次世代生体認証システムと仮想化対応

Next-generation System for Biometric Authentication and Virtualization

● 山嶋雅樹　● 和田篤志　● 鎌倉　健

あらまし

今日，企業では多数の業務システムが運用されており，それらを使用する際の認証手段としてパスワード認証が多用されている。こうした中，シングルサインオン(SSO)システムの導入や，アプリケーションによるID/パスワードの自動入力で利用者・管理者の負担軽減が図られてきている。しかし，この方式には認証に用いるID/パスワードを安全に運用しなければならないという課題がある。富士通では，ID/パスワードを一元管理する個人認証専用サーバ「Secure Login Box」や生体認証実施後にID/パスワードを自動入力するソフトウェア「SMARTACCESS/Premium」によるSSOシステムを提供してきた。近年では，業務システムの運用効率化から従来のITシステムと業務アプリケーションのWebサービス化や一部クラウドサービスを利用して構成される複合型のシステムが広がりつつあり，認証システムはこのようなシステム構築の動向に対応していく必要がある。

本稿では，認証システムの現状と課題を整理した上で，設計・開発した次世代の生体認証システムについて述べる。

Abstract

Today, there are many IT systems in companies, and most of them require a password for personal authentication. In such circumstances, a single-sign-on function and a function to automatically input IDs and passwords have been developed, and these are useful not only for administrators but also for end users. However these functions have problems in terms of security. So Fujitsu has developed a personal authentication server, “Secure Login Box,” and client software, “SMARTACCESS/Premium,” which support biometric authentication and single-sign-on. Recently IT systems have been moving to Web-based and cloud-based ones to make system management easier, and authentication systems should follow these environment changes. This paper describes the current status of and problems with personal authentication technologies and the next generation of biometric authentication systems developed by Fujitsu.

ま え が き

従来，企業におけるITシステムは企業内ネットワークを敷設した上に構築されるクライアント/サーバ型の業務システムが主流で，複数の業務システムで異なるID/パスワードが用いられることもしばしばあった。IDの決め方としては，企業内ディレクトリサーバのIDのほかに，メールアドレスやグループ企業が独自に管理するID，所属コードや管理サーバを使って決めるものなど様々である。また，複数の業務システムが存在することで，パスワード要件も異なるケースがあり，最小文字数，有効期限の設定，利用可能な記号などが異なるといった具合に，異なるパスワードの設定を余儀なくされることがある。こうした状況から，ある特定のディレクトリシステムの適用範囲を拡大することや，ID/パスワード自動入力アプリケーションを用いることで認証ポイントを単一化することが図られてきている。しかし，一組のID/パスワードで全ての業務を利用可能にすることはその一方で，そのID/パスワードを安全に運用しなければならないという運用管理義務が課されることを意味する。

富士通では，ID/パスワードを一元管理する個人認証専用サーバ「Secure Login Box」や生体認証実施後にID/パスワードを自動入力するソフトウェア「SMARTACCESS/Premium」によるシングルサインオン（SSO）システムを提供してきた。(1)

2011年の東日本大震災を契機にディザスタリカバリの重要性が再認識されるとともに，業務システムの効率化を目指し，従来のITシステムと業務アプリケーションのWebサービス化や一部クラウドサービスを利用した複合型のシステムが広がりつつある。認証システムはこうしたシステム構築の動向に対応していく必要がある。すなわち，このようなシステムを安全に運用するためには，使用するのは許可された本人か，認証結果は信頼されたシステムから得られたか，といった情報を確実にチェックすることが必要である。

本稿では，認証システムの現状と課題を整理した上で，設計・開発した次世代の生体認証システムについて述べる。

パスワード認証の課題

● パスワード認証技術の課題

個人認証を行うための技術としては，パスワードを使った認証（知っている情報），ICカードによる認証（持っている情報），生体情報を使った認証（本人固有の情報）などがあるが，現在最も利用されているのはパスワードによる認証である。これは専用のハードウェアを要しないことが大きい。

ただし実装が容易な反面，多くの課題が以前より指摘されている。パスワードは「使用者だけが知っている」ことが大前提であるが，パスワードが文字列の情報であることから，本人が覚えられずメモを残したり，入力の際にのぞき見されたりすることでパスワードが漏えいする危険性を持っている。これを解決する手段として，使用している複数のパスワードを記憶しておくソフトウェアが存在するが，それを使用するためにはやはりパスワードが必要となり，危険性を排除するまでの根本的な解決には至っていない。

● パスワードを利用したシステム運用の課題

企業では多数の業務システムが運用されており，それらを使用する際の個人認証の手段としてその多くはパスワード認証が使われているが，以下のような課題がある。

一つ目は，企業としてのリスクである。近年多くの情報漏えい事件が発生しており，その一つの原因がパスワードの漏えいとなっている。例えば顧客情報の漏えいは企業活動において信頼を落とすことになり，発生を未然に防ぐ対策が求められる。

二つ目は，管理者負荷という懸念もある。先にも述べたとおり使用者が多くのパスワードを管理しなければならなくなると，それを忘れてしまい管理者に問い合わせることとなる。これが管理者にとっての悩みの一つとなっている。逆にパスワードを忘れないように，一つのパスワードを複数のシステムで使い回すということになると，漏えい時の被害が拡大する可能性があるといった課題も残る。

● ICカード認証と課題

パスワード以外の認証手段としてはICカードなどの物理的な認証がある。ICカードは入退出管理

システムで多く使用されており，ITシステムと兼用することで使用者はカードを1枚持っていれば各種システムを利用できるというメリットがある。その一方で「持っている」ことで本人を確認することになるため，紛失や盗難による「なりすまし」のリスクがつきまとう。また不所持によりシステムが使用できない場合に代替手段を用意する必要があるという運用上の課題も残る。

生体認証の現状と課題

● 生体認証技術と課題

次に利用されているのが生体認証であり，現在，指紋・静脈・虹彩・顔・声紋などが認証手段として採用されている。生体情報は本人のみが持っている唯一の情報であり，また紛失・不所持といった問題が発生しない。ただし，一部の利用者が認証できない場合や，利用環境によって認証可否が左右されるといった課題が指摘されている。生体認証は，生体情報を読み取るセンサとその生体情報を基に本人かどうかを判別する処理があるが，センサと認証処理それぞれの改良が進み，これらの課題は解決されつつある。

ここで挙げた各種生体認証の中で現在最も利用されているのは指紋認証である。指紋認証は高い認証精度を持ち，またセンサの小型化が進んでいるため，PCだけでなく携帯電話・スマートフォン・タブレットといったモバイル端末でも多く採用されている。

また注目すべき技術としては静脈認証がある。手のひら静脈認証の場合，直接センサに触れることなく，かざすだけで高い認証精度を実現し，非接触で使用できることが特長である。また体内に存在する静脈の情報を用いるため，皮膚の状態に左右されずに認証できることも大きな特長である。

● 富士通の生体認証技術への取組み

富士通研究所では，生体認証技術に対する需要をいち早く予測し，1984年に指紋認証技術，1996年にクライアント/サーバ型生体認証システム技術，2000年に手のひら静脈認証技術に関する研究開発を開始している。また，2011年には手のひら静脈と3指の指紋の生体情報のみを用いて100万人から1人をわずか2秒で識別する生体認証技術を開発し，2012年にはその規模を1000万人に拡大する精度向上を実現している。富士通では，生体認証技術の開発成果を入退室管理システム・銀行ATM・パソコンのログインシステムなど様々な製品に展開して高度なセキュリティを実現し，その応用分野を広げている（**図-1**）。

● 生体認証システムの課題

生体認証を各種システムの認証手段として適用することでセキュリティレベルを向上させることができるが，万能というわけではない。利用シーンによっては新たな課題が見えている。

まず，パスワード認証と併用している場合である。例えばパスワードの定期的な更新がポリシーとして必須の場合，管理者および使用者はその作業を定期的に行う必要がある。これにより，以前に使用していたパスワードを覚えておく必要があるが，日常で生体認証を使用していることでこれを忘れてしまう危険性がある。また，第三者もしくは悪意のあるユーザのパスワードによるシステムへの不正アクセスの対策として，一定回数以上の連続失敗でアカウントがロックされるシステムであれば，正当な利用者がパスワードを勘違いすることでアカウントがロックされる恐れがあり，管理者，およびユーザへの負担が大きい。

次に，仮想デスクトップ環境へ生体認証を適用しようとした場合である。認証を行いたいのは仮想デスクトップ，またはそこから接続するシステムであるが，端末側に接続されている生体認証デバイスをいかに安全につなげるかが課題となる。また，生体情報は高い精度を保つ必要があるため，一定のデータサイズを要するが，データを仮想デ

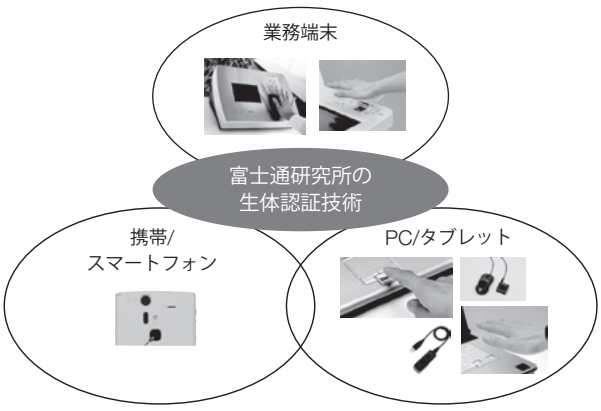

図-1　富士通の生体認証を採用した製品群

スクトップへ送信する際，ネットワークに負荷がかからないようにする必要がある。

更に別のケースとしては様々なサービス提供者と生体認証システムが連携する場合である。運用されているシステムがパスワード認証を採用しており，それに伴って生体認証システムは認証結果としてパスワード情報を渡してしまうこともある。すなわち，生体認証システムによる認証を必須とすることが困難である（**図-2**）。

次世代の生体認証システム

本章では，従来の認証システムの課題を踏まえ，端末・サーバ・サービスなどの多様な構成にも柔軟に対応する次世代の生体認証システムについて述べる。

● 想定されるリスクの場所

従来の生体認証システムでは，クライアント端末と生体認証サーバ，業務サーバを社内ネットワークに接続して運用することが前提となるケースが多かった。富士通が開発した個人認証専用サーバ「Secure Login Box（SLB）」と対応する個人認証クライアントソフト「SMARTACCESS/Premium（SMARTACCESS）」を利用した場合，処理の流れは以下のようになる。

- ID/パスワード入力画面を検知して生体情報の入力を促すダイアログボックスを表示
- 利用者が生体情報を入力してSLBに送信
- SLBで生体認証が成功するとID/パスワード情報を受信
- SMARTACCESSがID/パスワード情報を自動入力

クライアント端末とサーバ間で通信する生体情報やID/パスワード情報は暗号化されており，たとえ通信内容を傍受されたとしても内容が分からないようになっている。自動入力するID/パスワードは利用者が手で入力する場合と違いはなく，入力時点では平文であるが一般的にパスワードは「＊」で表示されるため画面をのぞき見されたとしても内容が分からないようになっている。しかし，クライアント端末にアプリケーション情報を詐取する悪意を持ったアプリケーションが動作している

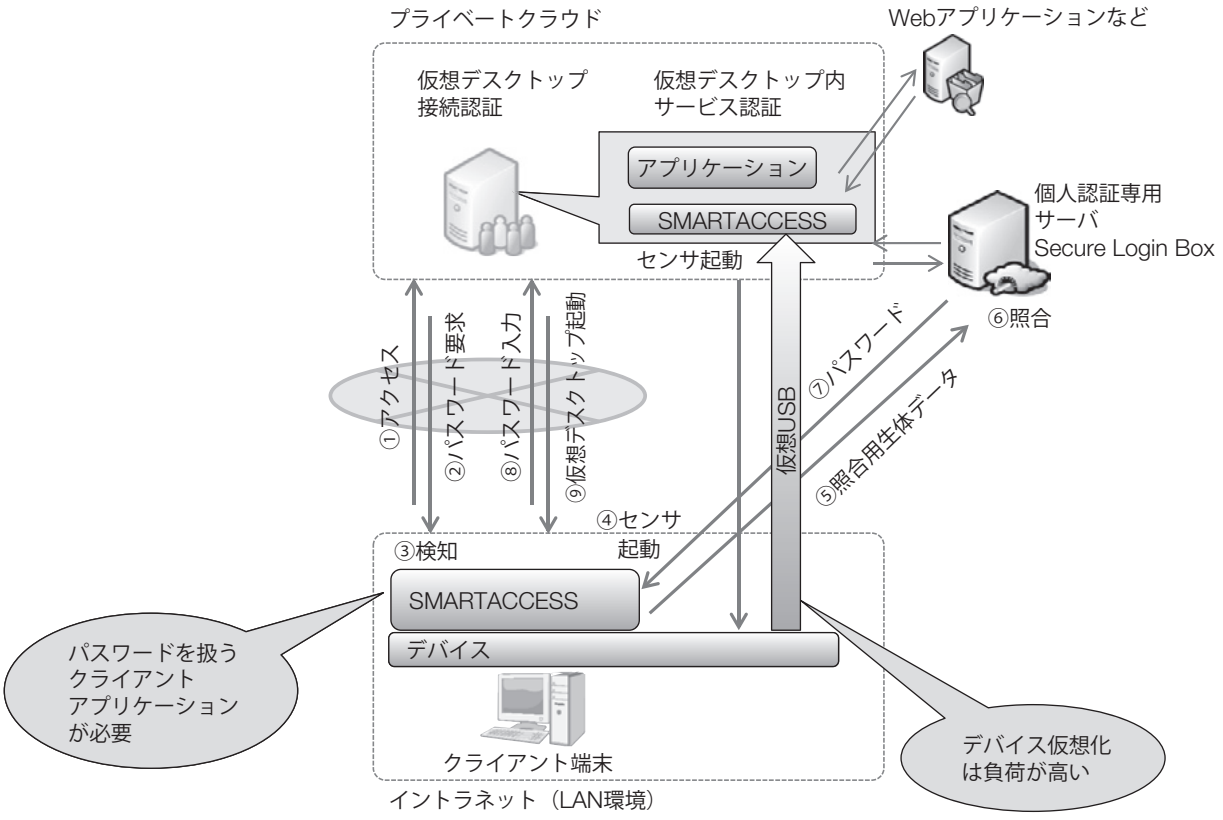

図-2　サービスと生体認証が連携した場合の課題

場合や，ブラウザや専用アプリと業務システム間の通信が暗号化されていない場合にはID/パスワード情報が漏えいするリスクとなる（**図-3**）。このため，一般に以下の対策が取られている。

・社内ネットワークに対する不正アクセス，ウイルス混入の防止
・不正な端末のネットワーク接続拒否

また，業務システムの一部に他社SaaSを利用する場合，安全性はSaaSの提供範囲内で確保することになる。例えば，第三者認証機関によるサーバ証明書を利用したSSLで通信するサービスを利用することで通信部分の安全性を確保することが可能である。

● 設計のポイント

SLBとSMARTACCESSのID/パスワード自動入力機能を利用したSSOシステムは，IDとパスワードのみを使用したSSOシステムと異なり，利用者とシステムの接点における認証が強固になるという特徴がある。しかし，今後システムの仮想化が進展すると，社内ネットワークの運用で守ることが困難な側面が出てくる。すなわち，クライアント端末の社外持ち出し，Bring Your Own Device（BYOD）に代表される社外端末からのアクセスなどアクセス環境の多様化や，業務システムのクラウド化，他社業務システムとの連携といった性質の異なるシステム要素が一つの業務システムを構成することを考慮して，多様な端末が接続される環境を従来の社内ネットワーク全体から仮想化環境上のシステムに限定して，その範囲を安全なネットワークとして扱う必要がある（**図-4**）。

そこで，アクセス環境を社内に限定せずに利用可能な個人認証サービスを前提とし，四つの観点で生体認証システムを新たに設計した（**図-5**）。

（1）クライアント端末とサービス間の通信路

通信路の安全性を確保するため，クライアント端末とサービス間はSSLによる暗号化を実施する。SSLはセッションごとに異なる鍵を生成し，通信ごとに異なるシーケンス番号を暗号化して通信の正当性を保証している。第三者もしくは悪意のあるユーザが全通信内容を傍受・保存してサービスを利用しようとしても，アクセスを受け付けることはない。

認証要求の集中による通信負荷を低減するため，通信量を最小化する。認証要求は通常，業務開始時に発生し，始業時間に認証要求が集中することが想定される。したがって，認証に必要な最小限のデータを送信することが望ましい。入力された生体情報から，生体の特徴となる情報だけを抽出

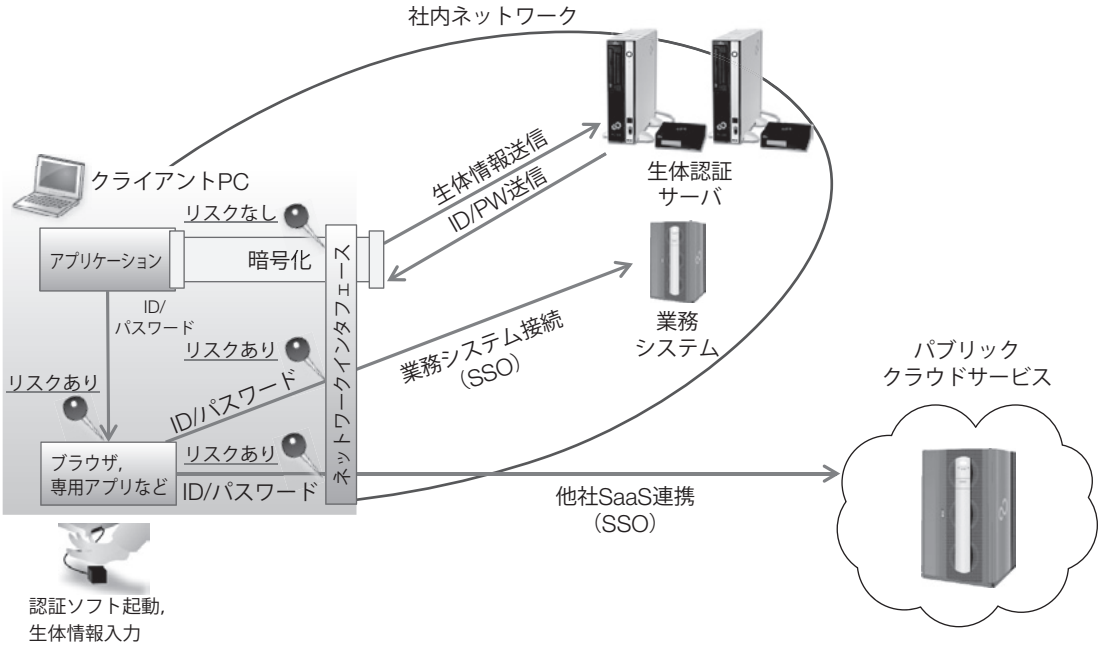

図-3　従来システムのリスク

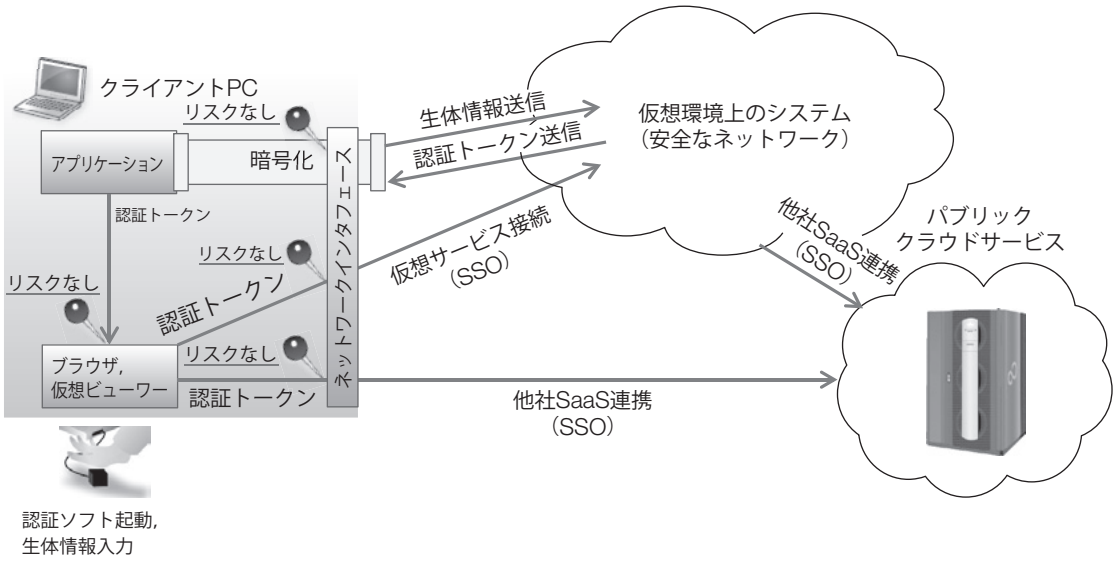

図-4　次世代生体認証システムの設計

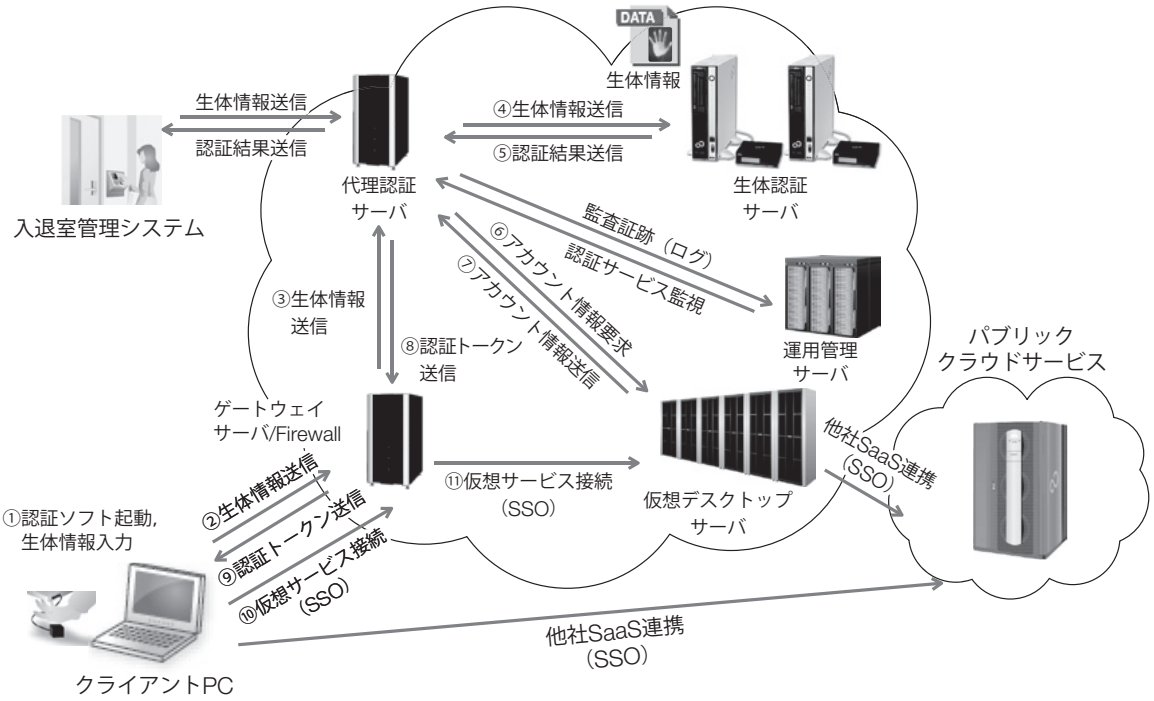

図-5　認証サービスを前提とした仮想環境

し，クライアント端末内で照合用生体データを生成する。特徴のない部分が元データから削除されるため，照合用生体データから元の生体情報に復元することは原理的に不可能であり，かつサービス側に送信するデータ量は，元データをそのまま送信する場合に比べて小さい。

（2）展開の容易性

ID/パスワードを利用したSSOシステムには，クライアント側のID/パスワード自動入力方式のほかに，既存の業務システムにエージェントを組み込む方式がある。この方式ではサーバ側で認証状態の管理が可能だが，エージェントを組み込むため，

例えば，サポート範囲が従来の業務システム開発元に閉じないことや，組み込むための工数がかかることから，システム全体への影響が大きい。

そこで，安全なネットワーク内における，システム同士のプロトコルではあえてID/パスワードを流通させてこの問題を解決する。仮想システム内のネットワークの安全性は，システムのフロントに設置するゲートウェイサーバ内部のファイアウォールで保証する。

(3) 連携の容易性

誰が認証されているかを代理認証サーバで一元管理して，社内システム間の連携，社外システムとの連携を容易にする。代理認証サーバにはセション（利用者がシステムに接続してから切断するまでのデータ通信の一連の動作）の概念を導入し，その範囲でSSOを実施する。

社外システムとの連携には，業界標準プロトコル（SAMLやShibbolethなど）を用いて，連携する際のセションは連携先で管理する。セションタイムアウトや通信切断が発生した場合，代理認証サーバに確認し，要求レベルに応じて再認証を実施する。この要求レベルは，業務システムごとのセキュリティポリシーで規定する。ポリシー設定の例を挙げる。

・同一の利用者が業務システムAとBを利用していた場合，Aはタイムアウトが発生したが，Bは継続して利用をさせるときは再認証を不要にする。
・利用者がロックした端末を解除する場合は再認証を必須にする。

また，入退室管理システムでは，退室時も認証を実施することを施設要件とすることがある。このような場合でも，当該施設内で利用可能な業務システムのセションを管理することが可能であり，施設退室時には，業務システムから自動でログアウトするといった運用を実現できる。

(4) 多様なアクセス環境における安全性

前述したとおり，クライアント端末とサービス間の通信には既存の安全な通信の仕組みであるSSLを利用し，認証にはソフトウェアトークン，もしくはトークン相当の情報を用いる。このようにすることで，例えばクライアント端末で利用者に気づかれずに動作する悪意を持ったアプリケーションが実行されていたとしても，攻撃するための情報が端末上に存在しないため，認証に関わる情報の漏えいやその情報を用いた攻撃をさせないことが可能である。

仮想化対応の取組み事例

● シンクライアント向け手のひら静脈認証

クラウドコンピューティングの普及に伴い，クライアント環境をサーバに集約し，必要に応じてシンクライアントから呼び出す仮想デスクトップや仮想アプリケーションの利用が増えている。従来のクライアントPCを起点にしたセキュリティ（SMARTACCESS/Premium）だけでは，様々な環境から外部ネットワークを介して仮想環境を利用されるお客様のシステム要件や運用要件に十分に対応できなくなってきている。そこで富士通では，新たにエンタープライズにおける認証システムに，使いやすく安全な個人認証を提供するために，次期認証ソリューションとして，Citrix社の仮想デスクトップ「XenDesktop」および仮想アプリケーション「XenApp」に対応した認証ソフトウェアを開発中である。

本章では，これらクライアント仮想化に生体認証技術を適用した試作システムの特徴について述べる。

● 特徴

本システムは，1回の生体認証でCitrix社の仮想デスクトップ，仮想アプリケーションの起動から，仮想デスクトップ上の複数WebシステムをSSOで利用することが可能なソリューションであり，以下の特徴を持つ。

(1) Citrixシステムとサーバ間で連携し，認証ルートを一本化することで，セキュリティレベルを強化
(2) 仮想デスクトップへのログオンから仮想インフラ（VDI：Virtual Desktop Infrastructure）内のWebシステムまで，SSOが可能
(3) Citrix社の認証サーバを秘匿することで，パスワードによる生体認証回避を防ぎ，より強固な個人認証を実現
(4) ユーザ情報を一元管理するActive Directoryや資産管理台帳との連携により運用負担を軽減
(5) Citrixシステムの改修が不要（運用中のシステムに追加導入可能）

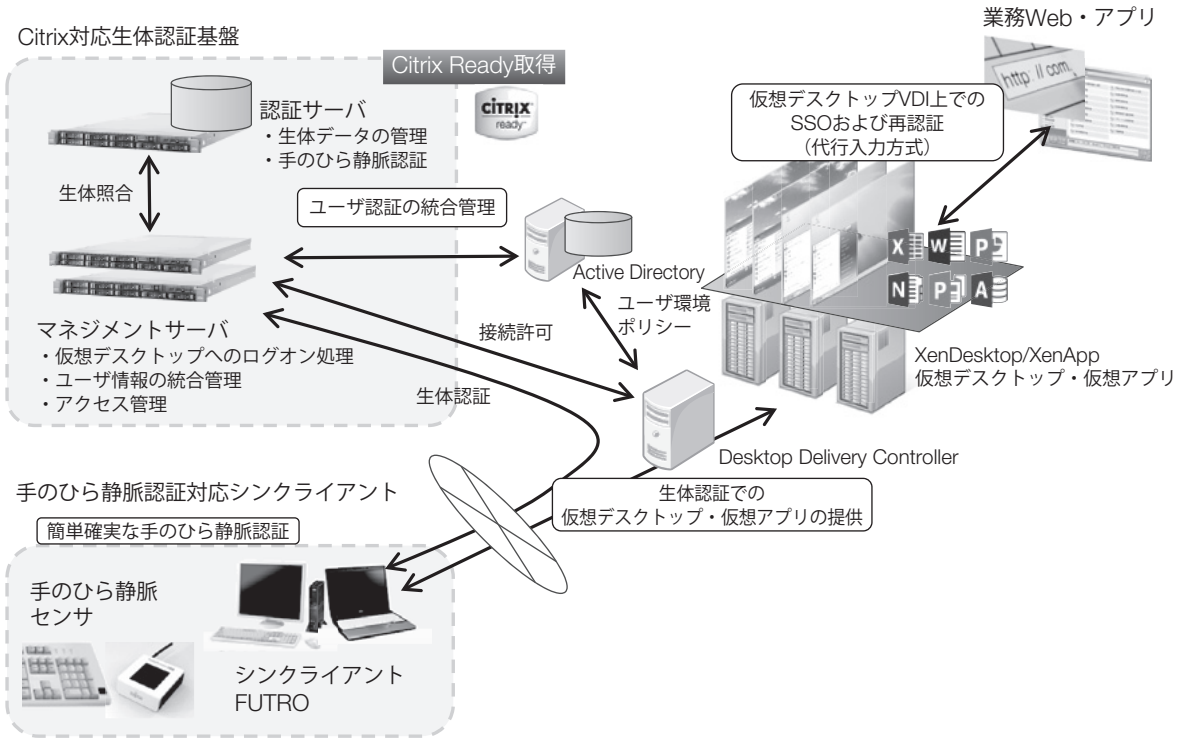

図-6　試作システムの構成

以上のように，クラウドを前提とした仮想化関連の商談で求められる，シンクライアント環境，強固な認証基盤，手のひら静脈認証の3要素を使いやすい形で運用することが可能になる。

●　生体認証システムの構成

従来のCitrix環境の認証フロントにマネジメントサーバを追加する構成となっている（**図-6**）。エンドユーザからのログイン要求を一括して受け付け，Citrix社のWebインタフェース（認証サーバ）や，仮想デスクトップ環境のエージェントソフトとの処理を管理することで，仮想環境の起動から仮想デスクトップ上のWebアプリケーションまでのSSOを実現する。

（1）マネジメントサーバ
・仮想デスクトップへのログオン処理（認証の中継）
・ユーザ情報の統合管理（ADと認証サーバDB）
・アクセス管理，セション管理
（2）認証サーバ
・生体データベースの管理
・生体データの照合による個人認証
（3）クライアントアプリ
・手のひら静脈センサから生体情報を抽出

なお，本システムは執筆現在，開発中であり，2013年度より提供開始を予定しているため，システムの機能および仕様に変更がある場合がある。

む　す　び

本稿では，富士通が開発した生体認証技術を活用して設計した次世代の生体認証システムの概要と取組み事例を紹介した。ID/パスワードを利用した認証システムは歴史が古く，様々な業務システムの認証ポイントで今現在も利用され続けているが，ネットワーク機器やインフラが整備され，仮想化の進展や端末利用環境の変化に伴う運用実態の変化に追随できていないのが現状である。すなわち，こうした環境の変化に対応する安全な運用が大きな課題であるが，大がかりなシステム変更やそれに伴うコストが，課題解決の阻害要因となっている。

生体認証を利用したSSOシステムは，こうした課題を解決する手段として注目されている。様々なシステム環境で安全，簡単に利用できる業務システムの認証に活用すべく，今後も次世代の生体認証システムの適用範囲を拡大していく。

参考文献

（1）坂巻健士ほか：Secure Login Boxによる簡単，確実な個人認証とシングルサインオンの実現．*FUJITSU*，Vol.61，No.2，p.100-108（2010）．

著者紹介

山嶋雅樹（やましま　まさき）
ユビキタスビジネス戦略本部クライアントソリューション統括部 所属
現在，クライアントソリューションの技術企画に従事。

和田篤志（わだ　あつし）
ユビキタスビジネス戦略本部クライアントソリューション統括部 所属
現在，クライアントセキュリティソリューションの技術企画に従事。

鎌倉　健（かまくら　けん）
ソフトウェア技術研究所セキュアコンピューティング研究部 所属
現在，生体認証システム関連の研究に従事。