



声紋認証技術のご紹介

POINT

01

偽造防止・安全性

パスワードと声紋の二重認証で、侵入率は**0.5%**以下
パスワードはランダム生成のため、録音は無効

POINT

02

ユーザビリティ

パスワードの読み上げにかかるのは **1 ~ 2** 秒のみ

音声の取得は簡単で手間も無く、誰にでも使用できる

パスワードが毎回発行される為、覚える必要がない

POINT

03

紛失・盗難防止

生体認証技術は自身の声を使用する

既存のセキュリティより紛失・盗難などのリスクが極めて低い

POINT

04

コスト

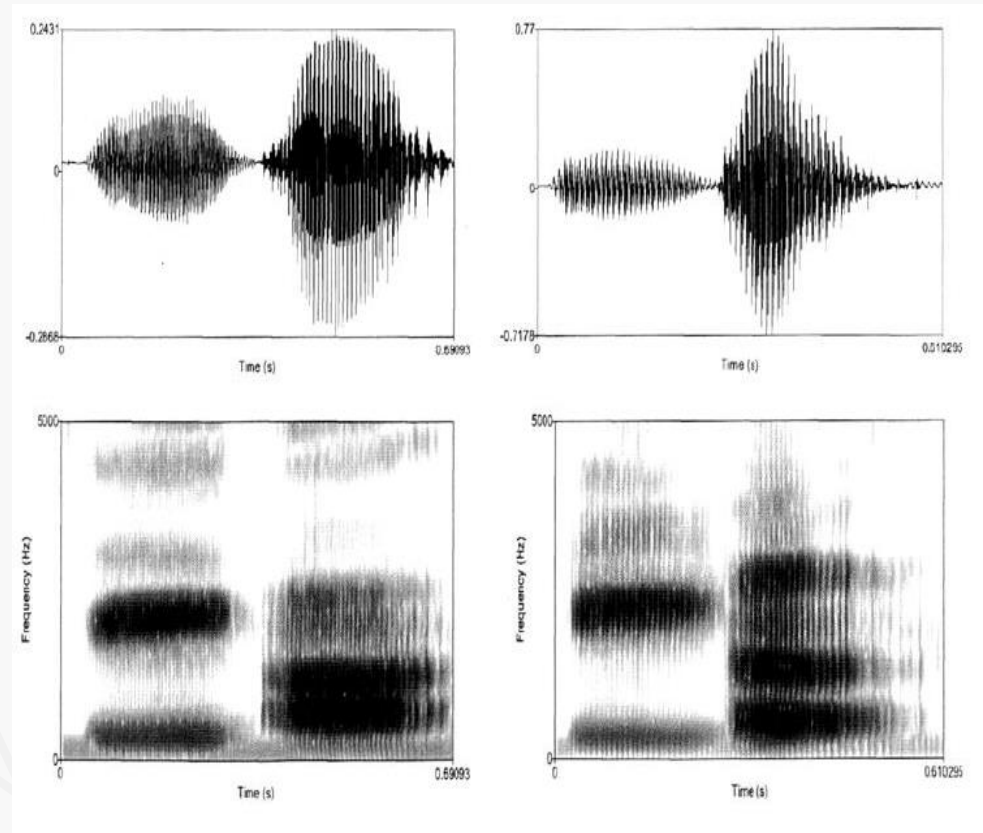
スマホを利用するので、認証端末が不要

生体認証

生体認証	読取	他人許可	本人拒否	偽造防止	処理性能
指紋	△	×	○	△	○
顔	○	○	×	△	△
瞳	×	×	△	○	×
声紋	○	△	○	○	○

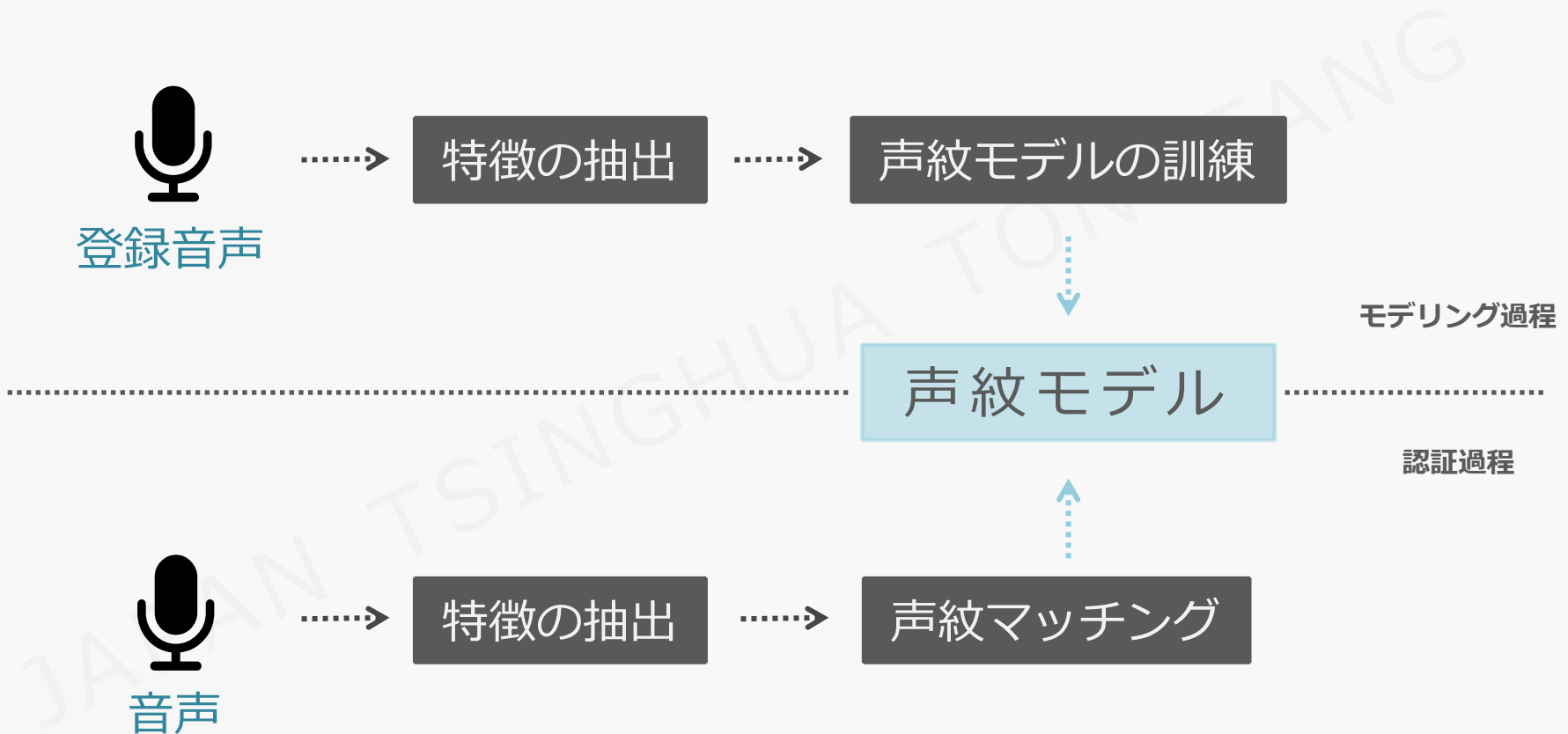
声紋認証は指紋認証・顔認証に比べ安全で、
且つ、行動的特徴なので偽造されにくい

原理 1



電声学機器により表示された音声の周波数スペクトルとスペクトログラムを声紋と呼ぶ。数理モデルで声紋の特徴を説明することにより、二つの声紋モデルの差異を量的に比較する

原理 2



実用化の影響



騒音の環境下では音声認識に影響がある
高性能のマイクを使用することによりその影響は減る



身体状況

感情・発音の仕方など正常な状態が前提である
その為、**身体状況**に応じて使用・不使用が選択できる
年齢変化にもシステムの自主学習により適応する

▶▶ 音声の長さ

音声の長さが長いほど声紋認証の性能は良く、
音声の長さが短いほど使いやすい
そこで、短い音声に対しても適応できるように、
声紋モデル作成段階の音声の長さを8桁×5組の数字
にした
識別時に必要なのは8文字の数字だけである

声紋認証の性能

FRR : 本人拒否率

発音する人間がユーザー本人なのに拒否される割合

FAR : 他人受容率

発音する人間がユーザー本人ではないのに受入される割合

Lv.1 : FRR=2.3% FAR = 2.3%以下

Lv.2 : FRR=3.1% FAR = 1.0%以下

Lv.3 : FRR=4.0% FAR = 0.5%以下

声紋登録時間 : 1000ms以下

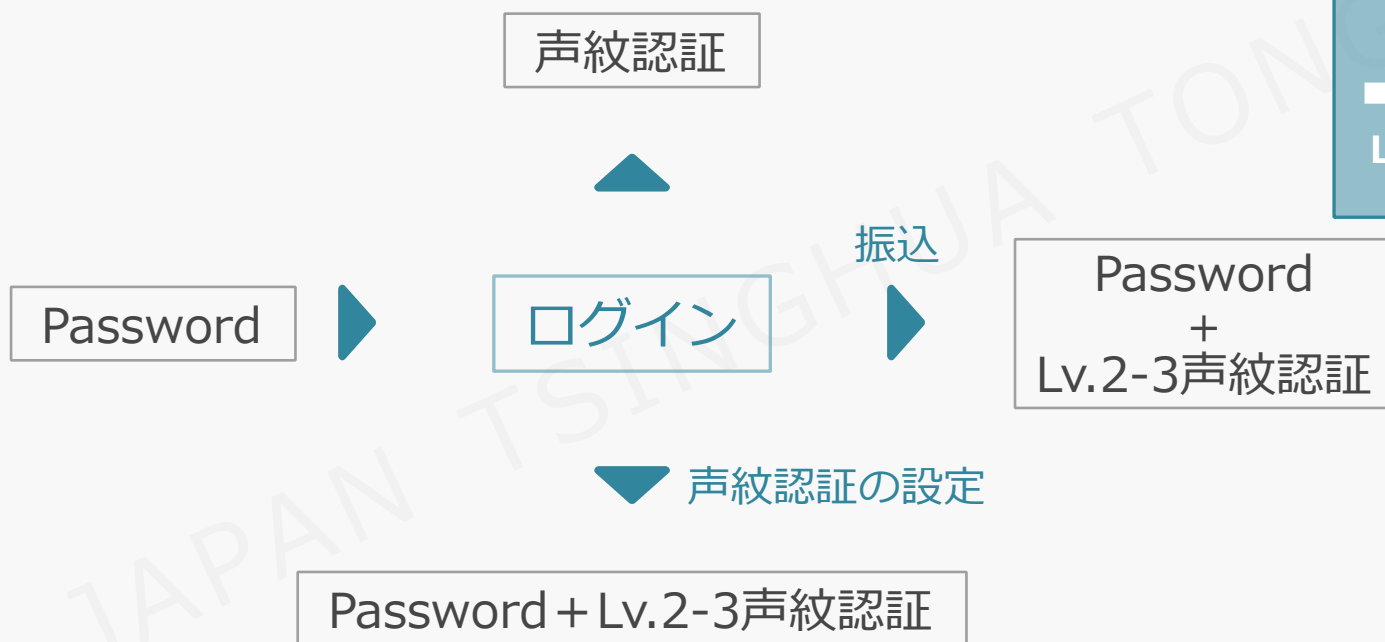
声紋確認時間 : 200ms以下

※声紋登録の長さが5秒以下、声紋確認の長さが1秒以下の条件で、
声紋確認はワンタイムパスワードが8桁の時の安全レベル

セキュリティ面の応用

スマホでのインターネットバンク

既存のパスワード認証システムの上に声紋認証を加え、
ユーザーアカウント情報の漏洩を防止

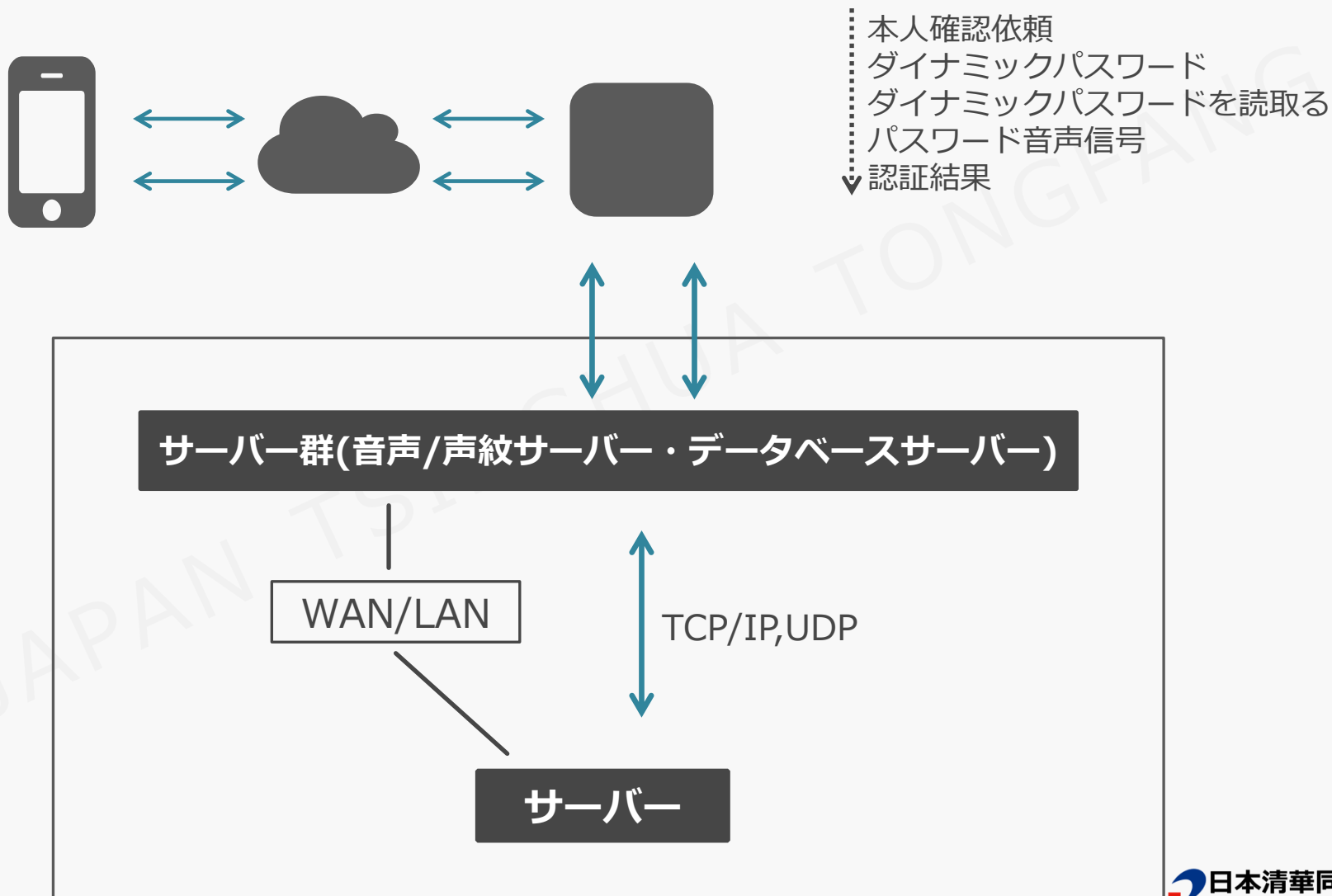


セキュリティレベルに
合う安全基準を適用

- ログインの場合
Lv.1の声紋認証
- 取引の場合
Lv.2~Lv.3の声紋認証

声紋認証のソリューション

声紋認証の仕組み



声紋認証の事例

モバイルバンキングのユーザー認証

中国建設銀行 **200**万ユーザーが利用

※2018年6月30日時点

声紋認証技術・音声認識技術とワンタイムパスワードを連携し、ユーザー認証を行うことで、より安全な取引環境を提供する

ワンタイムパスワードをユーザーのモバイル端末へ送り、ユーザーが読んだワンタイムパスワードの音声データを採集し、

暗証番号認証と声紋特徴認証を同時に分析しマッチングする二つの認証とも成功した場合のみ認証成功となる

声紋認証の事例

声紋勤怠管理システム

他の勤怠管理システムと比較して、
安全性、利便性、成りすまし防止などあらゆる面で優れている

声紋認証技術に基づき、モバイルと無線WIFIと企業内部LANの
IP解析技術を結合し、政府部門や企業内部の勤務管理において
社員や作業員の勤怠管理のワンストップでの実現が可能

オートロック声紋認証

オートロック声紋認証システムで「声紋」ユーザーキーとして管理し、
声紋の特徴と音声内容でユーザー認証をする
安全性・利便性・コストに優れている

ご清聴ありがとうございました