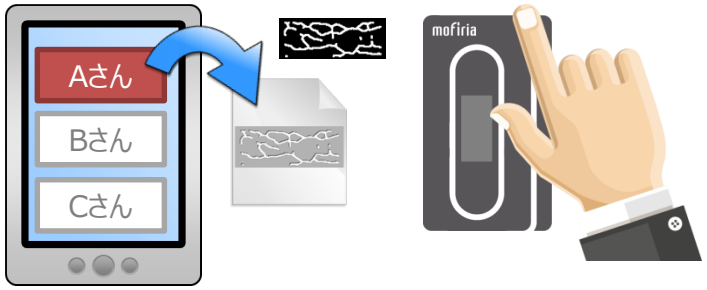
1対1認証と1対N認証

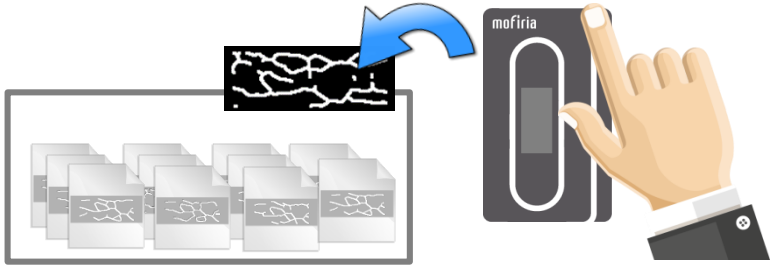
認証方式には、1対1認証と1対N認証の2種類があります。 精度 (セキュリティ) 重視、利便性重視など、用途に合わせて使い分けます。

静脈認証のみでの運用 (1対1認証)



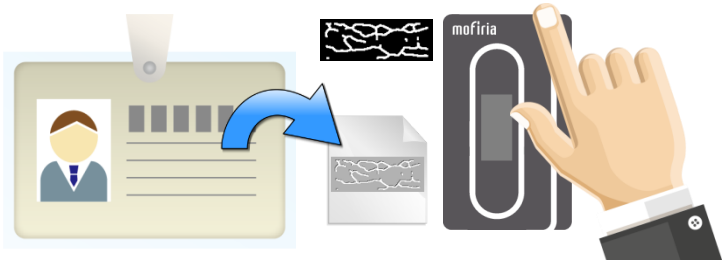
タッチパネルなどの画面で照合するメンバーを選び、そのメンバーに割り当てられている静脈情報と実際の指を照合する方式。

静脈認証のみでの運用 (1対N認証)



何も指定せずに、実際の指を登録されているすべての静脈情報と一つ一つ比較する方式。利便性は高いのですが、高精度、高セキュリティを要する場面には向いていません。

カードなどとの併用 (1対1認証)



ICカードに個々人の静脈情報を格納しておき、照合時にカード内の静脈情報を読み込んで、実際の指と照合する方式。もっともセキュリティ性の高い本人確認です。

1対1認証

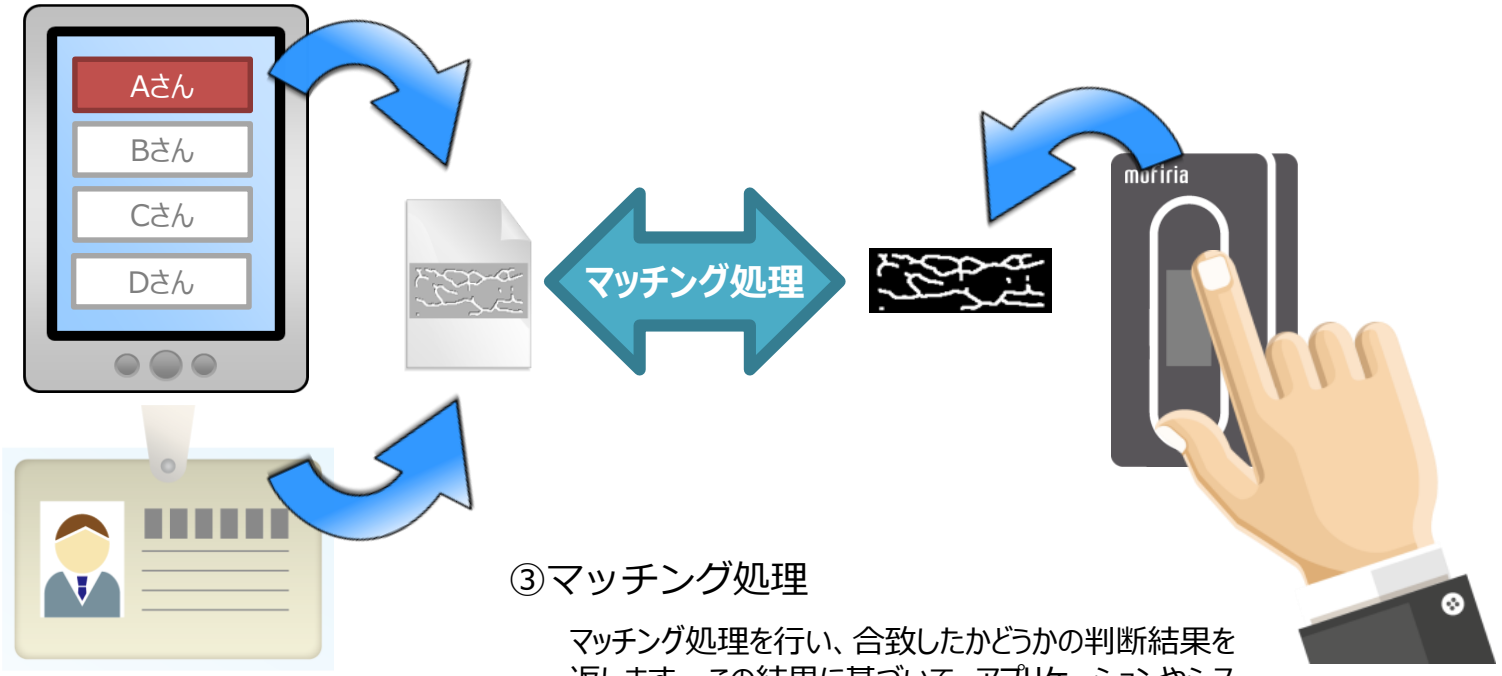
1対1認証とは、照合する本人のテンプレートを呼び出して、実際の指(静脈)との比較を行う方式です。 1対N認証に比べて利便性は劣りますが、認証の精度やセキュリティ性という点では遥かに優れています。

①認証するテンプレートの呼び出し

画面から名前の選択、IDの入力、あるいはICカードに格納されている静脈情報の読み込みなど、様々な方法で認証する1ユーザーの静脈情報を呼び出します。

②認証するテンプレートの読み込み

①で指定したテンプレートをデバイス内で認証する場合はデバイス内に読み込みます。サーバー上で認証する場合はテンプレートはサーバーで待機し、デバイスから暗号化された画像データをサーバーに送ります。



③マッチング処理

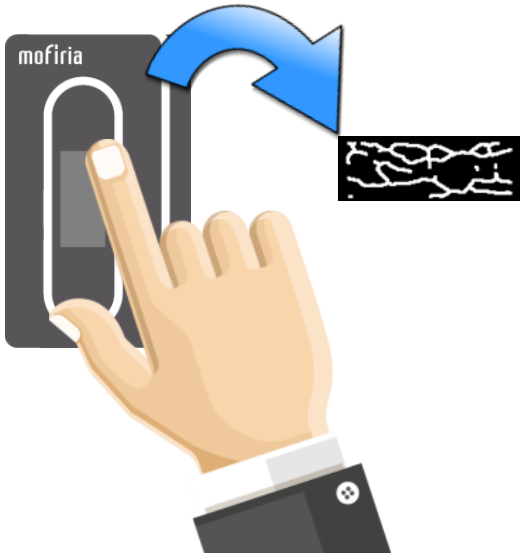
マッチング処理を行い、合致したかどうかの判断結果を返します。この結果に基づいて、アプリケーションやシステムが対応した処理を行います。

1対N認証

1対N認証とは、指を置くだけで予め登録されている多数のテンプレートの中から合致する1人を選ぶという方式です。 認証の精度、速度では1対1認証に比べて劣りますが、何も指定せずに指を置くだけで完結するので利便性に優れています。

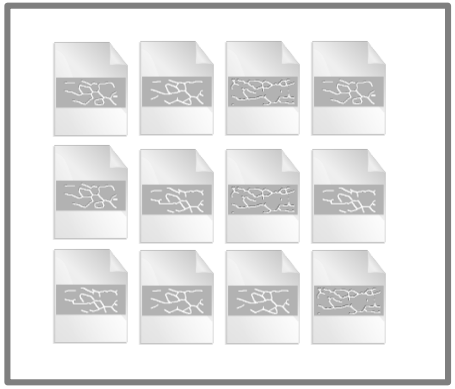
①指静脈データの取得

指静脈データをデバイスから取得、暗号化してサーバーに送ります。



②サーバー上でマッチング処理

予め登録され、サーバー上に格納されているすべてのテンプレートと比較処理を行います。そのため、比較対象が多くなるほど処理時間がかかります。



③結果のリターン

合致するテンプレートが見つかったら、そのテンプレートに割り当てられているIDを返します。

「今、指を置いているのはAさんです。」

1:1認証と1:N認証の比較

	1:1認証	1:N認証
利便性	△	◎ ➔IDなどの入力、指定が不要になります。
セキュリティ	◎	△ ➔原理的に比較するテンプレートが多くなればなるほど、誤認証が発生しやすくなります。 ➔誤認証の低減のためのアプリケーション実装が必要になります。
処理速度	◎	△ ➔複数のテンプレートと比較するため、処理時間が長めです。 ➔1:1000で平均1秒前後 ※実行環境や処理モードに依存
メモリ消費量	◎	△ ➔比較対象のテンプレートをすべてメモリ上に展開する必要があります。 ➔578バイト × N件分のメモリ容量が必要です。