手のひら静脈を中心としたクラウド型認証基盤サービスの社内実践

In-house Practice of Cloud-based Authentication Platform Service Centering on Palm Vein Technology

● 鈴木優子　● 新潟敦子　● 濱田真之

あらまし

富士通は，これまで培ってきた手のひら静脈による認証を中心として，デバイスの特性を活かす複数の高セキュリティな認証手段を提供するクラウド型認証基盤サービスの構築に取り組んでいる。本サービスは，富士通における生体認証および認証サービスに関わる知見を組織横断的に結集して具現化するもので，まず社内実践によって徹底的に活用し，ブラッシュアップした上でお客様や社会に提供することを目指している。認証手段は，手のひら静脈，虹彩，指紋などの生体認証や，専用媒体不要のワンタイムパスワード(OTP)などを提供し，認証連携インターフェースは，SAML(Security Assertion Markup Language)をはじめとする複数の標準プロトコルを取りそろえている。

本稿では，業界トップレベルの認証精度を誇る富士通の手のひら静脈認証技術を中心に，本クラウド型認証基盤サービスが提供する安心・安全な認証機能について述べる。

Abstract

Fujitsu has been working on constructing a cloud-based authentication platform service that provides multiple means of high-security authentication, making use of device characteristics. In this service, the central role is played by authentication via palm vein technology, which Fujitsu has cultivated up to now. This service is realized by cross-functionally bringing together knowledge relating to biometrics and authentication services at Fujitsu. It is intended to be offered to customers and society after it has been thoroughly utilized and brushed up by in-house practice. The authentication means offered include biometrics such as palm vein, iris and fingerprint authentication and one-time password (OTP) not requiring dedicated media. In addition, as authentication federation interfaces, multiple standard protocols including Security Assertion Markup Language (SAML) are available. This paper describes the safe and secure authentication features offered by this cloud-based authentication platform service, mainly including Fujitsu's palm vein authentication technology, which can boast of having one of the highest authentication accuracies in the industry.

ま え が き

近年，サイバー攻撃の被害は増大の一途をたどっている。この対策には，マルウェア検知，ネットワークセキュリティ，トレース機能の強化などによる多層防御が必要とされている。中でも，なりすましを防ぐ本人認証は重要な施策である。今や固定パスワードによる本人認証だけでは十分とは言えない（**図-1**）。[(1)] しかし，それに代わるICカードやPKI（Public Key Infrastructure），ハードウェアトークンによるワンタイムパスワード（OTP）などは，運用のコスト増大や難しさ，専用物理媒体を利用する煩雑さやその紛失・盗難リスクなどが普及の壁になっている。一方で，特に企業などの組織において，スマートフォンやクラウドサービスを活用し，外出先や在宅環境から手軽かつセキュアにシステムを利用できる環境が求められている。更にこの環境には，クラウドサービスのメリットを最大化するために「すぐに利用開始できる」ことや，既存システムとの連携なども必要とされている（**図-2**，**図-3**）。[(2)]

以上の状況から，認証には次の三つの大きな課題があると考えられる。

(1) 高度なセキュリティと利便性の両立

(2) 様々なサービスにセキュアに接続する柔軟性

(3) 必要なときに即時利用開始可能な仕組み

これらの課題は富士通社内でも同様で，現在運用中のICカードとPKIの組合せによる認証はセキュアであるが，新しいワークスタイルに十分応えられないという状況にある。

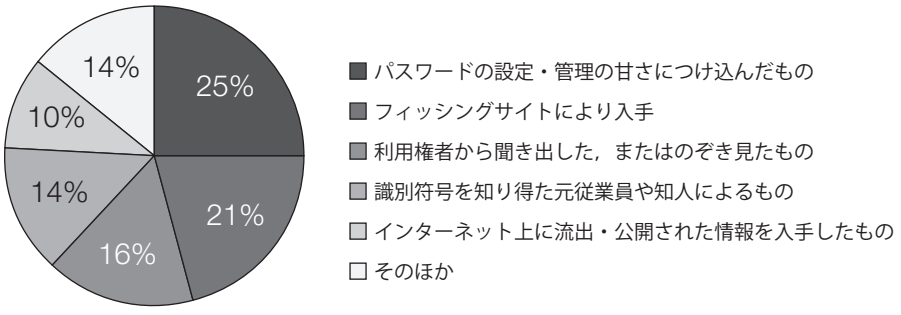
一つ目の課題を解決する有力な手段が生体認証である。富士通には，業界トップレベルの認証精度を持つ手のひら静脈認証技術[(3), (4)]がある。手のひら静脈認証による本人認証は，手をかざすだけの手軽さと，なりすましがほぼ不可能という高いセキュリティ強度を併せ持つ。二つ目の課題解決には，認証サービスとしてより多くの標準プロトコルによる認証連携インターフェースを準備することである。そして，オープンかつセキュアな業務環境を構築するには，この2点は必ずセットで提供する必要がある。三つ目の課題解決策は，認証サービス自体をクラウドサービス化することである。富士通ではこれらを実現するために，関係部門が連携して新たな認証基盤を構築し，社内実践を行った上でお客様へ提案することとした。

本稿では，社内における認証の具体的な課題と，その解決に向けた取組み，新たな認証サービスの特徴と導入効果，お客様へのソリューション提供に向けた今後の計画について述べる。

■2014年 不正アクセス行為の検挙件数

識別符号窃用型（検挙件数）	336件
セキュリティホール型（検挙件数）	2件

■2014年「識別符号窃用型（検挙件数）」の犯行手口内訳



「識別符号窃用型」のほぼ全てが固定IDパスワードに起因

総務省「平成26年度不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」を基に作成

図-1　2014年不正アクセス行為の検挙件数および「識別符号窃用型（検挙件数）」の犯行手口内訳

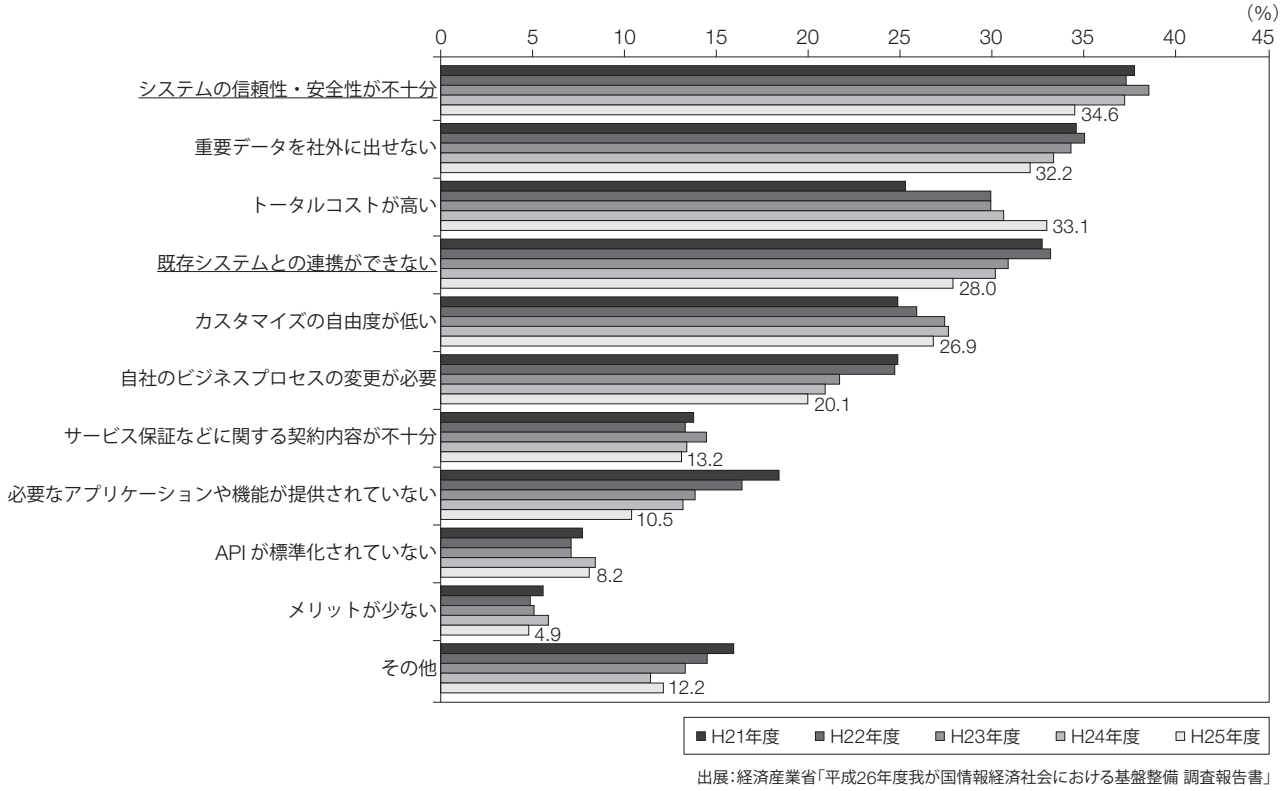


図-2　クラウドコンピューティングの導入・利用上の課題の推移

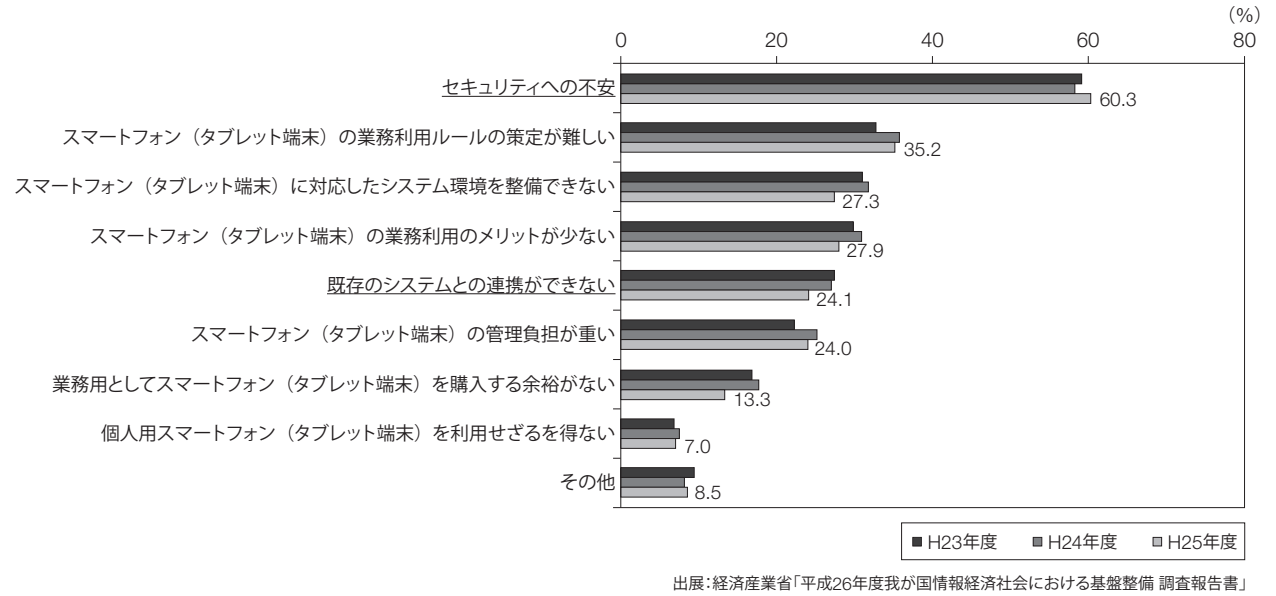


図-3　スマートフォンおよびタブレット端末の業務利用上の課題

ワークスタイル変革に伴う課題

富士通社内システムの認証は，情報の秘匿性に応じて，ICカードにPKI秘密鍵を格納して使用するPKIカード認証（高セキュリティ認証）と，ActiveDirectoryによるIDパスワード認証（基本認証）に集約してきた。しかし，近年のワークスタイル変革に伴い，まえがきで述べた三つの課題が

顕在化している。

(1) 高度なセキュリティと利便性の両立

いつでもどこでも業務ができる環境に向けて，スマートデバイスからのカレンダー/メールアクセスに加え，今後は社内情報へのアクセスも実現していく。このためには，高セキュリティ認証が必要である。現時点ではPKIカード認証を適用することになるが，その利用イメージは，まずカードを取り出し，スマートフォンにかざしながら秘密鍵を読み出すためのPIN（Personal Identification Number）を入力するというものである。この方法では，端末特性であるポータビリティ，手軽さ，ひいては業務スピードを著しく阻害する上，カードの紛失リスクも上がってしまう。このため，利便性を維持しつつ高いセキュリティを実現する新たな方法が必要となる。

(2) 様々なサービスにセキュアに接続する柔軟性

これまで，業務システムは社内に閉じており，認証連携インターフェースを独自方式で統一すれば，認証IDの一元化は成立した。今後クラウドなどのサービスを利用する場合も，IDは一元管理によって統制した上で活用すべきであるが，独自方式ではこうした統制はできない。業務環境を拡大するためには，様々なサービスとセキュアにつなげられる環境の提供が必要となってきている。

(3) 必要なときに即時利用開始可能な仕組み

業務や人のグローバル化に伴い，社内の情報資産もグローバルに均質なセキュリティで守る必要がある。また，世界のどこにいても，どの業務システムでも，同じ認証操作感であることが理想である。このためには，日本で構築した認証サービスを，容易かつ短期間で海外拠点にも横展開できる仕組みが必要である。

以上3点の課題解決に向け，以下の3本柱をコンセプトとした認証基盤サービスを構築することとした。

(1) 高セキュリティと利便性を両立させる生体認証
(2) 複数の認証連携標準規格サポート
(3) すぐに使えるクラウドサービス化

商用化を目指した基盤開発

基盤開発に当たっては，社内向けの基盤を作るのではなく，クラウド上の商用サービス化を目指した。手のひら静脈や虹彩といった生体認証技術とクラウドサービスは，富士通の強みである。この強みを組み合わせた認証基盤を社内実践を通じて徹底的にブラッシュアップし，そのままお客様に提供することが最良と考えた。一方，セキュリティビジネスを担う関連部門でも，前章で挙げた同様の課題に対し新ソリューションの検討を開始していた。そこで，社内IT部門とセキュリティビジネス関連部門で組織横断プロジェクトを立ち上げ，共同で開発に当たることとした。立上げ当初から商用化を目指して，社内IT部門とセキュリティビジネス関連部門が共同開発を実施するという取組みは，まさに富士通が標榜するFUJITSU Security Initiative[5]の実践である。

このメリットは，設計段階から利用・運用現場の声を盛り込めること，商用化を目指すため悪い意味での独自性や特殊性が自ずと排除されること，および実際に使用して得た実践知を反映したものをお客様に提供できることである。

社内IT事情の反映

前述の3本柱による認証基盤を社内に適用するに当たり，あらかじめ考慮すべき点がいくつかあった。その一つが，富士通グループでは実に多種多様なデバイスが業務に使用されていることである。更に，一人が複数のデバイスを保有し，事務所内や出先で適宜使い分けているということである。全てのデバイスに生体センサーを付けて生体認証に統一するのがベストであるが，10万人規模の利用者への適用は現実的ではない。かといって，脆弱性のあるパスワードで運用を続けるわけにはいかない。そこで今回は，あくまで生体認証を主要手段としながらも，ソフトウェアトークンによるOTPなど，デバイス依存性のない認証手段を準備し，デバイス特性に合わせた認証手段を選択できる仕組みを設けた（**図-4**）。生体認証と代替認証手段とのセキュリティ強度は同等ではないが，固定パスワード以上の高セキュリティ性と利便性は実現できる。この方法は，運用側においてはユーザーサポートの負荷が高くなるというデメリットもあるが，利用者側においては利便性のみを享受できる。

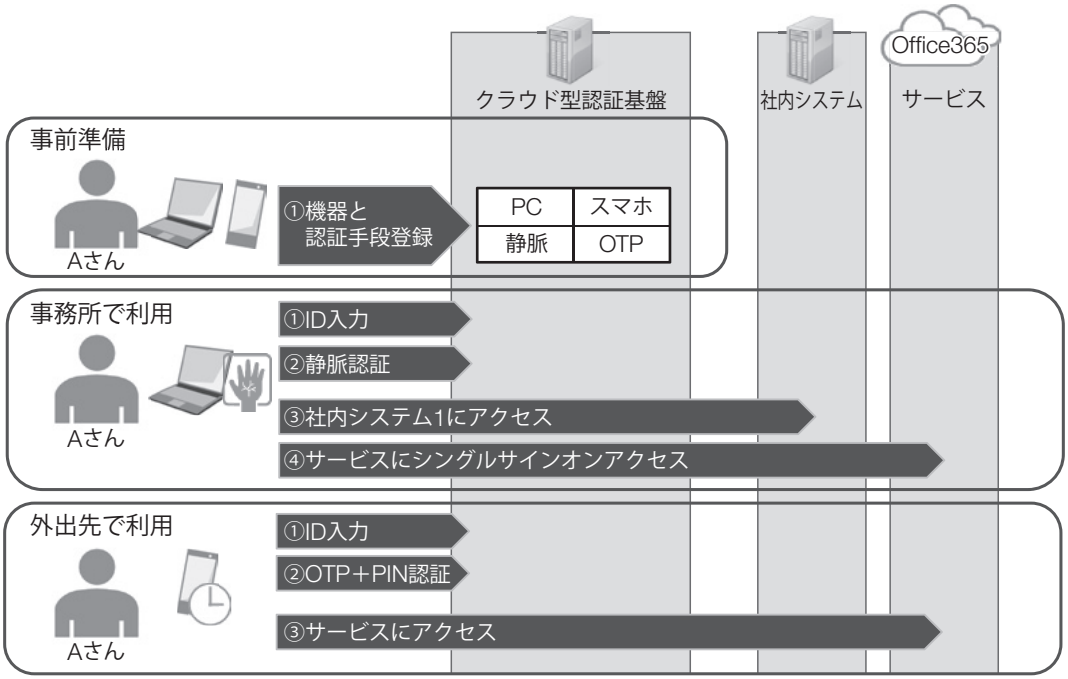


図-4　デバイス特性に合わせた認証手段

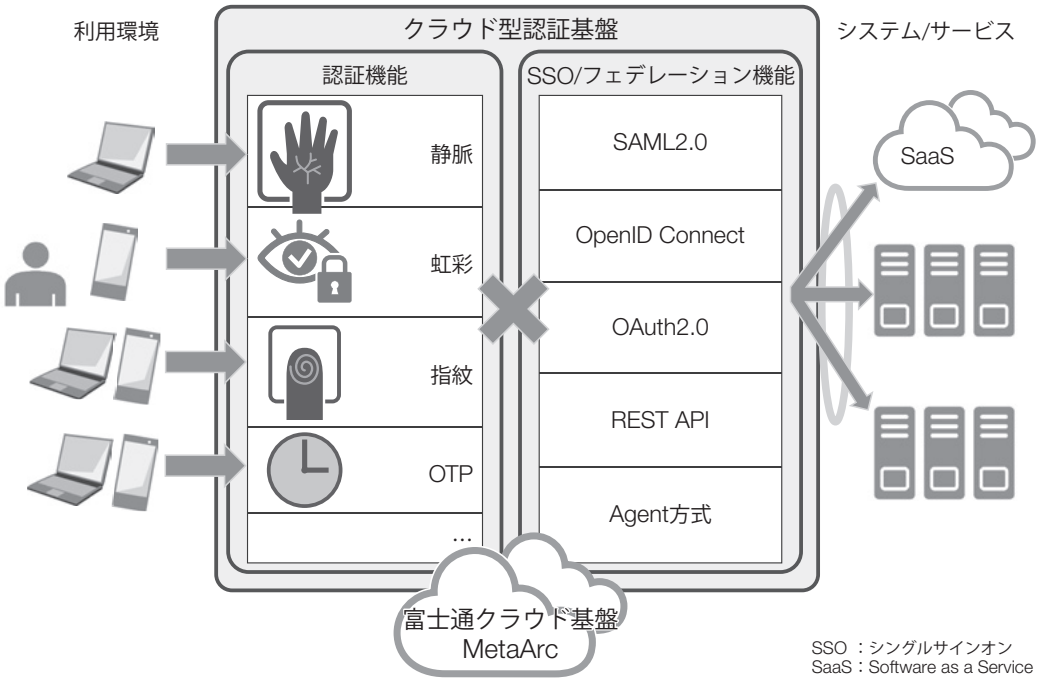


図-5　新認証基盤の主な機能

新認証基盤の特徴と導入効果

以上のようなプロセスを経て，前述の3本柱を盛り込んだ新たな認証基盤を以下のようなスペックで構築し，現在社内で試行中である（**図-5**）。

- インフラ：富士通クラウド基盤
- 認証手段：手のひら静脈，指紋，OTP｛ソフトウェアトークン，TOTP（Time-based One-time Password）方式｝
- 拡張検討中の認証手段：虹彩

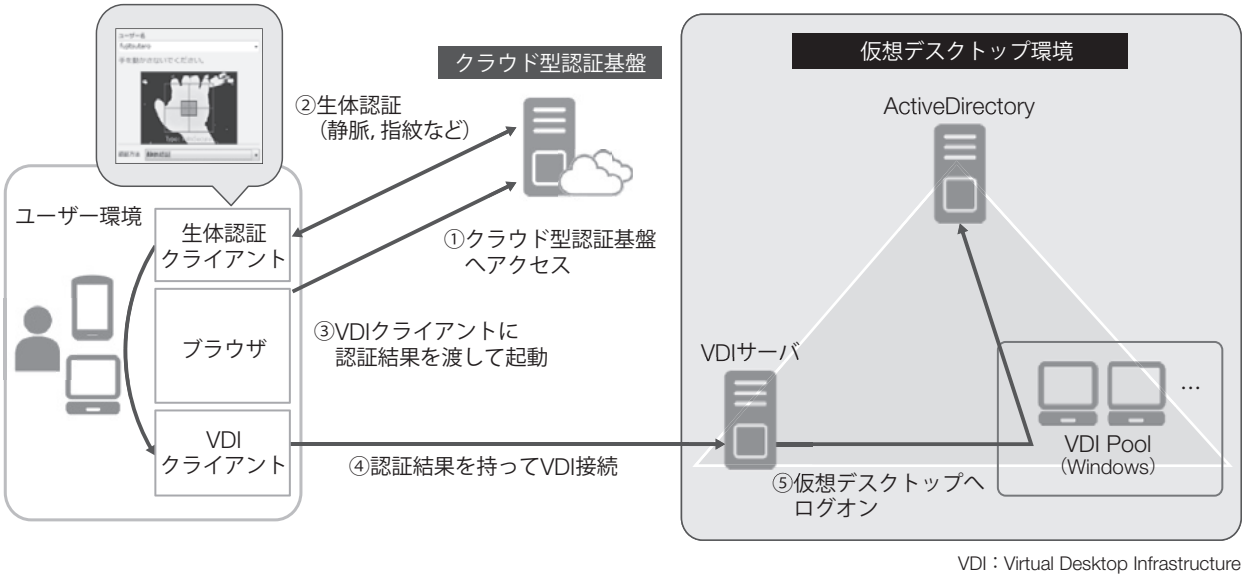


図-6　仮想デスクトップ環境への適用イメージ

・認証連携インターフェース：SAML（Security Assertion Markup Language）2.0，REST API，Agent方式，代理認証
・拡張検討中の認証連携インターフェース：OpenID Connect，OAuth2.0

本認証サービスは以下のような社内情報システム，および入退室管理システムなどを適用対象として検討中である。

・仮想デスクトップサービス
・Web業務システム
・Windowsログオン
・リモートアクセス
・無線LAN　など

また，商用サービス開始後，適用いただくお客様には以下のメリットがある。

（1）スマートデバイスなどの利便性を損なわない高セキュリティ認証の実現：安心・安全・便利なワークスタイルの確立。
（2）デバイス特性に合わせた高セキュリティ認証の使い分け：既存デバイスの有効活用。
（3）豊富な認証連携インターフェースで多くのクラウドサービスの認証を実施。

今後の計画

本認証基盤の今後の計画を以下に述べる。

（1）社内仮想デスクトップサービス認証への適用

2016年1月にトライアルとして適用し，2016年度から本格展開を開始する。認証インターフェースにはSAMLを用い，認証手段は生体およびOTPを提供する（**図-6**）。

（2）業務システムへの適用計画

富士通の社内システムは，今後5年の間に富士通のクラウド基盤FUJITSU Digital Business Platform MetaArc[6]に移行する方針であり，[7]これら移行システムに順次適用する。

（3）商用サービス化計画

社内実践でブラッシュアップした基盤機能を，MetaArcの共通認証基盤としてお客様にも提供する。また，今後の機能拡張も，社内実践を経てサービス化に移行する。

（4）機能拡張計画

社内要件として，リスクベース認証機能の提供，私物端末（BYOD：Bring Your Own Device）対応，および海外拠点への横展開を図る。

む　す　び

本稿では，スマートフォンやクラウドを外出先から活用するような環境でも，安心・安全に業務を行うための，手のひら静脈認証を中心とした新たなクラウド型認証基盤サービスについて述べた。現在は，数百の社内システムをいかにスムーズに

移行させるかという課題に取り組んでいる。この過程で得られるノウハウは，お客様にも活用いただけるものになると考えている。また富士通グループは，海外も含め17万人規模の従業員と数百の社内システムを抱える言わば巨大な実験場である。この実験場で，デバッグ，改善，ノウハウを蓄積した上でサービスを提供することは，お客様にとっても大きなメリットになると考えられる。この社内実践を通して課題解決，サービスレベルの向上を継続的に続けていく。

参考文献

(1) 総務省：平成26年不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況 別紙1「不正アクセス行為の発生状況」.
http://www.soumu.go.jp/main_content/000347975.pdf

(2) 経済産業省：平成26年度我が国情報経済社会における基盤整備 調査報告書.
http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H26_report.pdf

(3) 富士通：手のひら静脈認証FUJITSU生体認証PalmSecure.
http://www.fujitsu.com/jp/solutions/business-technology/security/palmsecure/

(4) 富士通：手のひらを専用センサーにかざすだけ！富士通の独自技術「手のひら静脈認証」.
http://journal.jp.fujitsu.com/2014/09/16/01/

(5) 富士通：セキュリティ.
http://www.fujitsu.com/jp/vision/2015/products/security/

(6) 富士通：デジタルビジネス・プラットフォーム「MetaArc（メタアーク）」.
http://journal.jp.fujitsu.com/metaarc/

(7) 富士通：グループ国内外すべての社内システムを次世代クラウド基盤へ刷新.
http://pr.fujitsu.com/jp/news/2015/02/18.html

著者紹介

鈴木優子（すずき　ゆうこ）
IT戦略本部デジタルビジネスプラットフォーム推進室 所属
現在，生体認証技術による本人認証基盤の社内実践プロジェクトに従事。

濱田真之（はまだ　まさゆき）
IT戦略本部デジタルビジネスプラットフォーム推進室 所属
現在，本人認証基盤の社内実践プロジェクトにおいて，主にワンタイムパスワード認証およびWeb業務システム適用推進を担当。

新潟敦子（にいがた　あつこ）
IT戦略本部デジタルビジネスプラットフォーム推進室 所属
現在，本人認証基盤の社内実践プロジェクトにおいて，主に基盤開発および仮想デスクトップサービスへの適用などを担当。