(19)日本国特許庁(JP)

(12)特許公報(B1)

(11)特許番号
特許第7311721号
(P7311721)

(45)発行日　令和5年7月19日(2023.7.19)

(24)登録日　令和5年7月10日(2023.7.10)

(51)国際特許分類

Ｇ０６Ｆ　21/42　(2013.01)		Ｇ０６Ｆ	21/42
Ｇ０６Ｑ　20/40　(2012.01)		Ｇ０６Ｑ	20/40

ＦＩ

請求項の数　11　（全22頁）

(21)出願番号　特願2023-14744(P2023-14744)
(22)出願日　令和5年2月2日(2023.2.2)
(62)分割の表示　特願2022-109157(P2022-109157)の分割
原出願日　令和4年3月7日(2022.3.7)
審査請求日　令和5年2月2日(2023.2.2)
早期審査対象出願

(73)特許権者　519110124
ＰａｙＰａｙ株式会社
東京都千代田区紀尾井町１番３号
(74)代理人　100149548
弁理士　松沼 泰史
(74)代理人　100154852
弁理士　酒井 太一
(74)代理人　100181124
弁理士　沖田 壮男
(74)代理人　100194087
弁理士　渡辺 伸一
(72)発明者　大西 朋史
東京都千代田区紀尾井町１番３号 ＰａｙＰａｙ株式会社内
審査官　局 成矢

最終頁に続く

(54)【発明の名称】　情報処理装置、情報処理方法、およびプログラム

(57)【特許請求の範囲】

【請求項１】

利用者によって使用される端末装置であるとして既に認証されている第１端末装置と、まだ認証されていない第２端末装置と通信可能な情報処理装置であって、

前記第２端末装置からログイン要求があった場合に、第１認証情報がコード化された第１コード情報を生成した後、前記第１認証情報とは異なる第２認証情報がコード化された第２コード情報を生成するコード情報生成部と、

前記コード情報生成部によって生成された前記第１コード情報および前記第２コード情報を、前記第１端末装置および前記第２端末装置のうちのいずれか一方に送信する送信部と、

前記第１コード情報を撮影してデコードすることによって得られた前記第１認証情報および前記第２コード情報を撮影してデコードすることによって得られた前記第２認証情報を、前記第１端末装置および前記第２端末装置のうちのいずれか他方から受信する受信部と、

前記受信部によって受信された前記第１認証情報および前記第２認証情報に基づいて、前記第２端末装置を認証する認証部と、

を備え、

前記第１コード情報は、前記第２コード情報よりも先に撮影され、

前記第１認証情報および前記第２認証情報は、時限的な情報であり、

前記第１認証情報と比較して不正取得されることをより防止するために、前記第２認証

情報の時限的な期間は、前記第１認証情報の時限的な期間よりも短い、
情報処理装置。
【請求項２】
利用者によって使用される端末装置であるとして既に認証されている第１端末装置と、まだ認証されていない第２端末装置と通信可能な情報処理装置であって、
前記第２端末装置からログイン要求があった場合に、第１認証情報がコード化された第１コード情報を生成した後、前記第１認証情報とは異なる第２認証情報がコード化された第２コード情報を生成するコード情報生成部と、
前記コード情報生成部によって生成された前記第１コード情報および前記第２コード情報を、前記第１端末装置に送信する送信部と、
前記第１コード情報を撮影してデコードすることによって得られた前記第１認証情報および前記第２コード情報を撮影してデコードすることによって得られた前記第２認証情報を、前記第２端末装置から受信する受信部と、
前記受信部によって受信された前記第１認証情報および前記第２認証情報に基づいて、前記第２端末装置を認証する認証部と、
を備え、
前記第１コード情報は、前記第２コード情報よりも先に撮影され、
前記第１認証情報および前記第２認証情報は、時限的な情報であり、
前記第１認証情報と比較して不正取得されることをより防止するために、前記第２認証情報の時限的な期間は、前記第１認証情報の時限的な期間よりも短い、
情報処理装置。
【請求項３】
利用者によって使用される端末装置であるとして既に認証されている第１端末装置と、まだ認証されていない第２端末装置と通信可能な情報処理装置であって、
前記第２端末装置からログイン要求があった場合に、第１認証情報がコード化された第１コード情報を生成した後、前記第１認証情報とは異なる第２認証情報がコード化された第２コード情報を生成するコード情報生成部と、
前記コード情報生成部によって生成された前記第１コード情報および前記第２コード情報を、前記第２端末装置に送信する送信部と、
前記第１コード情報を撮影してデコードすることによって得られた前記第１認証情報および前記第２コード情報を撮影してデコードすることによって得られた前記第２認証情報を、前記第１端末装置から受信する受信部と、
前記受信部によって受信された前記第１認証情報および前記第２認証情報に基づいて、前記第２端末装置を認証する認証部と、
を備え、
前記第１コード情報は、前記第２コード情報よりも先に撮影され、
前記第１認証情報および前記第２認証情報は、時限的な情報であり、
前記第１認証情報と比較して不正取得されることをより防止するために、前記第２認証情報の時限的な期間は、前記第１認証情報の時限的な期間よりも短い、
情報処理装置。
【請求項４】
前記第１認証情報の時限的な期間は、前記第１コード情報を撮影するためのカメラ機能の起動時間よりも長い期間である、
請求項１から請求項３のうちの何れか一項に記載の情報処理装置。
【請求項５】
前記送信部は、前記認証部による前記第１認証情報に基づく認証が完了した後で、前記第２コード情報を送信する、
請求項１から請求項３のうちの何れか一項に記載の情報処理装置。
【請求項６】
利用者によって使用される端末装置であるとして既に認証されている第１端末装置と、

まだ認証されていない第２端末装置と通信可能な情報処理装置が、
前記第２端末装置からログイン要求があった場合に、第１認証情報がコード化された第１コード情報を生成した後、前記第１認証情報とは異なる第２認証情報がコード化された第２コード情報を生成し、
前記第１コード情報および前記第２コード情報を、前記第１端末装置および前記第２端末装置のうちのいずれか一方に送信し、
前記第１コード情報を撮影してデコードすることによって得られた前記第１認証情報および前記第２コード情報を撮影してデコードすることによって得られた前記第２認証情報を、前記第１端末装置および前記第２端末装置のうちのいずれか他方から受信し、
受信された前記第１認証情報および前記第２認証情報に基づいて、前記第２端末装置を認証し、
前記第１コード情報は、前記第２コード情報よりも先に撮影され、
前記第１認証情報および前記第２認証情報は、時限的な情報であり、
前記第１認証情報と比較して不正取得されることをより防止するために、前記第２認証情報の時限的な期間は、前記第１認証情報の時限的な期間よりも短い、
情報処理方法。
【請求項７】
利用者によって使用される端末装置であるとして既に認証されている第１端末装置と、まだ認証されていない第２端末装置と通信可能な情報処理装置が、
前記第２端末装置からログイン要求があった場合に、第１認証情報がコード化された第１コード情報を生成した後、前記第１認証情報とは異なる第２認証情報がコード化された第２コード情報を生成し、
前記第１コード情報および前記第２コード情報を、前記第１端末装置に送信し、
前記第１コード情報を撮影してデコードすることによって得られた前記第１認証情報および前記第２コード情報を撮影してデコードすることによって得られた前記第２認証情報を、前記第２端末装置から受信し、
受信された前記第１認証情報および前記第２認証情報に基づいて、前記第２端末装置を認証し、
前記第１コード情報は、前記第２コード情報よりも先に撮影され、
前記第１認証情報および前記第２認証情報は、時限的な情報であり、
前記第１認証情報と比較して不正取得されることをより防止するために、前記第２認証情報の時限的な期間は、前記第１認証情報の時限的な期間よりも短い、
情報処理方法。
【請求項８】
利用者によって使用される端末装置であるとして既に認証されている第１端末装置と、まだ認証されていない第２端末装置と通信可能な情報処理装置が、
前記第２端末装置からログイン要求があった場合に、第１認証情報がコード化された第１コード情報を生成した後、前記第１認証情報とは異なる第２認証情報がコード化された第２コード情報を生成し、
前記第１コード情報および前記第２コード情報を、前記第２端末装置に送信し、
前記第１コード情報を撮影してデコードすることによって得られた前記第１認証情報および前記第２コード情報を撮影してデコードすることによって得られた前記第２認証情報を、前記第１端末装置から受信し、
受信された前記第１認証情報および前記第２認証情報に基づいて、前記第２端末装置を認証し、
前記第１コード情報は、前記第２コード情報よりも先に撮影され、
前記第１認証情報および前記第２認証情報は、時限的な情報であり、
前記第１認証情報と比較して不正取得されることをより防止するために、前記第２認証情報の時限的な期間は、前記第１認証情報の時限的な期間よりも短い、
情報処理方法。

【請求項９】
利用者によって使用される端末装置であるとして既に認証されている第１端末装置と、まだ認証されていない第２端末装置と通信可能な情報処理装置に、
前記第２端末装置からログイン要求があった場合に、第１認証情報がコード化された第１コード情報を生成させた後、前記第１認証情報とは異なる第２認証情報がコード化された第２コード情報を生成させ、
前記第１コード情報および前記第２コード情報を、前記第１端末装置および前記第２端末装置のうちのいずれか一方に送信させ、
前記第１コード情報を撮影してデコードすることによって得られた前記第１認証情報および前記第２コード情報を撮影してデコードすることによって得られた前記第２認証情報を、前記第１端末装置および前記第２端末装置のうちのいずれか他方から受信させ、
受信された前記第１認証情報および前記第２認証情報に基づいて、前記第２端末装置を認証させ、
前記第１コード情報は、前記第２コード情報よりも先に撮影され、
前記第１認証情報および前記第２認証情報は、時限的な情報であり、
前記第１認証情報と比較して不正取得されることをより防止するために、前記第２認証情報の時限的な期間は、前記第１認証情報の時限的な期間よりも短い、
プログラム。
【請求項１０】
利用者によって使用される端末装置であるとして既に認証されている第１端末装置と、まだ認証されていない第２端末装置と通信可能な情報処理装置に、
前記第２端末装置からログイン要求があった場合に、第１認証情報がコード化された第１コード情報を生成させた後、前記第１認証情報とは異なる第２認証情報がコード化された第２コード情報を生成させ、
前記第１コード情報および前記第２コード情報を、前記第１端末装置に送信させ、
前記第１コード情報を撮影してデコードすることによって得られた前記第１認証情報および前記第２コード情報を撮影してデコードすることによって得られた前記第２認証情報を、前記第２端末装置から受信させ、
受信された前記第１認証情報および前記第２認証情報に基づいて、前記第２端末装置を認証させ、
前記第１コード情報は、前記第２コード情報よりも先に撮影され、
前記第１認証情報および前記第２認証情報は、時限的な情報であり、
前記第１認証情報と比較して不正取得されることをより防止するために、前記第２認証情報の時限的な期間は、前記第１認証情報の時限的な期間よりも短い、
プログラム。
【請求項１１】
利用者によって使用される端末装置であるとして既に認証されている第１端末装置と、まだ認証されていない第２端末装置と通信可能な情報処理装置に、
前記第２端末装置からログイン要求があった場合に、第１認証情報がコード化された第１コード情報を生成させた後、前記第１認証情報とは異なる第２認証情報がコード化された第２コード情報を生成させ、
前記第１コード情報および前記第２コード情報を、前記第２端末装置に送信させ、
前記第１コード情報を撮影してデコードすることによって得られた前記第１認証情報および前記第２コード情報を撮影してデコードすることによって得られた前記第２認証情報を、前記第１端末装置から受信させ、
受信された前記第１認証情報および前記第２認証情報に基づいて、前記第２端末装置を認証させ、
前記第１コード情報は、前記第２コード情報よりも先に撮影され、
前記第１認証情報および前記第２認証情報は、時限的な情報であり、
前記第１認証情報と比較して不正取得されることをより防止するために、前記第２認証

情報の時限的な期間は、前記第１認証情報の時限的な期間よりも短い、
プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、情報処理方法、およびプログラムに関する。
【背景技術】
【０００２】
従来、ＳＭＳ（Short Message Service）を利用した認証サービスが知られている。例えば、特許文献１には、予め登録されたモバイル機器にＳＭＳ認証値を送信し、利用者にＳＭＳ認証値を入力されるための認証窓を表示し、利用者によって入力されたＳＭＳ認証値に基づいて本人認証を行う認証システムが提案されている。
【先行技術文献】
【特許文献】
【０００３】
【文献】特表２０１９－５１７０８７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、特許文献１に記載の技術では、フィッシングサイトなどでＳＭＳ認証値が盗まれると、フィッシング犯による不正ログインが行われる場合があった。
【０００５】
本発明は、このような事情を考慮してなされたものであり、他人による不正ログインを防止することができる情報処理装置、情報処理方法、およびプログラムを提供することを目的の一つとする。
【課題を解決するための手段】
【０００６】
本発明の一態様は、利用者によって使用される端末装置であるとして既に認証されている第１端末装置と、まだ認証されていない第２端末装置と通信可能な情報処理装置であって、前記第２端末装置からログイン要求があった場合に、第１認証情報がコード化された第１コード情報を生成した後、前記第１認証情報とは異なる第２認証情報がコード化された第２コード情報を生成するコード情報生成部と、前記コード情報生成部によって生成された前記第１コード情報および前記第２コード情報を、前記第１端末装置および前記第２端末装置のうちのいずれか一方に送信する送信部と、前記第１コード情報を撮影してデコードすることによって得られた前記第１認証情報および前記第２コード情報を撮影してデコードすることによって得られた前記第２認証情報を、前記第１端末装置および前記第２端末装置のうちのいずれか他方から受信する受信部と、前記受信部によって受信された前記第１認証情報および前記第２認証情報に基づいて、前記第２端末装置を認証する認証部と、を備える情報処理装置。
である。
【発明の効果】
【０００７】
本発明の一態様によれば、他人による不正ログインを防止することができる情報処理装置、情報処理方法、およびプログラムを提供することができる。
【図面の簡単な説明】
【０００８】
【図１】電子決済サービスが実現されるための構成の一例を示す図である。
【図２】電子決済の大まかな流れを例示した図である。
【図３】決済サーバ１００の構成図である。
【図４】利用者情報１７２の内容の一例を示す図である。

【図５】ログイン認証処理の一例を示すフローチャートである。
【図６】第１認証処理の一例を示すシーケンス図である。
【図７】ＱＲコードが表示された第１利用者端末装置１０Ａの表示画面の一例を示す図である。
【図８】第１実施形態に係る第２認証処理の一例を示すシーケンス図である。
【図９】ＱＲコードが表示された第２利用者端末装置１０Ｂの表示画面の一例を示す図である。
【図１０】第２実施形態に係る第２認証処理の一例を示すシーケンス図である。
【発明を実施するための形態】
【０００９】
以下、図面を参照し、本発明の情報処理装置、情報処理方法、およびプログラムについて説明する。情報処理装置は、一以上のプロセッサにより実現される。以下の説明では、情報処理装置は、電子決済サービスを提供するものとし、「決済サーバ」と称して説明するが、情報処理装置は、ショッピング、オークション、チャット、ミニブログ、その他の、ログインを伴う任意のサービスを提供するものであってもよい。電子決済サービスは、店舗における商品やサービスの購買に係る決済をサポートするサービスである。店舗とは、例えば、現実空間に存在する物理的な店舗（実店舗）である。
【００１０】
＜第１実施形態＞
［電子決済サービス］
図１は、電子決済サービスが実現されるための構成の一例を示す図である。電子決済サービスは、決済サーバ１００を中心として実現される。決済サーバ１００は、例えば、一以上の利用者端末装置１０、および一以上の店舗端末装置５０のそれぞれとネットワークＮＷを介して通信する。ネットワークＮＷは、例えば、インターネット、ＬＡＮ（Local Area Network）、無線基地局、プロバイダ装置などを含む。
【００１１】
利用者端末装置１０は、例えば、スマートフォンやタブレット端末等の可搬型端末装置である。利用者端末装置１０は、少なくとも、光学読取機能、通信機能、表示機能、入力受付機能、プログラム実行機能を有するコンピュータ装置である。以下の説明では、これらの機能を実現するための構成をそれぞれカメラ、通信装置、タッチパネル、ＣＰＵ（Central Processing Unit）等と称する。利用者端末装置１０では、ＣＰＵ等のプロセッサにより決済アプリ２０が実行されることで、決済サーバ１００と連携して電子決済サービスを利用者に提供するように動作する。決済アプリ２０は、カメラ、通信装置、タッチパネルなどを制御する。
【００１２】
店舗端末装置５０は、例えば、店舗に設置される。店舗端末装置５０は、少なくとも、商品価格取得機能、光学読取機能、プログラム実行機能、通信機能を有するコンピュータ装置である。店舗端末装置５０は、いわゆるＰＯＳ（Point of Sale）装置を含み、ＰＯＳ装置によって商品価格取得機能や光学読取機能を実現してもよい。店舗コード画像６０は、店舗に置かれ、ＱＲコード（登録商標）等のコード画像が紙やプラスチックの媒体に印刷されたものである。なお、店舗コード画像６０は、店舗に置かれたディスプレイによって表示されてもよい。
【００１３】
決済サーバ１００は、利用者端末装置１０または店舗端末装置５０から受信した決済情報に基づいて電子決済を実現する。決済サーバ１００は、例えば、利用者ＩＤに対応付けて管理しているチャージ残高を増減させる（換言すると、電子マネーを入出金する）ことで、電子決済を行う。電子決済は、リボ払いやクレジット払い等の方法によって、購買時点のチャージ残高よりも多額の購買を可能にするものが含まれてよい。
【００１４】
図２は、電子決済の大まかな流れを例示した図である。電子決済には、パターン１とパ

ターン２の二つが存在してよい。パターン１の場合、まず利用者端末装置１０において決済アプリ２０が起動し、ＱＲコードやバーコード等のコード画像を表示する。利用者は利用者端末装置１０の表示面を店舗端末装置５０に翳す（提示する）。店舗端末装置５０は、光学読取機能によってコード画像をデコードし、アカウントＩＤ等の情報を取得する。そして、店舗端末装置５０は、アカウントＩＤ、決済金額、店舗ＩＤ等を含む決済情報を生成し、決済サーバ１００に送信する。決済金額の情報は、予めバーコード読み取りや手入力等によって取得されている。決済サーバ１００は、受信した情報に基づいて、ユーザの電子決済口座から店舗の電子決済口座に決済金額を移動させて決済処理を完了させる。

【００１５】

パターン２の場合、決済アプリ２０が起動した状態の利用者端末装置１０が、光学読取機能によって店舗コード画像６０をデコードする。店舗コード画像６０には、店舗名等の情報が含まれている。利用者は、店舗名等が表示された画面において、決済金額を利用者端末装置１０に入力する。そして、利用者端末装置１０は、アカウントＩＤ、決済金額、店舗ＩＤ等を含む決済情報を生成し、決済サーバ１００に送信する。決済サーバ１００は、受信した情報に基づいて決済処理を行う。なお、上記のいずれかのパターンでのみ電子決済が行われてもよい。また、図２で説明する「アカウントＩＤ」は、利用者の識別情報として用いられ得る他の情報（例えば電話番号）であってもよい。

【００１６】

［決済サーバ］

図３は、決済サーバ１００の構成図である。決済サーバ１００は、例えば、通信部１１０と、決済コンテンツ提供部１２０と、決済処理部１２２と、コード情報生成部１２４と、判定部１２６と、認証部１２８と、情報管理部１３０と、記憶部１７０とを備える。通信部１１０および記憶部１７０以外の構成要素は、例えば、ＣＰＵなどのハードウェアプロセッサがプログラム（ソフトウェア）を実行することにより実現される。これらの構成要素のうち一部または全部は、ＬＳＩ（Large Scale Integration）やＡＳＩＣ（Application Specific Integrated Circuit）、ＦＰＧＡ（Field-Programmable Gate Array）、ＧＰＵ（Graphics Processing Unit）などのハードウェア（回路部；circuitryを含む）によって実現されてもよいし、ソフトウェアとハードウェアの協働によって実現されてもよい。プログラムは、予めＨＤＤ（Hard Disk Drive）やフラッシュメモリなどの記憶装置（非一過性の記憶媒体を備える記憶装置）に格納されていてもよいし、ＤＶＤやＣＤ－ＲＯＭなどの着脱可能な記憶媒体（非一過性の記憶媒体）に格納されており、記憶媒体がドライブ装置に装着されることで記憶装置にインストールされてもよい。

【００１７】

記憶部１７０は、ＨＤＤやフラッシュメモリ、ＲＡＭ（Random Access Memory）などである。記憶部１７０は、決済サーバ１００がネットワークを介してアクセス可能なＮＡＳ（Network Attached Storage）装置であってもよい。記憶部１７０には、利用者情報１７２、決済コンテンツ情報１７４などの情報が格納される。

【００１８】

通信部１１０は、ネットワークＮＷに接続するための通信インターフェースである。通信部１１０は、例えばネットワークインターフェースカードである。通信部１１０は、ネットワークＮＷを介して情報を送信する送信部としての機能と、ネットワークＮＷを介して情報を受信する受信部としての機能を備える。

【００１９】

決済コンテンツ提供部１２０は、例えば、Ｗｅｂサーバの機能を有し、電子決済サービスの各種画面を表示するための情報（コンテンツ）を利用者端末装置１０に提供する。決済コンテンツ提供部１２０は、決済コンテンツ情報１７４から適宜、必要なコンテンツを読み出して利用者端末装置１０に提供する。利用者端末装置１０は、決済アプリ２０によってコンテンツが再生された状態で利用者による各種入力を受け付け、前述した決済情報などを決済サーバ１００に送信する。

【００２０】

決済処理部１２２は、利用者端末装置１０または店舗端末装置５０により送信された決済情報に基づいて、決済処理を行う。決済処理部１２２は、利用者情報１７２を参照しながら決済処理を行う。

【００２１】

［利用者情報］

図４は、利用者情報１７２の内容の一例を示す図である。利用者情報１７２は、利用者の登録情報の一例である。利用者情報１７２は、例えば、アカウントＩＤ（省略されてもよい）に対して、新規登録時に最低限必要な電話番号およびパスワードの他、メールアドレス、利用者ＩＤ、デバイスＩＤ、チャージ残高、銀行口座、クレジットカード番号、チャージ履歴情報、および決済履歴情報などの情報が対応付けられたものである。電話番号、パスワード、デバイスＩＤ、チャージ残高、チャージ履歴情報、決済履歴情報以外の情報は任意設定情報である。以下、これらの情報が対応付けられた利用者のインスタンス（電子決済口座）のことをアカウントと称する。電話番号は、電子決済サービスのログインＩＤとして使用されてもよい。

【００２２】

利用者ＩＤは、決済サーバ１００が利用者を識別するための利用者識別情報の一例であり、利用者のニックネームなど、利用者が任意に設定できる情報である。デバイスＩＤは、決済サーバ１００が利用者端末装置１０を識別するための情報の一例である。例えば、デバイスＩＤは、ＩＭＥＩ（International Mobile Equipment Identifier）、利用者端末装置１０の製造業者に関する情報、ＯＳ（Operating System）のＩＤなどの情報を組み合わせて生成された情報であってよい。

【００２３】

チャージ残高は、利用者が予めアカウントに送金することで設定された電子マネーの残高を示す情報である。送金の手段としては、指定業者（銀行）のＡＴＭ（Automatic Teller Machine）からの送金、登録された銀行口座からの送金などがある。銀行口座とクレジットカード番号のそれぞれは、電子決済サービスに入金可能な銀行口座またはクレジットカード番号の情報（口座番号、カード番号）である。チャージ履歴情報は、利用者が予め電子決済サービスに送金してチャージ残高を増加させた履歴である。決済履歴情報は、利用者が行った決済の内訳（日時、購買行動が行われた店舗の店舗ＩＤ、決済金額等）を、決済ごとに示す情報である。

【００２４】

［フィッシングの手口］

利用者は、スマートフォンの機種変更を行った場合等、利用者によって使用される端末装置であるとして既に認証されている端末装置以外の端末装置を用いて電子決済サービスにログインしようとする場合がある。この場合、利用者が既存の端末装置から認証情報を入力することで、新規の端末装置の認証処理が行われる。しかしながら、他人によって認証情報が不正に取得されてしまうと、他人の端末装置から電子決済サービスに不正ログインされてしまう可能性がある。このため、本実施形態は、他人（例えば、フィッシング犯）によって不正ログインが行われることを防止することを目的としている。そこで、本実施形態の処理の詳細を説明する前に、フィッシングの手口について説明する。

【００２５】

フィッシングとは、利用者のログインＩＤ、パスワード、および認証コード等の情報を、インターネットを介して取得するために行われる詐欺行為である。近年、フィッシングサイトの数が急増し、ログインＩＤ、パスワード、および認証コード等の情報を奪われる被害者が後を絶たない。本実施形態は、ログイン強度を高めることで、フィッシング犯のログイン試行自体を削減させるとともに、フィッシング犯に対してフィッシングサイトの立ち上げ意欲自体を失わせることを目的とする。

【００２６】

フィッシング犯は、以下の流れで利用者のログインＩＤ（電話番号など）およびパスワードを取得する。

（１）フィッシング犯は、利用者に対して偽のログインサイトにアクセスさせ、ログインＩＤおよびパスワードを入力させる。
（２）フィッシング犯は、入力されたログインＩＤおよびパスワードを利用して、フィッシング犯の端末装置から正規のログインサイトへのログインを試みる。このとき、利用者の端末装置以外からのアクセスであるため、不正アクセスを防止するべく、認証コードを記載したメッセージがＳＭＳ（Short Message Service）等で利用者の端末装置に送信される。
（３）フィッシング犯は、偽のログインサイトにおいてＳＭＳで通知された認証コードを入力させる画面を表示させる。
（４）フィッシング犯は、利用者によって偽のログインサイトに入力された認証コードを、フィッシング犯の端末装置を用いて正規のログインサイトに入力してログインを完了する。

【００２７】

上記のフィッシング犯の手口においては、利用者が偽のログインサイトにおいて認証コードを入力してしまうことが問題である。そこで、本実施形態では、利用者によって使用される端末装置であるとして既に認証されている端末装置（既存環境）と、まだ認証されていない端末装置（新環境）とが、物理的に近くにある状況にのみ、新環境の端末装置でログインできるようにする。本実施形態の詳細を以下説明する。

【００２８】

［ログイン認証処理］

図５は、ログイン認証処理の一例を示すフローチャートである。本フローチャートによる処理は、決済サーバ１００によって実行される。まず、決済サーバ１００の通信部１１０は、利用者端末装置１０からログイン要求を受信する（Ｓ１１）。ログイン要求には、ログインＩＤ（電話番号など）、パスワード、およびデバイスＩＤなどの情報が含まれている。

【００２９】

次に、認証部１２８は、ログイン要求に含まれるログインＩＤ（電話番号など）およびパスワードと、利用者情報１７２とを比較して、ログイン認証が成功したか否かを判定する（Ｓ１２）。具体的に、認証部１２８は、ログイン要求に含まれるログインＩＤ（電話番号など）が利用者情報１７２に登録されており、ログイン要求に含まれるパスワードが、利用者情報１７２に含まれるパスワードと一致する場合には、ログイン認証が成功したと判定する。一方、認証部１２８は、ログイン要求に含まれるログインＩＤ（電話番号など）が利用者情報１７２に登録されていない、またはログイン要求に含まれるパスワードが、利用者情報１７２に含まれるパスワードと一致しない場合には、ログイン認証が失敗したと判定する。

【００３０】

認証部１２８は、ログイン認証が失敗したと判定した場合、ログイン失敗通知を利用者端末装置１０に送信し（Ｓ１３）、本フローチャートによる処理を終了する。

【００３１】

一方、認証部１２８は、ログイン認証が成功したと判定した場合、ログイン要求に含まれるデバイスＩＤと、利用者情報１７２とを比較して、新環境からのログインであるか否かを判定する（Ｓ１４）。ここで、新環境とは、利用者によって使用される端末装置であるとして認証されていない端末装置を意味する。また、既存環境とは、利用者によって使用される端末装置であるとして既に認証されている端末装置を意味する。

【００３２】

具体的に、認証部１２８は、ログイン要求に含まれるデバイスＩＤと、利用者情報１７２に含まれるデバイスＩＤとが一致しない場合には、新環境からのログインであると判定する。一方、認証部１２８は、ログイン要求に含まれるデバイスＩＤと、利用者情報１７２に含まれるデバイスＩＤとが一致する場合には、既存環境からのログインであると判定する。

【００３３】
認証部１２８は、新環境からのログインではないと判定した場合（すなわち、既存環境からのログインであると判定した場合）、ログイン成功通知を利用者端末装置１０に送信し（Ｓ１５）、本フローチャートによる処理を終了する。
【００３４】
一方、認証部１２８が新環境からのログインであると判定した場合、判定部１２６は、決済アプリ２０からのログインであるか否かを判定する（Ｓ１６）。認証部１２８は、決済アプリ２０からのログインであると判定した場合、後述する第１認証処理を実行する（Ｓ１７）。一方、認証部１２８は、決済アプリ２０からのログインではないと判定した場合、後述する第２認証処理を実行する（Ｓ１８）。決済アプリ２０からのログインではない場合は、例えば、ＷＥＢブラウザからのログインの場合である。
【００３５】
決済アプリ２０は、スマートフォンやタブレット端末など、カメラを搭載した端末装置にインストールされる。このため、決済アプリ２０からのログインである場合、ログイン要求を送信した利用者端末装置１０のカメラを用いる認証処理である第１認証処理が行われる。一方、決済アプリ２０からのログインではない場合（例えば、ＷＥＢブラウザからのログインの場合）、利用者端末装置１０にはカメラが搭載されていない可能性がある。このため、決済アプリ２０からのログインではない場合、ログイン要求を送信した利用者端末装置１０のカメラを用いない認証処理である第２認証処理が行われる。以下、第１認証処理および第２認証処理の詳細について説明する。
【００３６】
［第１認証処理］
図６は、第１認証処理の一例を示すシーケンス図である。本シーケンス図を説明するにあたり、利用者によって使用される端末装置であるとして既に認証されている端末装置（既存環境）を第１利用者端末装置１０Ａとし、まだ認証されていない端末装置（新環境）を第２利用者端末装置１０Ｂとする。以下、第２利用者端末装置１０Ｂから決済サーバ１００にログイン要求があった場合の第１認証処理について説明する。
【００３７】
まず、決済サーバ１００の通信部１１０は、既存環境である第１利用者端末装置１０ＡにＳＭＳ通知を送信する（Ｓ１０１）。ＳＭＳ通知は、利用者の電話番号を利用したショートメッセージによる通知である。ＳＭＳ通知には、決済アプリ２０を起動するためのＵＲＬ（Uniform Resource Locator）が含まれている。
【００３８】
第１利用者端末装置１０Ａは、決済サーバ１００からＳＭＳ通知を受信すると、決済アプリ２０を起動する（Ｓ１０２）。例えば、第１利用者端末装置１０Ａは、ＳＭＳ通知に含まれるＵＲＬが利用者によって選択されたことに応じて、決済アプリ２０を起動する。
【００３９】
次に、決済サーバ１００のコード情報生成部１２４は、認証情報がコード化されたＱＲコードを生成する（Ｓ１０３）。例えば、認証情報は、ワンタイムパスワード等の時限的な情報であってよい。また、コード情報生成部１２４は、生成されたＱＲコードを通信部１１０から第１利用者端末装置１０Ａに送信する（Ｓ１０４）。第１利用者端末装置１０Ａは、決済サーバ１００からＱＲコードを受信すると、決済アプリ２０の画面にＱＲコードを表示する（Ｓ１０５）。
【００４０】
図７は、ＱＲコードが表示された第１利用者端末装置１０Ａの表示画面の一例を示す図である。図７に示されるように、第１利用者端末装置１０Ａの表示画面には、ＱＲコードＣと、「新しい端末でＱＲコードを読み取ってください」というメッセージ等が表示される。
【００４１】
次に、新環境である第２利用者端末装置１０Ｂは、第１利用者端末装置１０Ａに表示さ

れたＱＲコードを撮影する（Ｓ１０６）。具体的に、利用者は、第２利用者端末装置１０Ｂのカメラを用いて、第１利用者端末装置１０Ａに表示されたＱＲコードを撮影する。

【００４２】

また、第２利用者端末装置１０Ｂは、撮影したＱＲコードをデコードすることにより、認証情報を取得する（Ｓ１０７）。そして、第２利用者端末装置１０Ｂは、取得した認証情報を決済サーバ１００に送信する（Ｓ１０８）。

【００４３】

決済サーバ１００の通信部１１０が第２利用者端末装置１０Ｂから認証情報を受信すると、決済サーバ１００の認証部１２８は、認証情報の照合処理を行う（Ｓ１０９）。具体的に、認証部１２８は、第１利用者端末装置１０Ａに送信したＱＲコードに含まれる認証情報と、第２利用者端末装置１０Ｂから受信した認証情報とが一致するか否かを判定する。認証部１２８は、第１利用者端末装置１０Ａに送信したＱＲコードに含まれる認証情報と、第２利用者端末装置１０Ｂから受信した認証情報とが一致しない場合、ログイン不許可通知を通信部１１０から第２利用者端末装置１０Ｂに送信する。

【００４４】

一方、認証部１２８は、第１利用者端末装置１０Ａに送信したＱＲコードに含まれる認証情報と、第２利用者端末装置１０Ｂから受信した認証情報とが一致する場合、ログイン許可通知を通信部１１０から第２利用者端末装置１０Ｂに送信する（Ｓ１１０）。これによって、新環境である第２利用者端末装置１０Ｂからのログインが許可されることとなる。

【００４５】

その後、情報管理部１３０は、利用者情報１７２の更新処理を行う（Ｓ１１１）。具体的に、情報管理部１３０は、第２利用者端末装置１０Ｂから送信されたログイン要求に含まれるデバイスＩＤ（すなわち、第２利用者端末装置１０Ｂのデバイスｉｄ）を、ログイン要求に含まれるログインＩＤ（電話番号など）に関連付けて利用者情報１７２に書き込む。

【００４６】

以上説明した第１認証処理によれば、第１利用者端末装置１０Ａに表示されたＱＲコードを第２利用者端末装置１０Ｂで撮影する必要がある。すなわち、第１利用者端末装置１０Ａおよび第２利用者端末装置１０Ｂが物理的に近くにある状況で認証を行う必要があるため、フィッシング犯による不正ログインを防止することができる。

【００４７】

［第２認証処理］

図８は、第１実施形態に係る第２認証処理の一例を示すシーケンス図である。前述の第１認証処理では、決済サーバ１００が第１利用者端末装置１０ＡにＱＲコードを送信することとしたが、第２認証処理では、決済サーバ１００が第２利用者端末装置１０ＢにＱＲコードを送信することとする。これは、第２利用者端末装置１０Ｂにカメラが搭載されていない可能性があるためである。以下、第２利用者端末装置１０Ｂから決済サーバ１００にログイン要求があった場合の第２認証処理について説明する。

【００４８】

まず、決済サーバ１００の通信部１１０は、既存環境である第１利用者端末装置１０ＡにＳＭＳ通知を送信する（Ｓ２０１）。前述したように、ＳＭＳ通知は、利用者の電話番号を利用したショートメッセージによる通知であり、ＳＭＳ通知には、決済アプリ２０を起動するためのＵＲＬが含まれている。

【００４９】

第１利用者端末装置１０Ａは、決済サーバ１００からＳＭＳ通知を受信すると、決済アプリ２０を起動する（Ｓ２０２）。例えば、第１利用者端末装置１０Ａは、ＳＭＳ通知に含まれるＵＲＬが利用者によって選択されたことに応じて、決済アプリ２０を起動する。

【００５０】

次に、決済サーバ１００のコード情報生成部１２４は、認証情報がコード化されたＱＲコードを生成する（Ｓ２０３）。例えば、認証情報は、ワンタイムパスワード等の時限的

な情報であってよい。また、コード情報生成部１２４は、生成されたＱＲコードを通信部１１０から第２利用者端末装置１０Ｂに送信する（Ｓ２０４）。新環境である第２利用者端末装置１０Ｂは、決済サーバ１００からＱＲコードを受信すると、第２利用者端末装置１０Ｂの表示部にＱＲコードを表示する（Ｓ２０５）。

【００５１】

図９は、ＱＲコードが表示された第２利用者端末装置１０Ｂの表示画面の一例を示す図である。図９に示されるように、第２利用者端末装置１０Ｂの表示画面には、ＱＲコードＣと、「既存の端末でＱＲコードを読み取ってください」というメッセージ等が表示される。

【００５２】

次に、既存環境である第１利用者端末装置１０Ａは、第２利用者端末装置１０Ｂに表示されたＱＲコードを撮影する（Ｓ２０６）。具体的に、利用者は、第１利用者端末装置１０Ａのカメラを用いて、第２利用者端末装置１０Ｂに表示されたＱＲコードを撮影する。

【００５３】

また、第１利用者端末装置１０Ａは、撮影したＱＲコードをデコードすることにより、認証情報を取得する（Ｓ２０７）。そして、第１利用者端末装置１０Ａは、取得した認証情報を決済サーバ１００に送信する（Ｓ２０８）。

【００５４】

決済サーバ１００の通信部１１０が第１利用者端末装置１０Ａから認証情報を受信すると、決済サーバ１００の認証部１２８は、認証情報の照合処理を行う（Ｓ２０９）。具体的に、認証部１２８は、第２利用者端末装置１０Ｂに送信したＱＲコードに含まれる認証情報と、第１利用者端末装置１０Ａから受信した認証情報とが一致するか否かを判定する。認証部１２８は、第２利用者端末装置１０Ｂに送信したＱＲコードに含まれる認証情報と、第１利用者端末装置１０Ａから受信した認証情報とが一致しない場合、ログイン不許可通知を通信部１１０から第２利用者端末装置１０Ｂに送信する。

【００５５】

一方、認証部１２８は、第２利用者端末装置１０Ｂに送信したＱＲコードに含まれる認証情報と、第１利用者端末装置１０Ａから受信した認証情報とが一致する場合、ログイン許可通知を通信部１１０から第２利用者端末装置１０Ｂに送信する（Ｓ２１０）。これによって、新環境である第２利用者端末装置１０Ｂからのログインが許可されることとなる。

【００５６】

その後、情報管理部１３０は、利用者情報１７２の更新処理を行う（Ｓ２１１）。具体的に、情報管理部１３０は、第２利用者端末装置１０Ｂから送信されたログイン要求に含まれるデバイスＩＤ（すなわち、第２利用者端末装置１０Ｂのデバイスｉｄ）を、ログイン要求に含まれるログインＩＤ（電話番号など）に関連付けて利用者情報１７２に書き込む。

【００５７】

以上説明した第２認証処理によれば、第２利用者端末装置１０Ｂに表示されたＱＲコードを第１利用者端末装置１０Ａで撮影する必要がある。すなわち、第１利用者端末装置１０Ａおよび第２利用者端末装置１０Ｂが物理的に近くにある状況で認証を行う必要があるため、フィッシング犯による不正ログインを防止することができる。また、新環境である第２利用者端末装置１０Ｂにカメラが搭載されていない場合であっても、不正ログインを防止することができる。

【００５８】

以上説明したように、第１実施形態の決済サーバ１００（情報処理装置）は、コード情報生成部１２４と、通信部１１０と、認証部１２８と、判定部１２６とを備える。コード情報生成部１２４は、第２利用者端末装置１０Ｂからログイン要求があった場合に、認証情報がコード化されたＱＲコード（コード情報）を生成する。通信部１１０は、生成されたＱＲコードを、第１利用者端末装置１０Ａおよび第２利用者端末装置１０Ｂのうちのいずれか一方に送信するとともに、ＱＲコードを撮影してデコードすることによって得られ

た認証情報を、第１利用者端末装置１０Ａおよび第２利用者端末装置１０Ｂのうちのいずれか他方から受信する。認証部１２８は、受信された認証情報に基づいて、第２利用者端末装置１０Ｂを認証する。判定部１２６は、第２利用者端末装置１０Ｂのログイン方法に応じて、第１利用者端末装置１０Ａおよび第２利用者端末装置１０ＢのうちのどちらにＱＲコードを送信するのかを判定する。これによって、他人による不正ログインを防止することができる。

【００５９】

また、第１実施形態において、判定部１２６は、第２利用者端末装置１０Ｂからのログイン要求が決済アプリ２０からのログイン要求であるか否かに応じて、第１利用者端末装置１０Ａおよび第２利用者端末装置１０ＢのうちのどちらにＱＲコードを送信するのかを判定することとした。具体的に、第２利用者端末装置１０Ｂからのログイン要求が決済アプリ２０からのログイン要求である場合、判定部１２６は、第１利用者端末装置１０ＡにＱＲコードを送信すると判定し、第２利用者端末装置１０Ｂからのログイン要求が決済アプリ２０からのログイン要求ではない場合、判定部１２６は、第１利用者端末装置１０ＡにＱＲコードを送信すると判定することとした。決済アプリ２０からのログイン要求である場合は、第２利用者端末装置１０Ｂがカメラ機能を持つ携帯端末装置であると推定されるが、決済アプリ２０からのログイン要求ではない場合は、ＷＥＢブラウザを経由してのログインであって、第２利用者端末装置１０Ｂがカメラ機能を持たないＰＣ（Personal Computer）等であると推定されるためである。これによって、カメラが搭載された利用者端末装置１０によってＱＲコードの撮影が確実行われることとなり、認証処理を確実に行うことができる。

【００６０】

また、第１実施形態において、通信部１１０は、コード情報生成部１２４によるＱＲコードの生成に先立って、決済アプリ２０を起動するためのアドレスが記載されたＳＭＳ通知を第１利用者端末装置１０Ａに送信することとした。これによって、第１利用者端末装置１０Ａにおいて遅滞なく決済アプリ２０を起動させることができる。

【００６１】

＜第２実施形態＞

前述の第１実施形態では、ＱＲコードによる認証を１回だけ行うこととした。一方、第２実施形態では、ＱＲコードによる認証を複数回行うことで、セキュリティをより強化することとする。

【００６２】

図８のＳ２０５に示されるように、第１実施形態の第２認証処理においては、第２利用者端末装置１０ＢにＱＲコードを表示することとした。しかしながら、フィッシング犯がこのＱＲコードを偽のログインサイトに表示し、表示されたＱＲコードを利用者が既存環境の利用者端末装置で撮影すると、フィッシング犯の端末装置で不正ログインされる可能性がある。このため、第２利用者端末装置１０ＢにＱＲコードを表示する際には、できるだけ短時間かつ複数回表示させることが好ましい。なお、第２実施形態の第１認証処理は、第１実施形態の第１認証処理と同じであるため説明を省略する。以下、第２実施形態の詳細について説明する。

【００６３】

図１０は、第２実施形態に係る第２認証処理の一例を示すシーケンス図である。以下、第２利用者端末装置１０Ｂから決済サーバ１００にログイン要求があった場合の第２認証処理について説明する。

【００６４】

まず、決済サーバ１００の通信部１１０は、既存環境である第１利用者端末装置１０ＡにＳＭＳ通知を送信する（Ｓ３０１）。前述したように、ＳＭＳ通知は、利用者の電話番号を利用したショートメッセージによる通知であり、ＳＭＳ通知には、決済アプリ２０を起動するためのＵＲＬが含まれている。

【００６５】

第１利用者端末装置１０Ａは、決済サーバ１００からＳＭＳ通知を受信すると、決済アプリ２０を起動する（Ｓ３０２）。例えば、第１利用者端末装置１０Ａは、ＳＭＳ通知に含まれるＵＲＬを利用者が選択することに応じて、決済アプリ２０を起動する。

【００６６】

次に、決済サーバ１００のコード情報生成部１２４は、第１認証情報がコード化された第１ＱＲコードを生成する（Ｓ３０３）。例えば、第１認証情報は、ワンタイムパスワード等の時限的な情報であってよい。また、コード情報生成部１２４は、生成された第１ＱＲコードを通信部１１０から第２利用者端末装置１０Ｂに送信する（Ｓ３０４）。

【００６７】

新環境である第２利用者端末装置１０Ｂは、決済サーバ１００から第１ＱＲコードを受信すると、第２利用者端末装置１０Ｂの表示部に第１ＱＲコードを表示する（Ｓ３０５）。このとき、第２利用者端末装置１０Ｂは、第１ＱＲコードを第１時間（例えば、３０秒間）だけ表示する。例えば、第２利用者端末装置１０Ｂは、Ｓ３０４において、第１ＱＲコードとともに第１時間に関する情報を決済サーバ１００から受信し、受信した第１時間に関する情報に応じた時間だけ、第１ＱＲコードを表示してよい。

【００６８】

次に、既存環境である第１利用者端末装置１０Ａは、第２利用者端末装置１０Ｂに表示された第１ＱＲコードを撮影する（Ｓ３０６）。具体的に、利用者は、第１利用者端末装置１０Ａのカメラを用いて、第２利用者端末装置１０Ｂに表示された第１ＱＲコードを撮影する。

【００６９】

また、第１利用者端末装置１０Ａは、撮影した第１ＱＲコードをデコードすることにより、第１認証情報を取得する（Ｓ３０７）。そして、第１利用者端末装置１０Ａは、取得した第１認証情報を決済サーバ１００に送信する（Ｓ３０８）。

【００７０】

決済サーバ１００の通信部１１０が第１利用者端末装置１０Ａから第１認証情報を受信すると、決済サーバ１００の認証部１２８は、第１認証情報の照合処理を行う（Ｓ３０９）。具体的に、認証部１２８は、第２利用者端末装置１０Ｂに送信した第１ＱＲコードに含まれる第１認証情報と、第１利用者端末装置１０Ａから受信した第１認証情報とが一致するか否かを判定する。認証部１２８は、第２利用者端末装置１０Ｂに送信した第１ＱＲコードに含まれる第１認証情報と、第１利用者端末装置１０Ａから受信した第１認証情報とが一致しない場合、ログイン不許可通知を通信部１１０から第２利用者端末装置１０Ｂに送信する。

【００７１】

一方、コード情報生成部１２４は、第２利用者端末装置１０Ｂに送信した第１ＱＲコードに含まれる第１認証情報と、第１利用者端末装置１０Ａから受信した第１認証情報とが一致する場合、第１認証情報とは異なる第２認証情報がコード化された第２ＱＲコードを生成する（Ｓ３１０）。例えば、第２認証情報は、ワンタイムパスワード等の時限的な情報であってよい。また、コード情報生成部１２４は、生成された第２ＱＲコードを通信部１１０から第２利用者端末装置１０Ｂに送信する（Ｓ３１１）。

【００７２】

新環境である第２利用者端末装置１０Ｂは、決済サーバ１００から第２ＱＲコードを受信すると、第２利用者端末装置１０Ｂの表示部に第２ＱＲコードを表示する（Ｓ３１２）。このとき、第２利用者端末装置１０Ｂは、第２ＱＲコードを第１時間よりも短い第２時間（例えば、５秒間）だけ表示する。例えば、第２利用者端末装置１０Ｂは、Ｓ３１１において、第２ＱＲコードとともに第２時間に関する情報を決済サーバ１００から受信し、受信した第２時間に関する情報に応じた時間だけ、第２ＱＲコードを表示してよい。

【００７３】

なお、Ｓ３０６で第１ＱＲコードを撮影する際には、１回目の撮影であるためカメラ機能の起動時間を考慮して、比較的長い時間（例えば、３０秒間）第１ＱＲコードを表示す

ることとした。一方、Ｓ３１３で第２ＱＲコードを撮影する際には、既にカメラ機能が起動しているため、第２ＱＲコードの表示時間を短時間（例えば、５秒間）にすることとした。これによって、第２認証情報がフィッシング犯に不正取得されることをより確実に防止することができる。

【００７４】

次に、既存環境である第１利用者端末装置１０Ａは、第２利用者端末装置１０Ｂに表示された第２ＱＲコードを撮影する（Ｓ３１３）。具体的に、利用者は、第１利用者端末装置１０Ａのカメラを用いて、第２利用者端末装置１０Ｂに表示された第２ＱＲコードを撮影する。

【００７５】

また、第１利用者端末装置１０Ａは、撮影した第２ＱＲコードをデコードすることにより、第２認証情報を取得する（Ｓ３１４）。そして、第１利用者端末装置１０Ａは、取得した第２認証情報を決済サーバ１００に送信する（Ｓ３１５）。

【００７６】

決済サーバ１００の通信部１１０が第１利用者端末装置１０Ａから第２認証情報を受信すると、決済サーバ１００の認証部１２８は、第２認証情報の照合処理を行う（Ｓ３１６）。具体的に、認証部１２８は、第２利用者端末装置１０Ｂに送信した第２ＱＲコードに含まれる第２認証情報と、第１利用者端末装置１０Ａから受信した第２認証情報とが一致するか否かを判定する。認証部１２８は、第２利用者端末装置１０Ｂに送信した第２ＱＲコードに含まれる第２認証情報と、第１利用者端末装置１０Ａから受信した第２認証情報とが一致しない場合、ログイン不許可通知を通信部１１０から第２利用者端末装置１０Ｂに送信する。

【００７７】

一方、認証部１２８は、第２利用者端末装置１０Ｂに送信した第２ＱＲコードに含まれる第２認証情報と、第１利用者端末装置１０Ａから受信した第２認証情報とが一致する場合、ログイン許可通知を通信部１１０から第２利用者端末装置１０Ｂに送信する（Ｓ３１７）。これによって、新環境である第２利用者端末装置１０Ｂからのログインが許可されることとなる。

【００７８】

その後、情報管理部１３０は、利用者情報１７２の更新処理を行う（Ｓ３１８）。具体的に、情報管理部１３０は、第２利用者端末装置１０Ｂから送信されたログイン要求に含まれるデバイスＩＤ（すなわち、第２利用者端末装置１０Ｂのデバイスｉｄ）を、ログイン要求に含まれるログインＩＤ（電話番号など）に関連付けて利用者情報１７２に書き込む。

【００７９】

以上説明した第２実施形態によれば、第１実施形態と同様に、他人による不正ログインを防止することができる。また、第２実施形態によれば、コード情報生成部１２４が、第１認証情報がコード化された第１ＱＲコード（第１コード情報）を生成した後、第１認証情報とは異なる第２認証情報がコード化された第２ＱＲコード（第２コード情報）を生成し、認証部１２８が、第１ＱＲコードに基づく認証および第２ＱＲコードに基づく認証の両方が成功した場合に、利用者によって使用される端末装置であるとして第２利用者端末装置１０Ｂを認証することとした。これによって、フィッシング犯による不正ログインをより確実に防止することができる。

【００８０】

また、第２実施形態によれば、第２ＱＲコード（第２コード情報）を撮影可能な時間が、第１ＱＲコード（第１コード情報）を撮影可能な時間よりも短いこととした。これによって、第２認証情報がフィッシング犯に不正取得されることをより確実に防止することができる。

【００８１】

なお、第２実施形態によれば、一例として第２認証処理において第１ＱＲコードおよび

第２ＱＲコードに基づく認証を行うこととしたが、これに限らない。例えば、第１認証処理において第１ＱＲコードおよび第２ＱＲコードに基づく認証を行ってもよい。これは、既存環境である第１利用者端末装置１０Ａで表示されたＱＲコードを、何等かの方法でフィッシング犯が撮影できたとしても、できるだけ短時間かつ複数回ＱＲコードを表示させることは、不正ログインを防止する上で有効だからである。この場合、決済サーバ１００の通信部１１０は、第１ＱＲコードおよび第２ＱＲコードを第１利用者端末装置１０Ａに送信し、第２利用者端末装置１０Ｂは、第１利用者端末装置１０Ａに表示された第１ＱＲコードおよび第２ＱＲコードを撮影し、決済サーバ１００の認証部１２８は、第１ＱＲコードに基づく認証および第２ＱＲコードに基づく認証の両方が成功した場合に、利用者によって使用される端末装置であるとして第２利用者端末装置１０Ｂを認証してもよい。

【００８２】

なお、第１実施形態および第２実施形態において、通信部１１０が、コード情報生成部１２４によるＱＲコードの生成に先立って、決済アプリ２０を起動するためのアドレスが記載されたＳＭＳ通知を第１利用者端末装置１０Ａに送信することとしたが、これに限らない。例えば、通信部１１０は、コード情報生成部１２４によるＱＲコードの生成に先立って、決済アプリ２０を起動するためのプッシュ通知を第１利用者端末装置１０Ａに送信してもよい。プッシュ通知は、第１利用者端末装置１０Ａに直接送信可能なメッセージであり、通知音とともに第１利用者端末装置１０Ａに表示される。この場合、利用者は、プッシュ通知に基づいて第１利用者端末装置１０Ａで決済アプリ２０を起動することとなる。

【００８３】

また、第１実施形態および第２実施形態においては、第１利用者端末装置１０Ａに決済アプリ２０がインストールされている前提で説明を行った。しかしながら、第１利用者端末装置１０Ａに決済アプリ２０がインストールされていない場合、通信部１１０は、決済アプリ２０をインストールさせるためのＳＭＳ通知を第１利用者端末装置１０Ａに送信してもよい。これによって、第１利用者端末装置１０Ａにおける決済アプリ２０の利用が可能となり、決済アプリ２０からのカメラ機能の起動等が可能となる。

【００８４】

また、第１実施形態および第２実施形態において、通信部１１０は、第２利用者端末装置１０ＢのＩＰ（Internet Protocol）アドレスに基づく位置情報またはログインの目的（例えば、ログインしようとするサービス）に関する情報を、第１利用者端末装置１０Ａに送信して表示させてもよい。これによって、第１利用者端末装置１０Ａを所有する利用者は、フィッシング犯による不正ログインが行われようとしているか否かを判断することができる。

【００８５】

また、第１実施形態および第２実施形態の認証処理に加えて、認証部１２８は、第１利用者端末装置１０Ａの位置情報および第２利用者端末装置１０Ｂの位置情報を取得し、第１利用者端末装置１０Ａと第２利用者端末装置１０Ｂとの間の距離が所定距離以内である場合に、第１利用者端末装置１０Ａおよび第２利用者端末装置１０Ｂを同一人物が操作していると判定してよい。位置情報は、例えば、ＧＰＳ（Global Positioning System）によって得られる情報であってよい。また、認証部１２８は、位置情報の他、第１利用者端末装置１０Ａおよび第２利用者端末装置１０Ｂから得られるセンサ情報（操作時の利用者端末装置の傾き度合いや、気温情報、湿度情報など）に基づいて、第１利用者端末装置１０Ａおよび第２利用者端末装置１０Ｂを同一人物が操作しているか否かを判定してよい。

【００８６】

なお、第１実施形態および第２実施形態において、決済サーバ１００が認証処理を行うこととしたが、これに限らない。例えば、決済サーバ１００とは別に、認証処理を行う情報処理装置としての認証サーバを構築してもよい。

【００８７】

以上、本発明を実施するための形態について実施形態を用いて説明したが、本発明はこうした実施形態に何等限定されるものではなく、本発明の要旨を逸脱しない範囲内におい

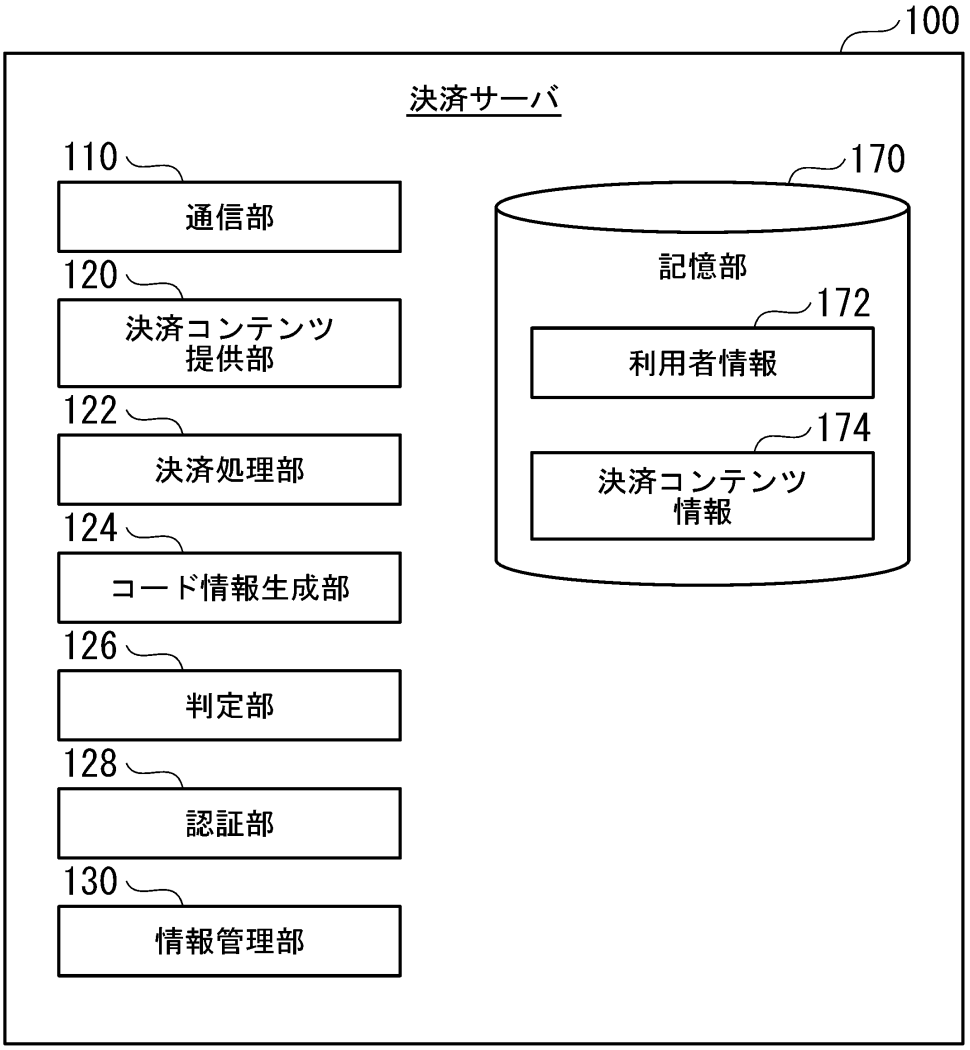
て種々の変形及び置換を加えることができる。

【符号の説明】

【００８８】

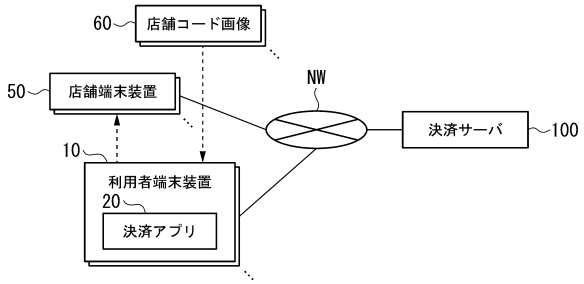
１０　利用者端末装置
２０　決済アプリ
５０　店舗端末装置
６０　店舗コード画像
１００　決済サーバ
１１０　通信部（送信部、受信部）
１２０　決済コンテンツ提供部
１２２　決済処理部
１２４　コード情報生成部
１２６　判定部
１２８　認証部
１３０　情報管理部
１７０　記憶部

【要約】
【課題】他人による不正ログインを防止することができる情報処理装置、情報処理方法、およびプログラムを提供すること。
【解決手段】利用者によって使用される端末装置であるとして既に認証されている第１端末装置と、まだ認証されていない第２端末装置と通信可能な情報処理装置であって、前記第２端末装置からログイン要求があった場合に、第１コード情報および第２コード情報を生成して前記第１端末装置および前記第２端末装置のうちのいずれか一方に送信し、前記第１コード情報を撮影してデコードすることによって得られた第１認証情報および前記第２コード情報を撮影してデコードすることによって得られた第２認証情報を、前記第１端末装置および前記第２端末装置のうちのいずれか他方から受信し、前記第１認証情報および前記第２認証情報に基づいて、前記第２端末装置を認証する情報処理装置。
【選択図】図３

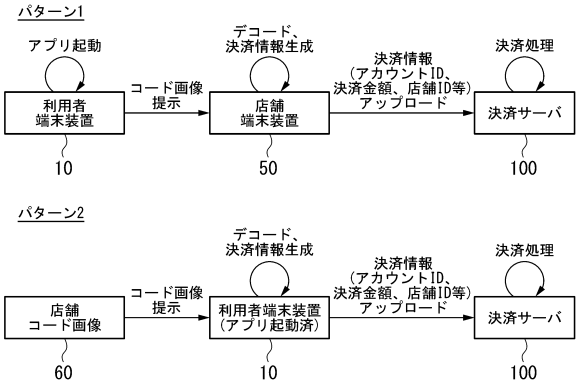


【図面】

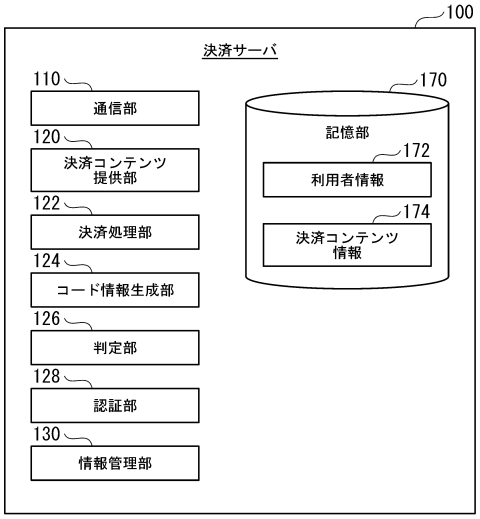
【図１】



【図２】



【図３】

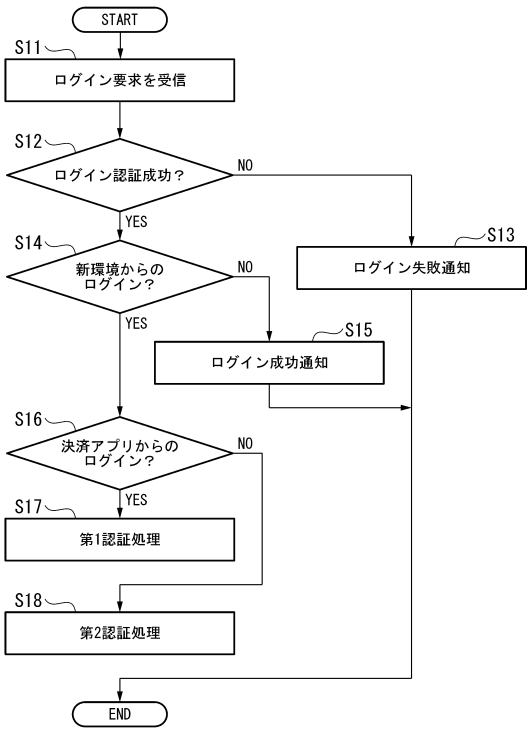


【図４】

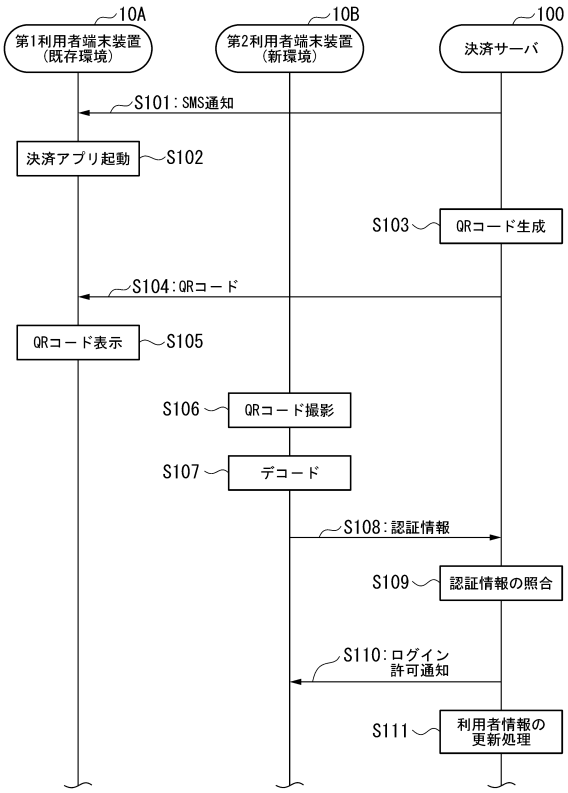
172

アカウントID	電話番号	パスワード	メールアドレス	利用者ID	デバイスID	チャージ残高	銀行口座	クレジットカード番号	チャージ履歴情報	決済履歴情報
001	090-****-****	AAAA1234	**@***.**	AAA	D001 D002	19,000円	…	…	チャージ履歴1 …	決済履歴1 …
002	070-****-****	BBBB9876	**@***.**	-	D003	6,400円	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…

【図５】


START
S11
ログイン要求を受信
S12
ログイン認証成功？
NO
YES
S13
ログイン失敗通知
S14
新環境からの
ログイン？
NO
YES
S15
ログイン成功通知
S16
決済アプリからの
ログイン？
NO
YES
S17
第1認証処理
S18
第2認証処理
END

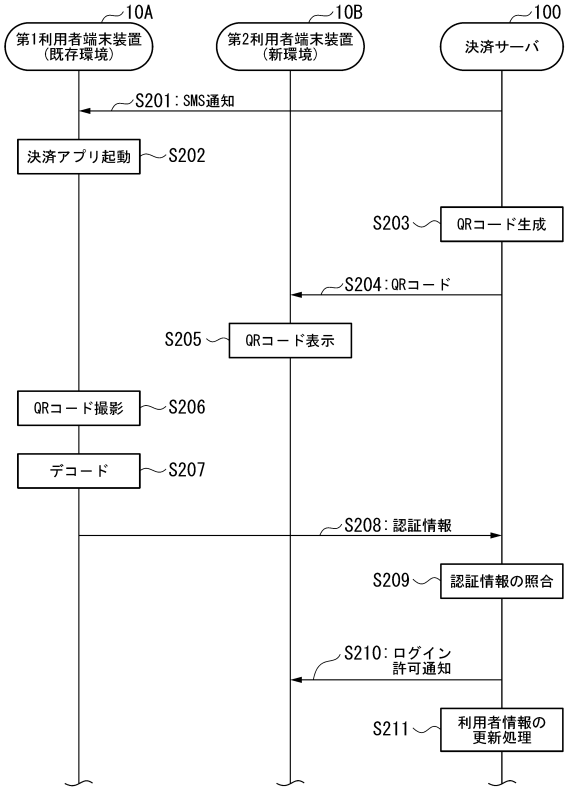
【図６】


10A
第1利用者端末装置
（既存環境）
10B
第2利用者端末装置
（新環境）
100
決済サーバ
S101：SMS通知
決済アプリ起動
S102
S103
QRコード生成
S104：QRコード
QRコード表示
S105
S106
QRコード撮影
S107
デコード
S108：認証情報
S109
認証情報の照合
S110：ログイン
許可通知
S111
利用者情報の
更新処理

【図７】


10A
C
新しい端末でQRコードを
読み取ってください
ログインを完了するには
QRコードによる認証が必要です

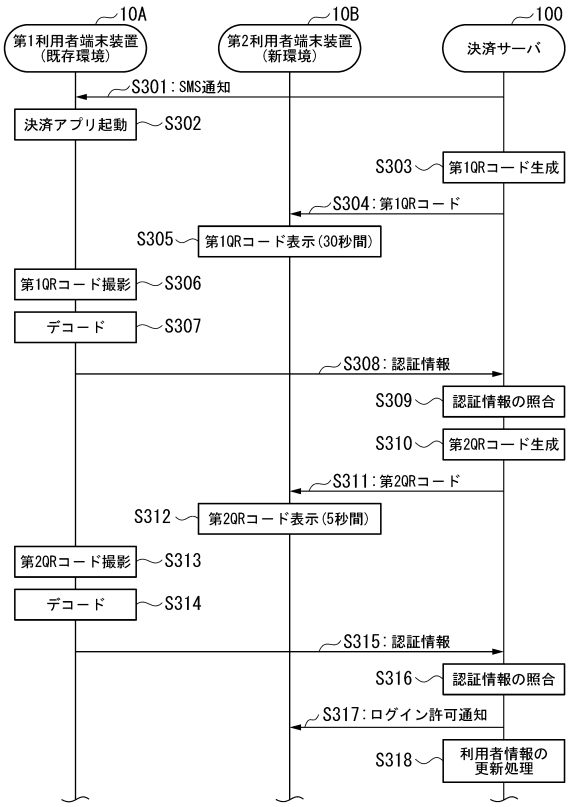
【図８】


10A
第1利用者端末装置
（既存環境）
10B
第2利用者端末装置
（新環境）
100
決済サーバ
S201：SMS通知
決済アプリ起動
S202
S203
QRコード生成
S204：QRコード
S205
QRコード表示
QRコード撮影
S206
デコード
S207
S208：認証情報
S209
認証情報の照合
S210：ログイン
許可通知
S211
利用者情報の
更新処理

【図９】


10B
C
既存の端末でQRコードを
読み取ってください
ログインを完了するには
QRコードによる認証が必要です

【図１０】


10A
第1利用者端末装置
(既存環境)
10B
第2利用者端末装置
(新環境)
100
決済サーバ
S301:SMS通知
決済アプリ起動
S302
S303
第1QRコード生成
S304:第1QRコード
S305
第1QRコード表示(30秒間)
第1QRコード撮影
S306
デコード
S307
S308:認証情報
S309
認証情報の照合
S310
第2QRコード生成
S311:第2QRコード
S312
第2QRコード表示(5秒間)
第2QRコード撮影
S313
デコード
S314
S315:認証情報
S316
認証情報の照合
S317:ログイン許可通知
S318
利用者情報の
更新処理

フロントページの続き

(56)参考文献 特開２０１４－０６３３９２（ＪＰ，Ａ）
特開２０２０－０３８６５９（ＪＰ，Ａ）
欧州特許出願公開第０２９２２０１０（ＥＰ，Ａ１）
特開２０１１－０７６５２０（ＪＰ，Ａ）
特開２０１６－２０１６６７（ＪＰ，Ａ）
特開２００５－１８２２９５（ＪＰ，Ａ）
特開２０１２－１８１６４５（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／４２
Ｇ０６Ｑ ２０／４０