情報処理学会論文誌 Vol.58 No.12 1954–1963 (Dec. 2017)

順番マルチサインオン方式の提案

岡本 学[1,a)]

受付日 2017年3月6日, 採録日 2017年9月5日

概要：個人情報や金銭を取り扱う Web サイトが増加しており，より安全にユーザ認証を行う強いセキュリティが必要となってきている．強いセキュリティを実現するには，単一の認証方式だけではなく，複数の認証方式を利用するマルチサインオンによる解決が有効である．一方で複数の認証方式を 1 つのサービス主体で提供するにはコスト負担がかかる課題があり，サービス主体と認証主体を分散する方式の検討もあわせて行われている．本論文では，ユーザがサービス・プロバイダ（SP）を利用するにあたって複数のアイデンティティ・プロバイダ（IdP）を指定した順番で認証を受けることで強いセキュリティを実現する順番マルチサインオン方式を提案する．この方式ではすべての IdP でなりすましされた場合においても，それら IdP を利用する順番が正しくなければ SP 上で本人と認めないとすることで追加のセキュリティを提供できる．ユーザは自身のライフスタイルにあわせて認証順序を設定すれば普段どおりの生活をするだけでマルチサインオンを受けることが可能である．なお本方式では認証情報交換の方式としてシングルサインオン技術を用いる．

キーワード：多要素認証，マルチサインオン，シングルサインオン，リスクベース認証

Authentication with Plural Servers in the Correct Order

Manabu Okamoto[1,a)]

Received: March 6, 2017, Accepted: September 5, 2017

Abstract: For enhanced security, in addition to passwords, biometric identification, IC cards, and PKI certification can also be utilized. Further, multi-factor authentication, which uses plural certification to facilitate a single login, can also be utilized. In this paper, we propose a new multi-factor authentication system in which, not only is it necessary to receive certifications from plural authentication servers, but it is also necessary for the user to receive each certification in a specific correct order. This order is decided by users beforehand, and single sign-on protocols are used to exchange authentication requests and responses between servers.

Keywords: single sign-on, multi sign-on, multifactor authentication, risk-based authentication

1. まえがき

近年，個人情報や金銭を取り扱う Web サイトが増加しており，より安全に認証を行うための強いセキュリティが必要となってきている．強いセキュリティを実現する方式として多要素認証（マルチサインオン）が提案されている．マルチサインオンとは単一の認証方式でユーザの本人確認を行うのではなく，複数の認証方式を用いてユーザ認証を行う方式である．たとえば ID・パスワード方式だけで本人確認を行うのではなく，これに加えて生体認証や所有物認証をさらに行い，すべてを突破できて初めてユーザ本人と認める方式である．しかし単一のサービス主体（サービスを提供する企業・団体・組織・サイト等）が複数の認証方式の提供を行う場合，コスト負担は単純に方式数分が積算される．たとえばネットバンクではワンタイムパスワード方式を採用している例がある [1] が，ワンタイムパスワードを発生させるトークン装置の購入・配布・運用管理はネットバンク自身がすべて請け負う必要がある．資本の乏しいサービス主体ではこれら強いセキュリティを実現すること

[1] 神奈川工科大学情報学部
Kanagawa Institute of Technology, Atsugi, Kanagawa 243–0292, Japan
[a)] manabu@nw.kanagawa-it.ac.jp

は難しい．

そこで分散マルチサインオン方式の提案を行う．分散マルチサインオン方式とはIdPと呼ばれる複数の認証サーバ（Identity Provider）がサービス主体であるSP（Service Provider．以下ではサービス主体をすべてSPと呼ぶ）の代理としてユーザ認証を行い，その結果をSPに通知する．SPは複数のIdPから認証結果の通知を受けることでユーザの本人確認とする．この方式ではSP自体においては認証に関する機能・設備を削減できる．一方で認証結果を通知するIdPを複数のSPで共有することができる点で効率的である．IdPは認証結果の通知という一種のセキュリティ・サービスを提供することでユーザ・アカウントの増加や，ユーザが認証行為のたびにアクセスすることによる広告収入に期待ができる．

これら分散マルチサインオン方式を採用し，複数のIdPで認証を受けさせる方式にすることで安全性は単純に向上するものの，それら各IdPで採用される認証方式の多くがID・パスワード方式になってしまう場合がありうる．生体認証や所有物認証には設備投資が必要な一方で，ID・パスワード方式においてはこれらコストが最小限で済むためである．たとえ複数のIdPを用いるとしてもすべてのIdPがID・パスワード方式を採用した場合，ユーザは複数のパスワードを使い分けるのではなく，パスワードの忘却を恐れ，すべてのIdPで同じパスワードを設定しがちであったりする．その場合マルチサインオンとしてのセキュリティの高さが生かされないという課題が発生する．

そこで本論文での提案方式では，複数のIdPにおいてユーザが事前に指定した順番で認証を受けることで強いセキュリティを実現する順番マルチサインオン方式を提案する．この方式の場合，たとえすべてのIdPでユーザが同じパスワードを設定し，しかも攻撃者にそれが漏えいした場合でも，登録したIdP認証順序を知られることがなければなりすましを難しくできる点においてさらなるセキュリティ強度を提供する．

2. シングルサインオン技術を用いた代理認証マルチサインオン方式

ここでいう「強いセキュリティ」とはより確実に本人確認を行うことでなりすましの可能性を低くすることを指すこととする．「強いセキュリティ」を実現する方法の1つとして多要素認証（マルチサインオン）があげられる．マルチサインオンとは複数の認証方式を組み合わせて利用する方式である．マルチサインオンには下記のような特徴・課題があげられる．

- マルチサインオンとして複数の認証方式を組み合わせることで「強いセキュリティ」を実現できる．実際NIST SP 800-63-3においては認証レベルを上げるためには異なる複数の認証要素を必要とする形をとっている [2]．ただし複数の認証方式を用いる場合は当然ながらユーザの作業負担は増える．たとえばID・パスワードを入力したうえで指紋認証を受ける必要があればそれだけ認証完了までの作業手順としての手間が増える．
- 複数の認証方式に答える必要があるユーザはそれら各方式に対応した記憶・生体情報・所有物を利用時にすべて保持している必要がある．
- さらにマルチサインオンを採用するSPが複数あり，これらをユーザが並行で利用する場合，当然ながらユーザはすべてのSPが提供する認証方式に利用する記憶・生体情報・所有物をすべて所持している必要がある．たとえば同じワンタイムパスワード方式とはいえ，AなるSPが提供するワンタイムパスワードと，BなるSPが提供するワンタイムパスワードとは異なるため，ユーザはその両方に対応するワンタイムパスワード発行装置あるいはソフトウェアを所持する必要がある．
- マルチサインオンを採用してユーザを認証するSP側においてもコスト負担がかかる．たとえば採用する追加認証方式としてワンタイムパスワード方式を想定すると，対応するシステムの開発に加えて別途ワンタイムパスワード発行装置またはソフトウェアをユーザに提供する必要があり，これらを開発・配布・保守運用するための膨大なコストがかかる．採用する認証手段が増えれば増えるほどこれらコストは積算される．

特に最後の項目については，小規模で資金力のないSPでは「強いセキュリティ」が実現できないことにつながり，サービス参入が難しくなりサービス活性化への障害となる．これは「強いセキュリティ」に必要な認証手段に関するすべての費用をSP単体で負担する必要があるためである．

そこでまず，シングルサインオンの代理認証の仕組みを用いた分散マルチサインオン方式について提案を行う．代理認証ではSP自身が認証手段を提供するのではなく，IdP（Identity Provider）と呼ばれる認証サーバに認証を依頼し，その認証結果を利用する方式である．代理認証を用いることで，マルチサインオンを実施する場合でもSP側の開発・運用負担は少なく，複数のIdPの認証結果を採用するだけで済む．

その前にそもそもシングルサインオンとは，ユーザが複数のWebサイトを利用する際に，それぞれのサイトで個別に認証を受ける必要がなく，1度どこかで認証を受けることで複数のWebサイトの利用を可能にする技術である．多くの企業や大学でシングルサインオン方式の提案・研究・商品化・実用化が行われている [3], [4], [5], [6], [7]．

シングルサインオン方式では，認証サーバと呼ばれるIdP（Identity Provider）で1度認証を受けることで複数のSP（Service Provider）をその認証セッションが有効な限

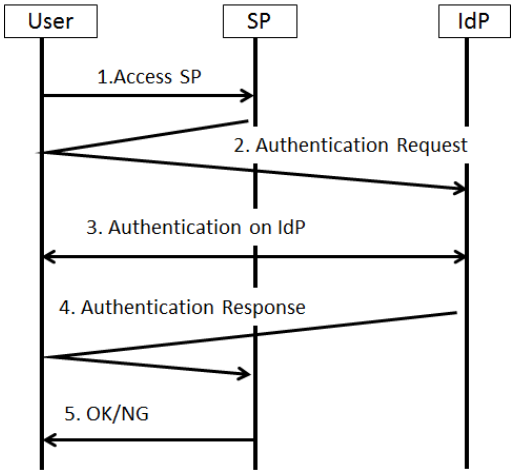

図 1 シングルサインオン基本シーケンス
Fig. 1 Sequence of single sign-on.

り利用できるようになる．ユーザにとっては複数の Web サイト（SP）を利用する場合でも IdP 上の認証情報を管理しておけばよい．具体的にいえば，認証手段が ID・パスワード方式であれば IdP 上の ID・パスワードだけ覚えておけば複数の SP にログインすることが可能になる．さらに SP 側においてはシングルサインオンを導入することでユーザ認証関連の運用管理の負荷を減らすことができる．

シングルサインオン方式はすでに標準化されており，主な標準規格に OpenID [8] や SAML [9] がある．基本的には両方式とも，認証サーバである IdP が SP の代理としてユーザの認証を行い，IdP から SP へ認証結果を通知する方式をとる．そのうち OpenID は，OpenID Foundation により普及・推進が行われているシングルサインオン方式の 1 つである．2005 年に OpenID1.0 が公開され 2007 年には OpenID2.0 を発表，2014 年に OpenID Connect が公開され現在 Yahoo!ID 連携 [10] 等で利用されている．

以下に一般的なシングルサインオンの基本シーケンスの概要を示し，対応するシーケンス図を**図 1** として示す．標準仕様の OpenID においても SAML においてもシングルサインオン・シーケンスの基本構成はほぼ同等であるためその共通の認証部分をここに示すものとする．

(1) サービスの利用者である User は自身が利用を望む Service Provider（SP）にアクセスを行う．そこで SP において認証を受ける代わりにシングルサインオンを利用するための動作を行う．たとえば「シングルサインオン・ボタンを押す」等がこれにあたる．
(2) SP は User を Identity Provider（IdP）へリダイレクトさせ，User の認証を IdP に対し要求する（Authentication Request）．
(3) User は IdP が設定した認証手段に従って認証を行う．ID・パスワード方式であるなら，User は IdP 上での ID・パスワードを入力して IdP の認証を受ける．
(4) 認証が成功した場合，IdP は User を SP へとリダイレクトさせる．あわせて認証結果を SP に伝える（Authentication Response）．認証結果はトークンと呼ばれる電子情報やアサーションと呼ばれる XML 情報で通知することが可能である．なお認証結果においては電子署名およびシーケンス番号，タイムスタンプを付与することが可能であり，なりすましやリプレイアタックを防止できる．
(5) SP は認証結果を評価し認証を完了する．認証結果に問題がなければ SP は User の利用を許可する．

図 2 シングルサインオンメニュー
Fig. 2 Menu of single sign-on.

OpenID に限らずシングルサインオン方式は実際に商用サービスで利用されている．図書館検索サイト「カーリル」（https://calil.jp/）[11] ではシングルサインオン方式によるログインを可能としている．実際のシングルサインオン用のボタン配置を**図 2** に示す．この図 2 において「Twitter でログイン」ボタンを押せば，この「カーリル」サイトでアカウントを所持していなくても SNS サービスである Twitter でユーザ認証を受けることですぐにサービスを開始することができる．SP が「カーリル」サイトであり，Twitter が IdP である．

このような実例にみられるように，SP はユーザ認証を IdP に任せることができ，サービスそのものに業務を集中できる点に利点がある．加えて小規模な SP では多数のユーザを自前で集客することは難しいが，多数のユーザをかかえる SNS 等の巨大サイトからユーザを勧誘できる点も利点である．一方で IdP では SP を自身のアカウントから利用できるサービスの 1 つとして提供でき，SP を利用する際には必ず IdP にログインする必要があるためユーザのアクセスを集めやすくなり，アクセス数に応じた広告収入に期待ができる．よって IdP・SP とも相互利益を得ることができるためこのように現実に利用されている．

このシングルサインオンの仕組みをマルチサインオンに利用することは簡単である．これを分散マルチサインオン方式と呼ぶことにする．方式としてはシングルサインオンの認証方式をそのまま利用するが，SP は 1 つの IdP の認証結果のみでユーザにサービスを許可せず，複数の IdP の

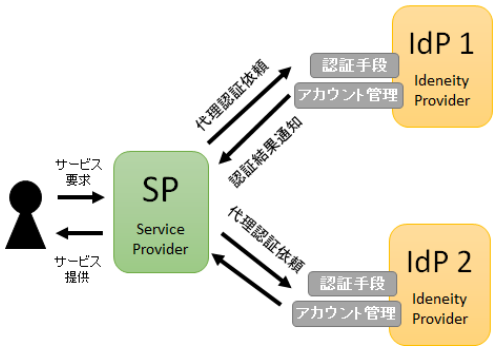

図 3 分散マルチサインオン方式
Fig. 3 Multi-sign on using single sign-on.

認証結果を受けて初めて SP の利用を許可する方式にすればよい．各 IdP–SP 間の認証情報のやりとりはシングルサインオン方式をそのまま利用できる．**図 3** にイメージ図を示す．シングルサインオンの方式はそのままに，シングルサインオンでは複数 SP の認証に単一の IdP を利用するが，分散マルチサインオンの提案では単一の SP に対し複数の IdP を利用する．

この分散マルチサインオン方式においてはこれまでのマルチサインオン方式で課題であったコスト負担の問題を分散することが可能になる．シングルサインオン同様に SP はユーザ認証に関する機能部分を IdP に委託することができる．よって SP はこれらユーザ認証に関わる費用負担を削減しサービスそのものに資金を集中することが可能になる．一方で IdP においてもシングルサインオン同様に自身が決めた認証手段で認証した結果を SP に通知すればよく，1 つの IdP が複数の認証手段を準備するわけではない．よってシングルサインオンとまったく同様に IdP は通常のサービス形態の一部として対 SP への認証情報の流通を行うビジネスモデルが成り立つ．

ただしこの分散マルチサインオン方式では課題もある．各 IdP では自由に認証方式を選択できるが，当然ながら IdP において ID・パスワード方式以外の認証方式を提供する場合にはその IdP には負担がかかる．結果，どの IdP も認証方式としては設備負担の少ない ID・パスワード方式を採用しがちである．実際に図 2 であげたサービスの例においても，ボタン一覧となっている IdP での認証方式はすべて ID・パスワード方式である．これをこのまま分散マルチサインオン方式に使用した場合，複数の IdP から認証結果通知を受ける必要があるものの，結局その結果はすべての IdP において入力された ID・パスワードが正しかったことにほかならない．

このように複数の IdP を利用した分散マルチサインオン方式が実現され，それらすべての IdP が ID・パスワード方式を採用した場合，ユーザはパスワードの忘却を恐れてすべての IdP において同じパスワードを設定してしまうという問題が発生しやすい．その場合セキュリティ的に問題である．実際，1 つの IdP からパスワードが漏洩した場合，それを利用して他のすべての IdP にログインできてしまえばマルチサインオンといえども簡単に突破され，なりすましで SP にログインすることが可能になる．

そこで本論文では分散マルチサインオン方式にさらにセキュリティを追加する方式の提案として，シングルサインオン技術を用いた代理認証方式による分散マルチサインオン方式ながら，ユーザが事前登録した順番どおりに IdP で認証を受けることで本人確認となる方式の提案を行う．この方式ではたとえすべての IdP で ID・パスワード方式が採用され，さらにユーザがそれらすべての IdP において同じパスワードを設定し，それらが漏洩した場合においても，IdP で認証を受ける順番さえ不明であればなりすましを難しくすることができる分散マルチサインオン方式である．本方式は「強いセキュリティ」を実現するマルチサインオン方式として期待でき，さらにはユーザが普段利用する認証サーバの順番によって本人確認を行う観点から，一種のリスクベース認証としても発展が期待できる．また IdP 認証順序は「普段利用する Web サイトの順番」といったユーザのライフスタイルの認証活用に近く，無理して記憶する情報とは異なる点でより気軽かつ身近に利用できるマルチサインオン方式として期待できる．

3. 提案方式

3.1 提案方式の概要

本章では，シングルサインオン・プロトコルを用いて，複数の IdP において，特定の順序で認証を行うことではじめて SP が利用できるようになる順番マルチサインオン方式を提案する．

前章で述べたとおり，代理認証を用いた分散マルチサインオン方式としては 1 つの SP が複数の IdP に対して代理認証を依頼することでこれを実現することができる．その場合，ユーザは複数の IdP すべてにおいて認証を受けない限り SP を利用することができずセキュリティは高くなる．これに加えて本提案での方式は，事前に登録した「認証の順番」どおりに IdP で認証を受けない限りは SP 上において本人確認を有効としない方式である．

また本方式は代理認証をベースにしたマルチサインオンとして，SP 自体にはユーザ認証そのもののための装置・機能・ソフトウェアを削減できる一方で，各 IdP ではそれぞれ独自の認証方式を提供し，SP およびユーザはこれらを組み合わせてマルチサインオンを行うことが可能である．IdP が ID・パスワード方式以外の認証方式を採用すればセキュリティはさらに高くなることが期待できる．

また本方式では，認証情報の流通にシングルサインオン標準仕様を採用することで，公的に安全性が保障された認証情報流通手段を用いて，互換性の高い接続性を可能とする．ただし本方式ではシングルサインオンのプロトコルを

改変する部分はいっさいなく，あくまで認証情報を流通させる目的のためだけに利用しているにすぎないため，採用する標準方式は OpenID 方式であっても SAML 方式であってもかまわない．

3.2 提案方式の条件

順番マルチサインオン方式においては下記の主体が登場する．

・Service Provider（SP）

ユーザがこれから利用しようとするサービスを提供する Web サイト．以下では SP と呼ぶ．SP は順番マルチサインオンによるユーザ認証を求めている．SP は自身のユーザ認証の手段として，複数の IdP からシングルサインオン方式に基づいて送付される認証情報結果通知を利用する．なおユーザは SP に「認証を受ける IdP の順番」情報を事前に登録しておくものとする．この事前登録情報と実際に認証を受けた順番を比較することによって順番マルチサインオンの最終的な本人確認とする．なお通常のシングルサインオンにおける SP とは，順番情報なる各ユーザが登録する機密情報を管理する点において異なる．

・Identity Provider（IdP）

SP に認証結果を提供する認証サーバであり，以下では IdP と呼ぶ．各 IdP ではそれぞれ IdP ごとの認証ポリシをもっており，その認証方式・セキュリティレベルは各 IdP によって異なってよい．IdP はシングルサインオン方式に基づいて認証結果を SP 側に通知する．IdP はユーザがどの順番で利用しているか，他のどの IdP を利用しているかについての情報については無知である．IdP は SNS サイトのように IdP 独自のサービスをユーザに提供する Web サイトであってかまわない．

・ユーザ

利用者のこと．ユーザは前提として複数の IdP と SP においてアカウントを所持していることを前提とする．なお各 IdP および SP における各ユーザのアカウントは連携・紐付けすることが必要であるが，運用対処に近い処理なため本論文では省略する．たとえば，ユーザはサービスを使い始める当初，SP 上にアカウントを所持していなくても，複数の IdP で認証を受けた後 SP でのサービス利用を許され，それら経由した全 IdP アカウントに連携・紐付けされた新たな SP 上でのユーザ・アカウントが作成され，以後利用できる．なお本提案である順番マルチサインオン方式はこのアカウント作成後にはじめて，ユーザが「強いセキュリティ」として順番マルチサインオン方式を以後追加できる形をとる．以降，IdP の順番を登録でき順番マルチサインオン方式を利用できる．つまりまったくの初回から順番を利用する方式ではないことに留意する．

・Circle of Trust

シングルサインオン標準仕様である OpenID では比較的簡易な随時信頼関係に基づく認証情報のやりとりが可能なことでオープンで動的なシングルサインオン機能が提供できる．その一方で，標準仕様 SAML においては事前に確固たる信頼関係を締結した Circle of Trust なるグループの相手のみと認証情報交換を許可する方式となっている．そこで本方式では SP および IdP との関係において，独立した Circle of Trust を構築していることを前提とする．つまり本方式に参加するすべての IdP と SP において認証情報の流通に関して同意している仮定する．本提案方式はどんな IdP・SP でも自由に随時参加できる方式ではなく，あらかじめ同意した IdP・SP 間でのみ実現できるマルチサインオン方式とする．具体的には，すべての IdP・SP において Circle of Trust に属さないサーバからの認証情報流通については無視するものとする．本方式が独立した Circle of Trust を必要とするのは，本方式の SP は通常のシングルサインオン方式とは異なり SP 自身も順番情報なる認証情報を保持する機関であり，かつ利用される IdP においては随時に利用される対象というよりは，ユーザが順番情報の対象として永続的に利用されるものであり，その実在性・信頼性の確保が必要となるためである．なお本方式ではどの IdP を順番に入れ込むことができるかどうかをユーザに示す必要があるが，その範囲が Circle of Trust となる．

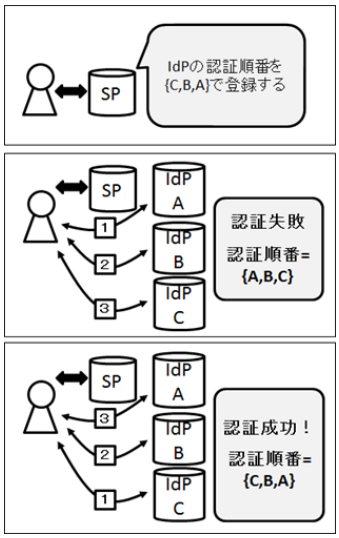

図 4 順番マルチサインオン方式概要
Fig. 4 Abstract of proposed method.

3.3 方式概要

ユーザは順番マルチサインオン方式を追加の「強いセキュリティ」認証方式として以後利用するにあたって，事前に該当の SP に対し認証を受ける IdP の順番を登録する．たとえば，図 4 のように IdP が A，B，C と 3 つある場合，ユーザはその IdP から C，B，A の順番で SP 上に登録を行ったとする．このとき，登録した順番は機密情報であり，ユーザと SP のみしか知ることのできない情報と

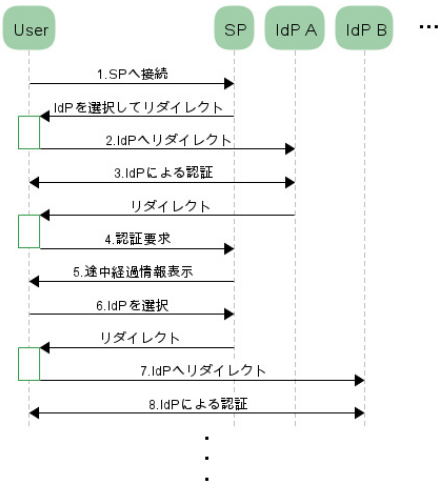

図 5 提案方式シーケンス図
Fig. 5 Sequence of proposed method.

なっている．

実際にユーザが SP で認証を受ける場合には，シングルサインオンでの認証と同様に，SP 上に準備された「IdP で認証」ボタンを押して，IdP にリダイレクトされて IdP で代理認証を受ける必要がある．シングルサインオンにおいても「IdP で認証」ボタンが並んでいたのと同様に，本方式で利用可能なすべての IdP に対応した「IdP で認証」ボタンが並ぶこととなる．

「IdP で認証」ボタンを押した後は，該当の IdP との間でシングルサインオン・プロトコルを用いて代理認証が実施される．ユーザが IdP A の認証ボタンを押せば，ユーザは IdP A にリダイレクトされ，そこで認証を受け，認証が正しく実行されれば IdP A は認証結果を SP に通知する．なおここでの認証依頼および認証結果通知については，IdP と SP の間で標準仕様とまったく変わらないシングルサインオン方式で実施される．

1 つの IdP で認証が完了しても，認証は終了しない．同様に以降ユーザは複数の IdP で認証を受け SP はその認証結果通知を評価しつつ，その IdP の順番を記録していく．ユーザが自分の登録した順番での IdP 認証が終了し，SP がその順番の正当性が評価した時点で初めて SP にログインが可能となる．

図 4 に示したとおり，ユーザは登録した順番である C，B，A の順で IdP で認証を受ければ SP での認証に成功し，一方で異なる A，B，C といった順番で IdP で認証を行った場合，ユーザが登録した順番とは異なるため，認証失敗となる．認証失敗の場合，当然ユーザは SP にログインできない．

図 5 に本方式のシーケンス図を示す．以下に説明を加える．

(1) ユーザが SP にアクセスを行う．ユーザは認証に必要な複数の IdP から認証を受ける必要がある．なおユーザは SP と契約合意した Circle of Trust 内の IdP 一覧を確認することができる．
(2) ユーザが SP 画面に表示されている IdP 一覧の中から IdP を 1 つ選択し，ログインを行う．ユーザが IdP を選びアクセスする際には，それぞれに対応した IdP の認証ボタンを押すことで，対応した IdP にユーザがリダイレクトされる仕組みである．
(3) 各 IdP は，ID・パスワード方式や指紋認証方式等，その IdP が提供する認証方式に従ってユーザ認証を行う．
(4) IdP で認証が完了すると，ユーザが SP へリダイレクトされると同時に認証結果が IdP から SP に通知される．SP は認証結果通知を検証したうえで問題なければその IdP では認証済みと記憶して，認証を受けた IdP 名を順番に記録する．
(5) SP は途中経過情報を表示する．ここでユーザはどの IdP で認証が完了しているかが把握できる．たとえば項目番号 1 での IdP 一覧の中で IdP 認証ボタンであったものが「認証済み」画像に変わる等したものが途中経過情報である．ただしこれら途中経過情報は明示的に示さなくても，秘密にしておいてもかまわない．以降，ユーザは自身が登録した順番どおりに認証行為を続ける．
(6) ユーザは再び SP 画面の IdP 一覧の中から選択を行い認証行為を行う．
(7) 項目番号 (2) と同様に IdP にユーザがリダイレクトされる．
(8) 項目番号 (3) 同様にユーザは IdP で認証を受ける．
(9) 以降同様に，自身が設定した認証順番どおりに認証が完了するまで上記のステップ (2)，(3)，(4)，(5) を繰り返す．
(10) 正しい順番どおりに IdP の認証が完了したとユーザが判断した時点で「SP にログイン」ボタンをユーザが押す．SP は事前登録した IdP の順番と実際に認証を受けた IdP の順番を比較し，同一であれば認証完了となりユーザはサービスを受けることが可能となる．

4. 評価

ここで本提案方式について評価を行う．評価項目としては文献 [6], [12] 等の先行研究同様に「利便性」「安全性」「運用性」について評価を行うが，本論文では安全性については機能的側面として扱い，さらに情報セキュリティの 3 要素「機密性」「完全性」「可用性」に掘り下げて評価を行う．さらに運用的側面として「利便性」をユーザ観点として取り上げ，加えて「運用性」については経済性・効率性を主な対象とし，別に「信頼性」なる項目を設けて運用上のセキュリティ課題をあげることとする．

また比較対象として元となる技術である「シングルサインオン方式」，さらに「集中マルチサインオン方式」「分散マ

表 1 順番マルチサインオン方式評価
Table 1 An evaluation of a proposed method.

	機密性	完全性	可用性	利便性	運用性	信頼性
シングルサインオン方式(代理認証方式)	認証情報流通は標準仕様要件における安全通信路で守る.	認証情報流通は標準仕様要件で完全性を担保. IdP 上でのなりすまし懸念のみ.	IdP に可用性が集中. よって代替の IdP の準備が必要.	複数の SP が個別の認証不要で利用可能でありユーザの利便性に優れる.	開発は標準方式利用で安価. SP における認証関連の運用コストは削減できるが, IdP は安全性確保のための運用コストが必要.	信頼性は IdP に集中するため IdP を集中的に安全に守る必要がある.
集中マルチサインオン方式	SP 自身がすべて自己責任で守る必要がある.	SP 自身がすべて自己責任で守る必要がある.	SP だけで可用性が閉じる	複数回の認証行為が必要で要求セキュリティとのトレードオフ検討が必要.	すべての認証に関わる運用コストを SP 自身が受けもつ必要がある. 認証手段が増えれば増えるほど運用コストは積算される.	信頼性は SP 自身ですべて管理.
分散マルチサインオン方式(代理認証方式)	認証情報流通は標準仕様要件における安全通信路で守る.	認証情報流通は標準仕様要件で完全性を担保. 複数 IdP 上でなりすます必要があるが, 逆に複数 IdP 利用のため認証情報漏洩箇所は増えることになる.	代替 IdP で可用性の保持が可能.	複数回の認証行為が必要. ただし IdP 共有化 = 認証要求物(トークン等)共有化による効率化あり.	開発は標準方式利用で安価. SP における認証関連の運用コストは削減できるが, すべての IdP において安全性確保のための運用コストが必要.	複数 IdP において信頼性保持が必要.
順番マルチサインオン方式(提案方式·代理認証方式)	認証情報流通は標準仕様要件における安全通信路で守る. 加えて順番情報を機密に守る必要がある.	認証情報流通は標準仕様要件で完全性を担保. 複数 IdP 上でなりすます必要があるが, 逆に複数 IdP 利用のため認証情報漏洩箇所は増えることになるが, さらに順番情報でなりすまし防止が可.	代替 IdP で可用性の保持が可能.	複数回かつ順番通りの認証行為が必要. ただし IdP 共有化 = 認証要求物共有化による効率化あり. また IdP の順番登録の手間が必要.	開発は標準方式利用で安価. SP での認証関連の運用コストは削減できるが, すべての IdP において安全性確保のための運用コストが必要. ただし順番情報を信頼性担保に加えることで一部運用コストの分散が可能. なお SP においても順番情報の機密保持のための運用コストが必要.	複数 IdP において信頼性保持が必要だが, 加えて順番情報が信頼性を守る認証情報になりうる.

ルチサインオン方式」をあげ**表 1** において比較する.「集中マルチサインオン方式」とは, 1 つの SP がすべての認証手段を提供するものをそう呼ぶことにする. 現状のネットバンク等のサービスがこれにあたり, 商用環境で ID·パスワード方式に加えてワンタイムパスワード方式を提供している例がこれにあたる. 一方で分散マルチサインオン方式とは 2 章図 3 で提案したもので, ユーザが 1 つの SP を利用するにあたって複数の IdP で代理認証を受ける方式である. なお 4 つの技術のうち「シングルサインオン方式」「分散マルチサインオン方式」「順番マルチサインオン方式(提案方式)」が IdP を用いた「代理認証方式」である.

4.1 機密性

代理認証方式の場合, IdP·SP 間の情報通信の機密性でいえば, 標準のシングルサインオン・プロトコルに従っている. つまりその標準方式が安全であればよいが, 標準シングルサインオン・プロトコルの安全性については公的に安全が保障, あるいは議論されており詳細についてはほかに譲ることとする. なお基本的にどの標準シングルサインオン・プロトコルにおいてもサーバ間の情報交換については SSL 等の安全通信路を利用することで機密性を守る前提であり, 本方式もこれに従うものとする.

ただし提案方式では, 接続する IdP の順番についても機密情報である. だがネットワーク上での監視や, 端末上の監視, 特にブラウザの履歴等によりユーザの接続順を追跡することが可能となってしまう点が本方式の課題である.

4.2 完全性・なりすまし

認証情報の流通に関しては, 利用する標準方式においては OpenID でも SAML でも電子署名情報を付加およびタイムスタンプ・シーケンス番号等のリプレイアタック防止パラメータ付加により完全性を守っており, 本方式もこれに従うこととなる.

このため, なりすましを行うためには代理認証方式においては, IdP 上でなりすましを行う必要がある. 一方で分散マルチサインオン方式および提案方式では複数の IdP に

認証を代理させているので，パスワード等の認証情報の漏洩箇所は増えることとなり，各 IdP 上でのなりすましの可能性は高くなる．さらに，たとえばユーザがすべての IdP で同じパスワードに設定している場合は，代理認証方式のマルチサインオンではセキュリティリスクは高くなる．

しかし提案方式では，もし万が一すべての IdP において認証情報が流出したとしても，それだけではなりすましが不可能な点が特徴となる．つまり，すべての IdP で認証を受けることができても，その認証を受ける順番が正しくない限りは SP を利用することができない．つまり本方式の「順番情報を守る」点が完全性上の最後の砦となりうる．

4.3 可用性

シングルサインオン方式は IdP が停止した場合，SP が利用できなくなる点で可用性に課題がある．このため図 2 に見られるように複数の IdP を利用可能にすることで可用性を高めている．同様に代理認証方式のマルチサインオン方式ではある IdP の認証において同じ認証レベルの別 IdP であればこれを代替できる取り決めをしておくことで，一部の IdP が動作しなくても利用が可能なある程度の可用性を実現できる．提案方式の場合も，順番一致の評価について，複数候補を準備しておき，そのいずれかに相当することで利用を許可する仕組みにしておくことでこの可用性対策に対応できる．

4.4 利便性

シングルサインオン方式では，個別の認証作業は不要ながらも複数の SP を利用できるため，ユーザの利便性は向上する．一方で，いずれのマルチサインオン方式においては当然ながら複数回認証行為を受ける必要があり，サービスを利用するまでの手数がかなりかかる点が課題となる．もっともその分マルチサインオンの安全性を得ることができるため，この点については SP においてどの程度の安全性の担保が必要かとのトレードオフに尽きる．

ただし代理認証を用いたマルチサインオンとしては，たとえばワンタイムパスワード方式を提供する IdP があった場合，これを SP1 からも SP2 からも利用できる．つまり複数のワンタイムパスワード・トークンを所持しなくても 1 つの IdP のものを共有できるため，利便性に優れる．

なお提案方式は「順番登録」の初期設定およびその継続的記憶が必要になる点はユーザ負担として追加となる．

4.5 運用性

本方式は認証情報の流通方式に関しては利用する標準シングルサインオン方式をそのまま踏襲することができる．IdP・SP 間のやりとりについては何の追加・改造も必要なく，完全に標準仕様に従って実施すればよい．よってこの部分の IdP および SP の開発は標準方式の採用だけですむ．なお採用するシングルサインオン方式は OpenID であっても SAML であってもその他方式であってもかまわない．つまり実運用を始めるにあたって，現存するフリー・ソフトウェアやオープン・モジュール等を利用することで安価・簡易に開発を行うことができ，効率性・経済性に優れる．提案方式はこれに加えて SP 上で順番を記録する機能と，順番情報を評価する機能部分だけを追加すればよい．

運用面のコストとしては，シングルサインオン方式，分散マルチサインオン方式および提案方式においては SP は完全に代理認証に依存することで認証情報管理のコスト削減ができる一方で，本提案方式の SP は順番情報なる認証情報と同価値の機密情報保持のための運用コストが必要となる．

また集中マルチサインオン方式においては，すべての認証方式に必要な開発コスト・運用コストはその SP がすべて負担する必要がある．最近では様々な認証方式が標準化されパッケージ化されることで安価に利用できるようになってはいるが，それでも維持管理等のコストが永続的に発生することには変わりがない．

分散マルチサインオン方式および提案方式においては，1 つの IdP から情報漏洩し，さらにユーザが同じ認証情報を他の IdP でも利用している場合は大きなセキュリティ懸念となりうるため，すべての IdP において認証情報を安全に守る運用が必要となり，Circle of Trust 全体での運用コストは高くなる．一方で提案方式ではその場合でもさらに順番情報なる機密情報が認証に必要となるため，運用コストの削減検討が可能である．

4.6 信頼性

シングルサインオン方式の場合はすべての信頼性は IdP に集中する．よって運用コストを IdP に集中させ，安全な IdP とすることでシステム全体の信頼性を向上させることができる．集中マルチサインオン方式ではすべて自身で信頼性を担保する必要がある．

一方で分散マルチサインオン方式および提案方式では信頼性も IdP 数分だけ分散するが，ユーザがすべての IdP で同じパスワードに設定する等の状況がありうるため，単純に IdP の数が増えればセキュリティが高まることにはならない．だが提案方式では，順番情報もまた信頼性を守る一要因となり，つまり順番情報が守られればすべての IdP でなりすましをされても SP は利用できないため，各 IdP での信頼性確保のためのコストを削減できる可能性が生まれる．

5. 考察

5.1 評価に対する考察

評価の章でも述べたとおり，マルチサインオン方式においては認証行為の手間がかかる点と，さらに代理認証方式

においては信頼性を守るためには各 IdP を安全に守る必要があるため全体の運用コストは高くなる傾向にあり，SP が必要とするセキュリティの高さとのトレードオフの関係となる．ただし提案方式に限っていえば，順番情報も認証情報の 1 つとして組み込むことで，順番情報の安全性をどの程度みるかによって全体の安全管理に必要な運用コストの削減の検討ができる点が優位である．つまり「すべての IdP でなりすましされても順番情報で守る」ポリシを選択できる点が異なる．

5.2 セキュリティ課題に対する考察

順番情報は，機密性の部分でも述べたが，ネットワークや端末上の監視により順番情報は洩れる可能性がある．特にショルダーハッキングや動画撮影等でユーザが認証を受ける様子を背後から確認することで，ユーザがどういった順番で IdP の認証を受けているかを把握することは可能である．ただしこの場合順番情報は盗まれてしまうが，その場合当然ながらそれとは別に攻撃者は各 IdP での認証情報すべてを盗む必要がある．

また提案方式では IdP の順番の組合せは全探索には当然ながら弱い．n 個の IdP のうち m 個を利用するマルチサインオンなら当然 ${}_nC_m$ なる組合せの数をすべて試せばよい．3 台の IdP なら 6 通り試せば簡単に正当な順番をみつけることができる．ただし本方式ではこのアタックに対し一定回数以上間違えた場合にロックアウトする機能を付加することである程度は対応できる．

5.3 実現可能性に対する考察

実現可能性上の課題としては，本方式の実現に向けてどれだけの数の IdP を準備できるかという点がある．図 2 のシングルサインオンの実例のように現状では 3 から 5 個程度の IdP が広く利用されているが，順番マルチサインオンとして利用する IdP としては数が多ければ多いほどその順番全数が大きくなるためより安全に利用できることとなる．しかし現状の IdP の数ではそれに乏しい．また現状の IdP は SNS サービスや大手ポータルサイトがほとんどであり，IdP の多様性に欠ける点も課題である．

加えて提案方式ではユーザが IdP の順番を登録する手間が必要である点も比較評価の対照になる．ただしこの順番登録については SP が自動学習することも検討可能である．つまり初期の利用段階では順番に関係なく自由に規定台数以上の IdP を使わせるだけとし，利用が進んだ段階から記録した最も利用頻度の高い順番情報に対し「以後この順番でしか許容しない」なるメニューを SP 側が提供することで，これを記録し本方式へと誘導することが可能である．あるいはリスクベース認証的に本方式を用いて，ユーザのライフスタイルとして普段利用している認証サーバの順番といま利用している順番とが異なることを用いてリスクと判断し，ユーザにさらなる認証を要求するといった利用方法も検討できる．

なお提案方式の基本的な考え方はあくまで追加セキュリティの位置づけである．各 IdP での認証の安全性が基本でまずあり，加えてそれら IdP を複数用いるマルチサインオンによりそれら安全性をさらに高め，加えて本方式で念押し確認をする，といった位置づけである．順番が判明しただけでは SP 上でのなりすましはできず，利用する全 IdP 上での認証情報とその利用順番情報，これらすべてが判明したときに初めて SP 上でのなりすましが可能となることで，なりすましの難易度を上げる提案である．

そこでこの点を逆に利用して，本方式で利用する IdP はシングルサインオンで利用する IdP と比較してそのセキュリティレベルは低くてかまわないポリシでも運用できる点に特徴をもつ．シングルサインオンの IdP ではそれがなりすましされた場合，その配下となる SP すべてにおいてもなりすましで利用できる．このため図 2 に見られる IdP では強いセキュリティを求めていて，電話番号の確認等，強力な本人確認を行うことでこれを担保している．しかし代理認証方式を用いるマルチサインオン方式においては，1 つの IdP で認証が完了しても SP としてはそれでサービスを許可しない．このため 1 つの IdP での認証における責任分担を低くすることができる．1 つのセキュリティの厳しい IdP を突破した場合と，セキュリティはさほど厳しくない IdP を 10 個突破した場合，どちらが安全かというのは数値的に評価・比較が難しく様々な観点によるトレードオフとなる．

ただ非常にセキュリティの低い IdP であっても本方式における順番の中に含めることで，全体としてはある程度のセキュリティ強度を維持することができる．たとえば IdP と名付けはするがなんら個人を特定する認証情報通知は提供せず，ただクッキー等を確認することで「このユーザは確かに私のサイトを訪問した」的な認証結果を提供する簡易 IdP であってもよい．具体的にはユーザはある IdP 相当の Web サイトを訪問する．この Web サイトではユーザ管理のいっさいを行っておらず，よって ID・パスワードを入力させるようなこともない．たとえばニュース情報サイト等がこれにあげられる．この Web サイトではユーザが訪問した記録としてブラウザのクッキーに証拠を残しておく．次にユーザは順番マルチサインオン方式で SP のログインを行う際に，順番の一部としてこの Web サイトを IdP として認証依頼をかける．この簡易 IdP はユーザがリダイレクトされるとブラウザのクッキーを確認しクッキーが存在しさえすれば認証結果通知を SP に通知する．この認証結果通知については当然ながらユーザ ID に関するなんら情報は含まず，その Web サイトで統一に付与した固定の ID 等を通知するだけにすぎない．つまりこの IdP は訪問確認の証拠として認証結果通知を発行する．そして SP は

あくまで順番情報の1つとしてこれを評価し利用する．他のIdPにおいてユーザを特定できる認証情報を含んだ認証結果通知をもらえればユーザ認証については問題なく実施でき，かつ順番情報の1つとしてその簡易IdPを利用できる．簡易IdPはシングルサインオン・プロトコルの実装は必要なものの，いっさいのユーザ管理機能を有することなくこれらマルチサインオン・グループに参入できる．つまり簡易なIdPの立ち上げが期待でき，IdPの数の取り揃えや多様性に期待ができる．

5.4 今後の課題に対する考察

今後の課題の1つとして，IdPの数を大きく増やした場合，ユーザの手間・負担の評価・検証が必要となる．加えて順番情報の忘却がどの程度の期間で発生するか等の評価が必要となってくる．

またあわせてマルチサインオン方式をスムーズに利用してもらうための分かりやすいユーザ・インタフェースの研究も必要となる．マルチサインオン方式ではただでさえユーザ手順が多くなり，どこまで認証が完了していてこの先何が必要なのかの案内がないとユーザが困惑することとなる．また特に本方式では順番登録といった手順も必要となる．これらを分かりやすくガイドしていく画面構成や手順の整理についても重要な課題となる．

さらにライフスタイルに合わせたリスクベース認証としての利用方法についてもより深い検討・提案が可能である．普段ユーザが利用するWebサイトは，そのユーザのライフスタイルとして毎回同じ順番で利用しているケースは少なくない．たとえば朝起きてPCを立ち上げ，Twitterを確認してからFacebookを確認，その後ニュースサイトに移り，といった順序であり，これが毎朝同じ動作である人も少なからずいる．よってこの順番を順番マルチサインオンに利用することで，一種の「ライフスタイル認証」になりうる点に今後期待できる．

6. むすび

本論文では，シングルサインオン・プロトコルを利用した代理認証を利用したマルチサインオン方式の新たな提案として，ユーザが複数のIdPにおいて登録した順番どおりのIdPで認証を受けることでSPでの認証を可能にする順番マルチサインオン方式を提案した．

順番マルチサインオン方式を実現することで，SPは自身のサービスに見合ったセキュリティを実現すべく必要なIdPを複数組み合わせて利用でき，さらに加えてそれらIdPの認証順序が正しくなければ本人と認めない方式をとることにより，単純なマルチサインオンに比べてよりなりすましが難しいセキュリティの高い方式として実現させることができる．この方式ではたとえすべてのIdPがID・パスワード方式で，さらにユーザがそれらすべてのIdPにおいて同じパスワードを設定し，それが漏洩した場合においても，IdPで認証を受ける順番さえ不明であればなりすましを防ぐことができるセキュリティの高いマルチサインオン方式である．

ユーザが普段利用する認証サーバの順番といった「意識的に覚えなくてもよい」知識認証として，「ライフログ」的な認証ともいえ，加えてリスクベース認証的な発展利用も期待できる．

参考文献

[1] みずほ銀行：みずほ銀行ワンタイムパスワード，入手先 ⟨https://www.mizuhobank.co.jp/direct/security/⟩（参照 2017-02-23）．

[2] Digital Identity Guidelines, available from ⟨https://pages.nist.gov/800-63-3/⟩ (accessed 2017-02-23).

[3] 江原康生：大阪大学における新全学IT認証基盤システムの構築と運用，電子情報通信学会論文誌D，情報・システム，Vol.J95-D, No.5, pp.1172–1182 (2012).

[4] 内藤久資，梶田将司，小尻智子，平野 靖，間瀬健二：大学における統一認証基盤としてのCASとその拡張，情報処理学会論文誌，Vol.47, No.4, pp.1127–1135 (2006).

[5] 合田憲人，東田 学，坂根栄作，天野浩文，小林克志，棟朝雅晴，江川隆輔，建部修見，鴨志田良和，滝澤真一朗，永井亨，岩下武史，石川 裕：高性能分散計算環境のための認証基盤の設計，情報処理学会論文誌，コンピューティングシステム（ACS），Vol.5, No.5, pp.90–102 (2012).

[6] 大谷 誠，江藤博文，渡辺健次，只木進一，渡辺義明：シングルサインオンに対応したネットワーク利用者認証システムの開発，情報処理学会論文誌，Vol.51, No.3, pp.1031–1039 (2010).

[7] 河野圭太，藤原崇起，稗田 隆：岡山大学事務情報システムにおけるShibbolethとの連携を考慮した多要素認証の導入，情報処理学会研究報告，Vol.2014-IOT-27, No.5 (2014).

[8] OpenID：OpenID仕様書，入手先 ⟨http://openid.net/developers/specs/⟩（参照 2017-02-23）．

[9] SAML：SAML仕様書，入手先 ⟨http://docs.oasis-open.org/security/saml/v2.0/⟩（参照 2017-02-23）．

[10] Yahoo! ID連携，入手先 ⟨https://developer.yahoo.co.jp/yconnect/⟩（参照 2017-02-23）．

[11] 図書館検索サイトカーリル，入手先 ⟨https://calil.jp⟩（参照 2017-02-23）．

[12] 有村汐里，藤田真浩，松野宏昭，可児潤也，司波 章，西垣正勝：i/k-Contact：物理的ソーシャルトラストを利用した適応型2段階認証，情報処理学会論文誌，Vol.57, No.12, pp.2654–2663 (2016).

岡本 学 （正会員）

平成22年早稲田大学大学院国際情報通信研究科博士課程修了．国際情報通信学博士．現在，神奈川工科大学情報学部情報ネットワーク・コミュニケーション学科准教授．