静岡大学 情報基盤センター　広報　Vol.1　2009

クラウドによる新情報基盤 SUCCESの紹介

Shizuoka University Cloud Computing Eco System

Center for Information Infrastructure
Shizuoka University

ISSN 2185-0089

3.7 統合認証・入退室管理システム

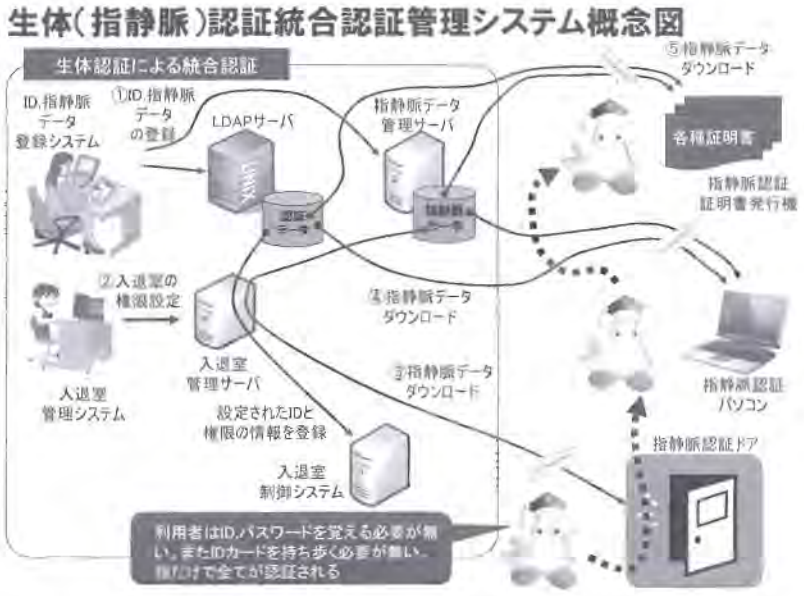
情報システムにおける認証には様々な方法が用いられてきた。現在の中心的な方法は、利用者が ID とパスワードを入力すると、その情報が正しく登録されているものか認証サーバによって判定され認可を与える、というものである。この方法は簡便で使いやすいが、一方でデータが漏洩しやすいという致命的な欠陥を有している。漏洩を防止するためにパスワードに有効期間を持たせるなどの方法が行われている。しかし、認証されるべき本人となんら関わりのないデータを用いている限りセキュリティ水準は一定値以下にしかならない。

これを解消するために利用者の身体的特徴を用いる方法も盛んに行われてきた。「指紋認証」はその代表的なものであるが「模倣されやすい」「利用者の状態で読み取り成功確率が変動する」などの課題を有していた。顔認証、虹彩認証、音声認証なども多くの課題を有しており、普遍的な方法にはなりえないことが明らかになっている。

これらに対し、本学では普遍的な手法として「指静脈認証」を長期間研究してきた。その成果は、このたびの更新での全面的な採用という成果に結びついた。

今回の統合認証の特徴は、パソコンのログイン時の認証と、学内の建物、フロア、部屋に対する入退室管理の認証を統合したことにある。将来的には「証明書の発行」「授業での出席管理」「在宅勤務での本人認証」「納品管理」など認証が必要なあらゆる場面で一元的な認証を可能とするものである。この技術、システムは汎用性が高いので多くの分野から「画期的なもの」と極めて高い評価を得ている。

次図は今回開発した生体認証による統合認証システムの概念図である。



従来から、学内 LAN を使用する場合は LDAP と呼ばれる認証サーバの認可を受ける。ここには教職員、学生、大学関係者全員の ID とパスワードが記憶されているデータベース(DB)が存在する。今回、これに対応する指静脈パターン DB を追加した。また、これらに対応する入退室権限設定システムも新たに開発した。

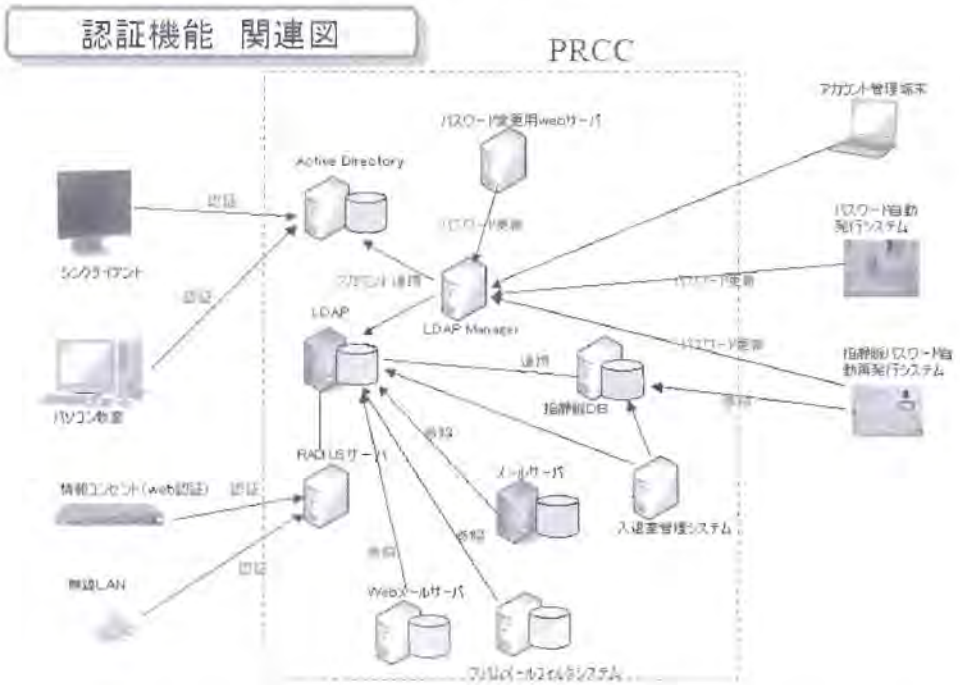
大学関係者は学内 LAN のための ID とパスワードを取得する。次に自身の指 2 本に対しそれぞれ 3 種類のパターンを登録する。これにより、指静脈読み取り装置が設置されている場所へ入退する場合は指を読ませるだけで OK となる。パソコンでログインする場合も同様である。

究極的には、大学内での作業には IC カード、磁気カードなどが不要になるだけでなく、ID やパスワードも覚える必要が無くなる。もちろん「他人のなりすまし」は原理的に不可能であるので、自身の情報、財産は最高水準で保持されることになる。

今回の更新では、基本システムは全て整備したが、現実的には「指静脈読み取り装置」がやや高価なので、一部の建物、フロアへの入退室の実現に限定されている。しかしながら、基本システムは全学のニーズを満足するように開発されているので、部局での導入は簡単である。

教育用端末、研究室のパソコンでのログインは実質的に「指静脈認証」で行える工夫がされている。すなわち指静脈認証自動パスワード発行機をキャンパス上に設置し、これを利用することで実現する。

従来、他人の学生証を使用した不正行為を防止するため IC カード学生証を使用したパスワード自動発行機は職員による対応を原則としていた。今回、確実に本人確認のできる指静脈認証自動パスワード発行機を開発しパスワード発行の完全自動化を実現した。



上図は、SUCCES の認証関連の図である。LDAP を中心に、メール、教育用端末、情報コンセント、無線 LAN、シンクライアントなどの各サービスを 1 つの ID とパスワードで利用できる仕組みとなっている。さらに、教職員番号、学籍番号を加えて入退室管理システムを含めた統合認証システムを実現している。

現在は画面から ID、パスワードを入力することが多いが、非接触 IC カードの情報(教職員証、学生証)の読取及び生体認証(指静脈)を組み合わせることで全体のセキュリティ向上と利便性向上を両立させる工夫を行っている。

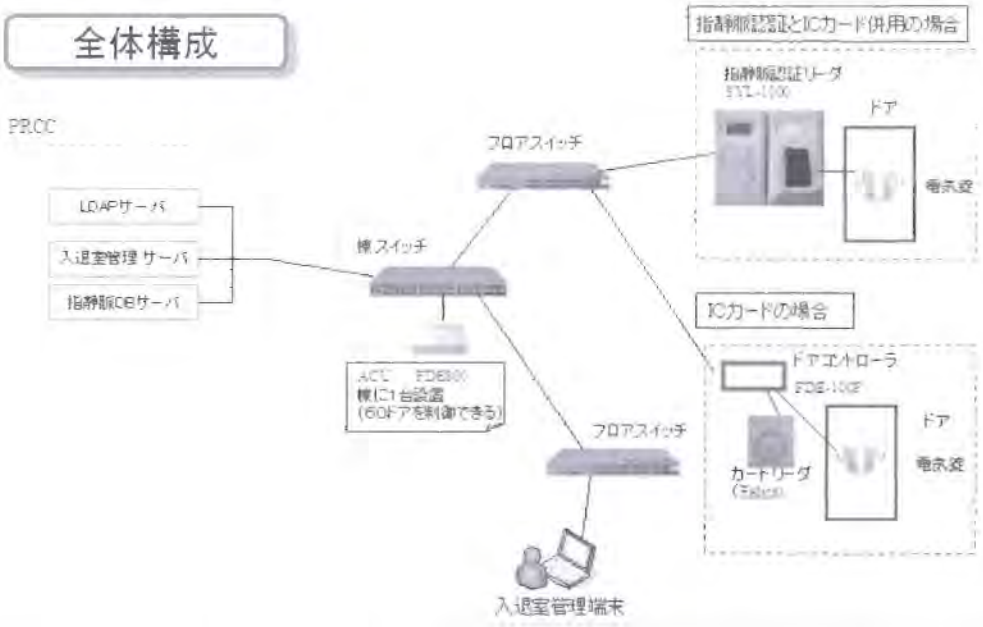
指静脈認証自動パスワード発行機は、静岡オフィスに先行設置され、人数の指静脈登録の円滑・効率的な登録手順を確立した後に設置場所を拡大していくものとする。

登録された指静脈情報は、指静脈データベースで管理されパスワード再発行だけでなく入退室管理システムにも使用可能である。指静脈データは、全学で一元管理となり一度登録すれば、指静脈認証自動パスワード発行機や指静脈認証による入退室のドアが増えた場合、あるいは将来的に指静脈認証を利用する新たなシステムが追加設置された場合でも直ちに利用することができるようになる。勿論、部局で指静脈認証による入退室を追加設置した場合も、新たな登録行為等は不要である。

入退室管理システムは、施設の管理組織毎に実施されているため利用する施設毎に申請手続きが必要であり、複数の入退室カードを携帯する必要があるなどの不便がある。また、主に使用されている磁気カードでは磁石の接触による磁気テープの損傷、カード券面の汚れ又は磁気カードリーダの磁気ヘッドの汚れや帯磁などによる読み取りエラーで開錠操作がうまくできないなどの問題も多く発生している。

今回、教職員証及び学生証を使用した非接触 IC カード方式の入退室管理システムの導入と統合認証システムとの連携でこれらの問題を解決することとした。

この入退室管理システムは先に述べた指静脈認証にも対応している。入退室管理システムの全体構成を示す(下図)。



入退室権限データベース、指静脈データベース、入退室記録などはPRCCに設置されたサーバにまとめられている。学内 LAN によってドアを制御するドアコントローラや入退室権限の設定及び入退室履歴の確認を行う入退室管理端末と接続されている。

開錠操作

左の写真がドアの隣に設置される端末で、ICカード専用と指静脈＋ICカードの2種類がある。

今回、学生はどちらの端末でも学生証(ICカード)による開錠操作としている。教職員も教職員証による開錠操作が可能であるが、希望者は指静脈を登録すれば指静脈認証による開錠操作をできるようにしている。

IC カードによる開錠操作は、学生証又は教職員証を IC カードリーダにかざす(軽く触れる)だけである。IC カードリーダの表示が点灯し、電子錠が開錠される。

指静脈による開錠操作は、指静脈リーダに登録した指を置くと認証結果が左のディスプレイに表示され、電子錠が開錠される。教職員証を持ち歩かなくても入退室が可能となる。今回、入退室管理システムの設置された場所は以下の通りである。

設置場所一覧

キャンパス	建物	階	部屋名	区分	備考
静岡	共通教育L棟	1F	情報基盤センタ1Fフロア入口	入退室	指静脈あり
			情報基盤センタ静岡オフィス	入室	
			主計算室	入室	
		2F	情報基盤センタ2Fフロア入口	入退室	指静脈あり
			CIO室兼応接室	入室	指静脈あり
			中央管制室&ショールーム	入室	指静脈あり
			ピロティ階段全体入口	入室	指静脈あり
			ITCP推進室	入室	
			会議室	入室	
浜松	工学部事務棟	1F	サーバ室	入室	
	工学部5号館	3F	電子計算機室	入室	
	工学部7号館	2F	計算機室1，2	入室	

本システムは、学生証、教職員証を使用するため、専用カードの発行や個別の登録手続きが不要であり管理稼動の大幅な低減が図れる。また、非接触 IC カードを使用するため券面の汚れ、磁石の接触などによる動作不良がなく、ID カードホルダや財布等に入れた状態でも開錠操作が可能であり利便性の向上に実現している。

静岡、浜松キャンパスを 1 組の入退室管理サーバ、指静脈 DB サーバで制御しているため、ドアの追加が容易であり、利用者の属性(学生・教職員などの区分や所属組織など)で入退室権限設定が可能な場合は、利用者が手続を行う必要がない。

教職員の指静脈認証による開錠はいつでも追加登録可能で、情報基盤センターのオフィスで指静脈の登録を実施すればすぐに指静脈認証のみで開錠操作が出来るように工夫されている。

PRCC に指静脈データベースを設置し、学内 LAN に設置された「指静脈認証自動パスワード発行機」、指静脈認証入退室端末が共通して利用することで、パスワードの不要な情報基盤に一歩近づいたといえる。しかし、指静脈認証の利用箇所が増えると設置場所の違いや、操作するときの利用者の姿勢などにより指静脈リーダに指を置く位置がずれることによる読み取り精度の低下の可能性があることが判明した。そこで、右写真のような説明シールを指静脈リーダ部分に追加することで本来の読み取り精度を維持する工夫を行った。

生体認証を、組込んだ統合認証システムは事例が少ないため、このような運用ノウハウはほぼ皆無の状態といえる。利用拡大に向けて、引続き研究開発を進めていく。