる．

これらリスト攻撃検知システムと追加認証については，本論文では議論しない．

4. 実装

本論文では，ブロックチェーンプラットフォームである Hyperledger Fabric を利用し，IP アドレスの登録とそれに対応する「悪性」投票数と「良性」投票数を取得する，簡易的な動作検証を行った．最初に，動作検証の環境について述べ，次に実際に行った動作検証について説明する．

4.1 環境

Windows 10 が稼働する PC 上に仮想化ソフトウェアを用い，ゲスト OS として Ubuntu Desktop 19.04 が動作する仮想環境を構築した．その際に，ゲスト OS にメモリを 8G，2 つの CPU コアを割り当てた．その後，ゲスト OS 上で Docker version 19.03.1 をインストールし，Docker を利用して Hyperledger Fabric v1.2.0 を動作させた．

4.2 動作検証

本論文では，Go 言語利用してチェインコードを作成した．主に以下の関数を実装し動作検証を実施した．

- getVote

getVote 関数は，IP アドレスを引数として受け取り，それに対応する「悪性」投票数と「良性」投票数をブロックチェーン上から取得する関数である．

最初に，IP アドレスとそれに対応する「悪性」投票数と「良性」投票数で State DB を初期化した．State DB を IP アドレスを表す文字列「192.168.0.50」と，それに対応する「悪性」投票数と「良性」投票数を表す文字列「0:0」で初期化した．その後，getVote 関数に IP アドレスを表す文字列「192.168.0.50」を渡し，関数を呼び出すと，「悪性」投票数，「良性」投票数を表す文字列「0:0」が得られた．

5. まとめ

本論文では，リスト攻撃による不正ログインの対策の検討を行った．我々は，複数会員制サービス間でリスト攻撃情報を共有すれば，不正ログインの成功率が高いリスト攻撃による不正アクセスを未然に防ぐことが可能ではないかと考え，ブロックチェーン技術を利用したシステムを提案した．また，ブロックチェーンプラットフォームである Hyperledger Fabric を利用し，簡易的な動作検証を行った．今後の課題としては，Hyperledger Fabric を利用した，提案システムの本格的な実装を行い，リスト攻撃のシミュレーションを通じて不正ログインの防止に関する定量的な評価を実施することが挙げられる．その他，ブロックチェーンネットワーク上で共有する情報として，IP アドレス，「悪性」や「良性」投票以外も検討することが挙げられる．

謝辞 本研究は JSPS 科研費 JP17H01736, JP17K00139, JP18K11268 の助成を受けたものです．

参考文献

[1] UNIQLO ユニクロ「「リスト型アカウントハッキング（リスト型攻撃）」による弊社オンラインストアサイトへの不正ログインの発生とパスワード変更のお願いについて」, [online]https://www.uniqlo.com/jp/corp/pressrelease/2019/05/19051409_uniqlo.html（2019 年 8 月 15 日参照）.

[2] 暮らしのマネーサイト「インターネットサービス「暮らしのマネーサイト」での不正ログイン発生のお知らせおよびパスワード変更のお願いについて」, [online]http://www.aeon.co.jp/information/201906_info/index.html（2019 年 8 月 15 日参照）.

[3] 株式会社セブン&アイ・ホールディングス「「7pay（セブンペイ）」 サービス廃止のお知らせとこれまでの経緯、今後の対応に関する説明について」, [online]https://www.7andi.com/library/dbps_data/_template_/_res/news/2019/20190801_01.pdf（2019 年 8 月 15 日参照）.

[4] トレンドマイクロ株式会社「アカウントリスト攻撃」, [online]https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/

threat-solution/access.html（2019 年 8 月 15 日参照）.
[5] トレンドマイクロ株式会社 「パスワードの利用実態調査 2017 ーパスワードを使いまわしている利用者が 8 割以上」 available at: https://www.trendmicro.com/ja_jp/about/press-release/2017/pr-20171005-01.html（2019 年 8 月 15 日参照）.
[6] 総務省 「リスト型アカウントハッキングによる不正ログインへの対応方策について」 available at: http://www.soumu.go.jp/main_content/000265403.pdf（2019 年 8 月 15 日参照）.
[7] ebookJapan「【重要なお知らせ】不正ログインに関する最終報告」, [online] http://www.ebookjapan.jp/ebj/information/20130405_access.asp（2019 年 8 月 15 日参照）.
[8] ITmedia エンタープライズ「Citrix のネットワークに不正アクセス、国家が絡むサイバースパイか　FBI が捜査」, [online] https://www.itmedia.co.jp/enterprise/articles/1903/12/news064.html（2019 年 8 月 22 日参照）.
[9] 日本マイクロソフト「Azure AD と AD FS のベスト プラクティス: パスワード スプレー攻撃の防御」, [online] https://blogs.technet.microsoft.com/jpazureid/2018/03/19/password-spray/（2019 年 8 月 15 日参照）.
[10] J. Al-Jaroodi and N. Mohamed. "Blockchain in Industries: A Survey." *IEEE Access* 7(2019): 36500-36515.
[11] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
[12] Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." *IEEE 6th International Congress on Big Data* (2017): 557-564.
[13] Xu, Xiwei, et al. "A taxonomy of blockchain-based systems for architecture design." *IEEE International Conference on Software Architecture (ICSA)* (2017): 243-252.
[14] 株式会社三菱総合研究所 「ブロックチェーン技術を活用したシステムの評価軸整備等に係る調査」, [online] https://www.meti.go.jp/english/press/2017/pdf/0329_004b.pdf（2019 年 8 月 15 日参照）.
[15] Ethereum Project available at:https://www.ethereum.org/ (accessed 2019/06/16).
[16] Hyperledger - Open Source Blockchain Technologies available at:https://www.hyperledger.org/ (accessed 2019/06/16).