Vol.2010-IOT-10 No.8
2010/7/16

指静脈認証統合システムによるリスク管理手法

戸部剛男[†1]　長谷川孝博[†1]　水野信也[†1]
井上春樹[†1]　山崎國弘[†1]　吉田仙良[†1]

従来の LDAP システムを中心とした IT 統合認証システムに，指静脈データ登録と入退室管理を統合した BIDM システムを大規模組織の情報基盤として整備し，その運用と可能性について検討した．本システムは，指静脈認証による個人特定の機能と認証システム連携することによって，利用者の利便性向上と統合認証の物理的，論理的リスク低減を実現できる．また，国際規格 ISO/IEC27001 に基づく情報セキュリティマネジメントシステム (ISMS) で提唱される境界のセキュリティの強化できる．

Risk management system using finger vein BIDM

Takeo Tobe,[†1] Takahiro Hasegawa,[†1]
Shinya Mizuno,[†1] Haruki Inoue,[†1]
Kunihiro Yamazaki[†1] and Noriyoshi Yoshida[†1]

A biometrics integrated identity management system using finger vein was developed into a large network system as an IT infrastructure of a university. Doors control system and automatic password issue system are integrated into this BIDM system. A high identification performance of this system can improve not only information security proposing ISMS, but also IT-infra usability. In this paper, we discuss the advantage of this system and the possibility in application system.

†1 静岡大学情報基盤センター
Center for Information Infrastructure, Shizuoka University

1. はじめに

統合認証管理システム（IDM: Integrated iDentity Management system）の導入は，パスワード管理の利便性と安全性を両立させるが，一度にすべての情報へのアクセス権を与えてしまう危険も包含している．生体認証による統合認証（BIDM: Biometrics IDM system）を用いることで，このような第三者からのリスクの低減が可能となる．さらに，情報システムと入退室システムを統合した生体認証は，より高い利便性とセキュリティを同時に実現できると期待される．

ISMS[1),2)] の観点から見た指静脈認証の特徴として，入退室管理においては環境照度範囲が広く，軽度な汚れや水濡れに対応できるため屋外の出入り口に設置が可能なこと，統合認証においては偽造が困難で認証が容易なことが挙げられる．また，認証の対象が指であるため対象物とカメラの距離を短く出来ること，対象物が小さいことから装置の小型化と低コスト化の可能性が高いなどの利点を挙げることができる．したがって，境界のセキュリティを重視する ISMS において，低コスト導入で高セキュリティ境界を保持するための有用なツールとなり得る．本報では，静岡大学の情報基盤整備で導入された指静脈統合認証システムの構成，導入，運用について報告する．また，同システムの今後の課題と応用について述べる．

2. 導入事例

本指静脈認証システムは，利用者が何時でも何処でもストレス無く使用できることを設計思想に挙げている．これには体内にある指静脈データの正確な読み取り，蓄積データとの高速で高精度な認証技術が必要となる．これを実現するために本システムでは，指静脈認証の認証データを作成する際の 2 値化を行わず，曖昧さを持たせた多値化データのままデータベースに保存した．保存される指静脈認証データは，体調変化や環境変化を受けやすいため，認証精度の向上のために学習機能を付加している．これによって，設置環境や利用条件に左右され難い，高い認証成功率のシステムを開発することができた．

図 1（左）は，パソコン等 IT 機器への組込用指静脈読取装置（FDS 社製）である．サイズ，重量，読取精度，読取速度については実用に耐える要求を満足している．また他の同種製品に比べ，光外乱に対し頑強なので屋外でも使用できるという利点がある．残る課題はコストであるが，これは量産により容易に解決できるものと期待している．同じく図 1（右）は,「入退室管理システム」「パスワード発行機」「証明書発行機」など多くの場面への適用が可能な入退出管理用指静脈＆ IC カード読取装置（FDS 社製）である．この装置にはテン

図 1 指静脈読み取り装置

図 2 パスワード再発行装置への組込み例

キー入力装置，IC カードリーダーが組み込まれており幅広いニーズに応えることが出来る．

図 2 は，組込用指静脈読取装置を実装したパスワード再発行装置の導入事例である．パスワードを頻繁に失効または失念してしまう利用者は，窓口にて任意に指静脈データを登録することができる．一度，指静脈データを登録すると，24 時間無人運転される同装置からパスワードを自動発行できる．そこには，証明写真などによる対面での本人確認はもはや必要ない．指静脈認証の精度は，対面認証よりも遙かに高いためだ．

図 3 は，本学に導入した BIDM システムの概要図である．メールシステムや Active Directory システムなどの従来の認証システムの他に，指静脈 DB と管理サーバ，指静脈データ登録システム，パスワード発行装置（証明書発行装置），入退室管理システム（指静脈認証ドア）が統合されている点である．

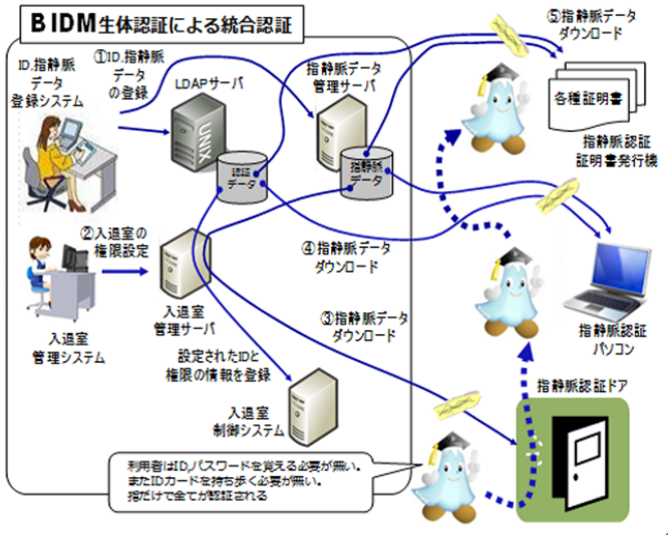

図 3 BIDM 統合認証管理システムの概要

3. 運用状況と課題

3.1 第三者アクセスのセキュリティ

今回導入した入退室管理システムでは，施設への第三者による入退出管理として，ゲスト用 ID カードを使用しエリアを限定した入館の許可を与えるという運用を行っている．施設へ訪問した第三者は，身元確認の手続きをした後，配布されるゲスト用 ID カードに指静脈の登録を行うことで，指静脈認証による扉開閉ができるようになる．短期利用を終えて返却された ID カードは，登録された指静脈を完全に抹消することで，第三者の権限を失効させている．

3.2 物理的リスクへの対応

重要情報を管理する上で，第三者に対する情報管理手法としては，施錠が可能な場所への保管と保管されている場所が容易に識別されないようにする必要がある．保管場所の施解錠

システムを全て電気錠にするにはコストの面での問題が生じるため，既存のキャビネットやロッカーの鍵を指静脈認証の鍵管理システムで管理することにより，利用者ごとのアクセス権を設定することが出来る．すなわち，指静脈認証の鍵管理システムは，利用者毎の鍵に対するアクセス権を設定できると同時に鍵の貸し出し及び返却簿としても機能する．

3.3 入退室管理とセキュリティレベル

電子情報への不正アクセス防止のセキュリティ対策と同様に，入退室の不正アクセス防止のセキュリティ対策は重要である．入退室管理システムを使用することにより，利用施設の管理のために高セキュリティエリアとフリーエリアなどに区分けされたエリア間の人の移動を監視できる．これによって，セキュリティエリアへの不正アクセスを早期に発見し，重大インシデントの未然防止に繋げることが出来る．また，高セキュリティエリアへの入室は指静脈認証を使用することで，ID カードの不正利用による成り済ましなどをほぼ完全に防ぐことが出来る．

ゲスト用 ID カードを発行された一時的な登録利用者が，セキュリティエリアへ入退室を行う場合には，有効な権限を持つ別の登録者の追加認証を要求することが出来る．また，ゲスト用 ID カードを持った登録利用者には，必要な時間に限られた部屋へのアクセス権のみを与えるこができる．すなわち，カード認証，静脈認証，などの認証モードを使い分けることで，各部屋のセキュリティレベルの設定をコントロールすることが出来る．

4. 今後の課題

システムサーバ内に生体情報である指静脈認証データを保存することに抵抗がある利用者は少なからず存在する．これらの利用者の多くは，暗号化した指静脈認証データを ID カードに記録して本人が持ち歩ける仕組みならば安心を得られるかもしれない．この方法によれば，指静脈認証データをシステムサーバ内で預かる必要はなく，利用者だけでなく，システム運用者側の心的負担も軽減できる．例えば次のような指静脈認証データ保管場所の順序を階層的に切り替える仕組みが考えられる．まず，カード内に指静脈認証データが記録されているかを調べ，記録されている場合はカード内のデータで認証する．失敗した場合には，次に認証装置内に記録（キャッシュ）されているデータで認証を試み，それでも失敗すれば，最後にサーバ内に記録されているデータで認証を実施する．静岡大学で導入した指静脈認証システムには，ID カードへの指静脈データの書き込みが選択不能（未実装）であるため，今後の開発課題である．

ただし，指静脈認証装置が生成する認証データは毎回パターンと暗号鍵が変更されるために，同一の指静脈認証データが発生する確率は非常に低い．このことを利用して，万一データが漏洩した場合でも，同一データでの認証を拒否すると同時に警告の記録を保存する方式を検討している[3]．これは，指静脈認証装置の ID と指静脈認証データを採取した時刻や採取毎のシーケンス番号を併用してサーバで管理していくことで実現している．

他の安全策としては，サーバ内で保管する指静脈認証データに関して，個別生体情報を類推されないための人口知能技術を用いた記号化や多項式を用いた隠蔽の手法や平面周波数を用いた画像変換が提案されている[4]．この方法は静脈情報のセキュリティ確保に有効な手法と考えられるが，演算の高速化が課題となるであろう．

しかしながら，いくら理論的に十分で高度な暗号化がなされていても，体内の生体情報を抜き出して電子データに書き下すことに不信感を抱く利用者は必ず居ることも忘れてはならない．組織の体質や規模によることもあるが，究極の個人情報とも言える生体情報を取り扱う認証システムの強制的な全面導入はあってはならず，あくまで利用者への説明責任を果たした上での任意利用が原則であると考える．よって，生体認証システムを完全拒絶する組織員が不利益を被らない仕組みや運用を並行して備えることは必須かつ重要である．静岡大学に導入済みの指静脈認証システムはこれらのことに留意した実装と運用を行っている．

5. ま と め

従来の LDAP システムを中心とした IT 統合認証システムに，指静脈データ登録と入退室管理を統合した BIDM システムを大規模組織の情報基盤として整備し，その運用と可能性について検討した．

(1) 従来から行われていた IC カードによる全組織員の扉認証の機能を保持したまま，高いセキュリティレベル要求する領域には指静脈認証を要求できる選択肢を獲得できた．一度指静脈データを登録した利用者は，IC カードなしに入退室が可能となった．その結果，物理境界における完全性と可用性のセキュリティ向上を実現することができた．

(2) IC カードと指静脈を組み合わせた個人認証を行う 24 時間無人運転可能なパスワード自動再発行機の運用を開始した．本機によればサービス窓口スタッフによる対面での本人確認作業が不要となり，業務の効率と利用者の利便性を共に向上することが出来た．

(3) 大規模組織へ導入する際の合意形成のためには，生体情報を利用したくない組織員に不利益のないシステム設計と運用が重要である．IC カードに指静脈データを書き込

んで本人のみが所有する仕組みはこの問題の打開策となる可能性があり，最重要課題として実装に取り組んでいる．

参 考 文 献

1) JIS Q 27001: 2006 (ISO/IEC 27001:2005): 情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステム要求事項，日本規格協会 (2006).
2) 長谷川孝博，伊藤賢，井上春樹，八巻直一：実践 ISMS 講座，静岡学術出版 (2007).
3) 静脈画像を鍵とする暗号化手法に関する研究：Optics & Photonics Japan 2008 講演予稿集
4) 渡邊幸聖，小田雅洋，山本匠，尾形わかは，菊池浩明，西垣正勝：曖昧性を含んだ多項式による特徴量関数を利用した非対称生体認証暗号と情報セキュリティシンポジウム予稿集 (2010)