

ARS(自動音声)認証 (電話認証サービス)

2017年11月15日版



FIDO (Fast Identity Online)

藤光樹脂株式会社 SNS事業部

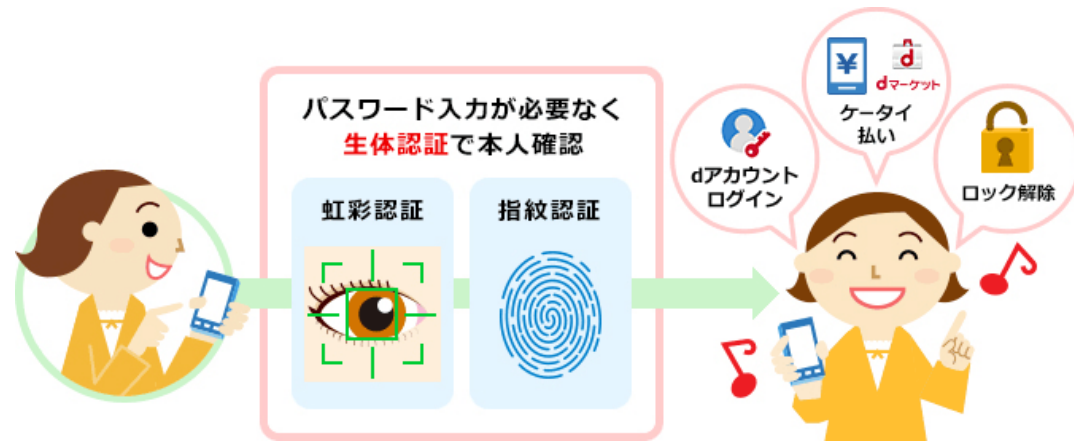
近年コンピュータやネットワークを利用する際に、利用者が本人であるかどうかを確認するためセキュリティ強化の動きに対応する企業が増加している。

警察庁、金融庁等からも不正送金対策として「2要素認証」を実施するように各金融機関へ通達があり、これまでの「ID／パスワード」等のユーザー認証に加えて、もう1段階、“認証”方式を組み合わせ、セキュリティ強化に努めているが使い易さの利便性には種々意見がある。

そのニーズに応え、様々な認証サービス中で一番強力、かつ利便性が優れたセキュリティである音声での認証サービスをご紹介します。

利用者確認の方法	利用者確認方法の例	セキュリティレベル
知識認証	・ID/パスワード ・合言葉「山」「川」	知識ベースなので、その知識を知っていれば誰でもなりすましが可能である。
所有物認証	・電子証明書 ・ワンタイムパスワード用のトークン ・MACアドレス	所有物を盗まれた場合になり済まされる可能性があるが、知識ベースと違って所有物を持った人だけがなりすまし可能になる。
生体認証	・指紋認証 ・静脈パターン認証 ・虹彩認証 ・声紋認証 ・顔認証 ・網膜認証	身体的な特徴を元にするので、盗まれることや貸し借りをすることができない。

指紋認証・虹彩認証



【課題】

虹彩: アルコールに
よる認証不可
高画質写真でも認識

指紋: シリコン等で複製可能



医療利用の高画質写真



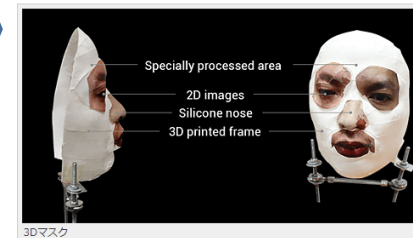
シリコンでのコピー

顔認証



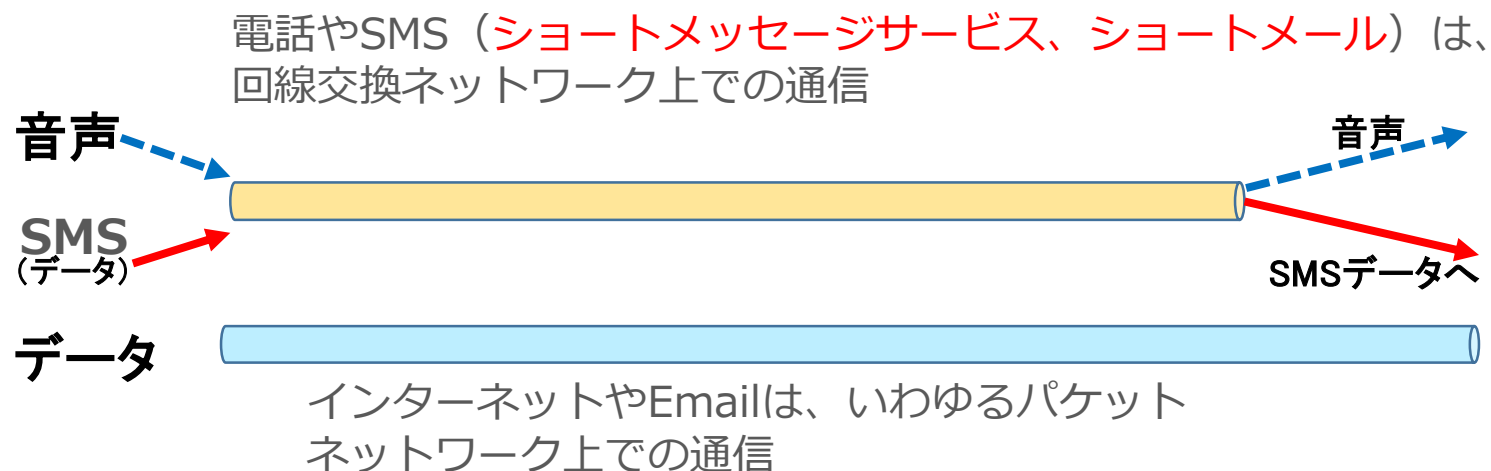
【課題】

本物の顔は変わる。
光の具合や全体の環境に大きく
左右される可能性あり



iPhone Xの顔認証システム
「Face ID」 3Dマスクで突破！
2017/11/10ニュース
ベトナム・セキュリティ企業
Bkav Corporation発表

電話回線での SMS認証 仕組みとは

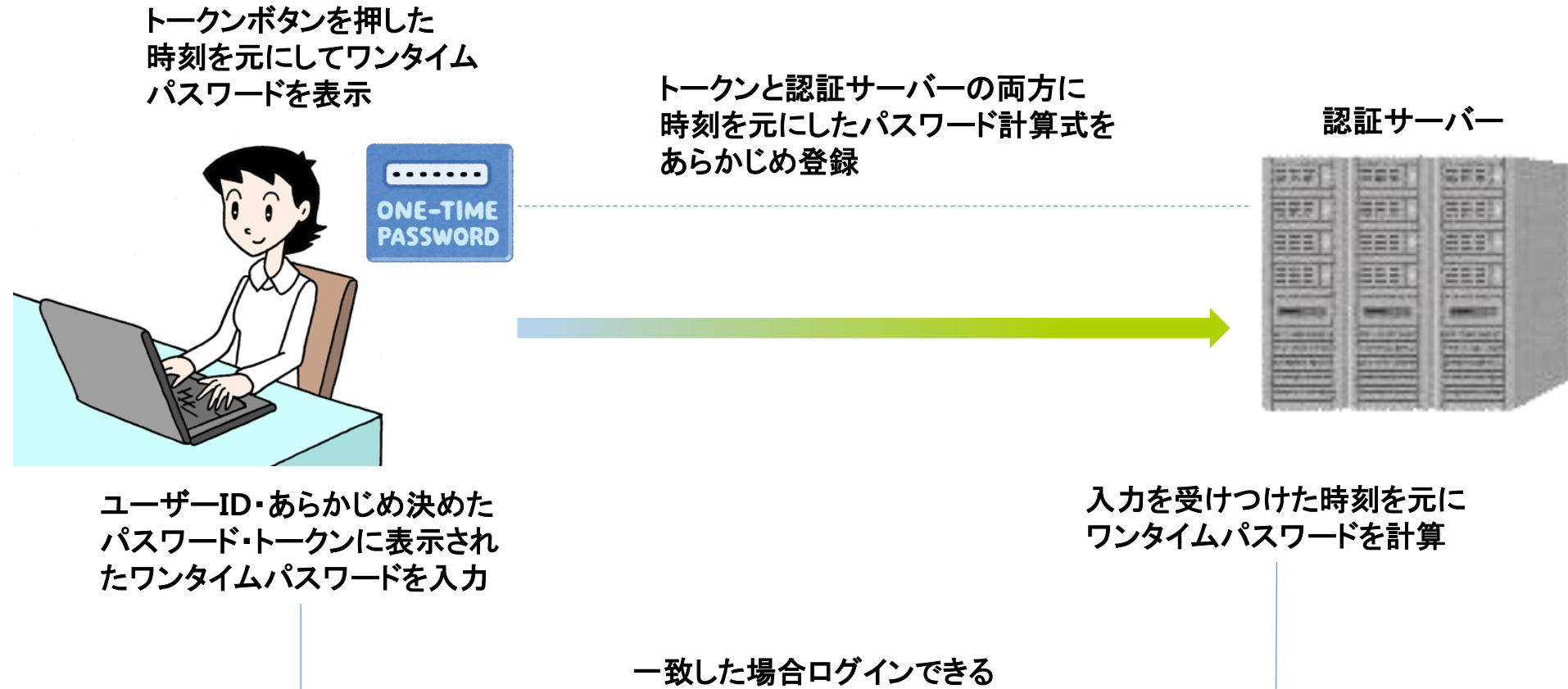


***しかし、NISTが警告、SMSでの二段階認証が危険な理由について公開した。**

米国立標準技術研究所(NIST)は「Digital Authentication Guideline」(デジタル認証ガイドライン)の草案を公開し、一般からの意見を募集しました。このガイドラインの最終版2017年9月発行。

ワンタイムパスワードを正しく生成するために使われる方式としては、「時刻同期方式」と「チャレンジ&レスポンス方式」の2つがあり、「時刻同期方式」が主流です。

「時刻同期方式」



ワンタイムパスワード(OTP)で不正アクセスを防止できない例

①IDとパスワードを中継する。



②ワンタイムパスワードをそのまま中継する。



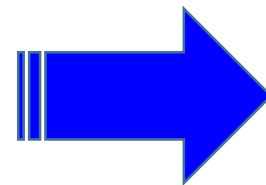
③承認が完了したら、ユーザーになりすまして操作する。



文字データは
ハッキングの
可能性大



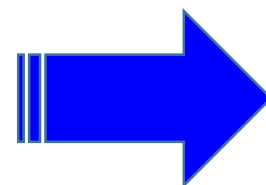
パソコンがウィルスに
感染したとしたら？



ワンタイムパスワード
(OTP) 認証も
安心できない！



本人の携帯電話が
ウィルスに
感染したとしたら？



SMS認証も
安心できない！

そこで！
音声のみを認証手段とする
電話認証は…



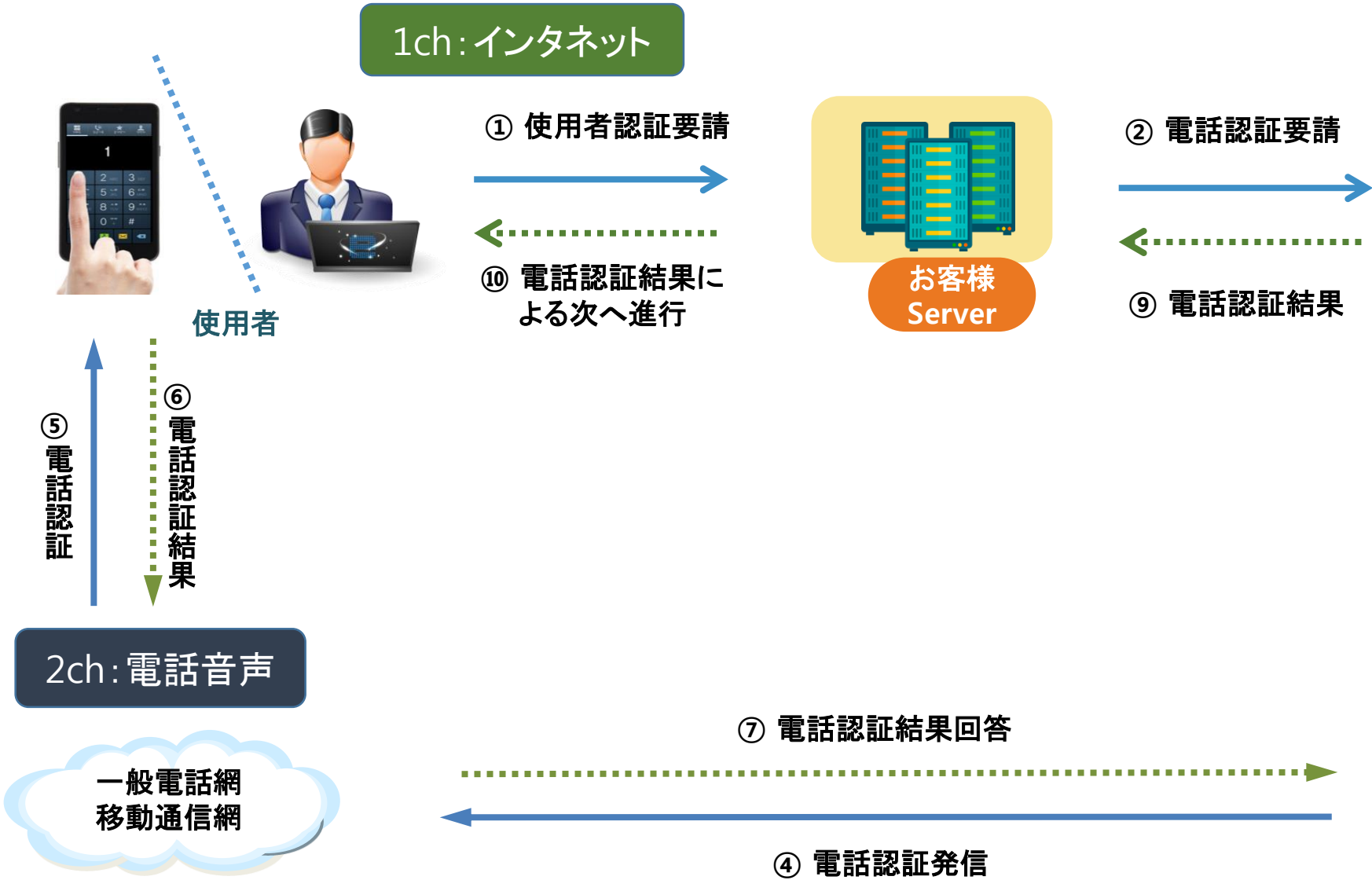
安全！ + 簡単、便利！

音声の伝達は回線交換方式(アナログ)！

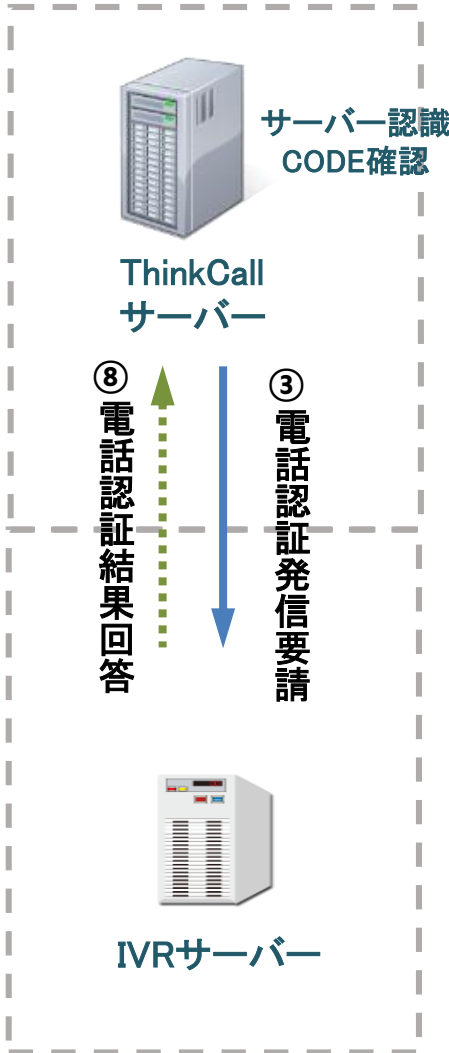
(インターネットのデータ通信パケット交換方式のネットワークではない！)



* 国際特許登録(日本を含む20ヶ国)



藤光樹脂(株)管理



さらに！

音声＋本人指紋認証で
完璧に本人確認ができる。

さらに安全！

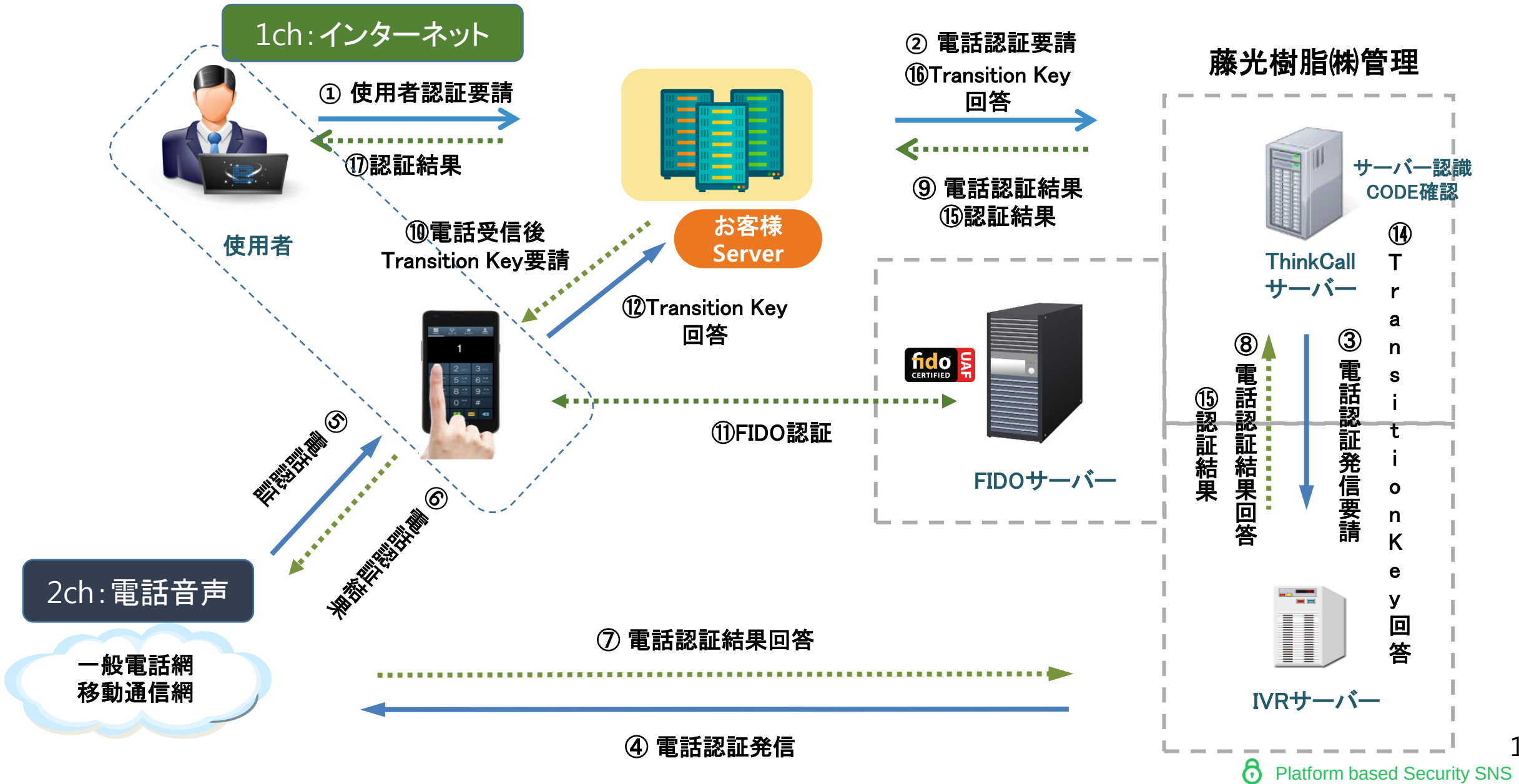
＋簡単、便利！



* Androidの場合 -ARS(音声)コメント後 ⇒ 自動で指紋認証画面へ切り替え ⇒ 認証

* iosの場合 -ARS(音声)コメント後 ⇒ PUSHメッセージが転送され ⇒ メッセージを選択 ⇒ 指紋認証画面へ切り替え ⇒ 認証

* FIDO (Fast Identity Online) 取得 * 国際特許出願中





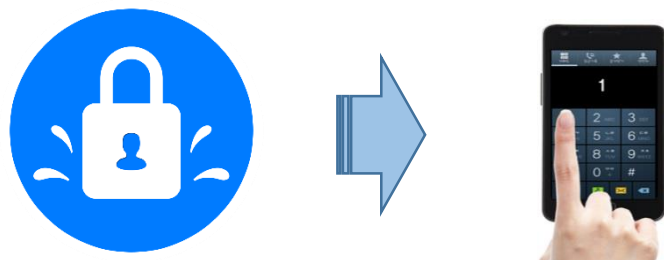
* 導入対応サービス

区分	内容	その他
認証方式	1) ARS 認証 2) 指紋 認証 3) ARS + 指紋認証 4) SMS + 指紋認証	統合認証モジュール(選択型)形態で提供し使用者の利便性を提供する。

* 導入時の対応可能な機器

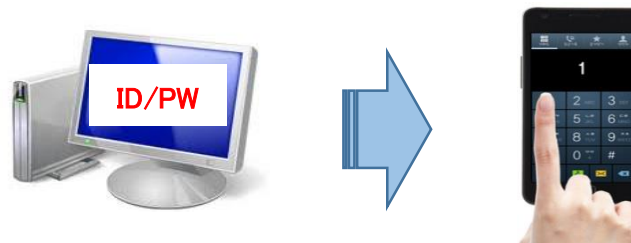
区分	サポート機器	その他
Android機器	android 6.0 以上の機器 (但し、6.0以下バージョンの場合はパスワード方式で対応可能)	指紋認証装置が付いている機器のみ可能
iOS機器	ios 6 以上	

◆アカウント登録時



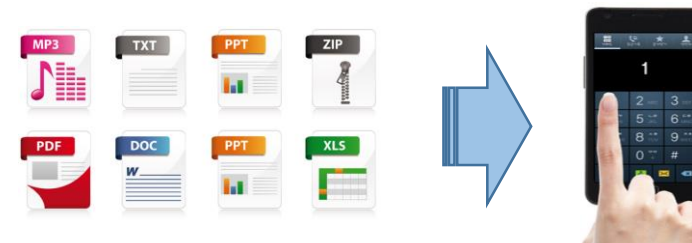
本人確認のため電話認証を行ってください！

◆ID/PW入力時



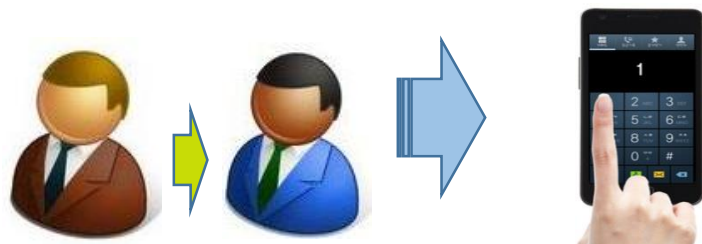
ログインのため電話認証を行ってください！

◆File閲覧時



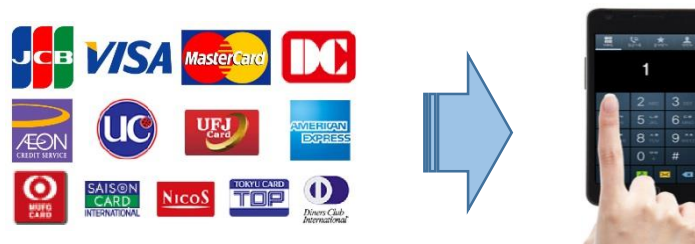
File閲覧のため電話認証を行ってください！

◆承認時



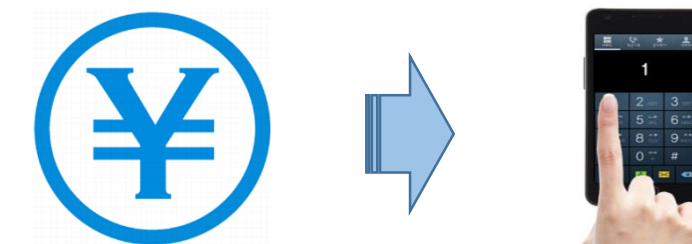
承認のため電話認証を行ってください！
課長⇒部長⇒常務(多段回可能)

◆クレジットカード決済時



クレジットカード承認のため
電話認証を行ってください！

◆決済・送金時



決済・送金のため電話認証を行ってください！
オレオレ詐欺防止！

区分	電話認証	Web認証	OTP	SMS
認証情報 入力方法	ARS(音声)で認証番号発信 認証値を電話機で直接入力	端末機へ直接入力	PCへ入力	直接 or PCへ入力
予備認証方法	事前登録の予備番号使用可能	無い	無い	無い
個人情報の 盗難認知 (安全性)	盗難・紛失した場合のため多段階の電話番号指定可能 (非常に高い)	可能/不可能 (低い)	不可能 (高いがPCがウィルスに感染される可能性あり)	可能 (携帯電話の盗難・盗み見のリスクあり)
対応バージョン	一般固定電話 PHS,2G,3G,4G	Web設置 されているパソコンのみ	共用 OTPの場合は共通に 使用可能	一般電話不可
利便性	便利	Webが繋がらないと 認証はできない	持ち歩き不便 (紛失の恐れあり)	便利
セキュリティー 問題	無し	OS及びアプリケーション ハッカー可能	OTP 待機時間にハッカー されやすい	ボイスフィッシング対応が 難しい
初期費用	無し	有り	有り OTP購入、在庫負担	有り

業種	サービス内容
公的機関	電子政府サービス 本人確認手段強化
銀行・証券	金融乗っ取り予防サービス他
クレジットカード	決済手段
保険	使用者の認証
一般企業	サーバー接近制御, VPN使用者認証
ゲーム	本人情報保護サービス