

認証連携と法律

ファイ法律事務所
弁護士 安藤広人

アジェンダ

1. ドコモ口座事件
2. 本人確認と認証
3. ID連携

ドコモ口座事件

令和2年9月8日
金融庁

預金取扱金融機関 各位

スマホ決済等のサービスを利用した不正出金に関する注意喚起

1. 事案の概要

一部報道もなされておりますが、NTT ドコモが提供するスマホ決済等のサービス「ドコモ口座」を利用した口座振替による不正出金が複数の金融機関で発生しています。

2. 影響

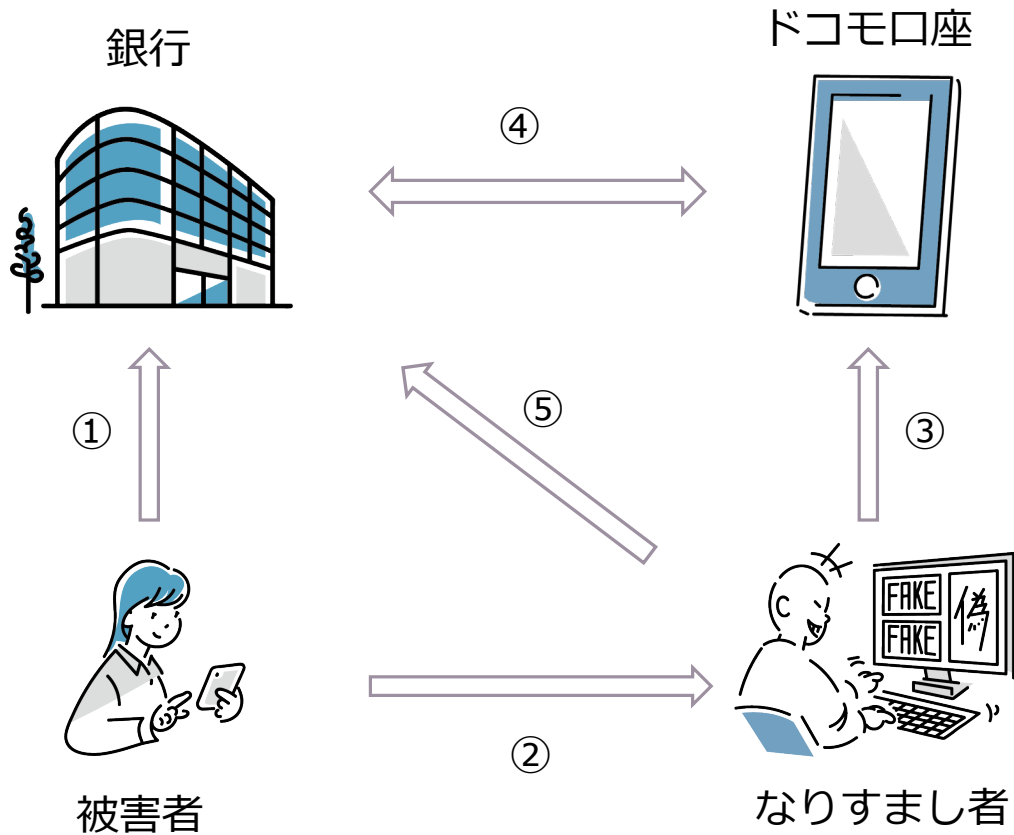
悪意のある第三者が預金者の名義でドコモ口座を開設し、銀行口座と連携した上でドコモ口座へ預金をチャージすることで不正な引出が発生します。

なお、ドコモ口座に銀行口座を連携させる際の手順が、各金融機関で異なっておりますが、不正に盗み出した銀行の口座番号やキャッシュカードの暗証番号等を用いることで、口座の連携が可能な金融機関で被害が発生していると考えられます。

金融庁ウェブサイトより

2020年 9月8日	金融庁、「ドコモ口座」を利用した口座振替による不正出金が複数の金融機関で発生しているとの注意喚起
9月10日	NTTドコモ、「ドコモ口座」への新規の銀行口座登録を停止 金融庁、NTTドコモに対して報告徴収命令
9月15日	金融庁、銀行及び資金移動業者に対して、セキュリティ強化の要請
9月28日	NTTドコモ、被害総額が11行219件、2848万円になったことを発表
10月28日	NTTドコモ、判明被害の補償完了 128件で2885万円

「ドコモ口座事件」関係図



①	被害者が、銀行口座を開設、取引
②	なりすまし者が、何らかの方法で銀行口座の情報（名義、口座番号、暗証番号等？）を入手
③	なりすまし者が、被害者に成りすまして「ドコモ口座」開設
④	「ドコモ口座」と被害者の銀行口座とを連携
⑤	なりすまし者が、被害者の銀行口座に送金指示し、ドコモ口座に資金を移動

イラスト：Loose Drawing

「ドコモ口座事件」への対応

2020年9月15日	金融庁、銀行及び資金移動業者に対して、セキュリティ強化の要請
11月30日	全銀協、「資金移動業者等との口座連携に関するガイドライン」の策定
2021年2月26日	金融庁、「事務ガイドライン（第三分冊：金融会社関係）」、「主要行等向けの総合的な監督指針」等の一部改正
2021年1月29日	NTTドコモ、「ドコモ口座」における銀行口座の新規登録および銀行口座からのチャージ再開

監督指針等の改正

主要行等向けの総合的な監督指針の改正（Ⅲ－３－９ 外部の決済サービス事業者等との連携）

連携サービス全体でのリスクの把握	連携サービスに係る不正取引を防止し、顧客保護を図る観点から、連携サービス提供事業者と協力し、連携サービス全体のリスクを継続的に把握・評価し、当該評価を踏まえ、一定のセキュリティ・レベルを維持するために体制・技術、両面での検討を行い、適切な対策を講じているか。また、連携サービス提供事業者が行うリスク評価や検証に係る作業に協力しているか。
連携サービス利用時の適切な認証	預金者へのなりすましによる不正取引を防ぐため、連携サービス提供事業者において実施している当該サービス利用者に対する取引時確認や預金者との同一性の確認の状況等を継続的に把握・評価し、当該評価を踏まえた適切なセキュリティ管理態勢を構築しているか。また、必要に応じて、連携サービス提供事業者の実施する預金者との同一性の確認などに協力しているか。
連携時の本人確認の実施	預金口座との連携を行う際に、固定式のID・パスワードによる本人認証に加えて、ハードウェアトークン・ソフトウェアトークンによる可変式パスワードを用いる方法や公的個人認証を用いる方法などで本人認証を実施するなど、実効的な要素を組み合わせた多要素認証等の導入により預金者へのなりすましを阻止する対策を導入しているか。

アジェンダ

1. ドコモ口座事件
2. **本人確認と認証**
3. ID連携

電子的な取引を開始する



事業者



電子的な取引を開始する

本人確認 (identity proofing)



本人確認書類



アカウントの発行

事業者



2回目以降の取引



事業者



2回目以降の取引

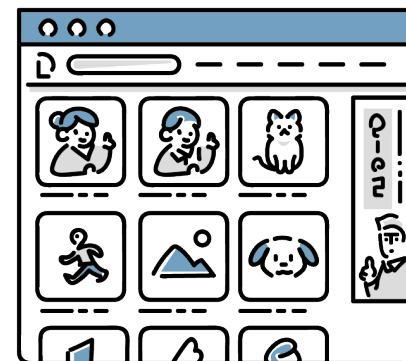
認証 (Authentication)



ID・パスワード



事業者



本人として認証



基本概念の整理

本人確認 (identity proofing)



本人確認書類



アカウントの発行

事業者



認証 (Authentication)



ID・パスワード

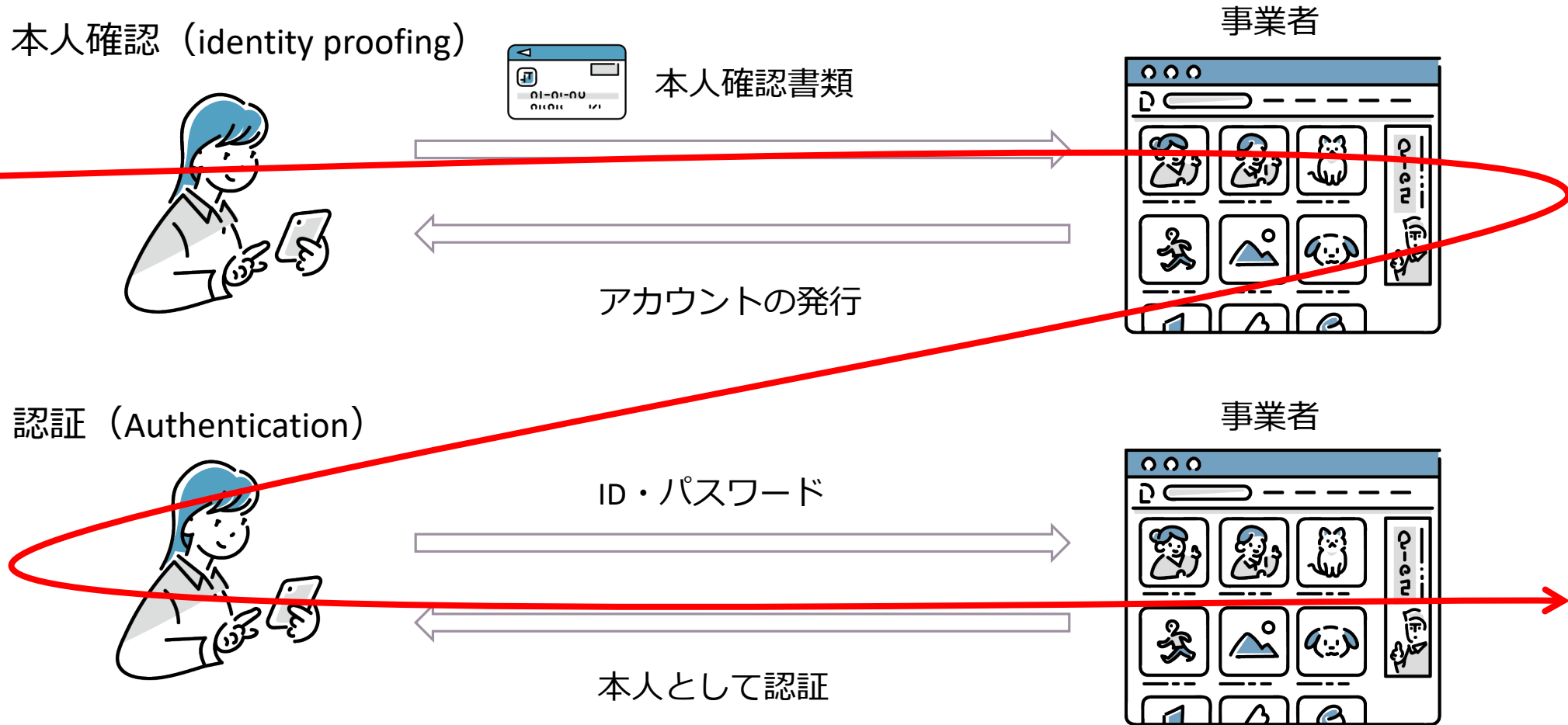


本人として認証

事業者



基本概念の整理



法令との関係

不正利用（なりすまし）対応の観点及び認証情報の利用の観点から法令で一定の規制

	不正利用対応		認証情報の利用
	通常時	インシデント発生後	
本人確認プロセス	<ul style="list-style-type: none"> ・ 犯収法、各業法による本人確認義務 ・ 各業法によるセキュリティ確保義務 	<ul style="list-style-type: none"> ・ なりすましと本人への効果帰属（民法） ・ 刑事上の保護（電子計算機使用詐欺等） 	<ul style="list-style-type: none"> ・ 個人情報保護法
認証プロセス	<ul style="list-style-type: none"> ・ 各業法によるセキュリティ確保義務 	<ul style="list-style-type: none"> ・ なりすましと本人への効果帰属（民法） ・ 刑事上の保護（電子計算機使用詐欺、不正アクセス禁止法等） 	<ul style="list-style-type: none"> ・ 個人情報保護法

セキュリティとの関係

それぞれのプロセスについて適切なセキュリティのレベルが選択される必要がある。

本人確認プロセス	LV 1 (IAL1)	身元識別情報が確認される必要がなく、身元確認の信用度がほとんどない。身元識別情報は、自己表明若しくは自己表明相当である。
	LV 2 (IAL2)	身元識別情報が遠隔又は対面で確認され、身元確認の信用度が相当程度ある。
	LV 3 (IAL3)	身元識別情報が特定された担当者の対面で確認され、身元確認の信用度が非常に高い。
認証プロセス	LV 1 (AAL1)	認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、単要素若しくは複数要素を使うことにより、本人認証の信用度がある程度ある。
	LV 2 (AAL2)	認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、複数要素を使うことにより、本人認証の信用度が相当程度ある。
	LV 3 (AAL3)	認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、耐タンパ性を有するハードウェアを含む複数要素を使うことにより、本人認証の信用度が非常に高い。

「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」より

アジェンダ

1. ドコモ口座事件
2. 本人確認と認証
3. **ID連携**

ソーシャルログインとID連携


キャンセル **zoom** ▾


メールアドレス


パスワード


サインイン

[パスワードをお忘れですか？](#)

 SSOでサインイン

 Appleでサインイン

 Googleでサインイン

 Facebookでサインイン

ログインの際に、ID・パスワードでのログイン以外に、他のSNSでサインインできることが示される。

ソーシャルログインとID連携



SNSを選択すると、注意喚起の画面が共有される。

ソーシャルログインとID連携


 Google にログイン



アカウントの選択

「Zoom」に移動

 安藤広人

 別のアカウントを使用

続行するにあたり、Google はあなたの名前、メールアドレス、言語設定、プロフィール写真を Zoom と共有します。このアプリを使用する前に、Zoom の [プライバシー ポリシー](#) と [利用規約](#) をご確認ください。

Googleからzoom側に共有される情報の内容とzoomのプライバシーポリシー、利用規約へのリンクが示される。

ソーシャルログインとID連携

 Google にログイン



安藤 広人



続行するには、まず本人確認を行ってください

パスワードを入力

パスワードを表示する

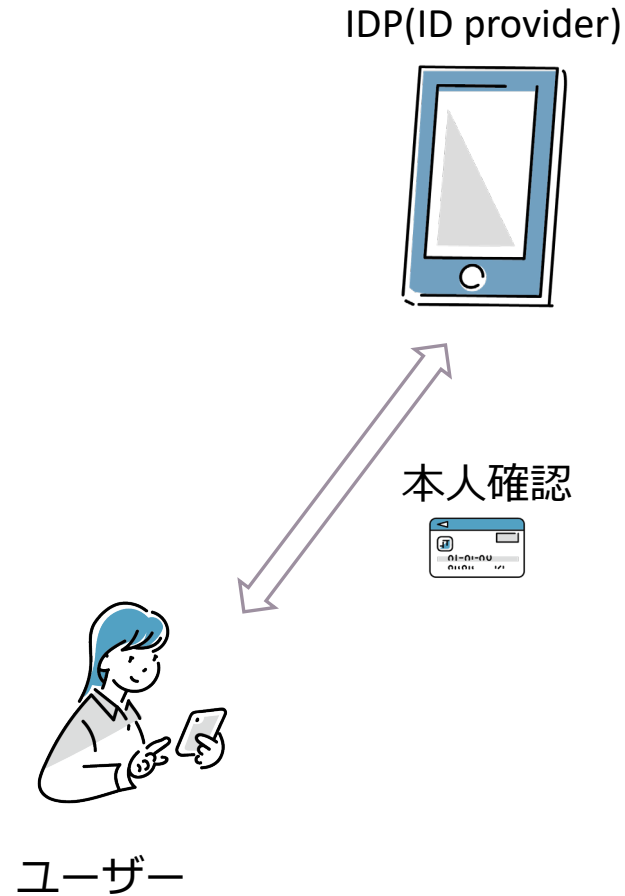
パスワードをお忘れの場合

次へ

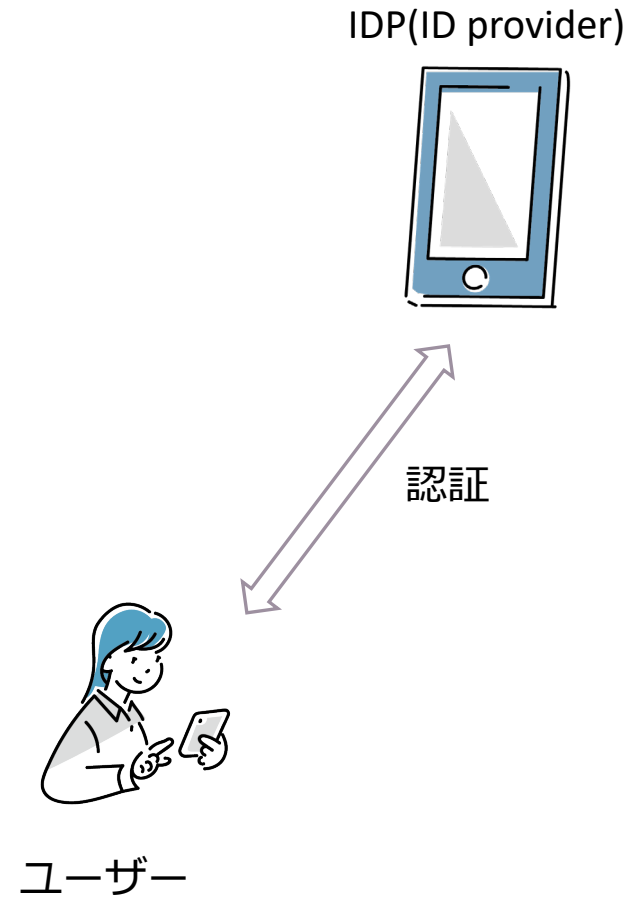
Googleのログイン画面が表示され、認証が成功するとzoomにもログインできる。

ID連携とセキュリティ

ID連携：利用者のID情報及びそれに付随する属性情報を連携して交換する仕組み



ID連携とセキュリティ

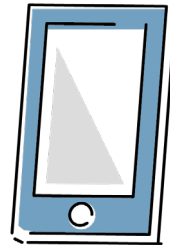


ID連携とセキュリティ

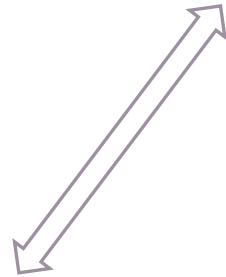
SP(service provider)



IDP(ID provider)



ユーザー

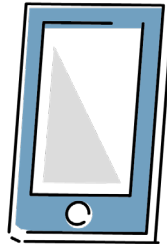


ID連携とセキュリティ

SP(service provider)



IDP(ID provider)

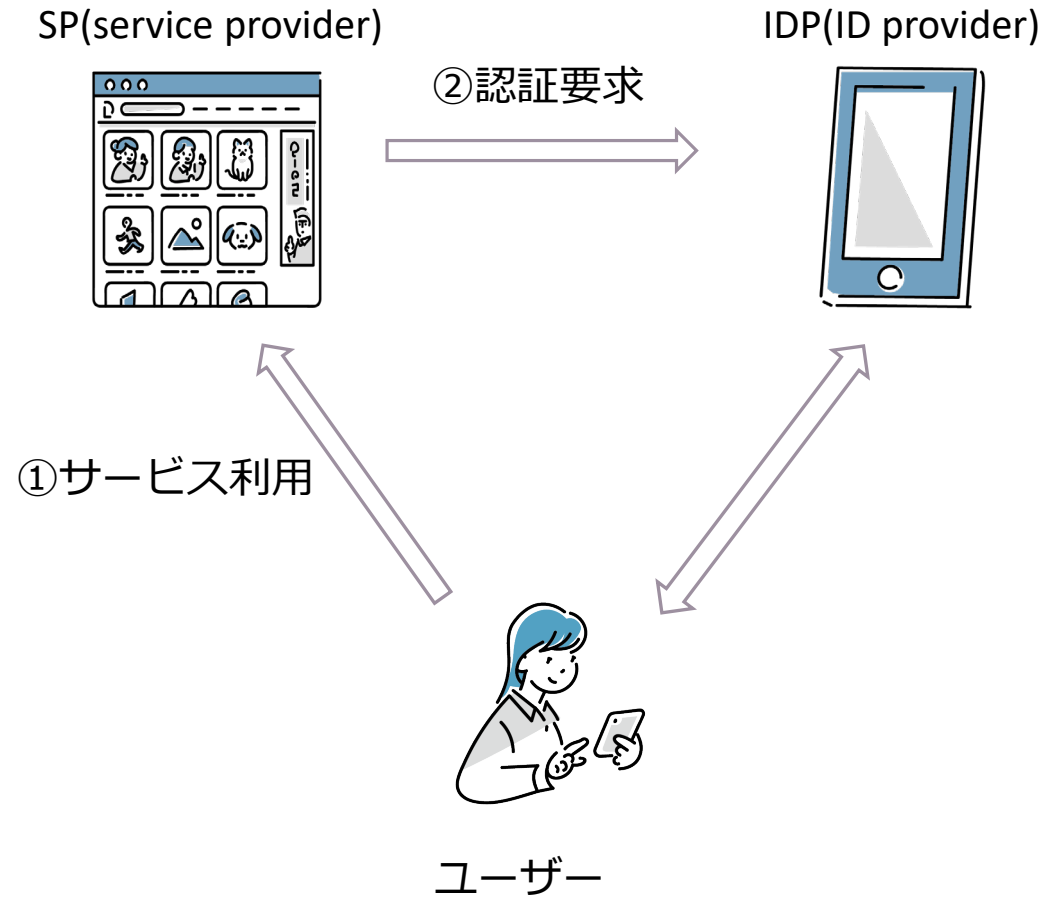


① サービス利用

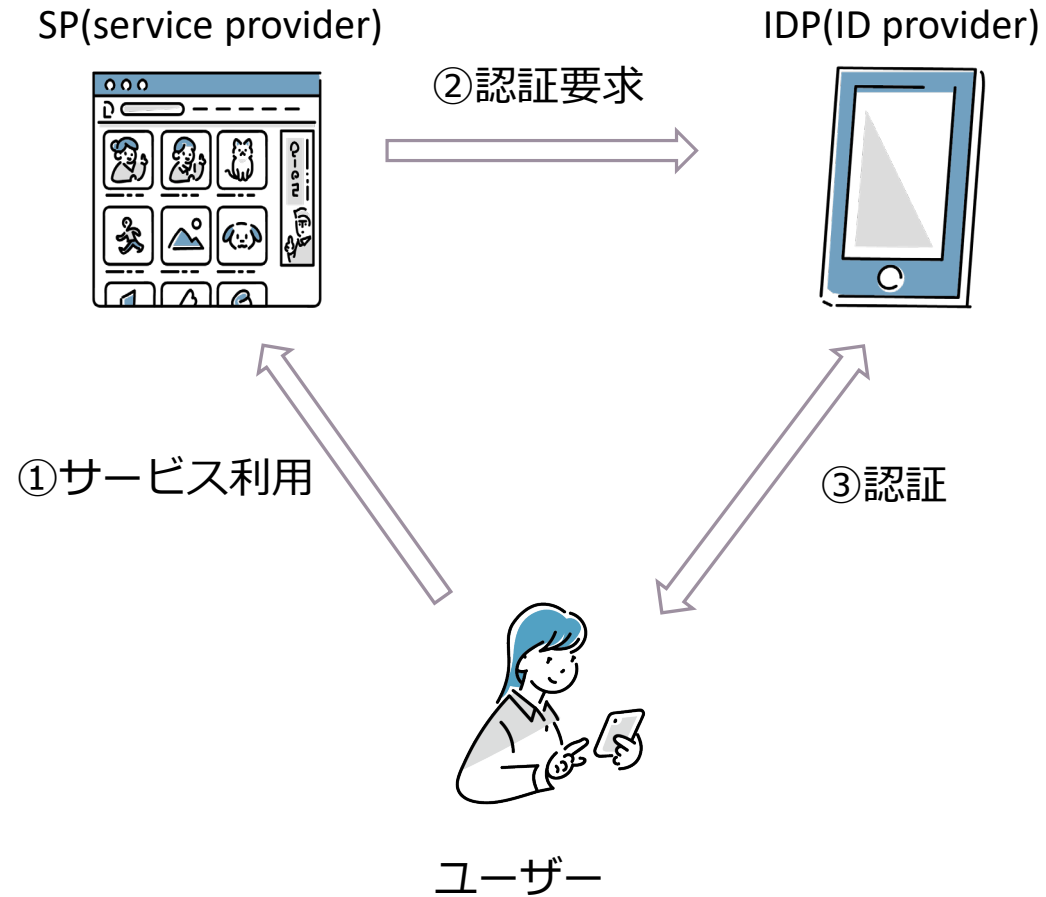


ユーザー

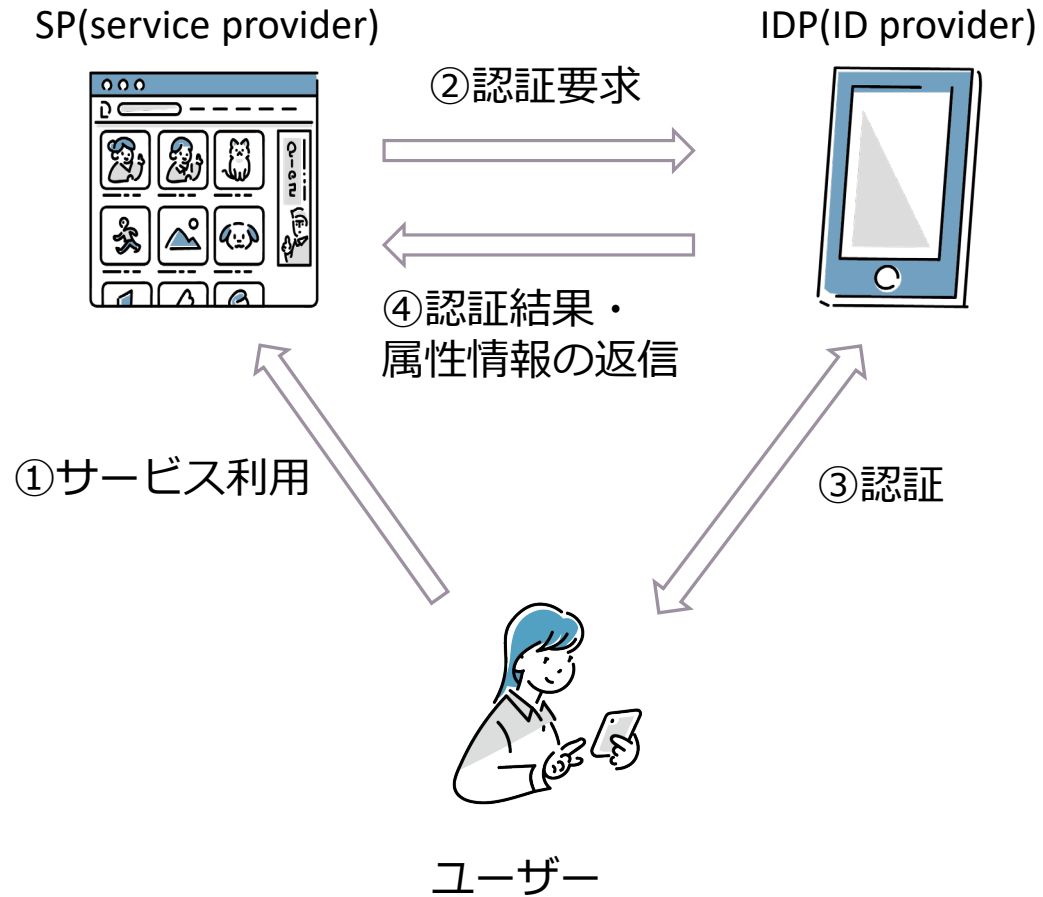
ID連携とセキュリティ



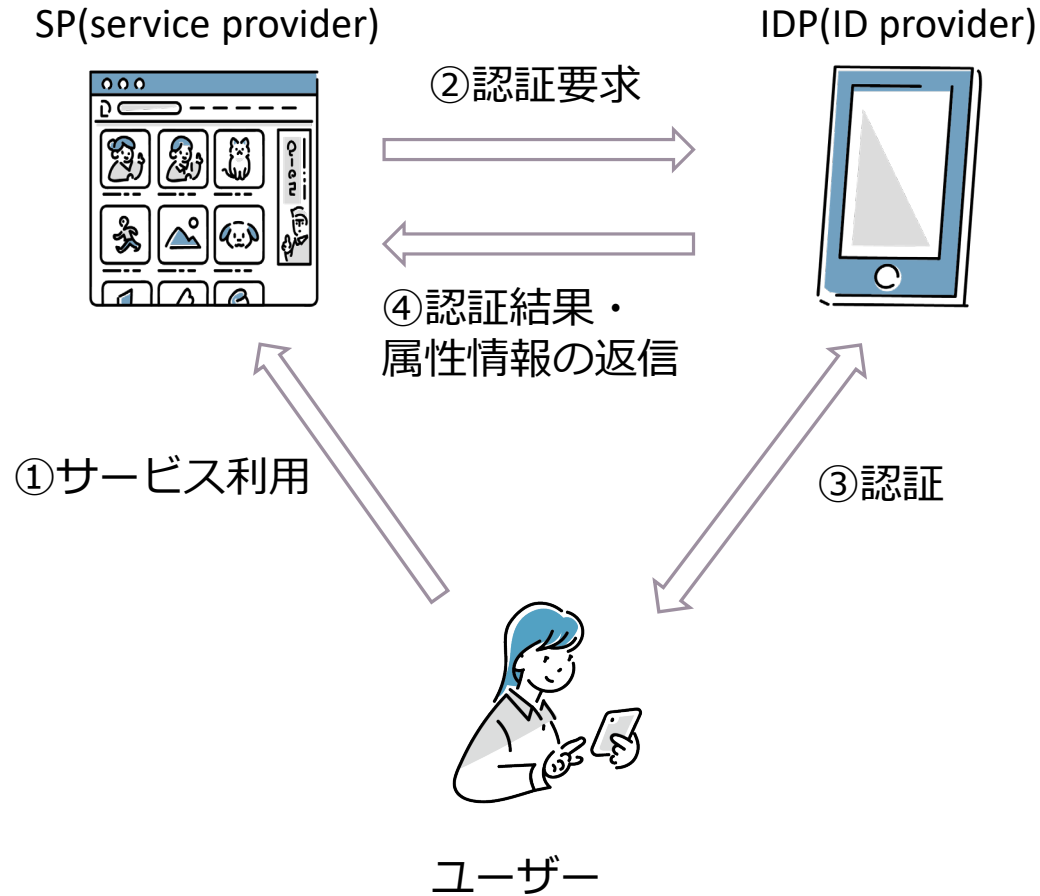
ID連携とセキュリティ



ID連携とセキュリティ



ID連携とセキュリティ



ユーザー側のメリット

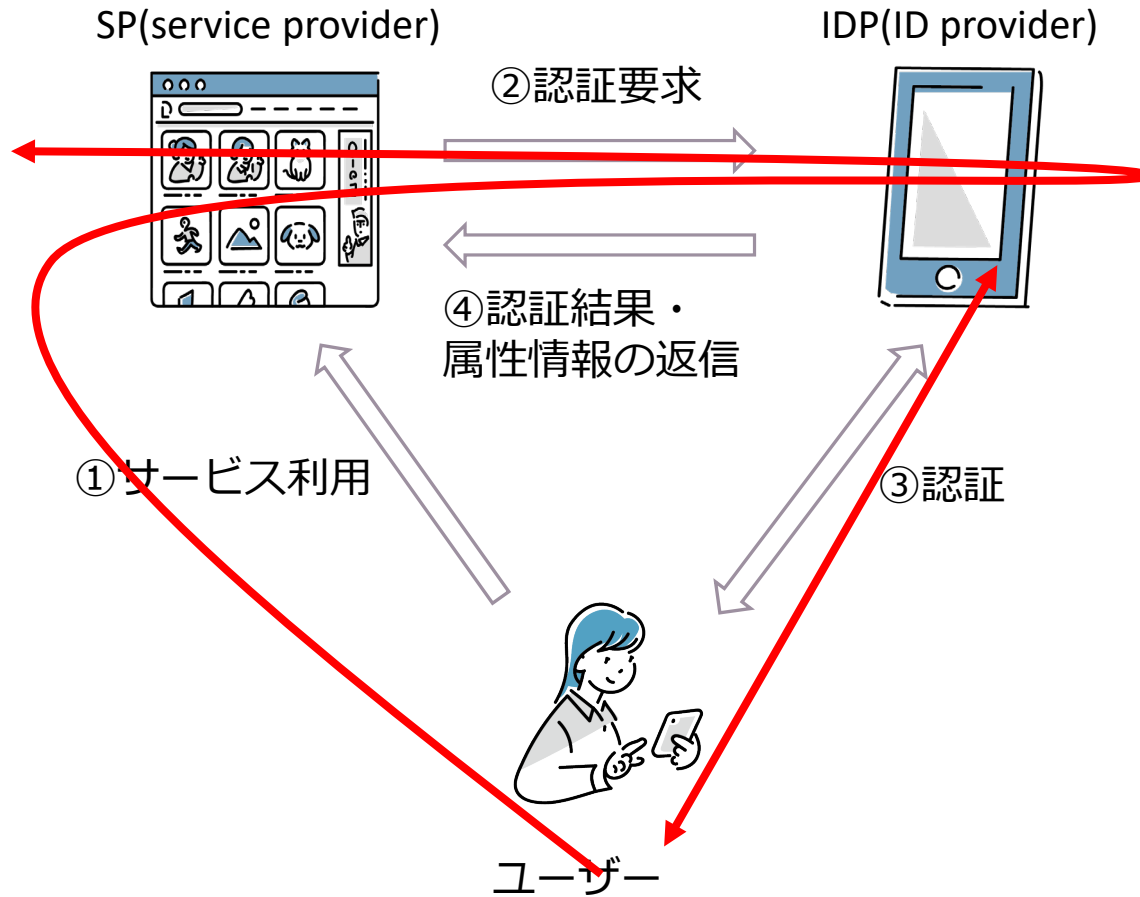
- 複数のパスワードを使う必要がなくなる

サービス提供側のメリット

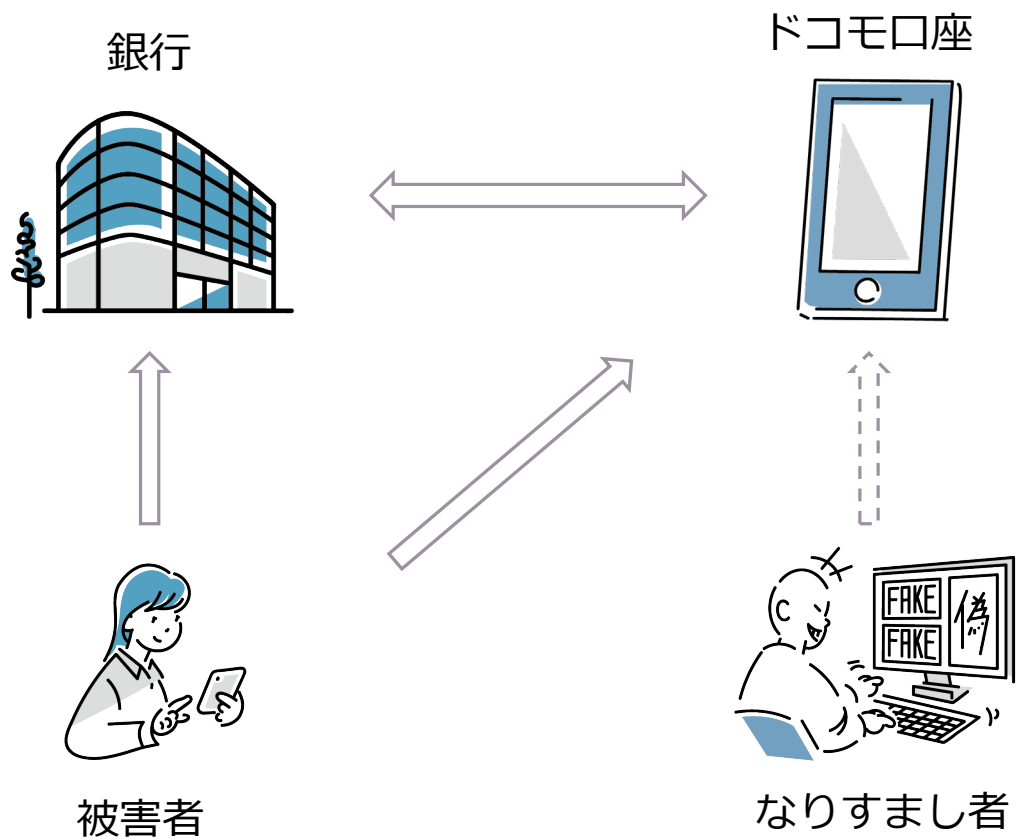
- 登録段階での離脱率を下げるができる
- IDPが保有している属性情報を取得できる

ID連携とセキュリティ

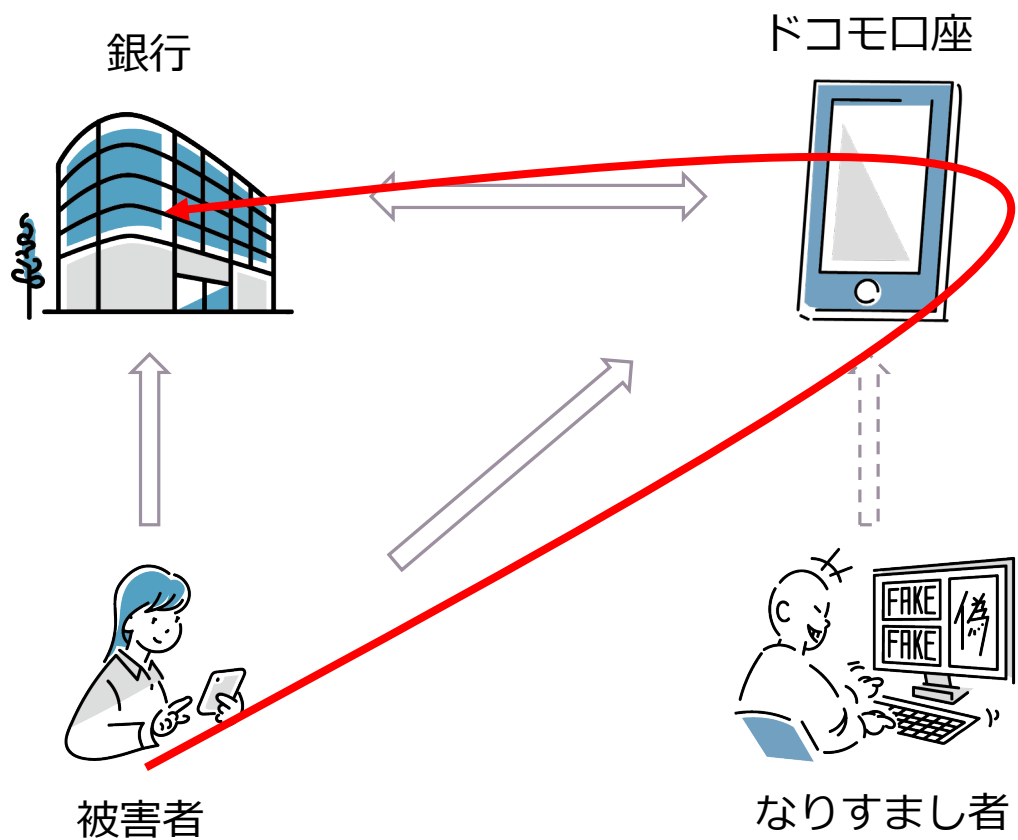
不正利用を防ぐためには、一連の過程がセキュアである必要がある。



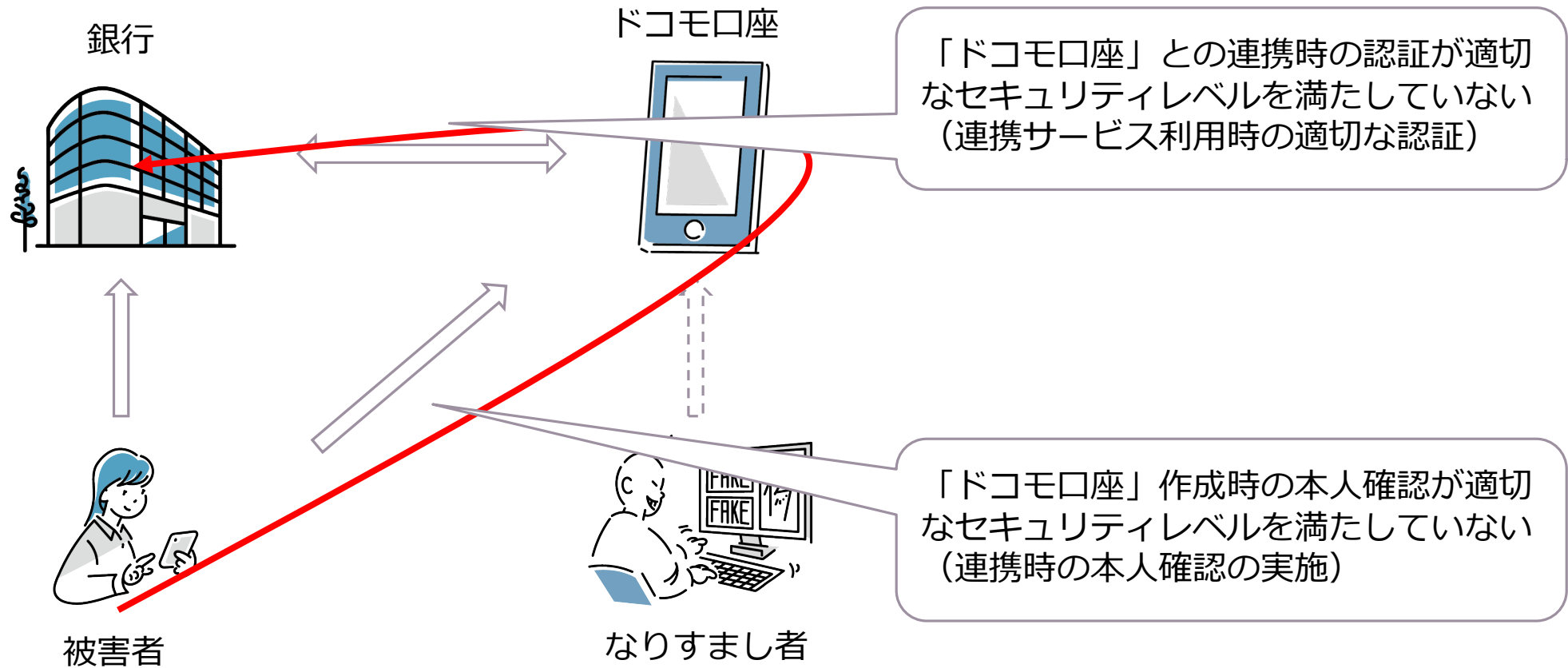
「ドコモ口座事件」関係図



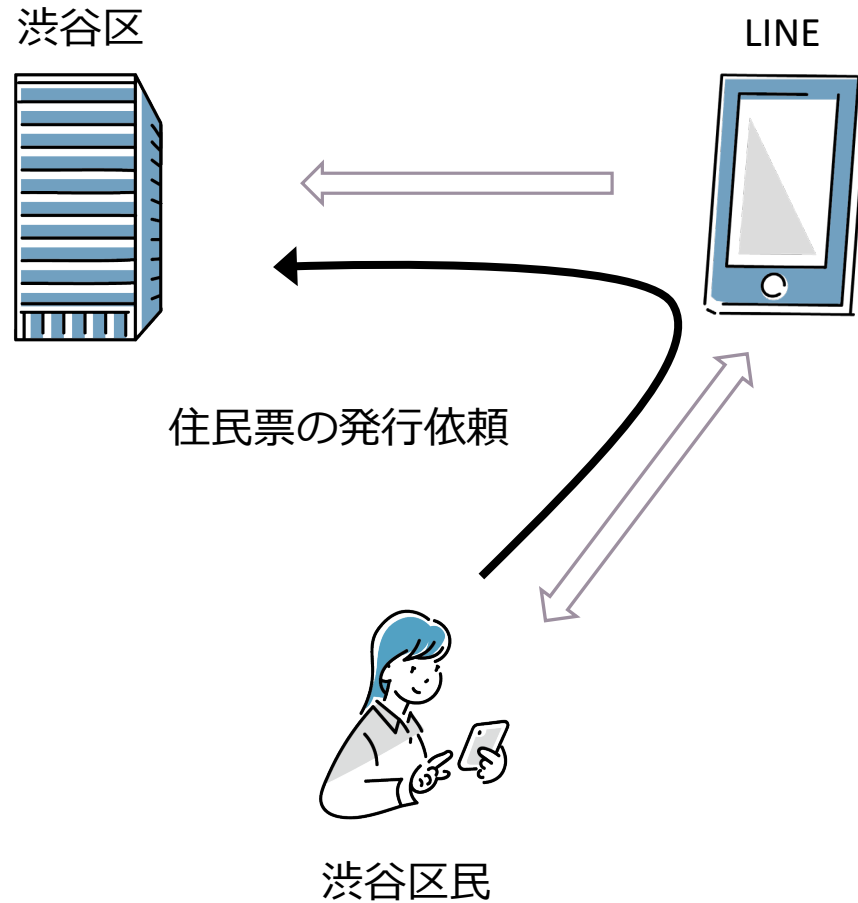
「ドコモ口座事件」関係図



「ドコモ口座事件」関係図



「LINE」を用いた住民票請求サービスの適法性確認請求事件



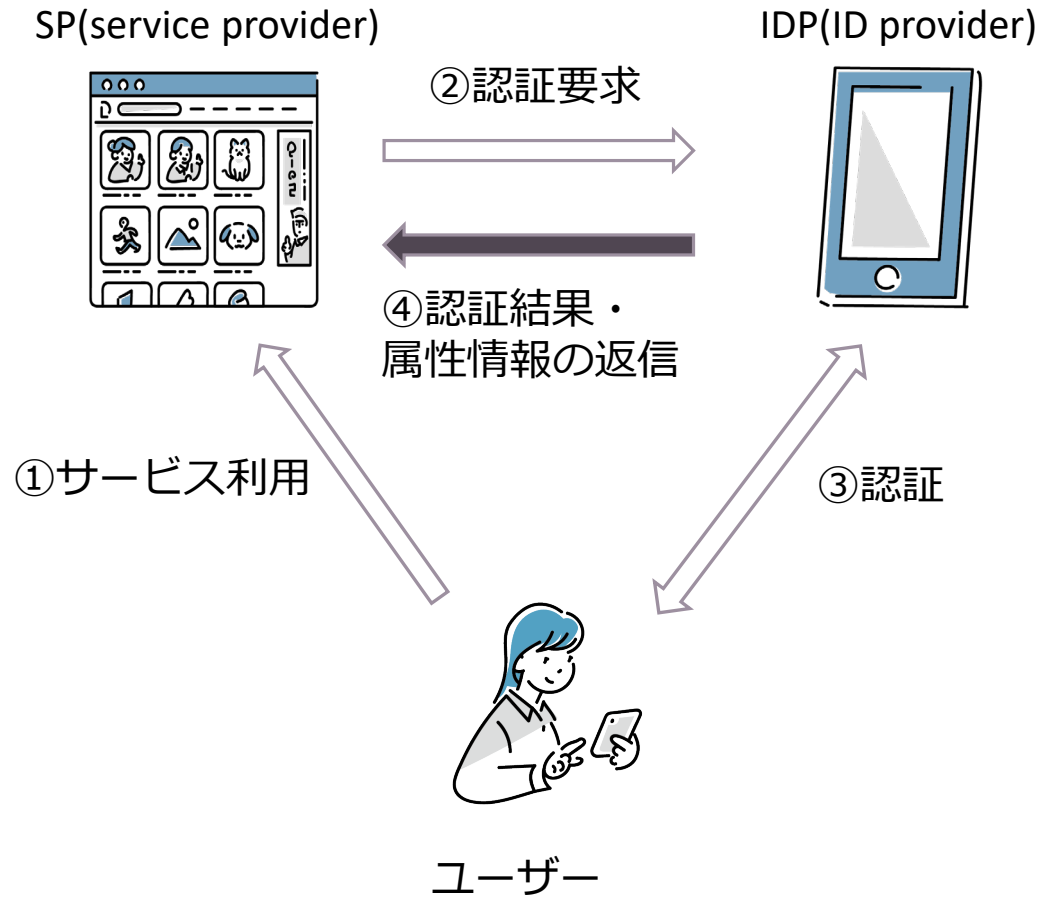
- ① 住民はLINEで住民票を申請する。
- ② 本人確認書類および本人の複数の顔写真を照合して本人確認をおこなう。
- ③ LINE Payで手数料を決済する。
- ④ 郵送で住民票が住民票記載の住所に届く。

総務省通達

請求を行う者は、入力する事項についての情報に電子署名を行い、当該電子署名を行った者を確認するために必要な事項を証する電子証明書と併せてこれを送信しなければならない

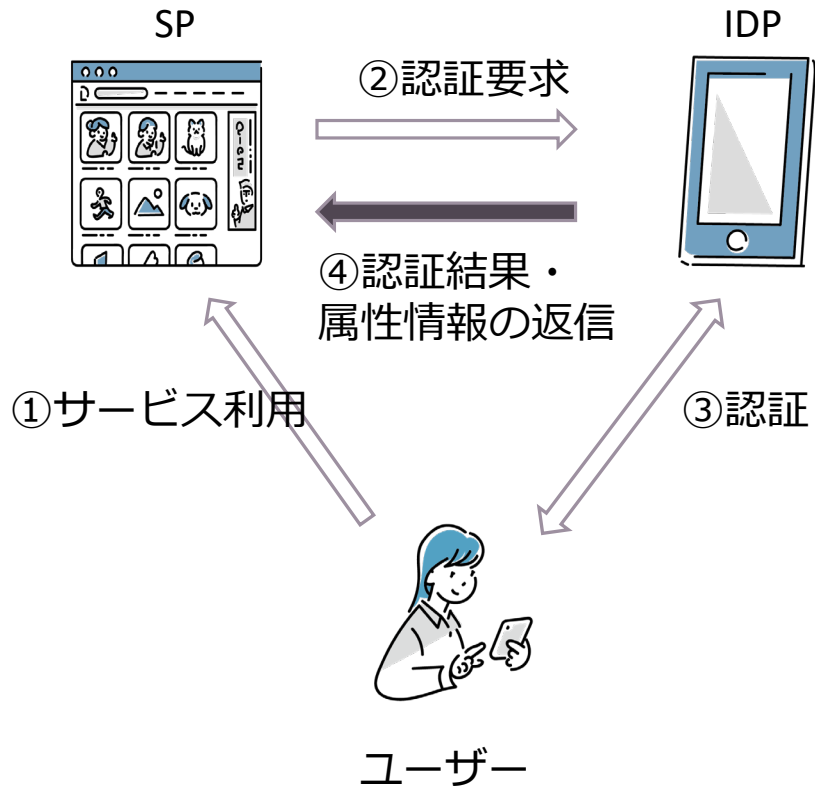
現在訴訟係属中で12月8日に確認訴訟の一審判決が出る予定

ID連携と個人情報保護法



属性情報のやり取りが生じるため個人情報保護法上の問題が生じうる

ID連携と個人情報保護法



	取扱う個人情報	取扱いの態様	対応	問題点
SP		間接取得	利用目的の公表	直接取得とほぼ同じ態様であり、利用目的を明示すべきではないか。
IDP	認証情報 属性情報	第三者提供	第三者提供の同意	「本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示さなければならない。」（通則編GL）

安藤 広人 (あんどう ひろひと)



2004年

弁護士登録

2004年

弁護士法人英知法律事務所入所

2015年

第一東京弁護士会総合法律研究所IT法研究部会副部長

2019年

ファイ法律事務所開設

フィーチャ株式会社監査役就任

東京都情報公開審査会・東京都個人情報保護審査会委員

2021年

第一東京弁護士会総合法律研究所IT法研究部会部長。

◆著書・論文等 (いずれも共著)

✓ 『データ戦略と法律 攻めのビジネスQ&A』 (日経BP 2018年)

✓ 『デジタル法務の実務Q&A』 (日本加除出版 2018年)

✓ 『Q&A個人情報保護法の法律相談』 (民事法研究会 2017年)

✓ 『デジタル証拠の法律実務Q&A』 (日本加除出版 2015年)