



4984 El Camino Real, Ste 200  
Los Altos, CA 94022  
Phone: 650-969-7884  
Fax: 650-969-2783  
[www.sutisoft.com](http://www.sutisoft.com)

## **SECURED BioPass™:**

**Fingerprint-based Access Control for the enterprise**

**企業用指紋ベースアクセス制御**



輸入代理店：シンデン・ハイテックス株式会社  
〒104-0043 東京都中央区港1丁目1番12号 湊ビル3F  
電話：03-3537-0101 FAX：03-3537-0202  
URL: <http://www.shinden.co.jp>

## 目次

目次.....	1
優れたアクセス制御の必要性： .....	4
バイオメトリクスの利点.....	5
SECURED BioPass™：企業用指紋ベースアクセス制御.....	6
強固な安全性： .....	7
最高度の指紋アルゴリズム： .....	7
機種を問わないセンサー： .....	8
Plug-and-Play デザイン： .....	8
フェイルセーフ： .....	8
指紋ベース認証の容易な導入： .....	9
指紋の安全性： .....	9
SECURED BioPass™設計仕様： .....	10
Simple Sign-on 機能： .....	11
ファイルとホルダーの暗号化： .....	11
SECURED BioPass の価値ある提案： .....	12
コスト節減： .....	12
安全性： .....	12
時間節約の利便性： .....	12
SECURED BioPass™と他の方法の比較.....	13
総 論： .....	14
参考資料： .....	14



## 概要：

現在の企業環境において、侵入行為の予防、情報の窃盗に対する防御は、重要な問題となっています。貴重な情報の損失は、企業にとって、多くのビジネス上の問題と法的論争を引き起こしています。顧客は多くの場合、セキュリティに対する方針と対策に関心を持っていない企業と、ビジネスを行なうことを拒否しています。

結果として、企業は自社の IT 源へのアクセスを安全にすることに、益々関心を持っています。認可されていないユーザー、認可されていないネットワークデバイスから、自社のネットワークの安全を確保することとは別に、プライバシーの保護と情報アクセスの秘密性を提供するために、厳しい身元確認の実施メカニズムにおおきな関心が払われるようになりました。

認可されていないユーザーが明らかに脅威を与える一方、多くのケースでは、企業の従業員の意図にかかわらず、企業のインフラへの不正アクセスに、彼らが関与する結果になっています。調査によれば、2000 年においては 70% の会社が、少なくとも一度は非認可アクセスに関連するセキュリティの破綻を経験しています (Christensen, 2001\*1)。このことは今日の企業において、この伝染性のある問題に対して予防と防御の必要性を強調しています。



## パスワードの問題について：

企業の資源へのアクセスを制御するための、最も普遍的な方法は、常にパスワードベースのものです。各ユーザーには、ユーザーID と初期パスワードが与えられます。ユーザーはシステムに初めてログインする時に、最初のパスワードを変更することが期待されています。一つか二つのアカウントがあるいはアプリケーションである限り、ユーザーがこの方法を履行することは、単純で易しいものです。しかし、アカウントの数が大きなものとなった時に、殆どの企業のユーザーが現在経験しているように、この方法は深刻な問題を引き起こすことになりました。ユーザーはすべてのユーザーID と、彼等の異なったアプリケーションアカウント用の関連パスワードを記憶することが、非常に困難であることがわかったのです。

多くのユーザーID とパスワードに直面したときに、あるユーザーは、ID とパスワードのリストを作成し、彼等のコンピューターのスクリーンに張り付けています。またあるユーザーは、彼等の家族、友人、同僚にそのアカウント情報を分かち与えています。結果として、会社のインフラのセキュリティーと、セキュリティー強化のプロセスの統一性が損なわれています。



## 優れたアクセス制御の必要性：

アクセス制御は、企業が履行しなければならない最初の、そして最も重要なセキュリティ手段です - すなわち、これは侵入者が出会う最初のハードルです。脆弱なアクセス制御では、アクセス制御メカニズムに少々の知識と経験を持つ者であれば、そのバリアーに打ち勝ち、企業の貴重な情報にアクセスができることを意味します。

ユーザーID とパスワードによる方法は、アクセス制御を行う上で、もっとも容易であり、普遍的な方法ですが、ユーザーは、その情報（ユーザーID とパスワード）を保護するために、相当の注意をはらわなければなりません。又、多くのアプリケーションを使用するユーザーが、幾つもの異なるユーザーID とパスワードを上手く管理することは、大変にやっかいなものです。

パスワードベースのアクセス制御をさらに厳密に実施するために、ほとんどのシステムは、ユーザーに定期的にパスワードを変更することを要求しています。パスワードのセキュリティを強化するために、数字、小文字、大文字の組合せによるパスワードを要求しています。これらのパスワードは、結果として複雑で入り組んだものとなります。そのような規則を守ろうとするユーザーは、そのパスワードを記憶し、入力するために、多くの労力を費やします。企業における IT サポート部門が、ユーザーのパスワードリセットのサポート、そしてこの厳密な規則の履行で、大変に忙しい思いをしていることは、共通の悩みとなっています。

ガートナーグループの調査によれば、ほとんどの企業では、パスワードの維持のために要する年間の費用として、ユーザー一人あたり 340 ドルを必要としています。（Christensen 2001\*1）

これは、多くのユーザーがいる企業においては、巨額なコストとなります。

アクセス制御を実行する他の方法として、認証用にハードウェアトークンを利用することがあります。このアプローチに伴う問題としては、ユーザーが幾つものトークン（各アカウントに一個のトークン）を持つことになり、ユーザーがそれらを携行し、管理することの難しさがあげられます。加えて、トークンを紛失する恐れがあり、管理上高価なものとなります。アクセス制御にバイオメトリクスを利用することは、従来のパスワードのみ、もしくはトークンベースの手段に伴う脆弱性、コスト、不便性を含めた諸問題を、軽減することができます。



## バイオメトリクスの利点

バイオメトリクスは、各人の物理的特徴と、あるいは動作に基づく個人の認証を可能とします。

通常のバイオメトリクスは、指紋、音声パターン、網膜パターン、顔面特性を意味しています。バイオメトリクスの数ある種類の中で、指紋による認証、検証は、このマーケットで多数を占めています。これには多くの理由がありますが、その中でも、低価格、高信頼性、システムの高速反応性があげられます。

ユーザーの認証用として指紋を利用することは、人々がパスワードもしくはトークンベースのシステムに、多くの問題を見出したことにより増加してきています。

指紋ベースの認証は、パスワードもしくはハードウェア・トークンの持つ全ての問題に、洗練された解決策を示しています。指紋技術が購入しやすくなり、信頼できるものになってから、ユーザー認証に指紋を用いるケースが、急速に増えています。ユーザーにとって指紋を利用することは、パスワードを記憶し入力することや、もしくはトークンを携帯することに比べ、容易で手軽なものです。

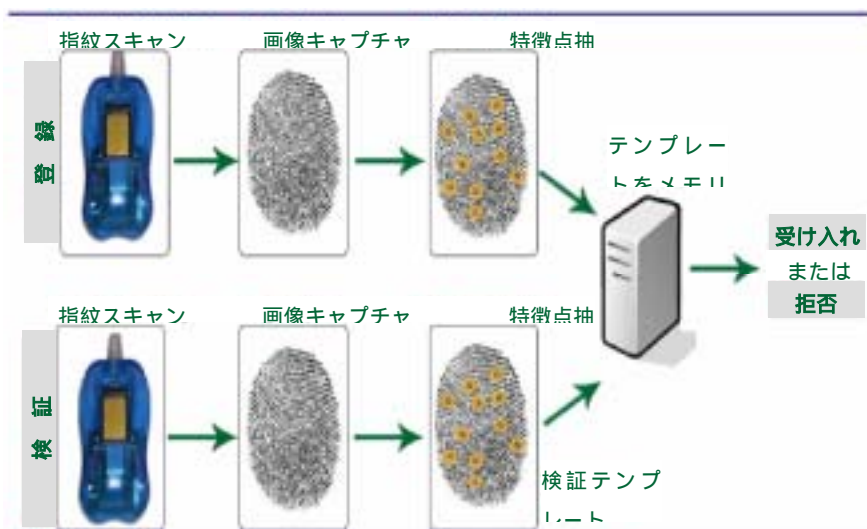
SutiSoft 社が提供する SECURED BioPass は、論理的アクセス制御用として指紋を利用することで、洗練された方法を提供します。



## SECURED BioPass™：企業用指紋ベースアクセス制御

SECURED BioPass は、パスワードでなく、指紋により登録されたユーザーを認証することにより、企業の IT インフラ用の効果あるアクセス制御を可能とします。そしてパスワードベース認証の脆弱性に焦点を当てています。バイOMETリック ID 検証技術と最高度の特徴点抽出・照合技術を組み合わせることにより、SECURED BioPass™ は企業 IT インフラ用として高度に信頼できるアクセス制御メカニズムを可能としました。

SECURED BioPass は、クライアント/サーバー型の指紋認証ソリューションを提供します。全ての正当なユーザーの身分情報が、SECURED BioPass サーバーに保存されます。企業が SECURED BioPass™ を設置しますと、ユーザーは彼等のコンピューター（暗いアノド PC）にログインする際には、ユーザー ID と指紋を準備する必要があります。SECURED BioPass サーバーは、各々のユーザーが事前に登録しておいた指紋と照合します。事前に登録された指紋と一致しない場合に、そのユーザーは、コンピューターもしくはアプリケーション、それに企業のインフラへのアクセスを拒否されます。登録された指紋と一致した場合は、ユーザーはログインを許可されます。



認証された場合、ユーザーは普段と同じように、アプリケーション及びシステムを使用できますので、理想的なものとなります。SECURED BioPass 認証は、指紋センサーを装備するラップトップによる単純な指紋認証とは、明らかに異なったものであり、さらに優れています。

センサー付ラップトップは、ローカル認証が主たる目的です - すなわち、ユーザーはそのコンピューターへのローカルアクセスを許可されます。このような認証は有用ではありますが、ユーザーの、アプリケーションへのアクセスを、よりダイナミックに、確実にかつ強固な形で扱えるように、サーバーによるユーザーの認定を行ないたい企業にとっては、全く使い難いものです。また、SECURED BioPass は、ネットワークが稼動していない時に、ユーザーが自分のローカル・コンピューターにログインをさせることも可

能です。このように、SECURED BioPass は、ローカルログインシステムの機能に合わせることも可能です。SECURED BioPass のクライアントサーバーベースの利用は、パスワード情報の安全な保存を可能とする一方、パスワード変更方針のダイナミックな利用、そして必要な時にパスワードの自動更新を可能とさせます。

モバイルユーザーは、インターネットにアクセスできる環境であれば、あたかも会社にいるように SECURED BioPass にて、自分自身を認証すること可能です。

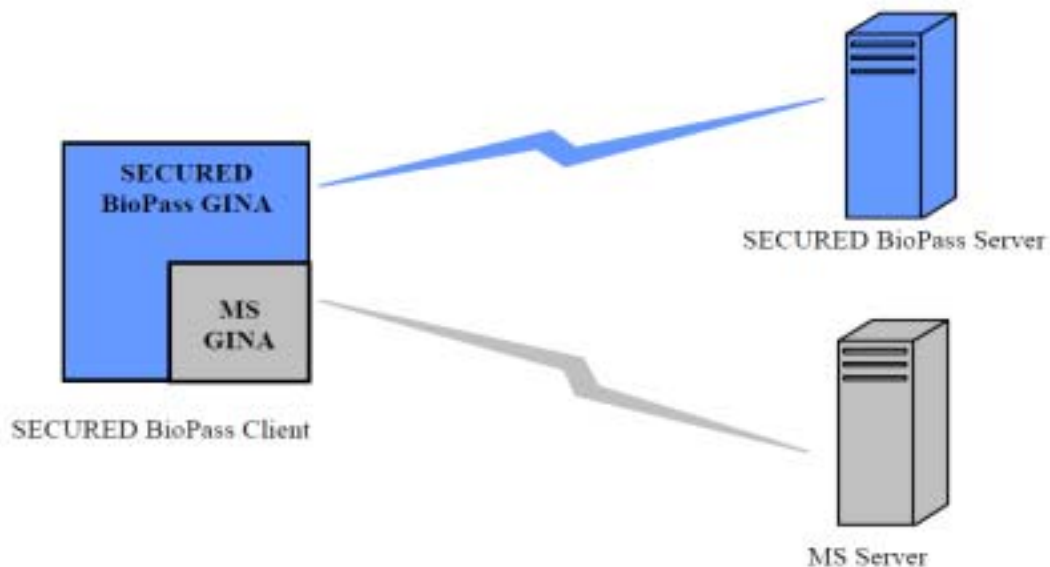
以下が SECURED BioPass の持つ特徴と利点です。

### 強固な安全性：

指紋ベースのアクセス制御の利用により、単純なユーザーID とパスワードタイプのアクセス制御に伴う脆弱性を解決します。SECURED BioPass は、企業 IT インフラのアクセス制御に、大変に強固な安全性を提供します。

### 最高度の指紋アルゴリズム：

SECURED BioPass は、NEC 社により開発された最高級のアルゴリズムを使用しています。NICT (National Institute of Standards and Technology)<sup>1)2)</sup> は、多くの指紋技術評価の中で、NEC のものをトップに行くものとして明確に位置付けしています。(NIST、2003) 指紋アルゴリズムは、指紋ベース認証システムの心臓部であり、アルゴリズムの質は最も重要な要素です。



## 機種を問わないセンサー：

SECURED BioPass は、センサーの機種を問いませんので、市場にある多くのセンサーが使用可能です。スワイプタイプとタッチもしくはエリアタイプの、両方のセンサーが利用可能で、単に SECURED BioPass をインストールすることで、幾つかの異なるタイプのセンサーが使用できます。ユーザーの指紋登録は、どのタイプのセンサーでも可能です。また、登録時と異なるタイプのセンサーによる認証も、全く問題にはなりません。

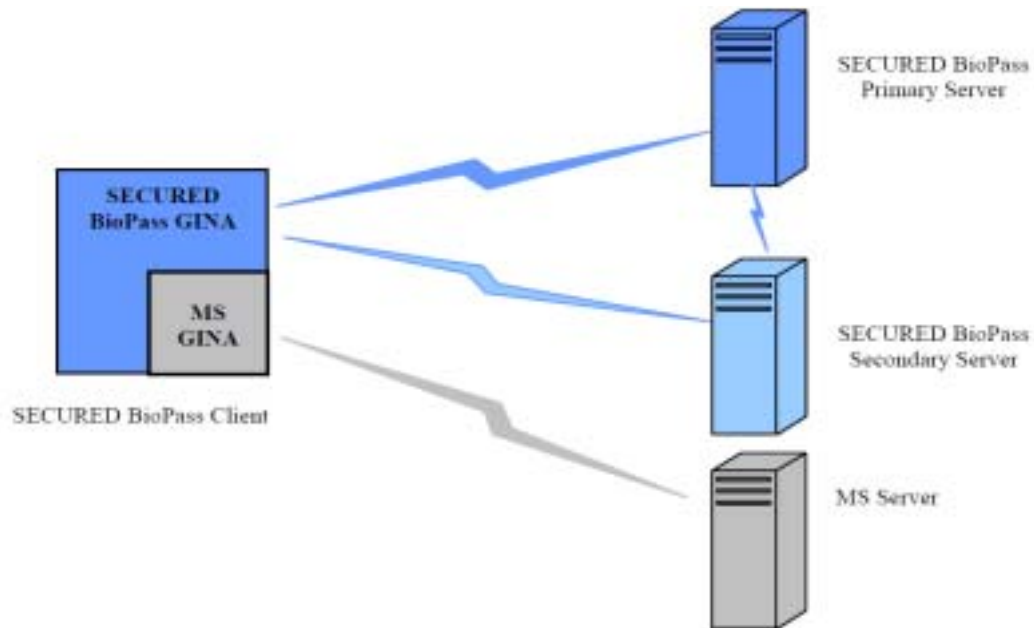
## Plug-and-Play デザイン：

SECURED BioPass は、Plug-and-Play に準拠しています。既存データベースからユーザーのデータを引き出すことで、その機能が、自動的に組み込まれます。SECURED BioPass は、企業ネットワーク用の既存のスタンダード、今後アナウンスが予定されている、マイクロソフトスタンダードに完全に準拠しています。SECURED BioPass の自動登録機能は、指紋ベース認証を現在の IT システム稼働させる時間、コスト、努力を著しく軽減します。

## フェイルセーフ：

SECURED BioPass は、認証用サーバーのサービス停止を防ぐため、セカンダリーサーバーの接続をオプションとして用意しています。例えば、プライマリーサーバーにハードウェア故障が起きた場合に、自動的にセカンダリーサーバーに切り替わるため、認証作業が中断することはありません。セカンダリーサーバーは、プライマリーサーバーの完全な複製です。





## 指紋ベース認証の容易な導入：

SECURED BioPass は、システム管理者が指紋ベースアクセスを導入するプロセスを、容易にかつ企業が処理できる速さで、管理することを可能としています。導入の期間中に、SECURED BioPass は、同一ネットワーク上に指紋とパスワードベースの認証を共存させることが可能です。指紋システムに移行しながら、企業に自分の業務を止めることなど無い段階的導入を可能としています。

## 指紋の安全性：

SECURED BioPass は、ユーザーの指紋のイメージを保存しませんし、転送することもあります。イメージから、minutiae points と呼ばれる特徴点を抽出し、それらを認証目的用に用います。 minutiae points は指紋イメージから抽出しますが、そのデータから、オリジナルの指紋イメージを復元することはできません。このことは指紋イメージを紛失、盗難、誤使用されたりする可能性を除きます。

## SECURED BioPass™設計仕様：

SECURED BioPass システムは、以下のコンポーネントから構成されています。

- ログインクライアント
- 管理ユーティリティ
- SECURED BioPass サーバー
- 一連の付加価値のあるツール

SECURED BioPass クライアントソフトは、企業のシステムにログインする時に使用される、ユーザー用コンピューターにインストールされます。このプログラムは、ユーザー ID と指紋を取り込み、認証用の SECURED BioPass サーバーに、それらを転送します。認証されると、認証用サーバーは、次の処理用の MS ドメインサーバーに、システムの制御を渡します。

SECURED BioPass 管理ユーティリティの主機能は、システム管理者による SECURED BioPass サーバーの設定と管理です。新しいユーザーの登録は、このユーティリティのもとで行われます。システム管理者は、ユーザーの登録の状況、およびサーバーに生じた全ての活動を見ることができます。

SECURED BioPass サーバーは、このシステムの心臓部に当り、全てのユーザーの、ユーザー ID と指紋を保存します。新しいユーザーが登録された時には、そのデータが、このサーバーに保存されます。このサーバーは又、ユーザーの登録、削除、そして認証の全ての活動ログを保持しています。サーバーは、全てのアクセスに対して、ユーザーの ID、日付、時間を記録しているので、システム管理者は必要に応じて、そのデータを参照することができます。

SECURED BioPass クライアントソフトは、インストール時に MS-GINA ( 認証機能を持つマイクロソフトのウィンドウ DLL ) を置き換え、ログイン用グラフィカルインターフェースを変更します。このソフトは、MS-GINA に代わり、認証作業及び MS Domain との通信を行ないます。

SECURED BioPass は、企業の厳しい信頼性要求をサポートするようにデザインされています。システムの予期できないトラブル ( ハード、ソフトの機能停止 ) に対応するために、セカンダリーサーバーをバックアップとして使用する設計になっています。SECURED BioPass は、プライマリーサーバーに何等かのトラブルが生じたことを検知すると、自動的にセカンダリーサーバーに切り替わります。セカンダリーサーバーは、データと機能性の両面において、プライマリーサーバーと同じ働きをします。例えば、新しいユーザーが登録されると、そのデータは、自動的に両方のサーバーに保管されます。加えて、両サーバーは完全な認証サービスを提供できます。この無停止のデザインで、サーバーの一つが一時的に故障したとしても、停まることのないサービスを可能としています。



## Simple Sign-on 機能 :

SECURED BioPass システムは、ユーザーにいくつかの有用な機能を提供しています。最も有用な機能として、Simple Sing-On(SSO)と、File や Folder の暗号化・復号化の二つがあります。

SSO 機能を使用することで、ユーザーは、ウェブベースのサービスのアクセスに使用する、ユーザーID とパスワードを保管、登録することができます。一度登録されると、ユーザーID とパスワードを覚える必要が無く、ユーザーは彼等の指紋認証で、そのサービスにログインすることが可能になります。

このシナリオでは、ウェブページもしくはアプリケーションがスクリーン上に現れると、SECURED BioPass クライアントは、指紋認証のスクリーンを出します。サーバーにより、ユーザーID と指紋の認証が行われると、ウェブページあるいはアプリケーションのユーザーID とパスワードのフィールドに、自動的に登録されているユーザーID とパスワードが表示されるので、ユーザーは、Enter キーを押すだけで、ログインプロセスを続行することができます。

## ファイルとホルダーの暗号化 :

暗号化/解読機能は、ユーザーに彼等の指紋を使ってファイルとフォルダーの暗号化・解読をすることを可能とします。この機能を使用することにより、ユーザーは、ファイルやフォルダーを解読するために、長いキーやパスワードを記憶する必要がありません。



## SECURED BioPass の価値ある提案：

SECURED BioPass を使用することにより、コストの節減、安全性、時間節約の利便性を含めた多くの利点を享受できます。これらの価値ある提案を以下に説明します。

### コスト節減：

ガートナーグループによると、パスワードの管理に年間 200 ドルから 500 ドルが必要されると推定されています。この費用は、定期的パスワードの変更、及びユーザーから依頼されたパスワードの再設定に伴い、サポート部門で発生するものです。SECURED BioPass では、指紋の再登録の必要が無いことから、この費用は全く必要無くなります。SECURED BioPass は、短時間に投資の採算がとれ、同時により安全な認証メカニズムを提供します。

### 安全性：

最も重要なこととして、SECURED BioPass は、企業の IT 資源へのアクセスに対し、強固なレベルの安全性を提供することがあげられます。一般的になりつつある、HIPAA、Starbanes Oxley のような厳しい安全規制にも、準拠しています。指紋ベース認証は、ユーザーを模倣しようとする誰かに、その指紋を貸したり、共用したりすることができないことを保証します。

### 時間節約の利便性：

パスワードを入力するより、認証に指紋を利用する方が明らかに迅速です。強力なパスワードを利用する企業では、アルファベット、数字、特殊文字等による長くて意味不明の文字列のパスワードを要求していますが、そのようなパスワードでは、入力に時間がかかるだけでなく、ユーザーは入力を間違え易くなり、しばしば再入力しなければなりません。時には 3 回、それ以上の回数でログインを失敗することとなり、システムは、そのユーザーを拒絶することになります。このケースでは、ユーザーはシステム管理者に連絡し、彼のアカウントの再設定か、新しいパスワードを入手しなければなりません。このことは、ユーザーの時間の浪費と、フラストレーション、そして IT 部門にとって、余計な維持コストを生じさせることとなります。SECURED BioPass は、安全な認証情報を提供するだけでなく、はるかに早くて便利な方法を提供しています。



## SECURED BioPass™と他の方法の比較

最近では、多くの指紋センサー付のラップトップコンピューターが、利用可能となっています。これらのラップトップは、指紋認証によるコンピューターへのログインの手段を提供しています。このログインと、SECURED BioPass によって提供されている、企業インフラへのログインとは、同じではありません。ローカルログインは有用ですが、企業ネットワークへのアクセスより、むしろ個人のコンピューターへのローカルアクセスを、認証するようにデザインされています。企業にとって、認証は不可欠なものであり、そのために、SECURED BioPass のサーバーによる認証が行われます。

SECURED BioPass は、企業 IT インフラへの完全なアクセス制御を可能としており、MS ウィンドウドメインコントローラーの働きを補助します。結果として、既存のインフラに影響することなく、指紋ベースのアクセス制御システムの構築を簡単に行えます。加えて、その設計の理念により、企業は SECURED BioPass を、迅速に、あるいは逆に徐々に、望むペースで導入することが出来ます。SECURED BioPass は、システム管理者が処理可能なペースに合わせて、指紋ベース認証へのユーザーの移行を計画することが可能です。



## 総論：

SECURED BioPass は、企業 IT インフラ用として、指紋ベースのアクセス制御を提供し、パスワードベースの認証に伴う、脆弱性を解決するものです。SECURED BioPass のアーキテクチャーは、システム管理者にとって、既存のシステムを変更することを必要としないので、企業に指紋ベースのアクセス制御を導入することを容易なものとして提供します。指紋ベースのアクセス制御への移行は、IT 部門にとって都合のよいペースで行うことができます。

SECURED BioPass は、厳密な信頼性と安全性に関する、企業の要求を満足させるべく設計されています。セカンダリーサーバーを用意することで、システムの予期できないソフト上、ハード上のトラブルに対して、動作の保証をしています。

SECURED BioPass は、指紋のマッチングに最高級のアプローチを使用しています。結果として、SECURED BioPass の処理に必要な時間と正確性は、反比例しません。加えて、SECURED BioPass は、指紋センサーの機種を問いません。このことは企業にとって最も彼等の要求にあうセンサーを使用することを可能とします。異なった種類のセンサーを混在させることも可能であり、使用者が好きな時にセンサーを交換することも可能です。

## 参考資料：

\*1Christensen, Thor A: Biometrics: Advancing Effective Security Mmanagement. DM Review, May2001(以下のオンラインにて入手可能です。

[http://www.dmreview.com/editorial/dmreview/print\\_action.cfm?articleId=3348](http://www.dmreview.com/editorial/dmreview/print_action.cfm?articleId=3348))

\*2NIST (2003). *Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report*. NISTIR 7123. 利用可能オンライン <http://fpvte.nist.gov/>

