

生体認証：FinTechにおける資産保全

2016年8月23日

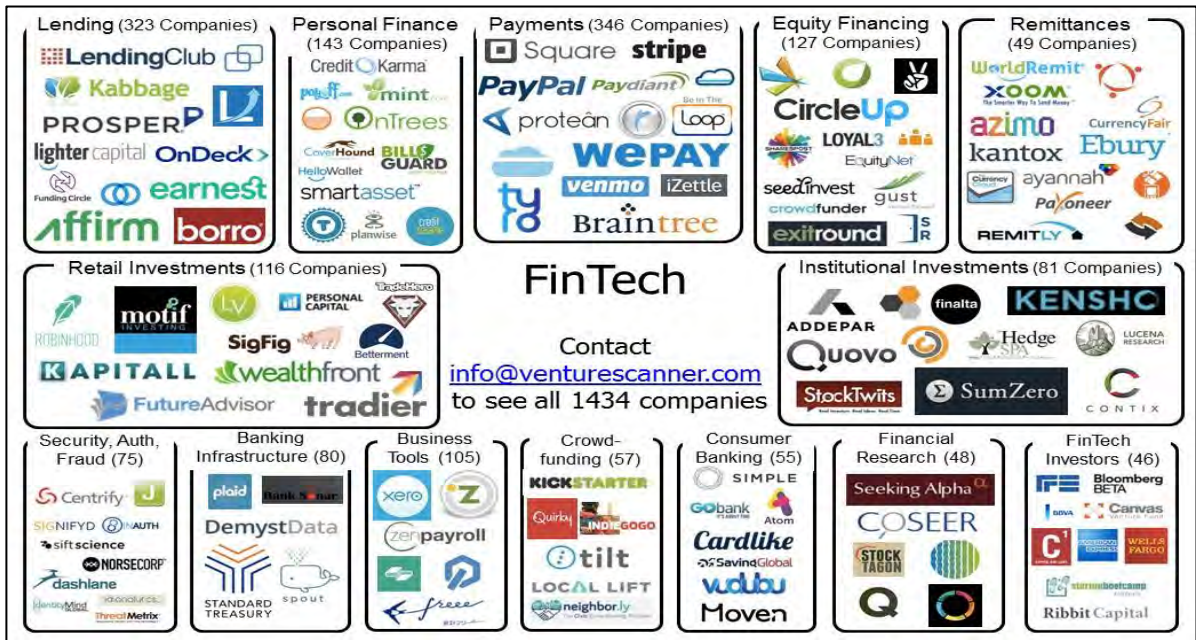
日本電気株式会社

\ Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

デジタル空間における資産/サービスの多様化とセキュリティ技術



リスク管理

安全性
利便性
網羅性

セキュリティ技術 (本人認証技術 (生体認証) ・ブロックチェーン…)

<http://insights.venturescanner.com/venture-scanner-sector-maps/>

あなたが誰であるかをどう知るのか

従来型本人認証手段の限界

●ID×パスワードの盗難・流通

✓米国Yahoo!

2016年8月、約2億人分のログイン情報（IDとパスワード）が流通

●本人証明書の限界

✓9.11アメリカ同時多発テロ

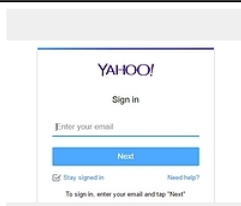
19人のハイジャック犯は正規の運転免許証を、全員で合わせて計63通取得

✓シリア パスポート

「シリアの空白パスポート・パスポートプリンタがテロ組織の手に落ちている」と米国土安全保障省が2015年に報告

“米Yahoo!ユーザー2億人のログイン情報、闇市場で流通か”

ITmedia エンタープライズ: 2016年8月3日



LinkedInやTumblrのユーザー情報流出にかかわったとされる人物が、今度は米Yahoo!のユーザー2億人の情報を闇市場で売りに出したと公言しているという。8月1日から2日にかけてメディア各社が伝えた。

【その他の画像】

Yahoo!アカウントのログイン画面

報道によると、「Peace」（別名「peace_of_mind」）を名乗る人物が、Yahoo!ユーザーのログイン情報と称するデータを1日に闇市場で売り出した。このデータは、過去にLinkedInやTumblrのユーザー情報を流出させたロシアの集団から入手したと主張しているという。

売りに出されたのはYahoo!のユーザー2億人分のユーザー名とハッシュ化されたパスワード（MD5のアルゴリズムで作成）、誕生日などの情報とされる。2012年当時の記録が大半と思われ、約1860ドルに相当する3ビットコインの値段が付いているという。

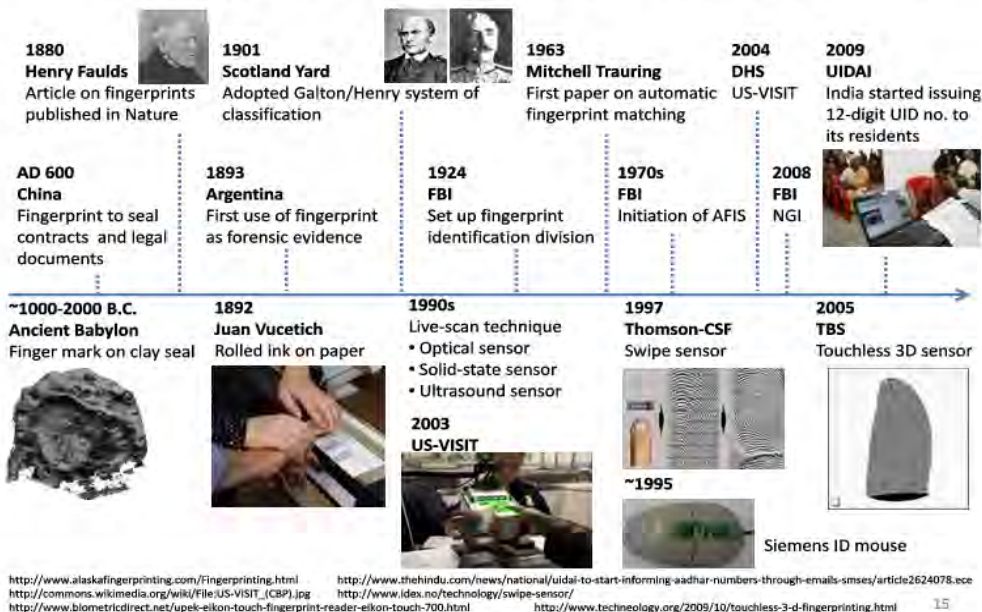
http://headlines.yahoo.co.jp/hl?a=20160803-00000036-zdn_ep-sci

指紋をはじめとする生体認証は古くから実用化されるも、 一般ユーザー向けにはまだ十分普及していない

生体認証（指紋）の主な歴史

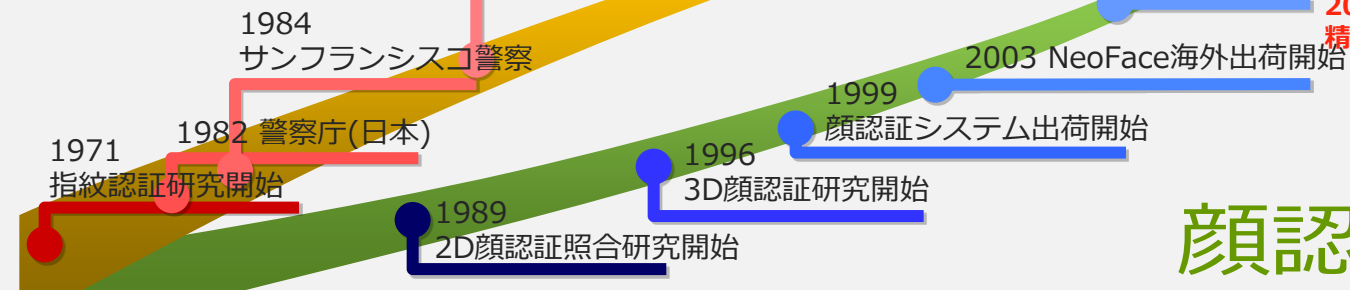
- 1800年代から指紋認証の利活用検討が進む。
- 1982年、世界で初めて、日本警察庁が指紋認証システム（AFIS）を導入。
- 1984年、米国で初めて、サンフランシスコ警察が指紋認証を導入。
- 2000年代に入りモバイルに指紋認証が搭載されるものの、普及せず。
- 2013年、iPhoneに指紋認証センサー「Touch ID」が搭載され、指紋認証の普及の兆しが見られるようになった。

Fingerprint Recognition Milestones



NECは40年以上に亘り、生体認証の研究開発及びビジネスを実施

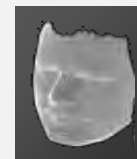
指紋認証



指紋、顔、静脈、虹彩など様々なバイオメトリクスを融合した認証

マルチモーダル照合へ

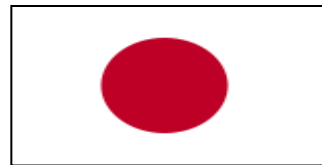
顔認証



※NECでは、顔認証・指紋認証・指ハイブリッド認証以外にも、DNA・話者・掌紋、虹彩など様々な生体認証技術の研究開発に取り組んでおります

バイオメトリクスを利用する水際での審査システム（法務省）

J-BIS (Japan Biometric Identification System)



- 指紋認証及び顔認証

自動化ゲート

バイオメトリック情報取得装置



据置型



簡易型



可搬型

自動化ゲート



事例：テイパース様 チケット本人確認システム

コンサートのチケット転売防止と円滑な入場を実現！

- ✓ ファンクラブ会員ページで事前登録した顔画像とイベント当日に会場設置のタブレット端末で撮影した来場者顔画像の照合にて、本人を確認。
- ✓ 顔写真付き身分証明書を用了目視での本人確認方法と比較し、確認時間を最大30%短縮し、来場者の円滑な入場を実現。
- ✓ ももいろクローバーZのコンサートでの運用実績など、数万人～十万人規模のイベントにも対応



※ NECプレスリリース http://jpn.nec.com/press/201412/20141205_01.html

インドUID : 世界最大の国民IDシステム



ユーザ Unique Identification Authority of India (UIDAI)

目的 二重申請者の検出



システム規模:

- データベース : 12億人以上(人類の1/6)
- システム負荷 : 100万人/日

主な特徴・トピックス

- マルチモーダルIDシステム: 指紋・虹彩・顔
- 高精度と高スループットを両立
二重申請者検出12億 x 12億
= 7.2×10^{17} 回照合
<-> 一年間は 3.2×10^{10} ミリ秒



Fingerprints capture (Right Hand)



Capture of face photograph



Iris capture



日々進化する攻撃 生体認証による取引は必ずしも安全とは限らない

“指紋「なりすまし」に注意、iPhoneも解除可能？”

The Wall Street Journal: 2016年2月25日



携帯端末の国際見本市「モバイル・ワールド・コン
gress (MWC)」(23日、バリエロナ) PHOTO:
GETTY IMAGES

もっと簡単に、端末の持ち主の協力なしにハッキ
ングする方法があると言う専門家もいる。シャーロ
ック・ホームズがやったように、指紋はワイングラ
スやスマホのスクリーンなどから採取できる。

米ミシガン州立大学コンピューターサイエンス・
エンジニアリング学部のカイ・カオ氏とアニル・

K・ジャイン氏が行った調査で、採取した指紋で比
較的に簡単にハッキングできることが明らかになっ
た。指紋の写真を撮り、特殊なインクでそれを印刷
し、その印刷された指紋を使用してスマホを解除す

れはいいだけだ。両氏によれば、この方法で韓国・サムスン電子の「Galaxy (ギャラクシー)
S6」と中国・華為技術 (ファーウェイ) の「Honor (オナー) 7」をハッキングできたという。

<http://jp.wsj.com/articles/SB10272610103318793334204581561782183509602>

生体認証に対する不安感を払拭する為にリスク見える化が必要

生体認証に関するリスクと対策

システムへのハッキングによる攻撃

対応

システムのセキュリティ強化

- ✓ 特徴点抽出SWのセキュリティ強化
- ✓ 特徴点照合SWのセキュリティ強化
- ✓ プロプライエタリシステムとする事



- ✓ 特徴点の秘匿分散保持、及び秘匿計算技術によるアプリケーションレベルでのセキュリティ強化が有効

物理的ななりすましによる攻撃

対応

HWセンサーのセキュリティ強化

- ✓ 一度ハッキングされるとセンサーの交換等、重いコスト負担



- ✓ 複数の認証手段を組み合わせた認証時のセキュリティ強化（多要素認証）が有効

■ 対面での認証場面：手ぶら認証

■ 非対面での認証場面：多彩な機能をもつスマートフォンを活用した認証

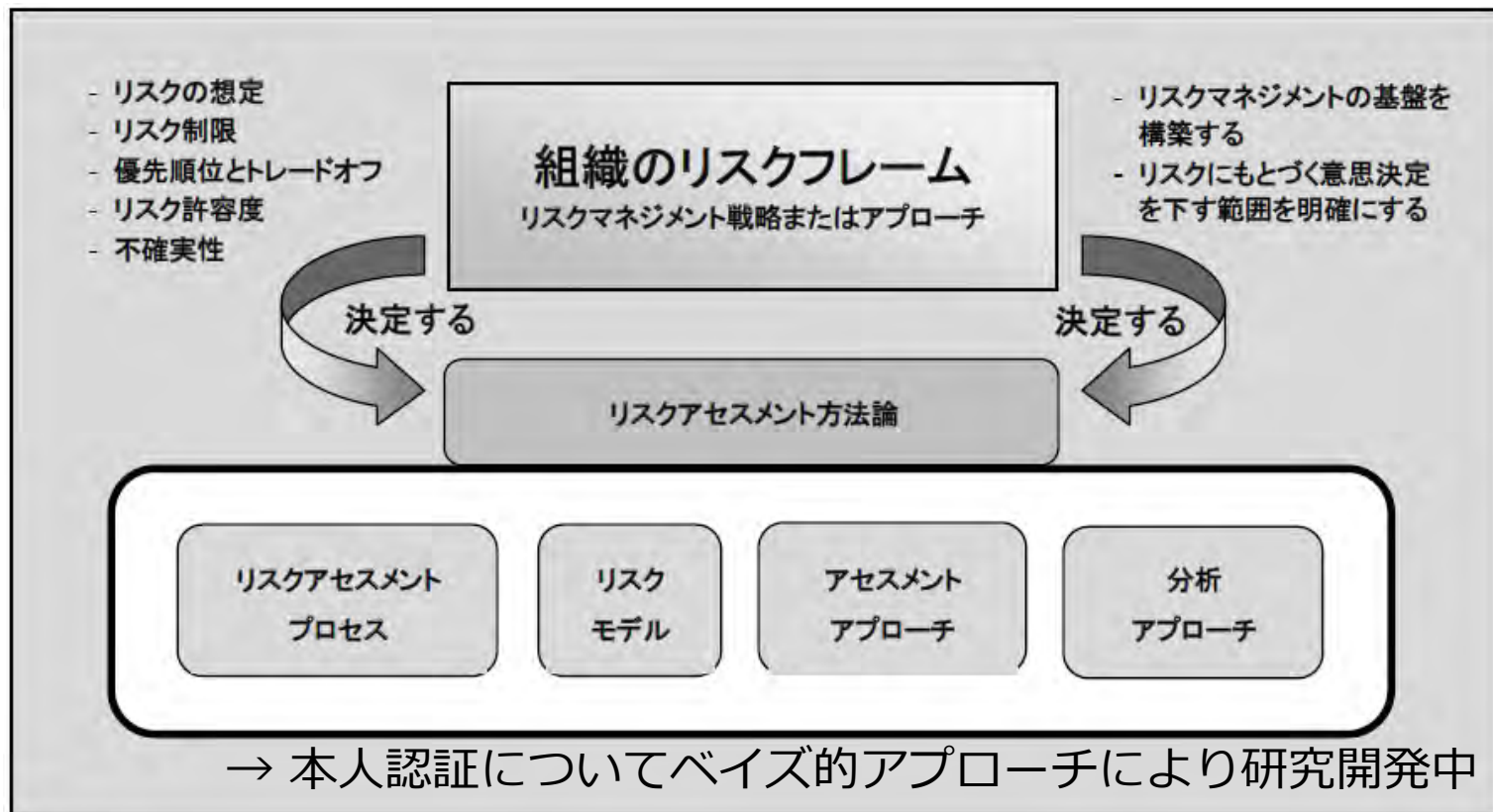
- (例) 虹彩認証×キャリアSIM×行動特徴等

スマートフォン機能の一覧 (例)

入力機器	センサー	外部への接続	出力	セキュアエレメンツ
タッチパネルキーボード	ジャイロセンサー	携帯電話網	Display	キャリア SIM
マイク	GPS センサー	Bluetooth	スピーカー	TPM
ボタン	温度計・湿度計	NFC	ライト	Felica
カメラ	光センサー	Wifi	バイブレーション	ソフトウェア SIM
指紋センサー	ガイガーカウンター	USB	本体メモリ	クラウド SIM
		CTIA	SD カード	

NECの立場：リスクを定量評価・管理してビジネスを行うことが重要

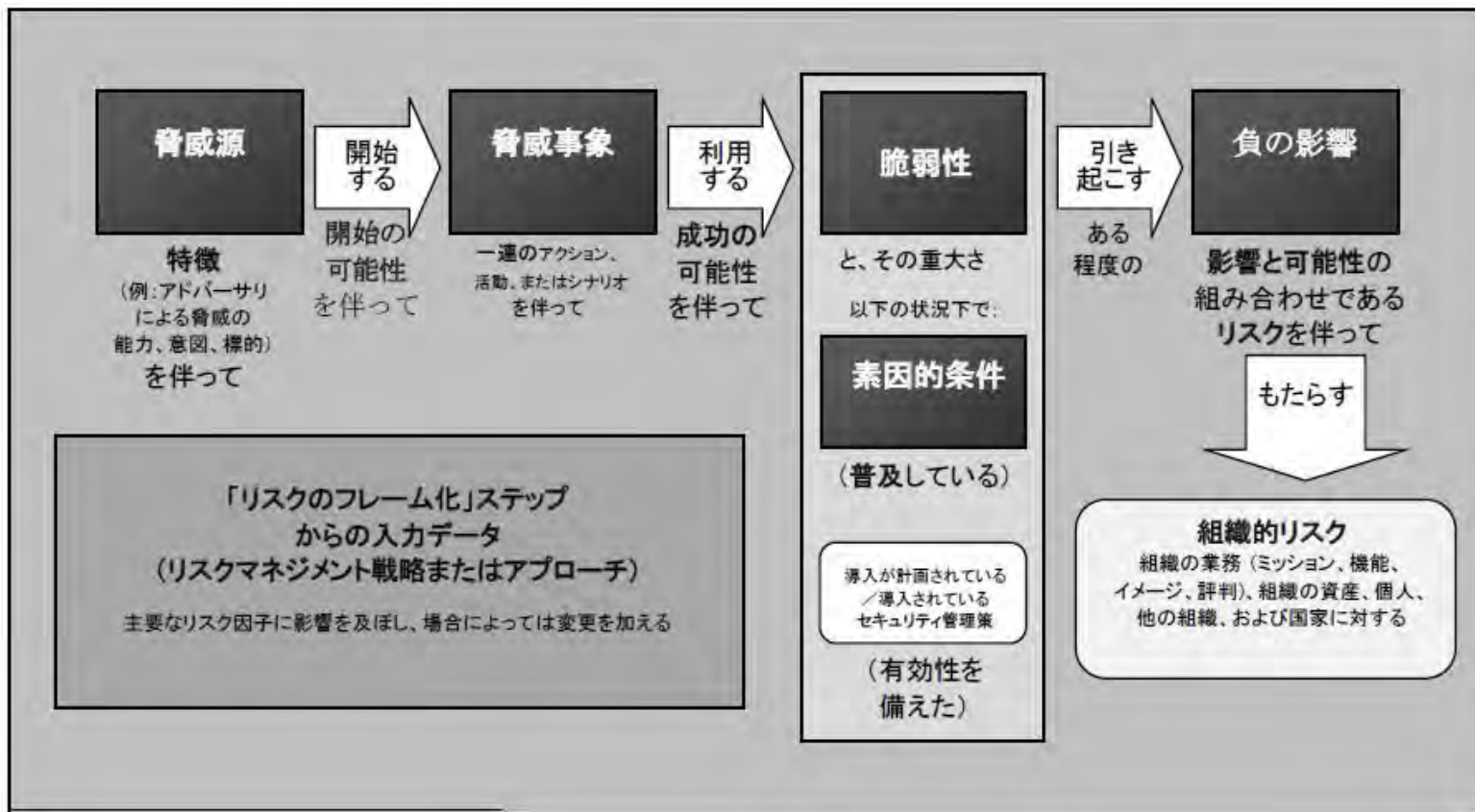
リスクのフレーム化の要素間の関連性（NIST SP800-30）



<https://www.ipa.go.jp/files/000025325.pdf>より引用

リスクモデル例 (NIST SP800-30)

認識要素毎にアドバーザリ
の能力や脅威事象に差異がある
↓
多要素認証導入メリット



<https://www.ipa.go.jp/files/000025325.pdf>より引用

リスクマネジメントへ向けての指標定義

日々進化する技術や攻撃に対し、**リスクレベルを定量化・日々の観測値によりアップデート、脆弱性発覚時のインパクトを事前シミュレーション**することで、対策を事前検討しておく事が重要

ARPT : Average Revenue per Transaction

→ 本人認証に関わる指標として次を定義

- ADPT : Average Damage per Transaction
- $\alpha\%$ ULDPT : $\alpha\%$ Upper Limit of Damage per Transaction
- AUPT : Average Usability per Transaction
- $\alpha\%$ LLDPT : $\alpha\%$ Lower Limit of Usability per Transaction

:

(例) 99%片側信頼係数で10営業日に亘る最大損失の評価を可能に

(近い) 来るべき未来へ向けての取り組み

生体認証「安全性」の向上

リスクマネージメントの確立が鍵

- ▶ 対面とそのかかわり度合・非対面などの場面に応じたリスク評価と適切な手段の選択を可能に

事業継続を担保するため

- ✓ 脅威、対策の評価基準の明確化
- ✓ 認証方法の適応的選択
- ✓ シミュレーションによる事前検討、AI技術等による異常検知

 **Orchestrating** a brighter world

NEC