使用したPCの履歴を自動記録。不正使用を抑止＆追跡！

ご紹介資料

エムコマース株式会社

USBメモリ運用の問題点

M-Commerce

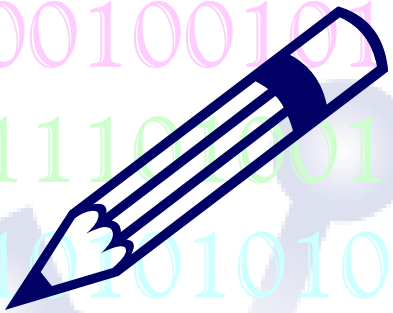
➢情報漏洩は外的要因と内的要因から起きています。

	外的要因	内的要因
情報漏洩	盗難・紛失 紛失時の内部データ・パスワード解析 ウィルスの侵入	データの無断持ち出し パスワードの漏洩 悪用、無許可PCでの不正使用（自宅、ネットカフェ等）
対　策	会社選定のUSBメモリを貸与 保存データの暗号化 生体認証の採用 ウィルス対策　デバイス制御	セキュリティポリシーの徹底
効　果・問題点	安全面で最善をつくした施策を行える。 安全面が優先になり、操作性、利便性がそこなわれてしまいがちになる。	操作性、利便性が優先され、遵守されない場合がある。 不正使用をしても発覚しないと思っている。 懲戒処分は免れない。

なぜパスワード暗号USBメモリではダメなの？

M-Commerce

ハッキングツールで
パスワード情報を盗難
（キーボードロガーなど）



パスワードを記録した
手帳などと
一緒に紛失・盗難

パスワード失念
などによる
運用上の問題

指紋認証ならキーボード入力のログを残さず、
紛失・失念のトラブルもありません。

さらに、Biocryptodisk-ISPX Trackなら、使用したPCの履歴情報を自動記録します。

指紋認証なら、どれも同じなの？

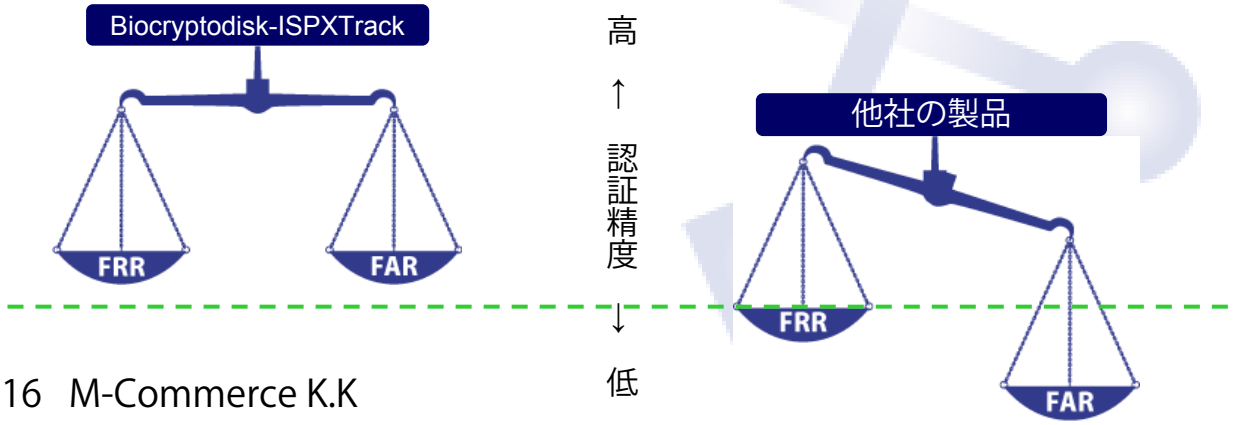
M-Commerce

➢認証精度を表す数値（数値が小さいほど精度が高い）

本人拒否率 （FRR：False Rejection Rate） 本人を誤って拒否してしまう確率	他人を拒否する精度が高まる一方、 本人も拒否しやすくなり、 使い勝手が悪くなる。
他人受入率 （FAR：False Acceptance Rate） 他人を誤って受け入れてしまう確率	本人を受け入れやすくする一方、 他人も受け入れやすくなり、 安全性が失われる。

➢本人拒否率と他人受入率それぞれ独立した値ではなく、相関関係を持っています。

「セキュリティレベルが高い」とは、
数値が小さく、かつ両方の数値のバランスがとれていることを示します。



エムコマースの指紋認証技術

エムコマースの指紋認証は、指紋の切れ目（端点）や分かれ目（分岐点）などの特徴点を相対座標データとして抽出し、登録されている特徴点データと照合することで実現しています。（特徴点抽出方式）

エムコマースの認証精度向上のしくみは、独自の画像エンハンスメント。
センサより得られた指紋画像が認証に不十分なレベルであったとしても、２値化画像を作成する際の最適化技術や、指紋取り込み条件の自動化処理等、エムコマース独自の画像エンハンスメント処理で、認証に十分なレベルに引き上げます。
これにより難指紋への対応が強化され、対応率も大幅に増加しました。

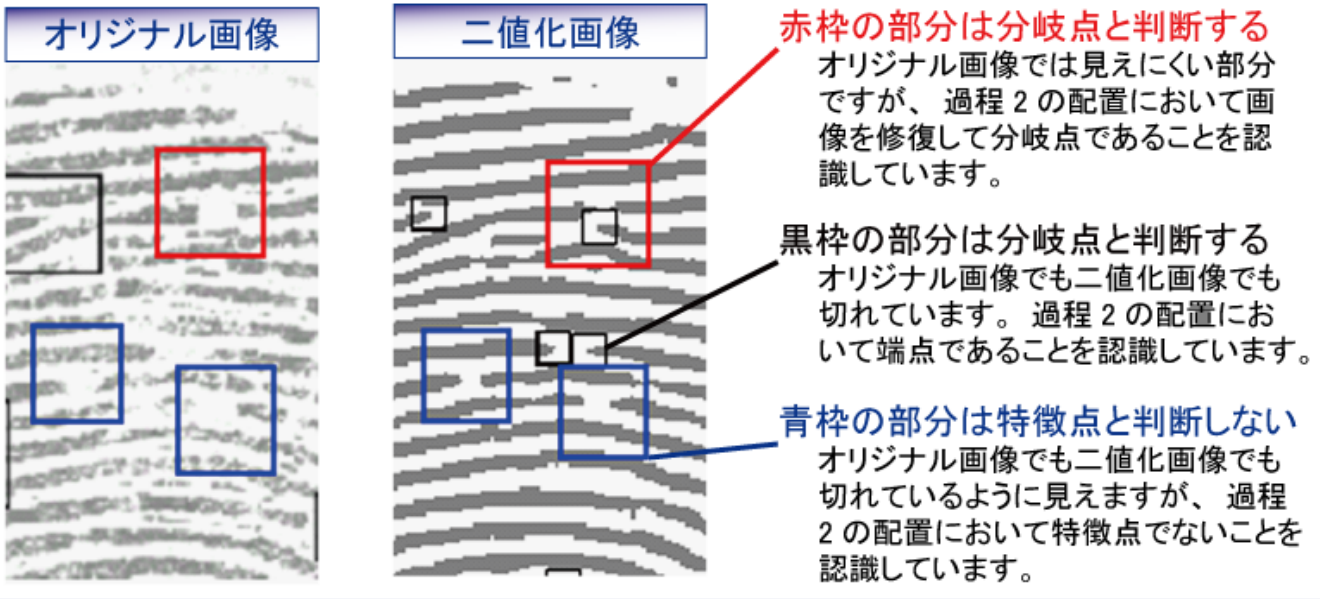
Image enhancement

ワンポイント）二値化とは黒と白の2色ではっきりとした画像に処理することです。
この際にノイズの除去を同時に行います。この作業が特徴点抽出には不可欠です。

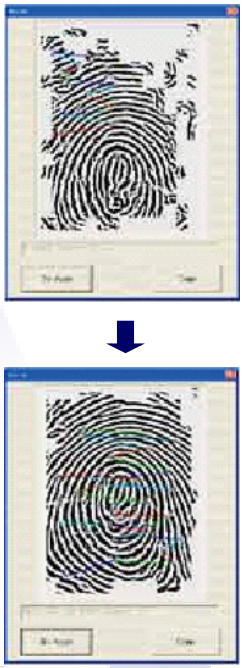
認証精度を上げるための独自技術（画像エンハンスメント）

M-Commerce

画像エンハンスメント例



指紋の欠損部を修復します。



読み取った画像をなるべく補正し、認証に適切な状態で登録することで画像に多少の欠損があってもスムースで確実な認証が行えます。
何度も本人認証に失敗する（本人拒否）ストレスは、この技術の差に起因します。
エムコマースは、独自の画像エンハンスメント技術により、7万分の4の本人拒否率を実現しています。

それでも情報漏洩は起こっています

M-Commerce

➢**個人所有PC、ネットカフェなど管理外のPCを利用できる環境が、管理者を悩ませています。**

☑ 社内のPCにはデバイス制御とウィルス対策
☑ 従業者にはセキュリティ対策USBメモリを貸与

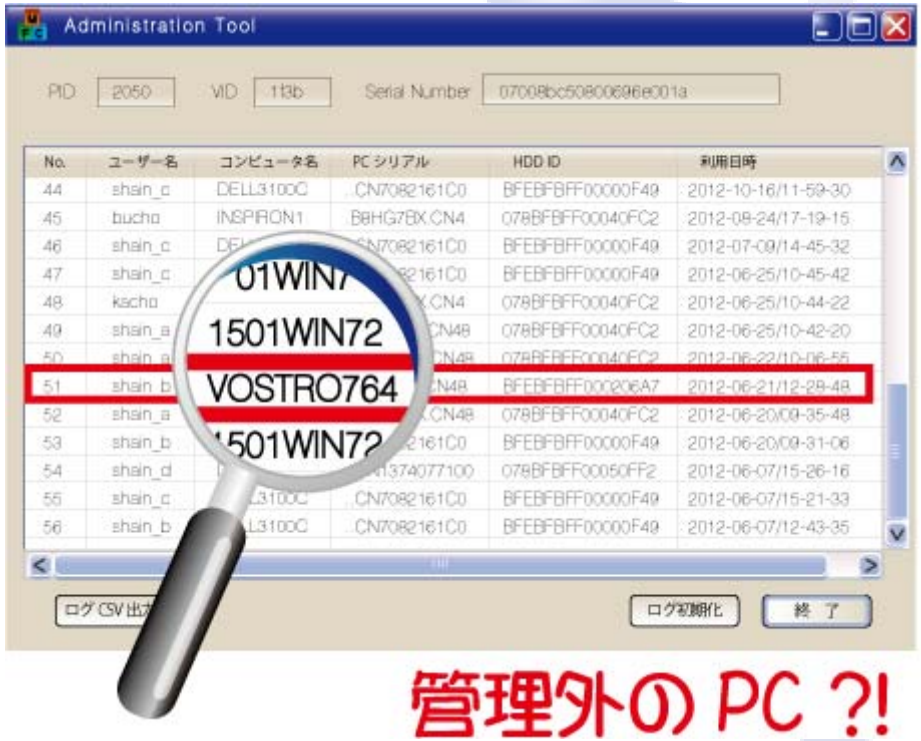
☑ 装置側の施策で情報漏洩を防止
☑ 情報セキュリティポリシーの徹底

☑ 許可された人 ＋ ☑ 許可されたデバイス ＝

それでも情報漏洩 ?!

➢使用したPCの履歴情報（ログ）の説明

- ➢履歴情報（ログ）はメモリドライブとは別の秘匿領域に自動記録されます。
- ➢一般利用者がフラッシュドライブをフォーマットしてもログは消えません。
- ➢ログの閲覧ツールは、一般利用者には提供されません。
- ➢ログは最新の2,000件（最大）が格納されます。
- ➢ログ情報をCSVファイルへ出力可能です。



ログには次の情報が含まれます。

① Biocryptodisk-ISPX Track 固体情報
② ユーザー名
③ 使用したコンピュータ名
④ PCのシリアル番号
⑤ PCのCPU ID
⑥ PCのHDD ID
⑦ 利用日時

Biocryptodisk-ISPX Trackの利用イメージ

指紋認証USBメモリ「Biocryptodisk-ISPX Track」の特長

M-Commerce

- **使用したPCの履歴情報を自動記録**
  使用したPCの履歴情報を自動記録することで、利用者のセキュリティポリシーに対する意識が高まります。

- **CDドライブ使用を禁止されたPCでも動作可能　（カスタマイズ版対応）**
  お客様のシステム構成にあわせて、必要なプログラムを読み出し専用のフラッシュディスクに格納できるため、CDドライブ使用を禁止されたPCでも動作します。

- **内部構成のカスタマイズ、OEMにも対応**
  「CDFS」「読み出し専用のフラッシュディスク」「指紋認証によって保護されたフラッシュディスク」の３種類の領域へカスタマイズにも対応いたします。

- **指紋認証以外のバックドア（抜け道）は、一切なし**
  指紋認証以外では、全メモリ領域の参照はできません。

- **AES-256 自動暗号化機能搭載！　512Bごとに独立した鍵で暗号化**
  メモリ内に保存される全てのデータは自動的に暗号化されます。

- **最高水準の認証精度**
  本人拒否率0.05%、他人受入率0.0001%、認証時間は0.6秒です。

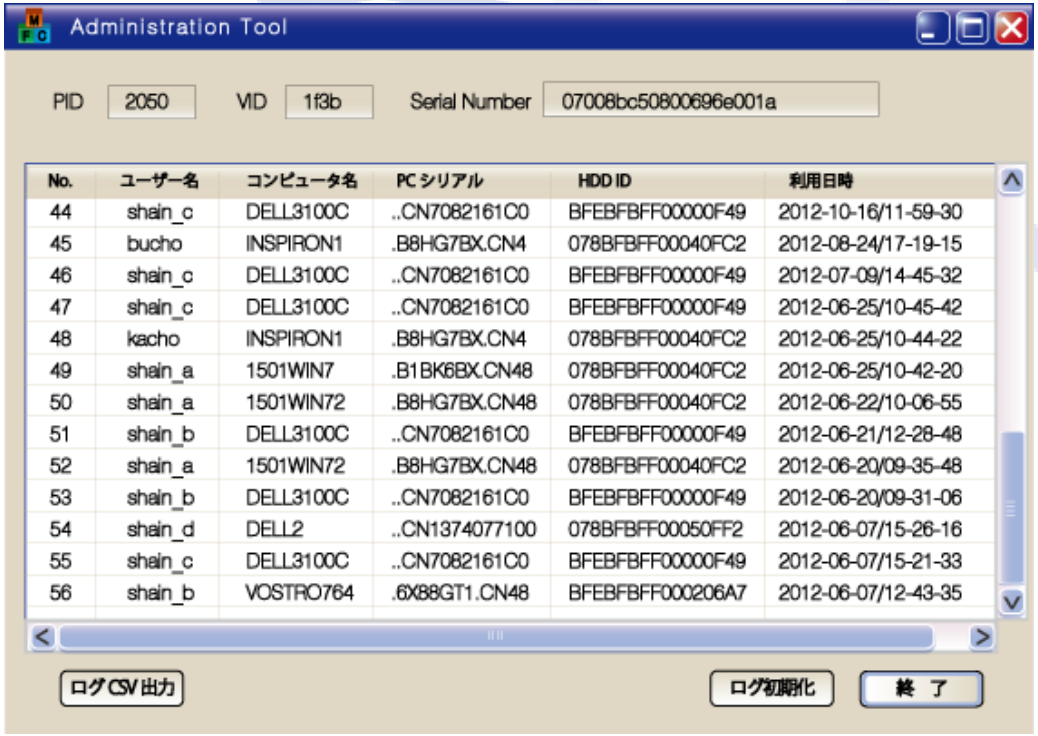
- **専用ソフト・ドライバーのインストールが不要だから幅広いOSに対応**
  Windows 8.1 / 8 / 7 / Vista 対応。

- **機器内指紋認証（インテリジェントタイプ）**
  ハッキングの対象となる指紋情報や認証信号も機器内から漏出しません。

Biocryptodisk-ISPXシリーズは、紛失や盗難などによって分解されても参照できない物理的な対策がとられています。
バックドアがあったり、認証精度の良くない製品ではセキュリティ対策の意味がありません。
絶対的な安全性で選んでください。

➢ 使用したPCの履歴情報を自動記録

Biocryptodisk-ISPX Trackは、USBメモリの不正利用という問題点に着目し、使用したPCの履歴情報を自動記録することで利用者のセキュリティポリシーに対する意識を高める、指紋認証USBメモリです。本人拒否率0.05%の認証精度を誇る「Biocryptodisk-ISPX」の基本技術を応用、利用履歴を記録する機能は機器内に搭載されており、専用ソフトをインストールする必要はありません。



指紋認証USBメモリ「Biocryptodisk-ISPX Track」の特長

M-Commerce

➢ CDドライブ使用を禁止されたPCでも動作可能　（カスタマイズ版対応）

セキュリティUSBメモリは、メモリ内部にCD領域(CDFS)を作成して必要なプログラムを組み込む方式が一般的ですが、セキュリティ対策を導入されている企業では、デバイス制御ソフトウェア等によりCDドライブを禁止している場合が多く、CDFSを用いたメモリは動作しません。
Biocryptodisk-ISPX Trackはお客様のシステム構成にあわせて、必要なプログラムを読み出し専用のフラッシュディスクに格納できるため、CDドライブ使用を禁止されたPCでも動作します。

ストレージエリアに2つの領域　※①または②のどちらか選択です。

① CDFS　セキュリティUSBメモリは必要なプログラムがこのエリアに組み込まれることが多い

デバイス制御ソフトウェアなどでCDドライブの使用を禁止するとCDFSが認識されセキュリティUSBメモリも動作できない。

② Public　読み出し専用のフラッシュディスク

Publicエリアに必要なプログラムを格納すれば、CDドライブの使用を禁止しながらセキュリティUSBメモリを使用できる。

③ Private　指紋認証によって保護されたフラッシュディスク

指紋認証＆自動暗号化で、強固なセキュリティUSBメモリとしてデータを格納。

※この製品の構成・カスタマイズ等に関しましては sales@m-commercekk.jp までお問い合わせください。

➢ 内部構成のカスタマイズ、OEMにも対応

「CDFS」「読み出し専用のフラッシュディスク」「指紋認証によって保護されたフラッシュディスク」の3つの領域のカスタマイズにも対応いたします。
例えば、USBメモリ起動型シンクライアントのカーネル部分をCDFS、必要なアプリケーションソフトを読み出し専用のフラッシュディスク、個人毎の設定情報を指紋認証によって保護されたフラッシュディスクに配置したいといった要望にも対応が可能になります。

例）
USBメモリ起動型シンクライアントとして利用する場合

CDFS	→	カーネル
Public	→	アプリケーション
Private	→	個人設定など

エムコマース社が提供するソフトウェア以外にも、ISV（インディペンデント・ソフトウェア・ベンダー）やお客様の独自のソフトウェアを機器の内部に組み込む「カスタマイズ」にも対応可能です。

指紋認証USBメモリ「Biocryptodisk-ISPX Track」は

M-Commerce

➢指紋認証以外のバックドア（抜け道）は、一切なし

データの参照は指紋認証に限定。

パスワード認証を併用すると、管理に膨大な負担がかかるほか、結果的に「なりすまし」による不正使用や悪用の抜け道ができてしまうのです。

精度の高い指紋認証の技術があればこそ実現できる、ストレスのない絶対の安全性です。

➢AES-256 自動暗号化機能搭載！ 512Bごとに独立した鍵で暗号化

内部データは、指紋情報やアプリケーションデータを含め、全て自動で高いレベル（AES-256）で暗号化され保存されます。さらに、単一ではなく512Bごとに自動生成された個別の暗号鍵を使用し、暗号化されます。

指紋認証USBメモリ「Biocryptodisk-ISPX Track」は

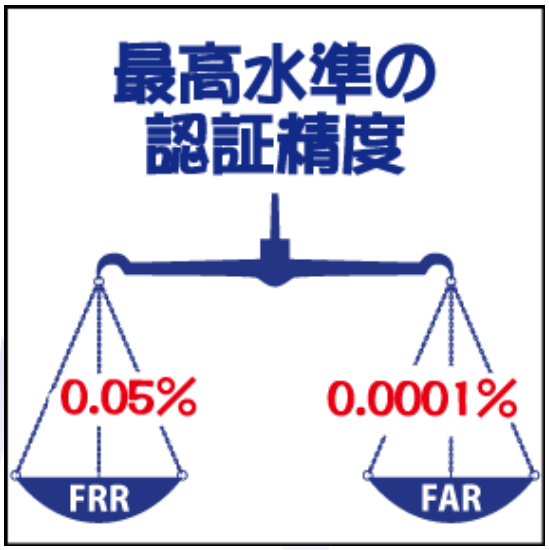
M-Commerce

➢最高水準の認証精度

認証速度は、平均わずか0.6秒。

速さに加え、本人拒否率は0.05%で、累計70,000人中なんと4人。他人受入率は0.0001%と、きわめて高い認証制度を誇ります。

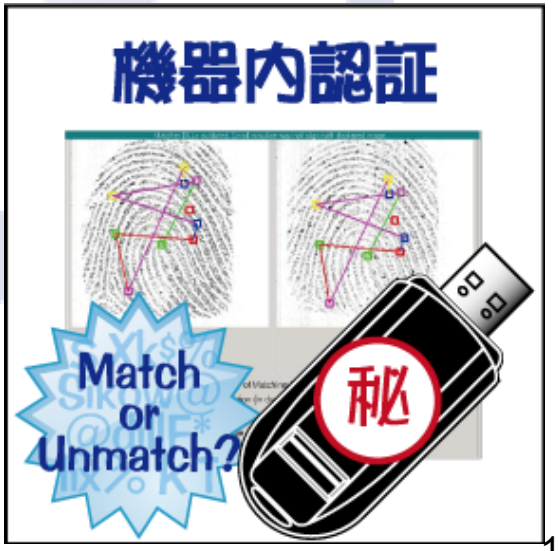
指紋認証はみな同じではありません。認証精度で選んでください。



➢機器内指紋認証（インテリジェントタイプ）

指紋情報は画像データではなく特徴点の座標情報を機器内の高度な秘匿エリアに暗号化して格納。外部からの読み出しは一切不可能です。

PC内認証タイプは、指紋認証機器とPC間で特徴点などの指紋情報や認証した結果の合否の通信が行われますが、この通信もハッキングのリスクがあります。



連携ソフトウェア「IDLoader（アイディローダー）」

M-Commerce

使用を許可するパソコンの固有情報をBiocryptodisk-ISPX Trackへ登録し

登録されたパソコン以外での不正使用を禁止するセキュリティ管理ソフトウェアです

- 使用を許可しないパソコンではBiocryptodisk-ISPX Trackを接続しても一切のデータの読み書込みを行うことができません。
- ファイル共有ソフト (Winny等)からの情報漏洩も防止できます。
- USBメモリ経由でのウィルス感染のリスクを回避する事ができます。

製品名称
指紋認証USBメモリ「Biocryptodisk-ISPX Track」連携ソフトウェア
「ID Loader（アイディローダー）」

製品型番　SLIDM-UT-1 (JANコード: 4582420182031)
動作環境　Windows 10 / 8.1 / 8 / 7 / Vista

Biocryptodisk-ISPX Track 製品仕様

M-Commerce

製品型番	HKISK-08-3X (JANコード: 4582420180068)
メモリ容量	８GB　(AES-256自動暗号化機能搭載)
転送速度	最大18MB/ 秒（書込み時）、24MB／秒（読出し時）
指紋センサ	静電容量式半導体センサ
解像度	508dpi
登録指紋数	6指（管理者2指+ユーザ4指）
インタフェ-ス	USB1.1/2.0（バスパワー）
対応OS	Windows 10 / 8.1 / 8 / ７ / Vista
動作温度	5℃～55℃、最大85%RH（結露無きこと）
保存温度	-20℃～65℃、最大85%RH（結露無きこと）

指紋認証USBメモリ
Biocryptodisk ISPX Track
バイオクリプトディスク
アイエスピーエックストラック