Vol.2016-CDS-16 No.18
2016/6/3

個人端末のコンテキストを使った本人性の検証

大神 渉[1,a)]　五味 秀仁[1,b)]

概要：電子チケットや施設予約など、オンラインでユーザーが登録したサービスを、オフラインの現場において本人であることを確認した上で提供したいというニーズが増えた。従来、ユーザー認証や本人確認を実施しないため、入手した権利を高値で他人に売りつける転売やなりすましが可能である。そのため、サービス提供者は購入者へ直接サービスを提供することが難しい。それに対して、サービス提供者は本人認証や厳密な本人性の検証を導入することで対応している。しかし、認証を施してもオフラインにおける本人と認証結果が必ずしも一致せず、厳密な本人性の検証を行うためにはユーザーとサービス提供者双方の負担が大きいという課題を抱えている。そこで、本稿ではオンラインでユーザーの本人性を検証した結果をオフラインで提示できるシステムを提案する。提案システムは、従来手法と比べて、転売やなりすましに耐性を持ち、ユーザーとサービス提供者の負担を軽減することができる。

キーワード：本人確認, 認証, アクセス制御, セキュリティ, 電子チケット

Identity Verification Using Personal Device's Context Information

Wataru Oogami[1,a)]　Hidehito Gomi[1,b)]

Abstract: It has increased needs that provide a service that the user registered online after verified purchased user identity at electrical ticket or reservation. Conventionally, user can resell and spoofing in order to not perform user authentication or verification identity. However, authentication result and offline identity is not necessarily match. On the other hand, strict identity verification forces the burden on the user to register her own biometrics or sensitive information. We face this problem by verifying user's device and context information at online and offline. Our approach is resistant to resale or spoofing, and our method can reduce the user's and service provider's burden.

Keywords: Identity verification, Authentication, Security, E-ticket

1. はじめに

オンラインシステムを通じて確実な本人性の証明を行った後でサービスを提供したいというニーズが増えた。例えば、電子チケットサービスでは、サービス提供者が当日現場でチケットを提示した人を購入者であることを確認したうえで入場を許可したい。

従来の手法では、持参したチケットを提示できれば、購入者以外であっても入場を許可していた。これは、買い占めなどによる不当な手段で入手したチケットであっても同様である。その結果、手に入れたチケットを高値で他のユーザーに売りつける転売が増え、サービス提供者は真に必要としているユーザーに直接サービスを提供することが難しくなった。この問題に対して、サービス提供者は主に2つの方法で提供する対象を限定する試みを行っている。

1つは、サービス提供者がユーザーをIDとパスワードによって認証した後にチケットを提示させる方法である。この方法では、IDとパスワードによる認証を行うため、なりすましや、転売によって金銭の授受が発生する状況でアカウントを共有するユーザーが使用する場合は、現場に来た人と購入者の同一性を確認することが難しい。もう1つ

[1] ヤフー株式会社 Yahoo! JAPAN 研究所
Yahoo! JAPAN Research, Minato, Tokyo 107 –6211 Japan
[a)] wogami@yahoo-corp.jp
[b)] hgomi@yahoo-corp.jp

は、サービス提供者が厳密な本人性の検証を行うことで本人性を担保する方法である。この方法は、ユーザー・サービス提供者双方に登録時に負担を強いてしまうという問題があった。例えば、入場時の条件として、ユーザーに顔写真を登録して照合を受けることを義務付けるケースでは、事前に正確なデータを登録する必要がある。そのため、ユーザーは光度や表情、向きなど複数の条件を満たす写真を撮影する必要があり、また、SP は送付された写真によって照合できることを確認するため、負担が大きい。

そこで、電子チケットなどのユースケースにおいて、不正行為や結託によって購入者がなりかわるケースを防止すると同時に、ユーザーとサービス提供者双方の登録にかかる負担の軽減を両立することが求められている。

本稿では、このようにオフラインで本人性の検証を行ったあとでサービスを提供するユースケースにおいて、ユーザーとサービス提供者双方の登録の負担を軽減し、適切な対象に限定するための識別手法を提案した。提案手法は、オンラインサービス利用時点と、オフラインの現場で入場できるかを判断する確認者と対面した時点のユーザー情報を、個人端末を経由して照合することでサービス提供者が容易に本人性を検証できるよう実装した。また、具体的な攻撃者モデル及び攻撃手法について考察し、提案手法と従来の本人性の検証方法を比較評価した。提案手法は従来手法に比べて高い攻撃耐性を有し、サービス提供者、ユーザー双方の登録の負担を軽減できることを示した。

2. 購入者と利用者の一致

2.1 本稿の扱う問題

オンラインで登録を受け付けてオフラインで提供を行うサービスにおいて、サービス提供者は適切なユーザーに対してサービスを提供することが難しい。例えば、チケットの購買では、入手したチケットを他のユーザーに高価で売りつける転売行為が問題視されている。転売が成功することで不当な買い占めが横行し、参加欲求の高い利用者のうちサービス提供者から直接購入できない者は、転売者から購入せざるを得ない。したがって、サービス提供者はサービスを真に必要とする利用者に対して販売を行えず、また、転売を利用せざるをえないためユーザーに定価より高い負担をさせてしまう。そのため、転売の抑止はサービスを適切なユーザーへ提供する上で重要な問題である。

サービス提供者は転売行為への対応として、主に 2 つの方法で購入者と利用者を一致させることを試みている。1 つは、ID とパスワードを使った認証を用いる方法 [1] であり、もう 1 つは、生体情報や公的書類などを使った厳密な本人性の検証をする方法 [2] である。前者は、ユーザーを認証することが可能だが、なりすましによってチケットを窃取される危険性や、転売によって金銭を授受することで結託し、積極的にアカウント共有を行うユーザーに対応できない。後者は、ユーザーが運転免許証などで検証できる住所情報や、顔や指紋などの身体的特徴情報を求められ、正確に登録するための負担や、センシティブな情報を入力するため心理的な負荷が大きい。また、人手による登録確認や生体情報を取得するセンサーの用意を行うため、サービス提供者の登録や運用にかかる負担も大きい。そこで、転売によるなりすましや結託がある状況で購入者と利用者の一致を確認し、サービス提供者とユーザー双方の負担を軽減する手法が求められている。

本稿の前提として、リスト型攻撃などユーザーに接触を行わずにアカウント情報を窃取する攻撃は対象としない。転売のモデルにおいて、アカウント情報を盗もうする攻撃者は、例えば高付加価値のチケットを狙うため、無差別なアカウントの乗っ取りを意図した上記の攻撃ではこれらを狙って行うことが難しく、合理性に欠けるためである。

2.2 転売への対策方針

転売問題を解決するために必要な技術要件を述べる。まず、電子チケットをはじめとするサービスは図 1 に示すように、2 つのフェーズで提供される。1 つ目のフェーズは

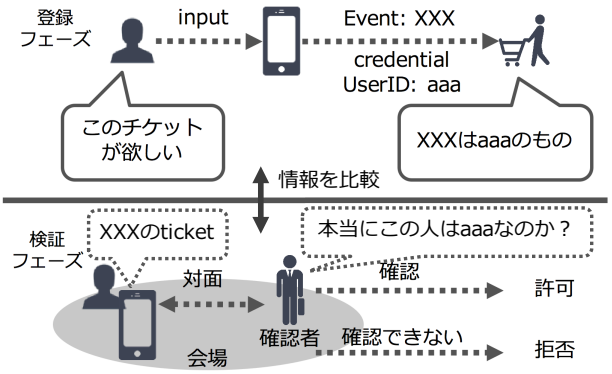

図 1 2 つのフェーズとユーザーの行動

ユーザーがサービス提供者 (Service Provider; SP) のオンラインサービスにアクセスし、オフラインで本人性の検証を必要とするサービスへの登録を行う**登録**フェーズである。もう 1 つのフェーズは、SP がユーザーと対面することで本人性の検証を経てサービスの提供を行う**検証**フェーズである。前提として、ユーザーはスマートフォンなどの個人端末を通じて SP のサーバーに対して登録を行う。

登録フェーズ　ユーザーは SP にユーザー ID (aaa) とパスワード (credential) を使って、ログインを行った上でオフラインで提供を受けたいサービス (XXX) を選択する。この時、転売やなりすましによる不正行為を図 2 に示す。図 2 において、SP はユーザー ID (aaa) を通して各ユーザーを識別しているため、アカウントを共有しているユーザー (BB) やなりすましを行い利用するユーザー（CC）が存在し、適切な対象 (AA) に絞ったサービスが提供できない。

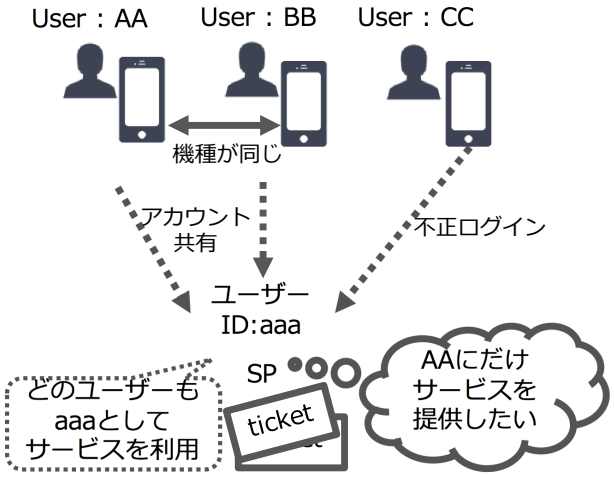

図 2 転売におけるユーザーの利用形態

SP が転売やなりすましを防ぐためには購入者と利用者を一致させる必要があるため、オフラインでユーザー AA と BB、CC を識別して本人性を検証するための情報をこのフェーズで取得する。

検証フェーズ 当日、現場を訪れたユーザーは、確認者と対面する。確認者は、現場でユーザーが購入者であることを確認し、入場の可否を伝える役割を持つ。まず、ユーザーはチケットを表示するためにログイン (ID と credential の入力) を行う。この時、転売者と結託しているユーザーや不正行為によってなりすましているユーザーは認証を成功することができる。そのため、ログインした後、SP が登録フェーズで取得しておいた情報と照合する必要がある。照合の結果は確認者に通知され、入場できるか否かを判断する。検証フェーズでは、登録フェーズで取得しておいた情報との照合及び確認者への伝達が必要である。

SP は 2 つのフェーズを通じて、転売やなりすましといった購入者と利用者が一致しない状況で利用する不正行為を防止することが必要な要件である。

2.3 提案手法

2.2 章の要件を満たすため、デバイス情報とコンテキスト情報を使い、ユーザーを正確に識別する手法と、識別した結果を確認者に伝達する手法を提案する。

2.3.1 デバイス・コンテキスト識別

SP はデバイスに対してユニークな情報を得ることで図 2 の破線矢印を各々識別する。これをデバイス識別と呼ぶ。デバイス識別を行うことで、異なるデバイスを使っているユーザーのなりすましを防ぐことができる。一方、正規のユーザー (AA) となりすましを成功させたいユーザー (BB や CC) が同じ機種を使っていた場合、デバイス識別だけでは対応できない。そこで、SP はユーザーの利用環境であるコンテキスト情報を取得して識別する。これをコンテキスト識別と呼ぶ。デバイス識別と組み合わせることで、SP は同じデバイスを使っていても、使用環境が異なるなりすましや、結託しているユーザーの利用を防ぐことができる。

デバイス識別とコンテキスト識別には、ユーザーによる申告ではなく、SP が収集できる情報を使うことが望ましい。これは、結託やなりすましを行う場合、自己申告する情報であれば共有・窃取しやすいためである。また、登録負担を少なくするため、情報の入力は登録フェーズにおいてユーザーが特別な動作を必要としないことも重要である。

これらを満たす手法として、ログイン情報を用いたデバイス・コンテキスト識別手法を提案する。この手法では、結託やなりすましを防ぎ、ユーザーと SP 双方の負荷を軽減するため、以下の条件を満たす。

- 攻撃者は識別要素を再現することができない
- ユーザーはログイン以外の作業を行わない
- SP は識別要素を精査しなくてよい
- 識別要素は容易に照合できる

なりすましや金銭の授受を通じた結託が行われるケースでは、ID とパスワードを使った認証だけでは攻撃者が識別要素を再現出来てしまう。また、厳密な本人性の検証を行おうとすると、サービス提供者はユーザーにログイン以外の作業を強制し、識別要素を精査しなくては正確な照合ができない。そこで、登録フェーズで予め認証を行ったユーザーのログイン情報を活用することでこれを解決する。具体的には、認証後ユーザー名と適当な nonce をつないだものをハッシュ化した文字列をシードとして、端末固有の情報変換を施すことで 4 つの条件を満たすことができる。

まず、「攻撃者が識別要素を再現することができない」条件は、シードを元にデバイスが固有で持つデバイス情報と、ユーザーの利用環境を表すコンテキスト情報を収集し、一方向関数などで不可逆に変換することで満たす。これにより、なりすましを行う攻撃者はデバイス情報を再現するため、該当するユーザーのシードを把握し、そのシードから該当する端末を入手し無くてはならない。また、結託を行ってシード情報が共有されたとしても、コンテキスト情報が一致しない場合、識別ができる。

次に、「ユーザーはログイン以外の作業を行わない」条件は、ログイン後の作業時に例えば Asynchronous JavaScript + XML (Ajax) や画面遷移時のパラメータとしてバックグラウンドで SP が受け取るようにすることは可能である。最後に、「SP は識別要素を精査しなくてよい」と「識別要素は容易に照合できる」条件については、変換後の情報をハッシュアルゴリズムにより文字列情報として照合すれば条件を満たすことができる。

2.3.2 識別結果の伝達

デバイス情報とコンテキスト情報は、現場で照合を受ける必要がある。後述するリファレンス情報を確認者に提示することで目前の人の本人性の検証を行う手法を提案する。

SP は照合が成功した証拠として、サービスへのリファレ

ンス情報をユーザー端末へ送信する。リファレンス情報とは、登録したサービス (XXX) を指し示す参照情報であり、2 次元バーコードや Near Field Communication (NFC) により確認者が読み取ることのできる情報に変換される。また、リファレンス情報には 20 から 30 秒程度の短い有効期限を設ける。有効期限が切れたリファレンス情報は、取得しなおさなければならず、取得のためには再度デバイス情報とコンテキスト情報の照合を受け無くてはならない。

ユーザーは顔や指紋を預けることなく、リファレンス情報の提示をすることでオンラインで登録を行ったユーザーであることを証明することが可能である。この方法により、ユーザーは確認者への提示直前で照合を受ける必要があるため、目前の人が照合を受けた対象であることがわかる。

3. 実装

図 3 に示すようにして提案手法を実装した。提案システムでは、個人端末が SP の web ページへアクセスし、相互に通信を行うことで正しいユーザーにだけサービスを提供する。図 3 の手順 1-4 を行うことで登録フェーズを、手順 1-6 を行うことで検証フェーズを実現できる。

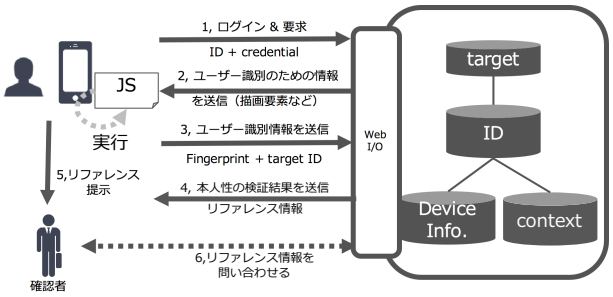

図 3 提案手法によるサービスの提供

3.1 ログイン情報を活用したデバイス・コンテキスト識別

提案手法のデバイス・コンテキスト識別手法の実装として、Web トラッキングに用いられる 2 つの情報を使う。Canvas Fingerprint というデバイス固有の情報と、User Agent (UA) などのユーザーの利用環境を表す情報である。それぞれの情報とその照合について詳しく述べる。

Canvas Fingerprint (CF) は、Keaton らが提案 [3] した。ウェブブラウザに搭載された WebGL を使って HTML5 の描画機能である canvas を使うと、同じ描画要素に対してハードウェア（グラフィックボード）やソフトウェア (OS やその上で動作するブラウザ) の違いにより、差分がでることを使った手法である。JavaScript の API のみを使って実装することができ、画像データではなく、そのハッシュ値として扱われるため、文字列の照合だけで特定の端末を追跡することが可能である。描画及びその送出は Ajax により非同期に実装することが可能で、ユーザーが意識せずにバックグラウンドで取得することもできる。

ユーザーの利用環境を表す情報として、UA など Hyper Text Transfer Protocol (HTTP) のヘッダ情報によってブラウザがリクエストと同時に送信する情報と共に別の情報も用いる。スマートフォンなどの個人端末の普及により、複数のブラウザにおける表示への対応をするため、解像度やタイムゾーン、使用言語などを使うことが SP 側に委ねられるようになった。例えば、JavaScript の Navigator オブジェクトを使うと、この他にもプラグインの種類などユーザー固有の操作環境を取得することができる。本稿では、これらの情報をコンテキスト情報として使用する。

2.3.1 章で述べたように、ユーザー ID と乱数による nonce を記録しておき、それを描画要素として生成したシード情報を使った CF と、Navigator オブジェクトを用いたコンテキスト情報を収集する。これらの情報をすべて収集して保存すると、容量が大きく、個別に照合するための処理時間がかかってしまう。そこで、容易な照合を可能にするためにこれらの情報を文字列として連結し、一方向関数による変換をしたものを単に Fingerprint と呼びデバイス・コンテキスト情報の識別情報として実装を行った。

3.2 データ管理

SP は検証フェーズで確実に照合するための情報を適切に管理しなくてはならない。

表 1 Target テーブル

ターゲット識別子	登録ユーザー ID	実世界条件 1
trgt0001	wogami	Tokyo

Target Target テーブルの例を表 1 に示す。Target テーブルは、対象となるサービスの情報を格納する。ターゲット識別子を指定することで登録ユーザー ID やサービスが提供される会場、時間などの具体情報を複数参照することが可能である。

表 2 ID テーブル

UUID	nonce	Fingerprint	取得時間	ユーザー情報
wogami	tawhrqn	34c6cb8b	1464706800	Minato, Tokyo...

ID ID テーブルの例を表 2 に示す。ID テーブルはユーザーの情報及び識別情報を格納する。後述する動作によってクライアント側で生成された Fingerprint やこれらの情報を登録した時間を格納する。

3.3 登録フェーズ

図 3 の手順 1-4 のフローに従いユーザー識別をするためのデータを取得する。

1. 登録要求 ユーザーはオフラインで受けるサービスを選択するため、SP のサイトへログイン後リクエストを送る。

2. 識別準備　登録要求を受けた SP は、Target 選択画面を表示すると同時に下記識別に必要な情報をクライアント側に送り返す。まず、nonce を作成し、ID テーブルへ保存する。CF のための描画要素として、ユーザー ID と nonce を接続した文字列を SHA-256 でハッシュ化したものをシードとして用いる。シードはユーザー ID の盗み見や総当りによるなりすましを防ぐために必要である。シードと CF 及び Fingerprint 生成用 JavaScript と一緒に送り返す。

3. 識別情報の送信　ユーザーには Target の選択画面が表示される。バックグラウンドでは、手順 2 で SP から送られた情報を用いて、ブラウザが自動的に Fingerprint を算出する。Fingerprint は JavaScript の API を使うことで取得できる。まず、CF はシードを Canvas 機能によって描画し、そのハッシュを取得する。次に、Navigator オブジェクトを使って以下の情報を取得して CF と共に連結した文字列に SHA-256 を施す。要素の選択にあたってはオープンソースで公開されている実装 [4] を参考にした。

- UA
- 言語
- 色の深さ
- 解像度
- セッションストレージの有無
- ローカルストレージの有無
- indexed DB の有無
- open database の種類
- CPU の種類
- プラットフォーム
- doNotTrack の有無
- インストールされているプラグイン名

JavaScript の動作によって、Fingerprint を作成できたら、所定のフォームに埋め込む。この埋め込みが完了するまでフォームの送信ボタンを無効化する。ユーザーが Target を選択し、決定を押下した際にターゲット識別子及び Fingerprint を送信する。

4. 識別情報の登録　サーバーは、手順 3 の情報を受け取り、Target テーブルに登録ユーザー ID として当該ユーザーを保存する。また、Fingerprint は ID テーブルに、登録した時間と共に保存する。両方の情報の保存が成功したら、登録要求を受け付けた旨を送り返す。

3.4　検証フェーズ

検証とは、オフラインでサービスを受ける場所において、登録時の識別情報との同一性を検証する作業である。図 3 の手順 1 において、ログインを行い、Target の選択要求を行う。手順 2 と 3 については 3.3 同様のことを行う。ただし、手順 3 については登録フェーズで登録したものの中から選択する。以降の手順 4-6 について説明する。

4. ユーザー識別情報の照合　Fingerprint がクライアントから送られてくるため、SP は登録フェーズで登録しておいたそれと照合を行う。照合が成功すれば、リファレンスを送信する。リファレンスは、ターゲット ID と作成時間のタイムスタンプ (Unix time) を連結した文字列に AES を用いて暗号化した文字列である。

5. リファレンスの提示　手順 4 によって手に入れたリファレンスは例えば店員や確認者といった現地の確認者に提示する。本実装では提示を正確に早く行うため、二次元バーコードの形式で行う。

6. 検証　確認者は、ユーザーが提示した二次元バーコードを読み取り、SP のサーバーに送付することで、許可してよいかどうかを次に述べる 3 段階で判断することができる。

まず、1 つ目の段階は正しいリファレンスを提示された場合である。リファレンスは前述のとおり、リファレンス提示要求のあった時間のタイムスタンプが埋め込まれた暗号文である。そのため、送付されたサーバーではこのリファレンスを復号することによって照合を受けた時間を検証することができる。有効期限は 20-30 秒の短い時間に設定してあるので、確認者にリファレンスを提示する直前にオンラインで照合を行ったことがわかり、購入者本人であるため入場を許可することができる。

2 つ目の段階は、既に有効期限の切れたリファレンスを提示された場合である。これは、混雑で端末の通信機能が使えないなど、サービスを受ける現場においてコンテキストが再現できない場合や検証フェーズとは異なるコンテキストを持っている場合に該当する。この場合、確認者はその場でもう一度照合を受けてもらうための案内を行い、ユーザーが照合を経て正しいリファレンスを提示できない限り、該当するサービスの理由を拒否することができる。

3 つ目の段階では、リファレンスの提示ができない場合である。この時、確認者はユーザーが購入時と同じ操作環境を持たないことを理由に本人ではないと判断し、サービスの利用を拒否することができる。

4.　攻撃と評価

提案手法を実現したシステムが攻撃に対して耐性を持ちえるか評価を行う。攻撃とは、ユーザー A が登録したサービスに対して、別のユーザー B も対象として許容してしまうことである。転売における攻撃には「なりすまし」と「結託」の 2 つのモデルが考えられる。

4.1　なりすましモデル

B が攻撃者となって A として振る舞うことをなりすましモデルと呼ぶ。このモデルは B が A のユーザー端末を奪う直接接触と、A の端末にマルウェアなどの不正プログラムを駆使する間接接触による攻撃が存在する。

4.1.1　直接接触攻撃

直接接触は、攻撃者 B が A とネットワークを介さずに

直接接触を図ることで A になりすます攻撃である。提案システムにおいて、攻撃者がなりすますためには ID/パスワードの入力と Fingerprint の 2 つを再現する必要がある。直接攻撃者は例えば盗み見により ID/パスワードを、また、端末をそれぞれ窃取することで、攻撃は成立する。しかし、ID/パスワードとユーザー端末の両方を窃取することは難しく、また、端末を使用するための PIN やパターンを提示するロックを突破できない可能性は高い。

B が現場の確認者に許可を得るためには、窃取した端末を使ってネットワークに接続する必要があり、攻撃者の所在や攻撃を A に知らせてしまうため、攻撃者としてのリスクが高い。この時、A が現場に来て B の端末を自分のものであることを証明すれば攻撃を防ぐことができる。

4.1.2 間接接触攻撃

間接接触は、攻撃者 B が A の端末に不正プログラムなど間接的な手段で接触することで A になりすます攻撃である。B が入手したいのは、ID/パスワードと Fingerprint である。例えば、マルウェアが管理者権限を持つ場合、A に同意なくメモリ上に乗ったこれらの情報を取得することは可能であり、送出情報を窃取し、なりすますことができる。

ただし、一部の条件を満たせば、この間接接触攻撃の成功は防ぐことが可能である。その条件とは、対象となるサービス 1 つに対してユニークなターゲット識別子が発行されていることである。例えば、興行の電子チケットでは、1 つの席に対してユニークなターゲット識別子が発行されている。この条件下で間接接触攻撃が成立している状況は A と B 両方ともが正しいリファレンスを提示できることを示し、そこでは衝突が起こる。つまり、ある対象に対して 2 人が正しいリファレンスを持ってきた場合にどちらか一人にだけ許可を出すことができれば良い。ここで、二人が正しいリファレンスを持ってきた場合、意図的にコンテキスト情報を書き換えることで、送出情報の変化を見て、B を拒否することができる。つまり、B は A の正しい ID/パスワード及び登録時の Fingerprint を知り、それらを B の識別情報として偽造して送出することでリファレンスを得ている。確認者と対面した状態で B のコンテキスト情報を書き換えても、その情報を A の (正しい) 送出情報に書き換えてしまい、反映できない。つまり、コンテキストに使う、UA や言語設定などを確認者が指定し、双方がコンテキストを書き換えたあと、Fingerprint に反映出来た方が正しいユーザーである。

4.2 結託モデル

結託とは、本来被害者であるユーザー A が攻撃者となり、金銭のやり取りなど一定の信頼関係を築いたユーザー B のなりすましを共同して成功させようとするモデルである。結託モデルには、例えば友人や家族などの親しい関係者同士での永続的な関係性の中で行われる永続結託攻撃と、金銭などのインセンティブにより一時的に結託する一時結託攻撃が存在する。これらの攻撃モデルに対して、本提案がどのように作用するかを述べる。

4.2.1 永続結託攻撃

永続結託攻撃は、親しい関係者同士の関係にある A と B 同士が積極的に協力することで、A が登録したサービスを B が享受できる。A と B の間には強い信頼関係が存在するため、A は B に対し取りうる限り積極的な協力をする。

A と B は積極的に端末を共有することが可能であり、サービスを受ける際にも衝突が発生しないため、検証による攻撃の検知が難しい。また、本人性の検証を経て正しい許可を受けることができるため攻撃を防ぐことができない。この攻撃は提案手法における脅威の 1 つである。

4.2.2 一時結託攻撃

一時結託攻撃とは、金銭などのやりとりを行うことで一時的に結託する攻撃であり、転売の典型的な攻撃方法である。電子チケットでは、攻撃者 A が購入したチケットを B に更に高値で売りつけることで、A が B に対して協力する動機となるため、A は B に対価を受け取る代わりに積極的な協力を行う。一方、永続結託攻撃に比べて弱い信頼関係しかないため、端末を貸与するとそのまま持ち去られてしまう危険性があるので、端末を貸与することはしない。そのため、一時結託攻撃では間接接触攻撃手法で用いられるように、SP への送出情報を共有することで攻撃を成功させようとする。つまり、SP にリクエストを送る際に B の送出情報を A のそれを共有して書き換える。

ただし、B は許可を得るために、以下のすべての動作をオフラインで満たさなくてはならない。

- A の送出情報を共有する
- B の送出情報を有効期限内に書き換える
- リファレンスを有効期限内に提示する

これらを確認者と対面しながら手動で行うことは難しく、自動化されたソフトウェアで書き換えても間接接触攻撃と同様にしてこれを拒否することができる。

4.3 従来の認証方法との比較

電子チケットのサービスでは、ログイン認証や生体情報を使った厳密な本人性の検証を行うことで、購入者と利用者を一致させようとしてきた。それぞれの場合について、攻撃への耐性及びユーザーや SP の負荷を評価する。

4.3.1 ID とパスワードによる認証

ID とパスワードを入力し、ログインが成功すれば、リファレンスを入手することで入場を許可する方法である。

なりすましモデルに対して、盗み見やマルウェアなどにより簡単に窃取されてしまううえ、直接的な接触をせずに攻撃者自身の端末によって攻撃が可能なため、脆弱である。また、提案手法で行った衝突の検知及びコンテキスト情報の書き換えによる確認はできず防御することができない。

さらに、結託モデルに対して、必要な情報を共有されるため脆弱である。一方、ユーザーが登録にかける負荷は、提案手法と同様だが、この負荷を軽くするためにユーザーがパスワードの強度を下げることで攻撃に対し更に脆弱になる。SP の登録負荷は、従来の認証基盤を活用できるため実装や運用は提案手法よりも容易にできる。

4.3.2 生体情報を使った厳密な本人性の検証

予め必要な顔や指紋などの情報を SP が預かり、会場にきた人間と照合することで入場を許可する方法である。

この手法はすべての攻撃モデルに対して、生体情報を使った照合の識別率に比例して頑健である。一方、ユーザーが情報を登録するための負荷は高い。例えば、予め顔写真を登録する場合、光度や表情、向きなどの条件を満たさなくてはならないうえ、センシティブな情報を預けるため心理的な負荷も高い。また、SP は運用や管理面での負荷も高い。例えば、顔写真の登録では識別が正しくできるものか目視で確認しなくてはならないうえ、認証が成功しない場合にユーザーにその理由を説明することが難しい。

4.3.3 関連手法

リファレンスを提示しない代わりに、ハードウェアとして独立した保護領域にある秘密鍵を使って署名した情報を NFC により提示する手法が提案 [5] されている。

この手法はデバイスを所持している人であれば提示ができるため、デバイスを奪う直接接触攻撃には脆弱である。一方、間接接触攻撃に対しては頑健である。これは、ハードウェアによる防御を行うことで秘密鍵を取り出せず、送出情報を正規のリーダー以外の手法で読み取るリプレイ攻撃を防ぐチャレンジーレスポンス応答によって読み取るリーダーを限定しているためである。また、永続結託攻撃では提案手法同様デバイス自体の譲渡が可能であり、脆弱だが、一時結託攻撃に対しては秘密鍵自体が取り出せないため、端末自体を貸与しないと攻撃が成立せず、間接接触攻撃と同様頑健である。

一方、ハードウェアとして Trusted Execution Environment (TEE) を前提とするなど機種が備える機構を要求するため、このシステムを利用するためのユーザーの負荷は高い。また、個別情報の確認はリーダーによる公開鍵の検証で行うため、SP の負荷は提案手法と同等である。

4.4 総合評価

表 3 に攻撃及び負荷に対する各手法による評価を示す。提案手法は、従来手法だけでなく関連手法に比べて永続結託以外の攻撃に対して頑健であり、またユーザーと SP 双方の負荷を軽減することがわかる。

表 3 それぞれの認証方法に対する評価

評価軸	提案手法	パスワード認証	生体情報	関連手法 [5]
直接接触攻撃	頑健	脆弱	頑健	脆弱
間接接触攻撃	特定条件で頑健	脆弱	頑健	頑健
永続結託攻撃	脆弱	脆弱	頑健	脆弱
一時結託攻撃	特定条件で頑健	脆弱	頑健	頑健
ユーザー負荷	低	低	高	高
SP 負荷	中	低	高	中

5. 考察

ログイン情報を用いたデバイス・コンテキスト情報を使ってオフラインでユーザーを検証する手法を提案した。提案手法の評価及び実装を通じて判明した 2 つの点について考察する。永続結託攻撃に対する防御と、コンテキスト識別の継続的な観測と実装方法である。

5.1 永続結託攻撃に対する頑健性

提案手法は、オンラインで登録を行ったユーザーとオフラインで対面しているユーザーが同じ端末を持ち、操作環境であるコンテキストを継続的に使用したうえでログインが可能なことを担保に本人性の検証をしている。そのため、永続結託攻撃に対しては従来の厳密な本人性の検証手法に対して十分な耐性が得られなかった。これは端末や操作環境といった、人に対して間接的な要素を照合に使ったためである。そこで、更に人に結びついた直接的な要素を照合する必要がある。しかし、既に述べたようにそこにはユーザーと SP 双方の負担があり、転売などの不当利用を行うケースのためにこれらの負担を新たにユーザーや SP が被り続けてサービスを継続することは難しい。

そこで、提案手法の改善によって永続結託攻撃への耐性を持たせるため、ユーザー識別を更に確実に行える手段についてユーザー識別の側面から検討する。永続結託攻撃では複数のユーザーが存在するため、様々な端末を使って同時並行的にチケットを取得する。この攻撃に対して、2 つの方向性が検討できる。

1 つは、端末をユーザーに強く関連付ける方法として、生体認証の結果をオンライン上で活用する Fast IDentity Online (FIDO[*1]) などを使う方法がある。この方法を採用すれば、登録した本人の生体情報や所持情報を確実に登録フェーズで結びつけることは可能である。ただし、生体情報による認証は端末内で行われているため、照合する正解情報が登録フェーズの時と同じことを確認できるような仕組みが必要である。　もう 1 つは、コンテキスト情報の種類を増やし、複数の情報を掛けあわせることで、細かくユーザーを識別する方法である。例えば、Internet of Things(IoT) と言われるネットワークに接続した種々のデバイスを使えば、デバイスとの接続やそのデバイスから取得できる行動履歴が取得できる。したがって IoT を用いて、購入者のプレゼンスを常に検証することができる。これらのコンテキスト情報を使って認証を行う手法は関連研究にも多いが、ユーザーからの同意を得ることや認証までにある程度の時間がかかるなど課題がある。

[*1] https://fidoalliance.org

5.2 識別情報の継続性

提案システムの実装において、デバイス・コンテキスト識別情報の継続性については考察が必要である。例えば、電子チケットサービスでは、販売がイベントの 6 ヶ月から 1 年前に行われる場合もある。他方、OS やブラウザなどのバージョンアップやプラグインの有効性など 1-2 週間の短い期間であってもコンテキスト情報が変わる場合や、端末の故障などによって機種変更することによってデバイス情報が使えなくなる可能性がある。

これらのケースでは、提案手法を用いるとユーザーは本人であっても入場を拒否されるため、サービスの提供ができない。そこで、これらの問題を解決するために 2 つの方向性を考える。

1 つは、追加の情報を受け入れる方法である。例えば、デバイス識別は、他の端末を同時に登録できるなどの条件を追加する、コンテキスト情報は、端末内の利用環境だけではなく、関連研究 [6] でも用いられている Wi-Fi などの信頼あるデバイスとの接続情報を使うことが考えられる。これらは、どの情報でも良いというわけではない。例えば Wi-Fi の SSID はアクセスポイントの操作さえできれば自由に書き換えることができ、一時結託攻撃で狙われやすい。また、取得方法についてユーザーができるだけ負担を感じないよう、プライバシーやユーザー体験など多方面からの検討を行う余地がある。

もう 1 つは、継続的な情報観測をしてユーザーを購入時だけではなく断続的に計測する方法 [6][7] である。例えば 1 日毎であれば大きくコンテキストが変わらない。また、コンテキスト情報も個別にみて、UA だけの変化であれば新しい情報に更新するなど、短いスパンでの小さな変化を受容することは Fingerprint の保存形式を工夫することで可能である。一方で更新を許しすぎると、他人のなりすましも許容し、別人の情報を登録することができるため、バランスを取る必要がある。これらは容易に決定できるものでなく、ユーザーの本人性の検証が可能な母集団において、その正解データと取得できるデバイスとコンテキスト情報を計測する実験による調整が必要である。

6. 関連研究

関連する研究に、Physical Access Control (PAC) がある。PAC の扱う問題は、実世界でのアクセスコントロールをユーザーの digital identity を通して行うことであり、本研究と目的が類似している。Buccafurri ら [8] は、端末の電力消費量をベースにしたワンタイムパスワードを作ることでオフラインにおける本人性を確保する提案をした。本稿のリファレンス情報もワンタイムパスワード同様にごく短い有効期限を用いる点で類似しているが、電力消費量はアプリの動作などに左右される要素であるため、ある時点でのユーザー情報を完全照合する本稿とは異なる。

また、本稿では検証のために用いたコンテキスト情報を認証手法に活用する研究として、石井ら [7] は位置情報の継続的追跡により、ユーザー識別をする手法について検討している。また、Preuveneers ら [6] はパスワードの代わりに Hoeffding trees を使って高速に近似コンテキストを特定することで接続している Wi-Fi など複数のコンテキストをリアルタイムで扱い、ユーザーを認証する手法を提案している。継続的な観測によるユーザーの追跡を行うことで、考察で述べたように提案手法を改善できる可能性があるが、本稿の課題設定とは異なる。例えば、これらの手法では電池の消費などユーザーに負担をかけるため、提案手法のようにある時点に限定した観測で解決を行うことができる。

7. おわりに

SP が適切な対象に限定してサービスを提供するため、オンラインでユーザーの本人性の検証を行った結果をオフラインで提示することで、対面した人とオンラインで登録を行った人の同一性を証明する手法について提案した。オンラインの登録時にユーザー識別情報としてログイン情報を活用した Fingerprint をクライアントで作ることで対面時のユーザーと識別情報を照合することで実現した。提案手法は従来手法と比べてユーザーと SP の負担を軽減し、オフラインで確認者と対面している人を正確に照合することで永続結託以外の攻撃においてそれを防ぐ手段があることを示した。今後、永続結託攻撃に対応するため、デバイス識別やコンテキスト識別を更に強化することでユーザーを更によく識別する手法について検討する。

参考文献

[1] Pass Market. `http://passmarket.yahoo.co.jp/`.
[2] TAPIRS. `https://www.tapirs.co.jp/face-authentication.html`.
[3] Keaton Mowery and Hovav Shacham. Pixel perfect fingerprinting canvas in HTML5. In Matt Fredrikson, editor, *Proceedings of W2SP*. IEEE Computer Society, May 2012.
[4] Anonymous browser fingerprint. `https://github.com/Valve/fingerprintjs`.
[5] Sandeep Tamrakar, Jan-Erik Ekberg, and N. Asokan. Identity verification schemes for public transport ticketing with nfc phones. In *Proceedings of the Sixth ACM Workshop on Scalable Trusted Computing*, STC '11, pp. 37–48, NY, USA, 2011. ACM.
[6] Davy Preuveneers and Wouter Joosen. Smartauth: Dynamic context fingerprinting for continuous user authentication. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing*, SAC '15, pp. 2185–2191, NY, USA, 2015. ACM.
[7] 石井智也, 鈴木宏哉, 山口利恵, 中山英樹, 山西健司. 個人認証を見据えた位置情報による識別に関する解析. コンピュータセキュリティシンポジウム 2015 論文集, 第 2015 巻, pp. 1035–1042, Oct 2015.
[8] Francesco Buccafurri and Gianluca Lax. A pervasive identification service for physical access control. In *Proceedings of the 5th International Conference on Pervasive Services*, ICPS '08, pp. 65–68, NY, USA, 2008. ACM.