実世界の消費者行動要求のための電子商取引制御システム

大神 渉 †　　五味 秀仁 †

† ヤフー株式会社 Yahoo! JAPAN 研究所
107-6211 東京都港区赤坂 9-7-1
wogami@yahoo-corp.jp hgomi@yahoo-corp.jp

あらまし 電子商取引における消費者同士の取引がその利便性を背景に拡大した。多様な取引形態が増える一方、不正取引や価格の高騰、実世界での買い占めなど様々な問題が現出した。その原因は、事業者が取引の状態や各利用者が持つべき権利を把握することが難しくなったことである。一方、事業者は利便性を損なわずに場の健全性を利用者に提供することが求められている。そこで、権利のライフサイクルを定義し、関係者の意図を反映することで場の健全性を実現するシステムを提案する。また、現実に考えられるユースケースに提案システムを適用することで、権利に関する様々な問題に対応できる事を示す。

E-commerce Transaction Management for Real World Activities

Wataru Oogami†　　Hidehito Gomi†

†Yahoo! JAPAN Research
9-7-1 Akasaka, Minato-ku, Tokyo 107-6211 Japan
wogami@yahoo-corp.jp hgomi@yahoo-corp.jp

Abstract Electronic commerce transactions between consumers become popular based on its convenience. As a result of the increase of various forms of transactions, improper activities have come to arise. This problem is caused by the difficulties for a service provider operating transactions to grasp their status and the rights of consumers that should hold in them. Therefore, the service provider is required to provide consumers with the health of the service without losing the convenience. We specify the lifecycle of the rights of consumers, and propose a system introducing the intention of parties involved with transactions. We also show that the proposed system can solve the above problem by applying it to use cases that are expected to appear.

1　はじめに

電子商取引（Electronic Commerce; E コマース）において、スマートフォンをはじめとする個人端末の広がりとともにその特徴を活かした消費者間 (Consumer to Consumer; C2C) 取引が拡大した。C2C 取引では、利用者個人の裁量で物品を自由に売買することができ、物品を安価で入手できたり、希少価値の高い物品を取引できたりする利便性がある。

C2C 取引の利用者はその利便性を享受する反面、不安や不満も持っている。それは、取引における詐欺などの不法行為、限定品の転売、実世界における買い占めなど多岐にわたる。これらは、取引形態の多様化に伴って生じた場の健全性の問題である。

E コマースを提供する事業者は、取引を更に活発化させるため、上記の利用者の懸念を軽減することが望ましい。一方、取引形態が複雑化し、物品が利用者から利用者へ多段階に流通するため、事業者は、個々の取引状態や権利の所在を正確に把握し続けることが困難になった。すなわち、事業者が適切に場に介在し、利用者の利便性を損なわずにその健全性を提供することが課題である。

本稿では、上記の課題に対し、事業者が健全な E コマース取引の場を実現するシステムを提案する。特に、取引の影響が実世界にも及ぶ “チケット” に着

目し、その状態を把握するためにライフサイクルを定義した。また、ライフサイクルを管理し、主体の意図を適切に反映するシステムを設計し、実現に必要な機能を提案した。さらに、ユースケースを使って提案システムによる制御の有効性を示し、チケットを取り巻く様々な問題点に対して考察を行なった。

2 定義

2.1 権限とチケット

本稿では、実世界における興行の入場などを実行するための権限を取り扱い、電子的に制御することを考える。実世界における入場などの実行は、与えられた権限を確認してもらうことで可能になる。権限内容とそれを自身が持つ事を正確に伝達して確認することは手間がかかり、大人数で都度行うことは非効率である。そのため、権限をもつ主体は該当する権限の内容と正当性を正確に素早く伝達するために後述する “チケット” を用いて提示を行う。

権限の内容は 2 つの情報群に分類できる。開催場所や時間など権限自体を表す情報群 (以降メタ情報と呼ぶ) と、所持者や有効期限、入手方法など流動的な状態を一意に指し示す情報群 (以降ステータス情報と呼ぶ) である。情報を提示する時、2 つの情報群を毎回読み取ることは非効率であるため、それを指す参照情報があれば提示された側は情報群を取得できる。この参照情報を “リファレンス” と呼ぶ。リファレンスは電子的に扱うために複数文字の羅列とする。リファレンスを人間がこのままの形で扱うと記憶や伝達に不利である。そこで、リファレンスを実世界に具現化して提示しやすく変換した形態を “CR(Converted Reference)” と呼ぶ。文字やバーコードが CR の代表例である。また、提示する主体が CR を表示するために用いる実世界での媒介を “メディア” と呼ぶ。例えば、紙やスマートフォン端末がメディアに該当する。CR が表示されたメディアを “チケット” と呼ぶ。権限をやりとりする手段として、チケットの取引が行われている。

2.2 場の健全性と利便性

チケットを扱うとき、E コマースの場の健全性には 2 つの要素が必要である。1 つは場の**公平性**である。つまり、販売者は多くのファンや観客にサービスを提供し、購入者は不当な買い占めの影響を受けずにチケットを手に入れたいというニーズである。もう 1 つは場の**安全性**である。つまり、販売者と購入者双方にとって使用できる本物のチケットである保証が欲しいというニーズである。また、場の健全性と利便性は二律背反となることがある。例えば、公平性のためにチケットの転売を禁止すると、急な用事によって参加できないユーザーが不利益を被る。

場の健全性は B2C 取引では実世界を含めた規制によって制御可能なものであった。一方、C2C 取引を中心とした E コマースにおいては、複雑な取引形態が生まれ、実世界における様々な状態や要望を正確に制御できなくなった。本稿は、利便性と場の健全性を両立させるために、チケットの取引に関わる主体が抱えるその取り扱いの意図を E コマースサービスや行動に対して反映するシステムを提案する。

2.3 エンティティ

E コマースでは、C2C や B2C などを組み合わせた様々な取引が行われる。取引に関わるエンティティを以下のように定義する。

販売主 Publisher (Pu) 権限を発生させる主体であり、B2C 取引では企業側に位置する。後述の SP に対してチケットの販売を委託する。

事業者 Service Provider (SP) 取引の場をサービスとして提供する主体であり、Pu の委託を受けてチケットを販売するサービスを提供することがある。SP=Pu でもよい。

ユーザー SP からサービスの提供を受ける主体である。販売者・購入者どちらにもなり得る。

2.4 チケットの検証

検証とは、SP がリファレンスを元に、それを提示したユーザーが本当にその権限を所有し、行使可能かを確認する作業である。SP は検証に必要な情報をユーザーに要求し続けることができる。SP はメタ情報とステータス情報と、要求した情報を使って検証を行う。

2.5　アクションとライフサイクル

エンティティがチケットを介して権限のステータス情報を変化させる要求とそれに基づく実世界の行動を “アクション” と呼ぶ。権限に対して必ず 1 回以上生起するアクションを示す。

発券 Pu が任意の数の権限を SP に委託することで SP が権限毎に識別子を割り当てる。

購入 ユーザーが Pu や SP に申し込みと対価の支払を行うことで権限を入手する。

行使 SP がユーザーの提示したチケットを検証する。

失効 エンティティの操作や有効期限などの条件を満たすことで権限が無効になる。

また、購入から失効までの任意のタイミングで発生するアクションを示す。

転売 ユーザーが対価と引き換えに自らの権限は失効する一方で、元の権限を別の未知ユーザーが保有するものにする。

譲渡 ユーザーが自らの権限を失効させる代わりに指定した既知のユーザーが保有するものにする。

活用 Pu や SP が権限の情報を分析し、システムにフィードバックする。

7 つのアクションによるステータス情報の変遷を権限の “ライフサイクル” と定義する。ライフサイクルにおけるアクション間の相関関係を図 1 に示す。

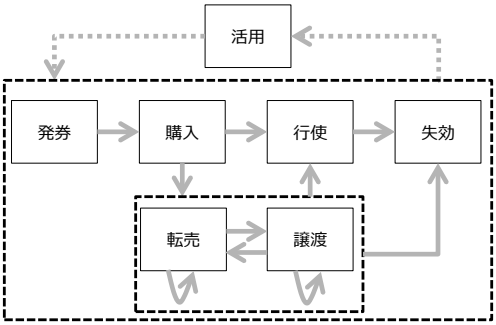

図 1: アクション間の相関関係

2.6　意図とポリシー

エンティティが実世界で抱える権限の取り扱い方を “意図” と呼ぶ。システムが意図を解釈して決まった制御の方針を **“ポリシー”** と呼ぶ。具体的に、ポリシーとは指定したアクションに対し、許可・禁止を決定する条件群である。例えば、「定価までの価格であれば転売を許可する」というポリシーが設定できる。ポリシーは JSON や XML などの構造化データ記述言語で記述する。

2.6.1　メタポリシー

ポリシーを規定するポリシーを “メタポリシー” と呼ぶ。メタポリシーは「どのようなポリシーを設定可能とするか」などシステム全体の様々な挙動を記述する。後述の「継承」のように SP 以外がポリシーの運用方法を決定するときや、SP 自体が事業者の複合体や複数の同種サービスを提供するとき、メタポリシーが記述されていないと分散処理を行うことができない。

2.6.2　ポリシーの指定要素

ポリシーは主に 4 つの要素によって指定され、その設定方法などはメタポリシーに規定する。以下にポリシー指定の例を示す。

1. 対象の指定　「ユーザー」などのエンティティ

2. アクションの指定　「活用」などのアクション

3. 権限の指定　「許可/否認」のいずれか

4. 条件の指定

取引内容　「定価までの価格」など E コマースサービスに関する条件

ユーザーの属性　「18 歳以上の男性」などユーザーそのものやその属性に関する条件

環境　「会場の近く」などユーザーの置かれた環境に関する条件

ステータス情報　「失効後」などステータス情報に関する条件

また、ポリシーには公開できない秘密情報が含まれる可能性がある。例えば、価格変動の要因や申し込み条件を公開しないなどのケースである。このケースの場合、秘密保持契約を結ぶなど保存と適用についての方法を予め Pu と SP が同意し、同時にメタポリシーに記述する。

2.6.3 継承

ある権限のポリシー適用に対して考慮すべき点は、ライフサイクル上で一貫してポリシーを適用することである。そのため、適用済みのポリシーも次のアクション時に適用できる (継承と呼ぶ) ことを考える。例えば、Pu によってユーザー属性「18 歳以上」が「購入」時に適用された権限は、ユーザーが「転売」する時にも「18 歳以上」という当初の「意図」が，以降の取引においても反映させることを望む場合がある。一方、ユーザー A がユーザー B にのみ「譲渡」をするというポリシーは、B の以後のアクションに拘束力を持たない。

あるポリシーの継承判断はメタポリシーに記述する。上記例では「18 歳以上」というポリシーは Pu が設定時に継承することを明記する。一方、ユーザー A が設定した「B に対してのみ譲渡可能」というポリシーは、例えばユーザー B の「誰に対しても譲渡可能」というポリシーと衝突する。この時、前者のポリシーは所有権の観点から継承を行わないことをメタポリシーに記述する。ただし、既に行なったアクションに対して、そのアクション発生より後に該当する権限に対するポリシーが追加されたとしても、それを遡って継承を受けない。SP はこのようにメタポリシーに記述することでライフサイクル上に一貫したポリシーを適用することができる。

3 システム設計

提案システムの目的はエンティティの意図をポリシーとしてライフサイクル上に一貫して反映することである。システムの構築例を図 2 に示す。

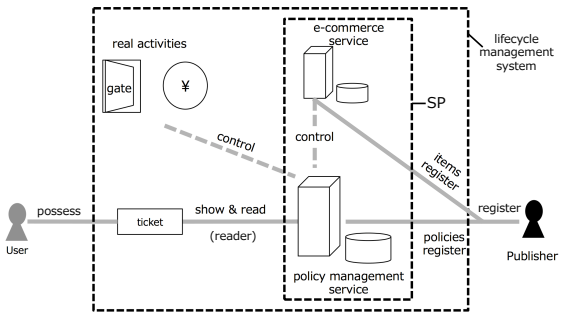

図 2: システム構築例

図 2 で示したとおり、提案システムが権限を操作し、影響を及ぼす範囲は、E コマースサービスだけではない。入場の制御を行うゲートや課金・商品の受け渡しなど、提示によりユーザーが求める権限の種類とそれに対する許可を判断し、それを実世界の運用にも反映しなくてはならない。つまり、SP はオンライン上だけでなく、様々な機器からそれが操作できるインターフェイスを持つ必要がある。

また、実世界において検証を行う際にもポリシーを適用する。“リーダー” とは検証時に用い、CR を読み取りリファレンスを取り出すための装置である。例えば、文字であれば人間、バーコードであれば専用の機器など、CR の種類だけリーダーが存在する。メディアは伝統的に紙を用いるため、CR として印字した文字を用いることが多いが、Passbook[1] に代表される電子チケットや NFC(Near Field Communication) など、技術の発達により様々な形態の電子的な提示と検証が可能となった。しかし、これらを用いるだけでは、実世界でのポリシーを適用する方法がなく、エンティティの意図は正確に反映できない。そこで、実世界でユーザーの手元にチケットを届ける際にポリシーを反映する手段として “配備” を考察する。

本稿では、実世界と E コマースに継続的にポリシーを適用するために、共通の API(Application Programming Interface) の設計と、電子チケットの配備手法について提案する。

3.1 権限情報

システムは権限に関する 2 つの情報を管理する。メタ情報とステータス情報を合わせた権限情報テーブル (以降 privilege テーブルと呼ぶ) とそのポリシー情報 (以降 policy テーブルと呼ぶ) である。

表 1: privilege テーブル

権限識別子	開催情報	所持者識別子	状態フラグ	関連権限
priv001	Nagasaki	usr0001	alive	usr0002
priv002	Nagasaki	usr0002	conv	usr0001

表 1 は権限の最新情報を格納する privilege テーブルである。それぞれが単方向あるいは双方向の任意の数のリストを持っており、各アクションの履歴の役割も持つ。表 1 にある「権限識別子」は一意に権限を指定する識別子である。「開催情報」はメタ情報の一例であり、任意に拡張することができる。メ

[1] https://support.apple.com/en-us/HT204003

タ情報のうち興行毎に共通した情報は、効率を考慮して参照だけを持つ。一方、このテーブルはステータス情報も柔軟に格納できる。「所持者識別子」はSP が提供するサービス上でユーザーを一意に識別するものである。「状態フラグ」は権限の状態であり、有効か、有効でない場合その理由を表すフラグである。「関連権限」は他の権限識別子に対する参照を持つ。例えば表 1 では、priv002 が失効しており、priv001 として usr0002 から usr0001 へ譲渡されたことを表す。提案システムはこのようにして任意の権限についてそのライフサイクルを完全に把握可能である。表 1 では、priv001、priv002 どちらをキーに参照してもこの状況を把握できる。

表 2: policy テーブル

ポリシー識別子	対象	制限アクション	条件	発効時間
poli0001	priv001	conv,resale	NULL	1445526000

表 2 はポリシーを格納する policy テーブルである。一般にポリシーは、その記述力が大きくシステムに影響を与えるため、XML や JSON などの構造化言語で記述する。表 2 の「ポリシー識別子」はポリシーを一意に識別するものである。「制限アクション」は制限を行うアクションであり、アクションの拡張などを考えてビットフラグとして表現する。「条件」は制限アクションを許可・拒否する条件の羅列を指定し、空欄 (NULL) とした場合には指定したすべてのアクションを制限する。「発効時間」はポリシーの上書き可能な時間を表す。これはポリシーの途中変更を許可する場合にコンフリクトを解消するために使用する。ただしコンフリクトやその解消は本稿で扱わない。

権限を操作するとき、必ず privilege テーブルの「権限識別子」を使って実在を確認し、次に policy テーブルの「対象」を検索することで、扱う権限に関するポリシーを参照することが可能である。

3.2 権限の操作

privilege と policy2 つのテーブルを使って権限を操作するための 5 つのインターフェイスとそのテーブル操作を設計する。

登録 任意のタイミングで権限とそれに基づくポリシーを追加・更新する。

ポリシー参照 指定されたリファレンスから、ポリシーを参照し適用すべきポリシーのみ返す。

失効 ポリシーで記述された条件を満たした時権限を無効化する。

1. バッチ処理やリクエストにより配備済みチケットに対するポリシー違反が検出される。
2. 該当する権限の状態フラグを「失効」状態として違反ポリシーを記録する。

付与 指定した権限とユーザーを紐付ける。

1. privilege テーブルの該当箇所を参照する。
2. 所持者がいないことを確認して所持者識別子欄にユーザーを追加する。

データ集積 権限操作データを利用可能な形にする。

1. 両テーブルを逐次サマリデータにする。
2. 両テーブルのログを逐次回収しておく。
3. リクエストに応じて上記データを引き出す。

これら 5 つのインターフェイスは SP の API として実装され、他のコンポーネントが内部テーブルを意識して作る必要がない。

3.3 配備

リファレンスを動的に整形して CR としてメディアに表示する環境を “実行環境 (Execution Environment; EE)” と呼ぶ。配備とは、ユーザーがチケットを表示する準備としてユーザーのもつ EE に対してリファレンスを搭載することである。また、動的書き換えができないメディアにおいて、配備とはユーザーが操作可能なチケットを配布することである。配備したチケットは 2 つの要素を担保する。

当人性　ユーザー本人だけが提示できる

真贋性　チケットが本物か確認できる

この 2 つの要素を確保する度合いは Pu や SP のポリシーに依拠する。本稿では、2 つの要素をより確保可能な EE を使った配備の手法を提案する。

まず、メディアはスマートフォンなどの個人端末でアプリケーション (以降単にアプリと呼ぶ) を追加可能なものとする。個人端末の普及は著しく、E コマースサービスでも使用されているため、本稿への適用は自然な設定である。ユーザーは SP が発行したアプリをインストールする。この時、EE はスマートフォン上のアプリである。

新しくチケットを配備するとき、アプリは 2 つの

要素を以下のように確保する。まず、アプリはユーザーを必要に応じてSPのサービスにて認証することで、チケットを購入した人と同一であることを確認し、**当人性**を確保する。アプリはポリシー参照機能を使ってアプリは配備可能なリファレンスとそのポリシーをSP側に要求する。SPは該当するリファレンスとポリシー、メタポリシーを送り返す。アプリは受け取ったポリシーとメタポリシーに合致するリファレンスのみを格納する。ユーザーは格納されたリファレンスのみをCRとして表示可能である。また、標準的な暗号アルゴリズムに依拠してポリシーやメタポリシー、リファレンスの内容を暗号化・難読化するため、偽造や内容の読み取りは難しく、外部から任意のリファレンスを挿入することはできない。このようにユーザーに特化した最新のポリシーを適用したリファレンスのみが配備されるため、**真贋性**が確保できる。

3.4 ライフサイクル管理の実現

5つのインターフェイスと「配備」によるライフサイクル管理の実現を示すためにユースケースを考える。システムの各動作とユーザに対する制御の効果について議論する。

3.4.1 設定

本ユースケースにおいてPuが持つ意図を示す。

1. 自社の登録会員に限定して先着で販売する
2. 定価を超える価格での転売を禁止する
3. 販売実績により次回の開催規模を決める

また、SPは前述のEEを使った配備が可能な電子チケットでの配備を行いたいという意図を持っている。CRとして二次元バーコードを採用する。

3.4.2 ユースケース

1. 発券　Puは観劇イベントを開催するので、チケットをSPに委託販売したい。まず、PuはSPのチケット登録フォームから販売するチケットとポリシーを「登録」する。

2. 購入　販売を知ったユーザーAは購入を決め、SPのEコマースサービスでusr0001としてログイン後、開いている席の購入ボタンを押す。システムは対応するリファレンスを指定して「ポリシー参照」を行う。購入ポリシーである「自社の登録会員に限定する」を満たすためシステムはAにPuでの認証連携(Puサービスを通してのログイン)要求をする。もし、この認証連携ができない場合、購入を拒否する。Aは認証連携を行い、その後、対価を支払った。システムは支払いを確認できたため、チケットの「付与」を行う。Aはアプリでusr0001としてログインした後、購入したチケットが「配備」され、二次元バーコードで表示することができた。なお、空席のチケットだけが購入できるため、「先着」のポリシーが適用されている。

3. 転売・譲渡　後日、Aは急な用事のためイベントに参加できないことに気づく。Aは既に売り切れているこのチケットを「どうせなら高く売ろう」という意図を持つ。SPのEコマースサービスで、Aは定価より高い値段で転売を申し込む。システムは「ポリシー参照」を行うことで、「定価より高い価格では転売できない」ポリシーを反映して転売申し込みをキャンセルする。Aにその旨が通知されると、Aは代わりに「知り合いのBに譲って」参加してもらおうという意図を持つ。Aは、SPのサービスでB(usr0002)を指定して譲渡を申し込む。システムは「ユーザーBにのみ譲渡する」というポリシーを「登録」する。その後、システムは「ポリシー参照」を行い、譲渡ポリシーがないため、継承した販売ポリシーを適用する。そのため、システムはBに対してログインとPuのサービスでの認証連携を要求する。Bはシステムから通知をうけ、usr0002でログインを行い、更にPuサービスでの認証連携を行った。システムはポリシーを満たすことを確認し、Bに「付与」した後アプリへの「配備」を行うと同時にAのアプリに配備した権限を「失効」させた。

4. 行使　当日、Bは会場に来場し、ゲートでチケットの提示を求められる。アプリを起動し二次元バーコードをリーダーにかざす。システムは「ポリシー参照」を実行する。行使ポリシーは無いが、セッションが切れていることがわかり、「自社の登録会員である」というポリシーが守られていないため、ゲートは開かない。その旨が近くにいる係員に提示され、説明を受けたBはアプリで再度ログインした後二次元バーコードをかざす。既に認証連携を行なっているためゲートが開き、Bは入場できた。

5. 失効　観劇を楽しんだBは、翌日も同じイベントが開催される事を知る。Bは前日に他の人がイベント中に退場や再入場ができていた場面を思い出し、

あわよくばまた観劇できる可能性を思いついた。会場で行使を試みるが、既に前日の閉幕直後にチケットの「失効」が実行されており、B は入場できない。

6. 活用　Pu は「データ集積」されたデータから、転売要求が多かったことで、会員でないユーザへの譲渡要求や潜在的なチケット価値の高さが判明した。そのため、次回イベントで良席の拡充や譲渡先は会員に限定しないことを決めた。

本ユースケースにおける制御を図 3 に示す。

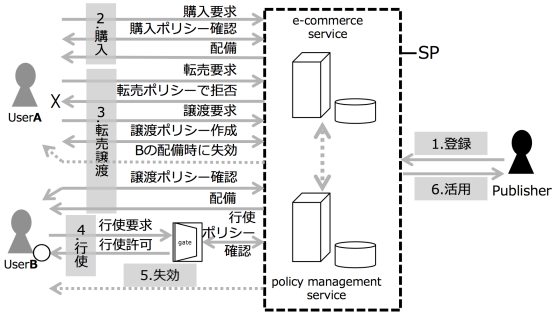

図 3: ユースケース

4　考察

実世界において、各エンティティはシステムを不正利用する可能性がある。そこで、Pu や SP の視点から不正なアクションを考察し、提案システムによりそれらを防ぐ方法を示す。また、ユーザーの視点からプライバシーについて議論する。

4.1　攻撃

“攻撃” とは、ポリシーに合致しない要求を行うことである。Pu/SP/ユーザーのいずれも攻撃者となる可能性がある。前述のユースケースを使い、特に実世界に影響が大きい 3 種の攻撃を考察する。

4.1.1　偽造

偽造とは、攻撃者が許可されていない任意のチケットを作成して行使しようとする攻撃である。本ユースケースで攻撃が成功すると、会場で偽のチケットを提示するユーザーの入場を許可する。偽造の手法は主に 2 つの場合が考えられる。

1 つ目は**解析・改ざん**である。これは、攻撃者が事前にチケットを配備したアプリのデータを解析し、そのリファレンスを書き換えることで任意のチケットを入手しようと企てる。この攻撃は、SP の権限情報を書き換えていないため、リファレンスを書き換えたとしても SP との同期によりそれが有効になることはない。また、リファレンスが攻撃者によって想定可能な情報でなくては成立しないため、ランダムに採番することで攻撃を成立させにくくすることができる。

2 つ目が**複製・持ち出し**である。これは、攻撃者が事前に購入したアプリのデータをコピーし、別の端末へ入れてチケットを移し替えることでポリシーで禁止されている価格での転売を行おうとする。この攻撃は、正規のアプリごと権限情報を移し替えるのでチケットの表示ができる。提示時に SP へポリシーとメタポリシーを問い合わせる動作をさせることでこの攻撃は防止できる。つまり、認証を通すことでシステムが異なるユーザーだと判断でき、移し替えたチケットは提示ができない。

4.1.2　譲渡の偽装

譲渡の偽装とは、攻撃者が譲渡を装ってチケットを譲る、あるいは譲り受ける攻撃である。本ユースケースで攻撃が成功すると、ポリシーで制限されている定価以上の価格での転売ができる。

譲渡の偽装として、主な手法の 1 つは**譲渡先の虚偽申告**である。これは、ユーザー C が攻撃者となり、譲渡先として例えば A の友人を名乗り、譲渡をする。一方、C は A に SP が感知しない方法で定価以上の金銭を渡すことで、転売が成立する。この攻撃は、データ活用を行い、悪性ユーザーを特定することで防止できる。

4.1.3　拒否

拒否とは、検証の結果を否定して権利を行使しようとする攻撃である。本ユースケースで攻撃が成立すると、権限がない人にも入場を許可する。拒否は、検証結果の曖昧さがその原因である。

UI の偽装はアプリに類似した UI やスクリーンショットなどによって二次元バーコード (CR) を表示して行使を認めさせようとする手法である。この場合、SP は配備されたリファレンスが EE によって会場で生成できていないことを理由に行使を拒否す

る。一方、攻撃者は CR が可読でないため、拒否する余地がある。提案システムでは、行使する時間等の変量に合わせて動的に CR を変化させることが可能である。そのため、変化が人の目からみても明らかに異なることを理由に拒否することができる。

また、アプリが起動できないなどの申告による虚言も考えられる。申告は必ずしも虚言ではないが、チケットの検証ができないため、攻撃者は購入の履歴などを使って拒否する余地がある。この攻撃も防ぐ方法はある。まず、SP が申告者から情報を受け取り該当ユーザーを特定する。例えば、アプリの起動ができなくても他の端末でのログインを通して特定可能である。次に、SP は事前に預かっていたユーザーの属性情報 (例えば、運転免許証など) を使って認証する。攻撃者であればその認証を通過できない。申告が事実である場合、救済手法として活用できる。

4.2 プライバシー

ユーザーが提案システムを受け入れることができるかは SP にとって重要な課題である。提案システムにおける利点とユーザーのプライバシーは二律背反の関係であることが多い。ユースケースでは、ユーザーはチケットを受け取るためにアプリ上で認証を受ける。SP は識別子を使ってユーザーを必要以上に追跡することのないように取得できる情報の管理を適切に行う。また、センシティブな情報が含まれるため、SP 自身がその情報の用途を明確にして、ユーザーに提示した上で同意を取るようにする。また、SP 間で共通の識別子を用いることで名寄せができないように複数の SP 間で同じ識別子を共有しないようにする。ユーザーへ有益なサービスを提供する上で、SP はプライバシーに対する配慮とともにサービス内容をよく考慮するバランスが必要である。

5 関連研究

Ungureanu[1] は E コマースの契約にポリシーを導入し動的に記述する言語を提案した。本稿はポリシーの適用を動的に行うことが出来る点で関連するが、実世界にまで拡大して適用した点で異なる。

また、Yang[2] は RFID を用いてバックエンドサーバーに繋がっていなくてもリーダーとタグが相互認証可能になる手法を提案した。本稿では、この手法をチケットとして柔軟に適用することができる。

また、Gudymenko ら [3] は NFC を用いて公共交通機関の電子チケットに対して複製や偽造のできないチケットを考察した。本稿では、複製や偽造をポリシー制御によって解決する点で異なる。

一方、Kerschbaum ら [4] や Gudymenko[5] が述べるようにチケットへのポリシー適用というビジネス的要求に対して、プライバシーの点で課題が残る。

6 おわりに

Pu と SP、ユーザー 3 者の意図を適切に反映し、ライフサイクルの管理を行うことでチケットに関する問題を解決できるシステムを提案した。今後、具体的な実装を進め、提案システムの有効性を提示する。

参考文献

[1] Ungureanu, V. Using Certified Policies to Regulate E-commerce Transactions. *ACM Trans. Internet Technol.*, Vol. 5, No. 1, pp. 129–153, February 2005.

[2] Yang, M. H. Controlled Delegation Protocol in Mobile RFID Networks. *EURASIP J. Wirel. Commun. Netw.*, Vol. 2010, pp. 69:1–69:13, April 2010.

[3] Gudymenko, I., Sousa, F., and Köpsell, S. A Simple and Secure E-Ticketing System for Intelligent Public Transportation Based on NFC. In *Proc. First International Conference on IoT in Urban Space*, URB-IOT '14, pp. 19–24, Brussels, Belgium, 2014.

[4] Kerschbaum, F., Lim, H. W., and Gudymenko, I. Privacy-Preserving Billing for E-Ticketing Systems in Public Transportation. In *Proc. 12th ACM Workshop on Workshop on Privacy in the Electronic Society*, WPES '13, pp. 143–154, NY, USA, 2013.

[5] Gudymenko, I. A Privacy-Preserving E-Ticketing System for Public Transportation Supporting Fine-Granular Billing and Local Validation. In *Proc. 7th International Conference on Security of Information and Networks*, SIN '14, pp. 101:101–101:108, NY, USA, 2014.