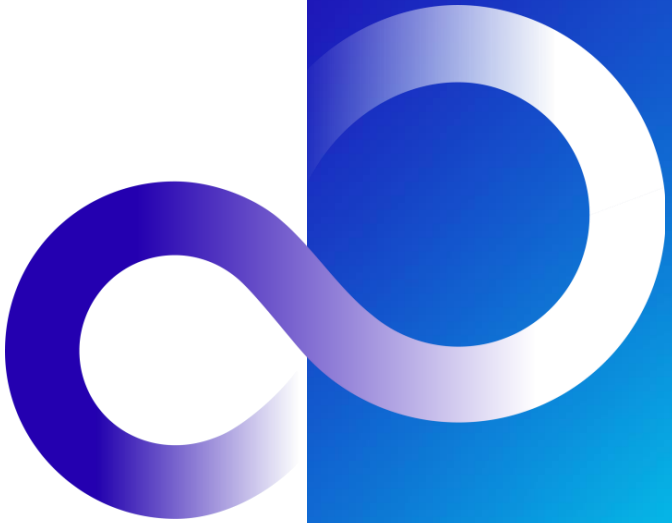
SS研システム技術分科会会合
2023年1月20日（金）

ゼロトラスト時代で
注目を集める生体認証技術

富士通株式会社　富士通研究所
コンバージングテクノロジー研究所
　プロジェクトディレクター
　山田　茂史



自己紹介

- **2000年 株式会社 富士通研究所入社**
  - 2006年 米ウェストバージニア州立大学の客員研究員
  - ～2018年 画像・バイオメトリクス研究センター、セキュリティ研究所
    生体認証技術(指紋、手のひら静脈、顔)の研究開発
  - 2019～20年 デジタル革新コアユニット 認証・決済PJ
    生体認証の応用研究(手ぶらでの決済)、上席研究員(バイオメトリクス)
  - 2021年～ コンバージングテクノロジー研究所 ソーシャルデザインPJ
    生体認証による社会課題解決の研究
- **社外：生体認証の評価方法の専門家**
  - ISO/IEC JTC 1/**SC 37(バイオメトリクス)のWG5(試験及び報告)、WG1(専門用語)主査**
  - ISO/IEC JTC 1/**SC 27(情報セキュリティ)のWG5(アイデンティティ管理とプライバシー技術)のエキスパート**
  - ISO/TC 68(金融サービス)委員
  - 経産省受託事業「令和2年度 **キャッシュレス取引のセキュリティ性に関わる生体認証精度評価**を容易とする精度評価方法に関する国際標準化」委員

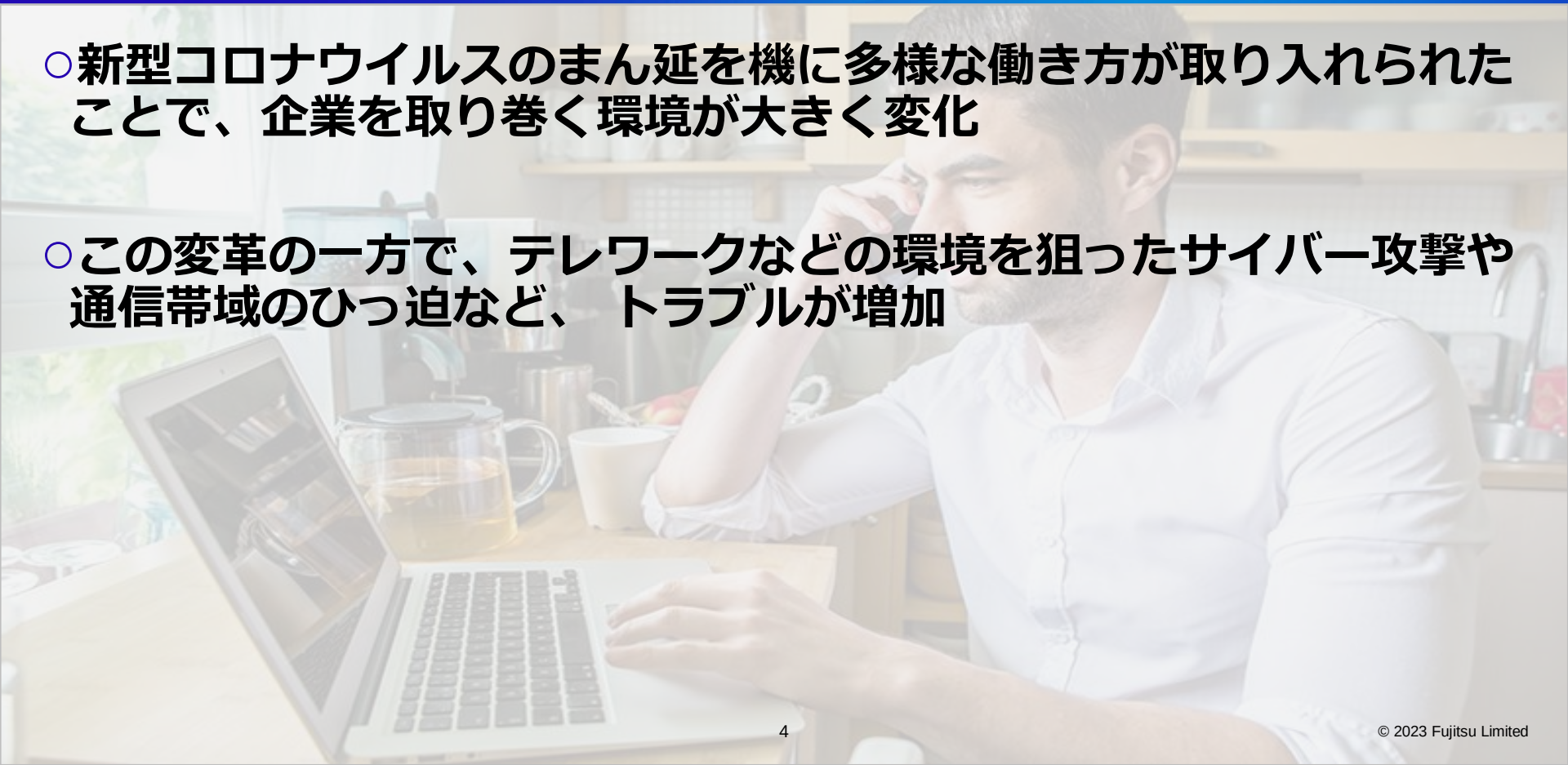
アジェンダ

FUJITSU

- 背景：新たな働き方の実現、ゼロトラストとは
- 認証技術の動向(多要素認証技術、パスワードレス等)
- 富士通の注力する領域：生体認証技術
- ユースケース紹介
- まとめ

新たな働き方の実現

FUJITSU



○新型コロナウイルスのまん延を機に多様な働き方が取り入れられたことで、企業を取り巻く環境が大きく変化

○この変革の一方で、テレワークなどの環境を狙ったサイバー攻撃や通信帯域のひっ迫など、 トラブルが増加

情報セキュリティ 10大脅威 2022

FUJITSU

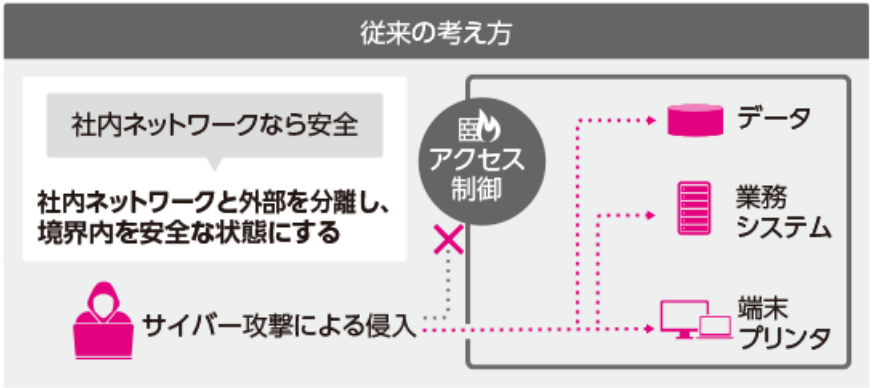
順位	組織視点	昨年順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の搾取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位
4位	**テレワーク等のニューノーマルな働き方を狙った攻撃**	**3位**
5位	内部不正による情報漏えい	6位
6位	脆弱性対策情報の公開に伴う悪用増加	10位
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
8位	ビジネスメール詐欺による金銭被害	5位
9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	不注意による情報漏えい等の被害	9位

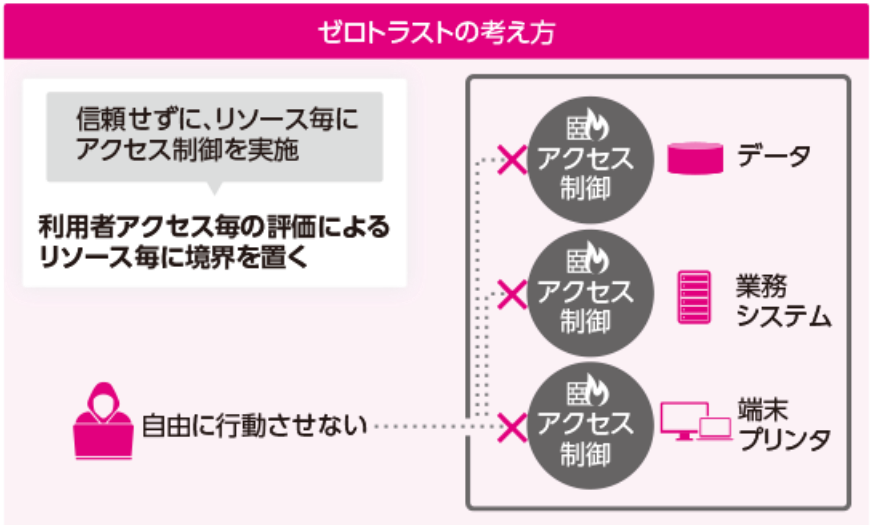
出典：情報処理推進機構　情報セキュリティ10大脅威 2022
https://www.ipa.go.jp/security/vuln/10threats2022.html

ゼロトラストとは

FUJITSU

○「ユーザ、デバイス」を「場所」で信頼せず都度検証する考え方、
アクセス制御が成功のカギ





FUJITSU

認証技術の動向
(多要素認証技術、パスワードレス等)

本人認証の手段

FUJITSU

- 本人が本物(正当)であるかを確実にすること（真正性の確認）
- 事前に登録されている本人に関する情報を用いて本人であることを確認
- 認証は用いる情報の特性により3要素のいずれかに分類

知識（記憶）認証

例）PIN、パスワード

貸し借り、忘却、盗難、
推測のリスク有

所有物認証

例）免許証、パスポート

貸し借り、紛失、盗難、
偽造のリスク有

生体認証

例）指紋、静脈、顔

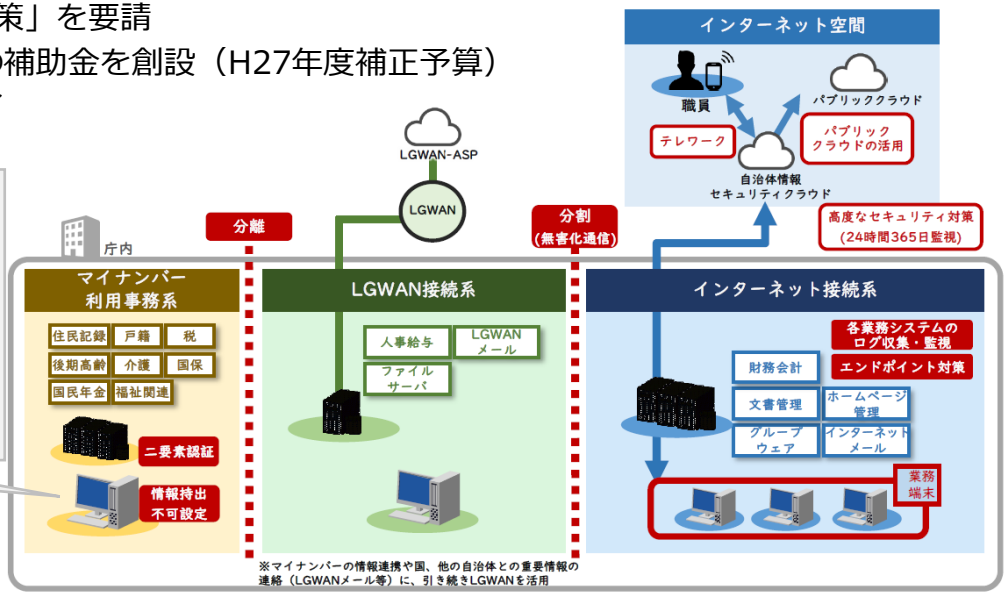
貸し借り、忘却、紛失、
盗難、偽造のリスク小

国内：自治体の情報セキュリティ強靭化(～2017年)

FUJITSU

- **総務省による「地方公共団体における情報セキュリティポリシーに関するガイドライン」**
- 対策要請の経緯
  - 2015.5 年金機構の情報漏えい事案発覚後、有識者による「自治体情報セキュリティ対策検討チーム」を設置
  - 2015.11 検討チームより自治体の対策内容（「三層の対策」）について報告
  - 2015.12 総務大臣通知により自治体に「三層の対策」を要請
  - 2016.2 自治体が「三層の対策」に取り組むための補助金を創設（H27年度補正予算）
  - 2017.7 自治体による「三層の対策」への対応完了

マイナンバー（個人番号）利用事務系：
原則として他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や**端末への二要素認証(①知識、②所有物、③生体認証の内、2種類を組み合わせて認証)の導入**等を図ることにより、個人情報の流出を徹底して防ぐこと



出典：総務省
https://www.soumu.go.jp/main_content/000777002.pdf

ご参考：自治体セキュリティ強靭化実績(2016年度)

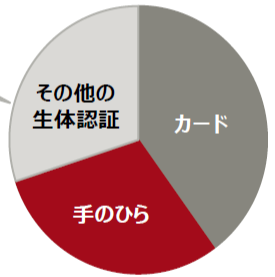
FUJITSU

全国約1,800の自治体の内、500団体以上が手のひら静脈認証を採用！

（カードが40%程度と仮定すると、生体認証の中で約50%のシェアを確保）

他方式（指紋・指静脈・顔）の合計で約30%程度

採用比率（想定）



PalmSecureが生体認証トップシェア

セキュリティ強靭性向上モデルとは

個人番号制度の開始に伴い、総務省が地方公共団体向けに複数のセキュリティ対策を義務付けたもので、必須事項の1つとして2要素認証が求められている。2要素認証とは①知識（パスワード）、②所持（カード、USBキー等）、③存在（生体）の内、2種類を組合わせて認証を行う形式。

米国：電子的認証に関するガイドライン(2017年)

FUJITSU

- **2017年6月に、米国政府機関のアメリカ国立標準研究所(NIST)が「Digital Identity Guidelines (NIST SP 800-63-3)」を発表**
  - 本ガイドラインは米国政府機関での利用を前提としているが、**各国の政府や民間企業により参考**にされている。
  - **SP 800-63-3 :Digital Identity Guidelines**
  - SP 800-63A :Enrollment and Identity Proofing
  - SP 800-63B :Authentication and Lifecycle Management
  - SP 800-63C :Federation and Assertions


NIST Special Publication 800-63
Revision 3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-63-3
Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
Applied Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, Calif.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

June 2017
Includes updates as of 03-02-2020

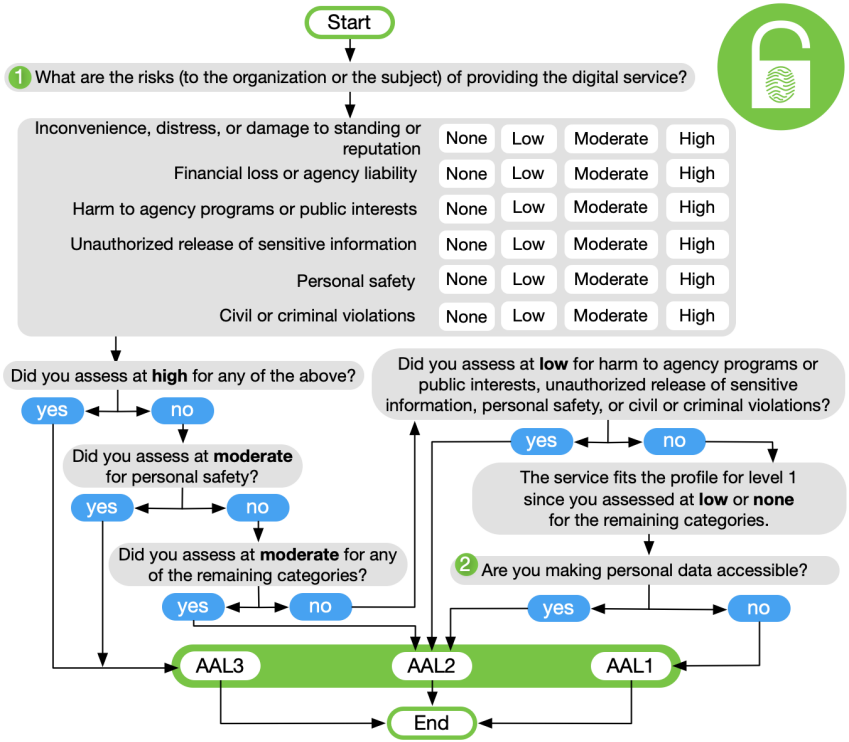
※NISTサイト：https://pages.nist.gov/800-63-3/sp800-63-3.html
※翻訳版：https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.ja.html

米国：電子的認証に関するガイドライン(2017年)

FUJITSU

- **保証レベル（Assurance Level）も3種類で定義**
  - IAL：Identity Proofing プロセスでの保証レベル
  - AAL：Authentication プロセスでの保証レベル
  - FAL：フェデレーションでの認証情報(および属性情報) をサービス提供者に伝達するAssertionの強度についての保証レベル

AAL	使用可能な認証要素
AAL1	単要素認証が必要
AAL2	2要素認証が必要
AAL3	2要素認証が必要（ハードウェアベースのCryptographic Authenticatorが必要）



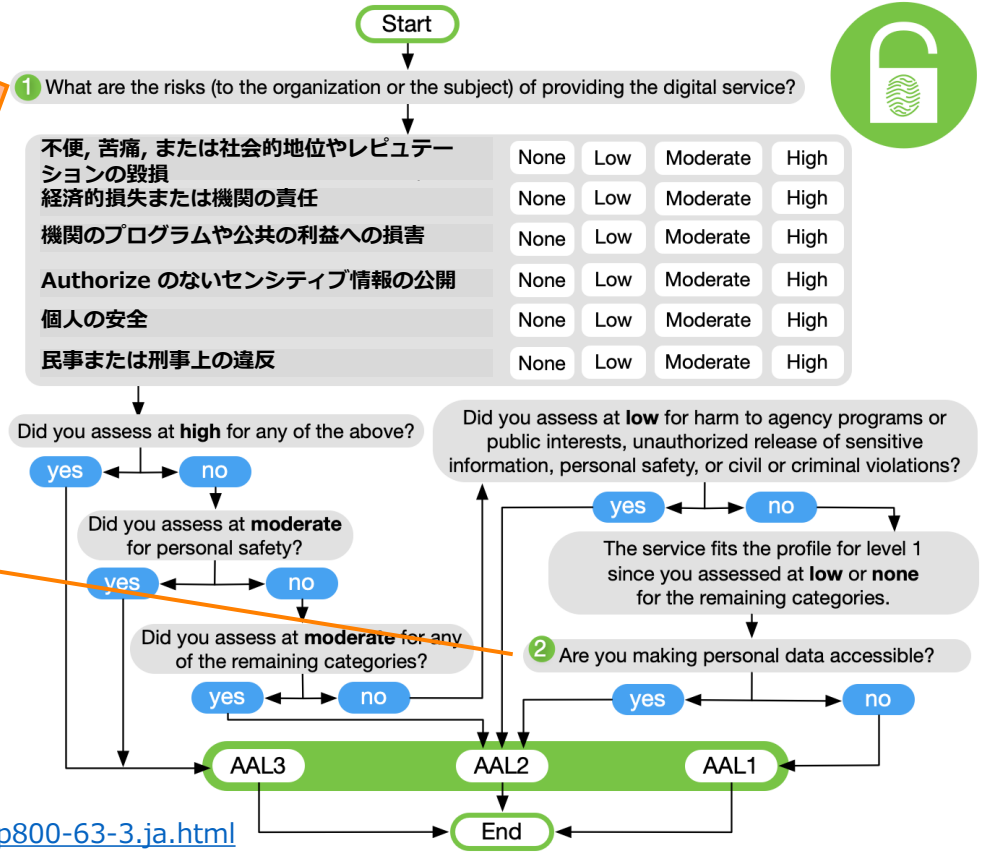
※出典：https://pages.nist.gov/800-63-3/sp800-63-3.html

米国：電子的認証に関するガイドライン(2017年)

FUJITSU

Authentication 失敗の潜在的影響に着目する. これはつまり, **Authorize されていないユーザーが正規のユーザーアカウントに Access できた場合, 何が起こるか**ということである. 片方にはネガティブな影響がない場合でも, もう一方には著しい被害が及ぶ可能性もあるため, **リスクは組織およびユーザーの両方の視点で考慮**すべきである. 機関の Risk Management プロセスはこのステップから開始されるべきである.

Personal Information にオンラインでアクセス可能な場合は, MFA が必要となる. この決定木の他のパスではすでに MFA が必要な AAL が確定しているため, Personal Information に関して問われるのはこの段階のみとなる. Risk Assessment 実施に際しては, 全ての AAL で Personal Information の公開に関して検討すべきである. このステップで重要な点は, Personal Information をオンラインで収集しない場合, AAL2 以上を要求するために Personal Information を確認・検証する必要はないということである. Self-asserted Personal Information の公開時も MFA によるアカウント保護は必要である. Self-asserted な情報は偽造可能だが, ほとんどのユーザーはデジタルサービスの恩恵を受けるため正しい情報を提供するであろう. したがって Self-asserted データは適切に保護しなければならない.



※出典：https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.ja.html

パスワードレス認証の動向

FUJITSU

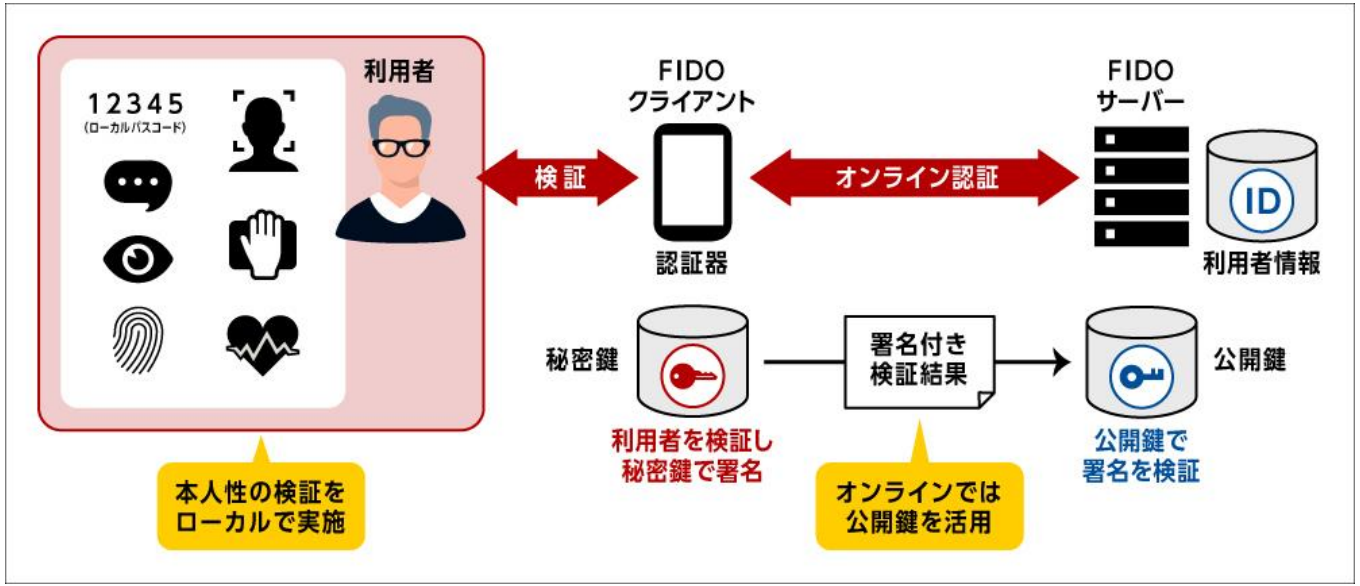
- **FIDO Alliance（Fast IDentity Online)**
  - **パスワードレスなオンライン認証技術**の標準化を推進する国際的な非営利団体(2012年2月発足)
    - 規格に加え、互換性・セキュリティ認定の仕組みも含む、エコシステムを構築
  - 約250の企業や組織、団体が参加
    - 富士通はスポンサー会員として2016年8月加盟

fido ALLIANCE simpler stronger authentication

FIDO認証の基本方式

FUJITSU

- **端末とサーバで秘密を共有しない方式**
  - 利用者がスマートフォンやパソコンなどの端末＝認証器（Authenticator）に適切な秘密鍵を保有し、それを検証することで認証を実現
  - 認証器側の簡単な操作だけで動的な多要素認証を達成

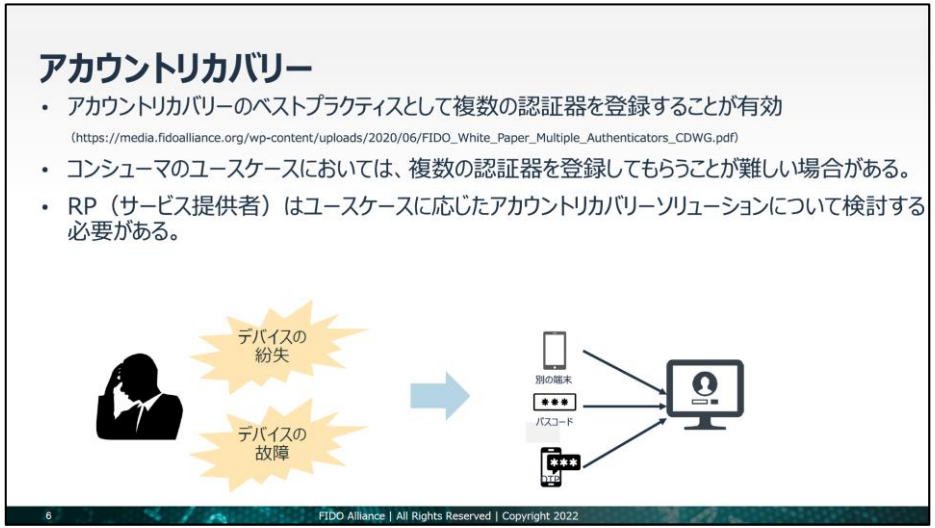


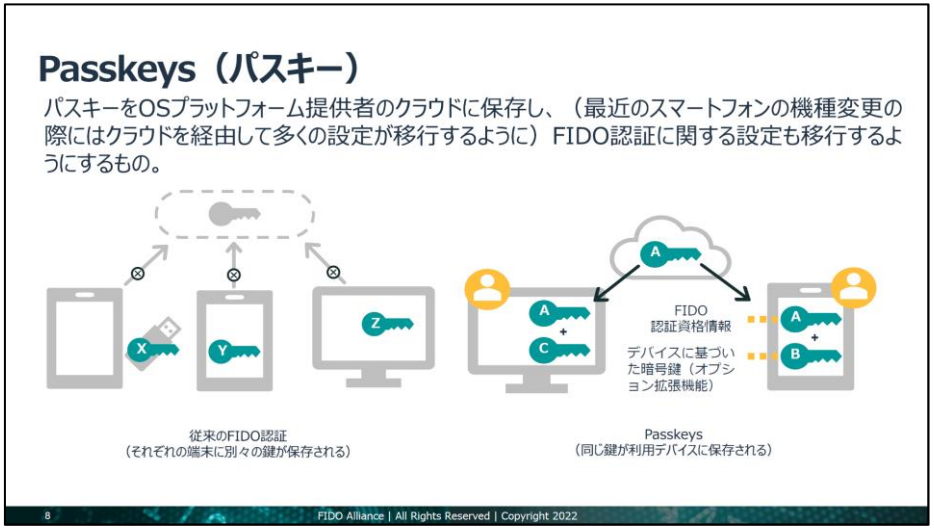
FIDOの最新動向

- **Apple、Google、MicrosoftがFIDO標準のサポート拡大にコミット、パスワードレス認証の普及を促進**(2022年5月)

  ※出展：https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins-jp/?lang=ja

- **アカウントリカバリーへの対応**(2022年12月)





※出展：https://media.fidoalliance.org/wp-content/uploads/2022/12/Keiko-Itakura_What-are-Passkeys-final-as-of-Dec-12.pdf

富士通の注力する領域：
生体認証技術

- 手のひら静脈認証
- 顔認証
- マルチ生体認証

本人認証の手段

富士通は、セキュリティと利便性を両立できる生体認証に注力
（利用者にとっては認証の手間、導入側にとっては導入のしやすさ）

知識（記憶）認証

例）PIN、パスワード

貸し借り、忘却、盗難、
推測のリスク有

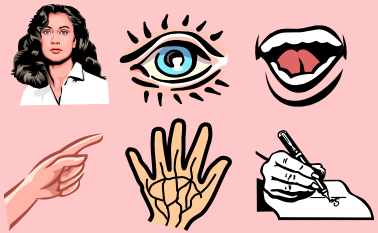
所有物認証

例）免許証、パスポート

貸し借り、紛失、盗難、
偽造のリスク有

生体認証

例）指紋、静脈、顔



貸し借り、忘却、紛失、
盗難、偽造のリスク小

生体認証とは

- **個人の身体的・行動的な特徴を用いて、個人を自動的に同定(認証、識別)する技術**
- 生体情報の基本的性質：
  - **普遍性（universality）**：誰もが持っている特徴であること
  - **唯一性（uniqueness）**：本人以外は同じ特徴を持たないこと
  - **永続性（permanence）**：時間の経過とともに変化しないこと

身体的特徴

顔

指紋

虹彩

静脈

行動的特徴

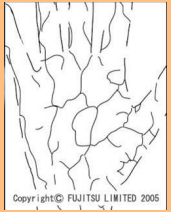
声紋

署名

一般的な生体認証の流れ

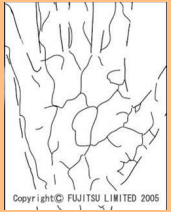
FUJITSU

登録時



①生体情報の入力　②生体情報の取得　③特徴抽出　④登録

認証時



①生体情報の入力　②生体情報の取得　③特徴抽出

④照合

⑤判定
「認証OK/NG」
に応じた処理

富士通の生体認証技術の研究開発

FUJITSU

1985 1990 2000 2010 2020

指紋


入退出管理


ノートPC


携帯電話


スライド指紋


スマートフォン

手のひら静脈


ATM


ノートPC


タブレット


一体型装置

クラウドサービス

顔認証


実用化


なりすまし検知 マスク対応

マルチ生体認証
(生体認証の利用者数拡大)


手のひら静脈と指紋


手のひら静脈と顔

生体認証で安全と便利さを提供

手のひら静脈認証技術

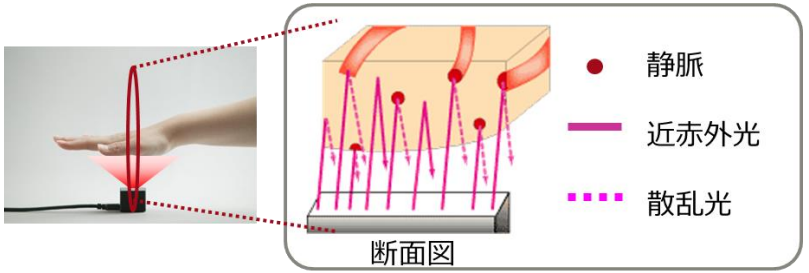
FUJITSU

○手のひらの静脈パターンで個人を識別する富士通独自の技術

安全性
- 静脈は体の中の情報なので**盗まれ難い**
- 静脈は**万人不同、経年変化しない**

認証精度
- 手のひらは**認証精度が高い**
- 幹線の**太い血管がメイン**に走っている

受容性
- 手のひら静脈は**誰でもいつでも**認証に使える部位
- 非接触で**衛生的かつ誰でも抵抗なく**利用できる



静脈パターンの取得方法

富士通研究所の実験装置で撮影した画像

○世界トップレベルの認証精度

- ○他人受入率0.000001%以下(**1億回に1回**程度)

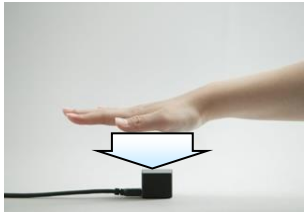
手のひら静脈認証の動作原理

① 手をかざす

手のひら静脈センサー

② 近赤外線照射

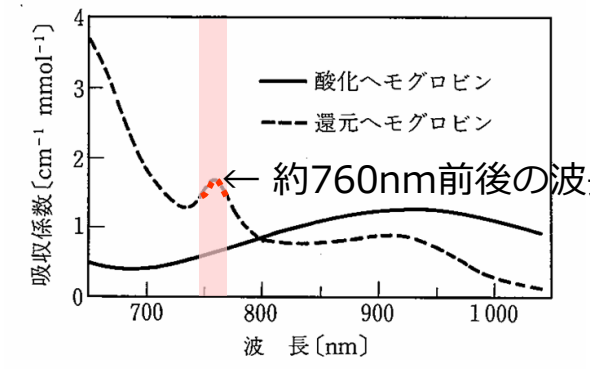
③ 撮像



⑤ テンプレート格納

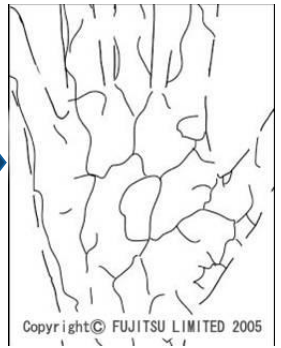
数値化＆暗号化

④ 抽出



ヘモグロビンの吸光スペクトル
コロナ社　生体情報の可視化技術編集委員会編
「生体情報の可視化技術」(1997)より

【近赤外画像】



【静脈パターン画像】

グローバルで利用される手のひら静脈認証

FUJITSU

EMEIA
2,000
万人

手ぶら決済

ATM

北米
3,200
万人

患者認証

医療保険
利用者確認

アジア
2,500
万人

個人情報アクセス

南米
2,300
万人

年金受給者
生存証明

世界約60ヶ国、1億人に利用される技術

全世界の静脈認証利用者の８割は手のひら静脈認証を使用

顔認証技術

FUJITSU

静脈認証で培った**生体認証技術**とAIで培った**深層学習技術**をベースに開発

1	業界トップレベルの認証精度	：他人受入率0.001%以下（10万回に1回以下）
2	高い安全性	：顔写真などによる他人へのなりすまし防止
3	評価実績	：30か国以上の被験者で評価、第三者機関の評価

顔は**非接触**で取得、**高速に照合**できるため、
大規模の登録者から類似している人を**高速に絞り込む用途**に適する

マスク着用したままでも利用可能に

FUJITSU

- **技術課題：情報量が低下して本人が認識されにくい**
  - マスクで隠れていない目領域から特徴量を抽出
  - 顔全体の特徴量が抽出できずに情報量が低下して本人が認識されにくい課題があった
- **開発技術：マスクを付加した画像を生成して学習**
  - 頭の姿勢を推定して重畳するマスクの形を変えることで自然なマスク着用画像を生成
  - あらかじめ色・柄・形のマスクを付加することで様々なマスクへ対応

米国NIST主催の顔認証ベンダテストで**世界3位、国内ベンダー首位を獲得**(2021年11月)
マスク非着用時と同等程度の**絞り込み精度99%以上**を実現

手ぶらでの認証の技術課題

FUJITSU

スーパーマーケット

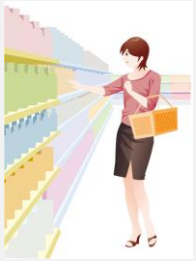
数万人

ショッピングセンター

十数万人

イベント会場

百万人規模



全国チェーンの
コンビニなど

それ以上・・・

手ぶらでの認証が活きる利用シーンでは100万人規模への対応が必要

一方で、**単一の生体情報のみの利用では数万人程度まで**

マルチ生体認証技術

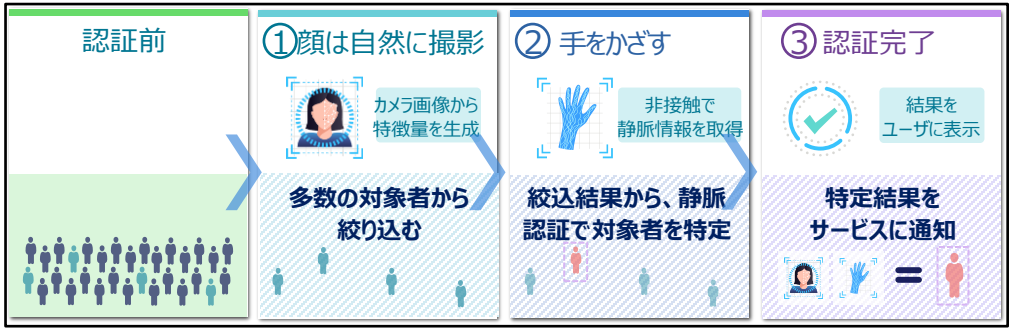
FUJITSU

○手のひら静脈と顔を組み合わせた生体認証技術

課題 一種類の生体情報だけを使う認証では数万人規模まで

解決策 1

手のひら静脈と顔の融合で100万人規模に拡大



課題 マスクを着用した状態での本人確認

解決策 2

マスク着用でも高精度な顔絞り込み

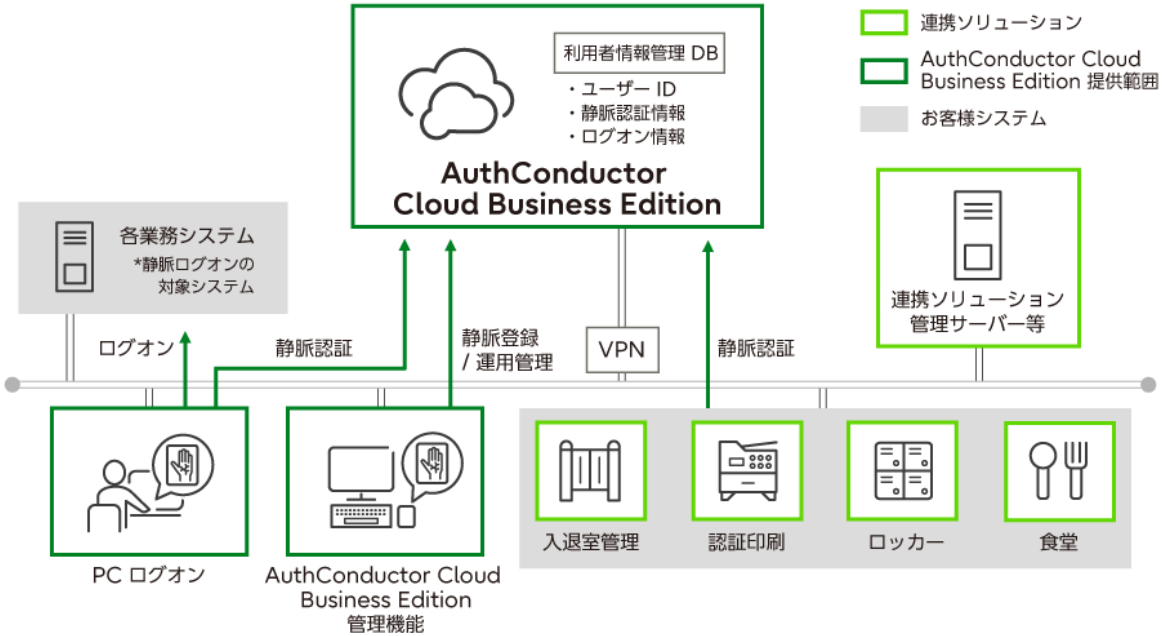
マスク着用部門で世界3位 (米国NISTのFRVT 1:1 21年8月)

ユースケース紹介

統合認証ソリューション

FUJITSU

○ 手のひら静脈認証でストレスフリーなオフィス環境を実現
FUJITSU Security Solution AuthConductor Cloud Business Edition



メリット：
パスワード、IC カード等の管理や接触による不安を解消

出典：https://www.fujitsu.com/jp/services/auth/solutions/authconductor/cloud-be/?auth

完全手ぶらにより、利便性の向上

従来のIDカード認証のように「持ち歩く意識」が不要。
忘れる心配もなく、ストレスフリーなオフィス環境へ。

端末セキュリティに閉じない様々なシーンへの適用

オフィス内の様々な用途への適用により、カードに変わる認証方式へ。
一度の登録で、全国拠点で利用可能（順次展開中）。

FUJITSU Kawasaki Tower 静脈認証 社内実践

あらゆるシーンで
手のひら静脈認証を採用。
手のひらでつながるオフィスを実現！

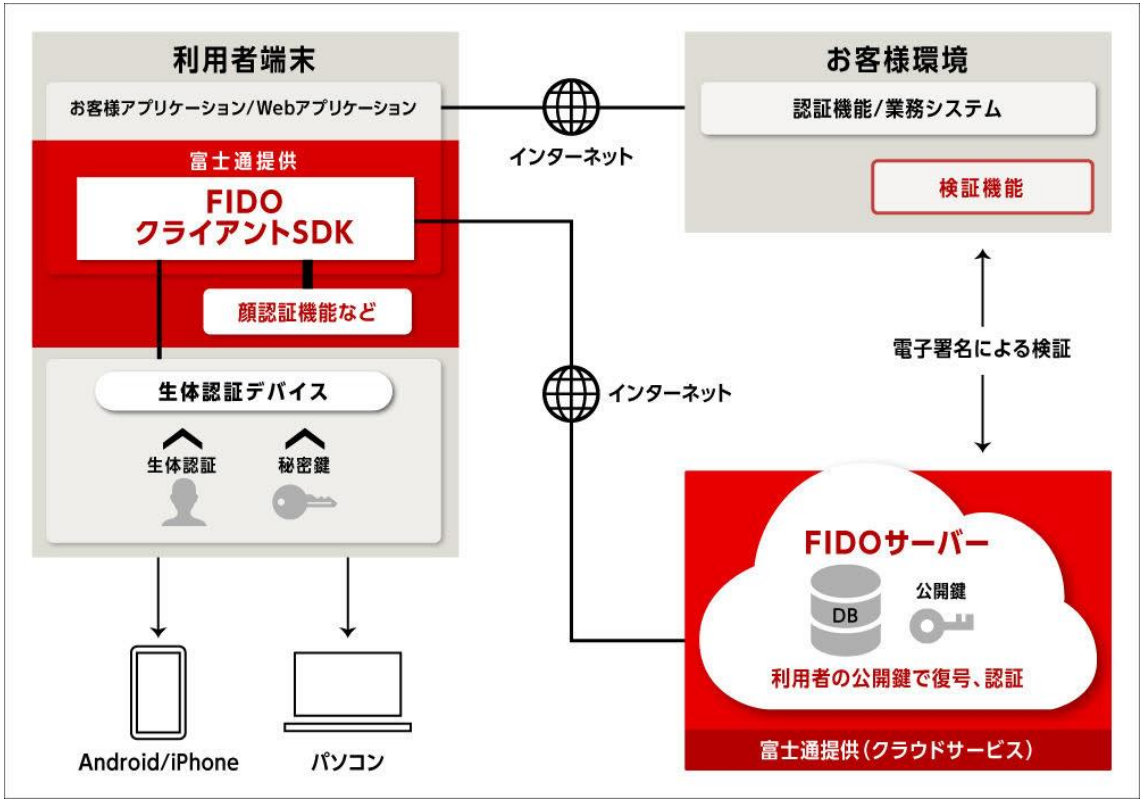
手のひらでつながるオフィス

サステナブルな
世界の実現に向けて、
生体認証テクノロジーの
社内実践で
見えてきたこととは

オンライン生体認証サービス(FIDO認証準拠)

FUJITSU

- **FIDOに準拠した認証機能を簡単に導入可能**
- 生体認証
  - 指紋、顔、虹彩、**手のひら静脈**



出典：https://www.fujitsu.com/jp/services/auth/solutions/bio-sensor-auth/?auth

多様なユースケース

まとめ

まとめ

FUJITSU

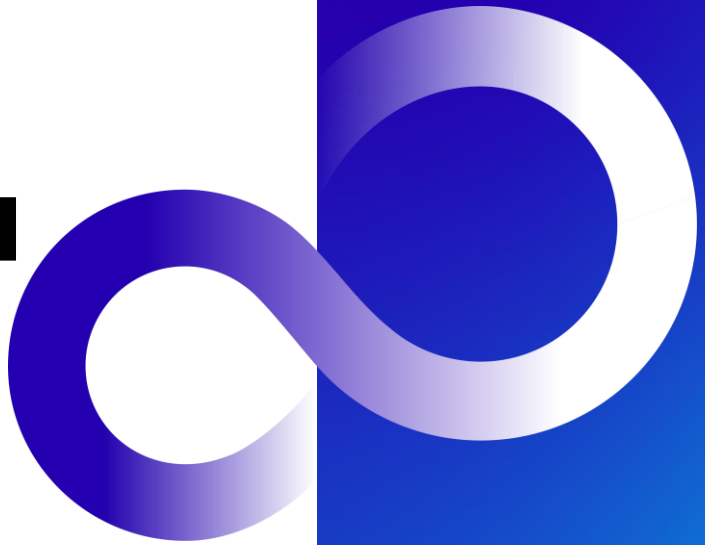
○新たな働き方の実現に向けて、利便性の向上とセキュリティ強化をバランスよく実現していくことが不可欠。ゼロトラストが重要に。

○認証技術の動向として、求められるセキュリティのレベルに応じて選択される多要素認証、利便性を求めてパスワードレス認証が普及。

○セキュリティと利便性を両立できる生体認証もまた注目。

○ユースケースを通じて、多様な認証シーンにおける、認証操作の利便性や、認証方式の統一のニーズを紹介。

Thank you



FUJITSU