



指紋認証機能付きUSBフラッシュメモリBiocryptodisk-ISPX  
の強固なセキュリティに関して

2015年6月

エムコマース株式会社

<http://www.m-commercekk.jp/>



# Biocryptodisk-ISPXセキュリティ対策

## 完全内部処理

- マイクロプロセッサを搭載し、指紋の登録・読み込み・照合作業の全てを内部で処理する為、指紋に関する情報を一切外部に出さない。

## データの分離

- フラッシュメモリと指紋情報を保存するメモリは別チップであるので、PCからアクセスできるフラッシュディスクをクラックしても指紋情報は取り出せない。
- 指紋情報を格納しているメモリはマイクロプロセッサ側に配置されているので、マイクロプロセッサと制御プログラムの許可無しに外部へ出力する手段は無い。

## 自動暗号化

- フラッシュメモリに書かれるデータはBiocryptodisk-ISPX内で自動暗号化(AES256方式)処理を行っている為、メモリチップを外して他のフラッシュメモリに搭載しても読み取り不可能。

## 物理的対策

- ケース本体は、はめ込みやネジ組み等ではなく強固な接着により組み立てているので、破壊しないと分解できない。
- メモリチップを基板から剥がそうとするとチップにダメージが加わり、再使用が不可能となる様な実装方法を採用。



# 登録された指紋情報の安全性に関して

## 安全な指紋情報

- 登録された指紋情報は機器内のマイクロプロセッサ内部に登録され、いかなる方法を用いても外部に読み出すことはできません。
- 指紋情報は自動暗号化され格納されます。

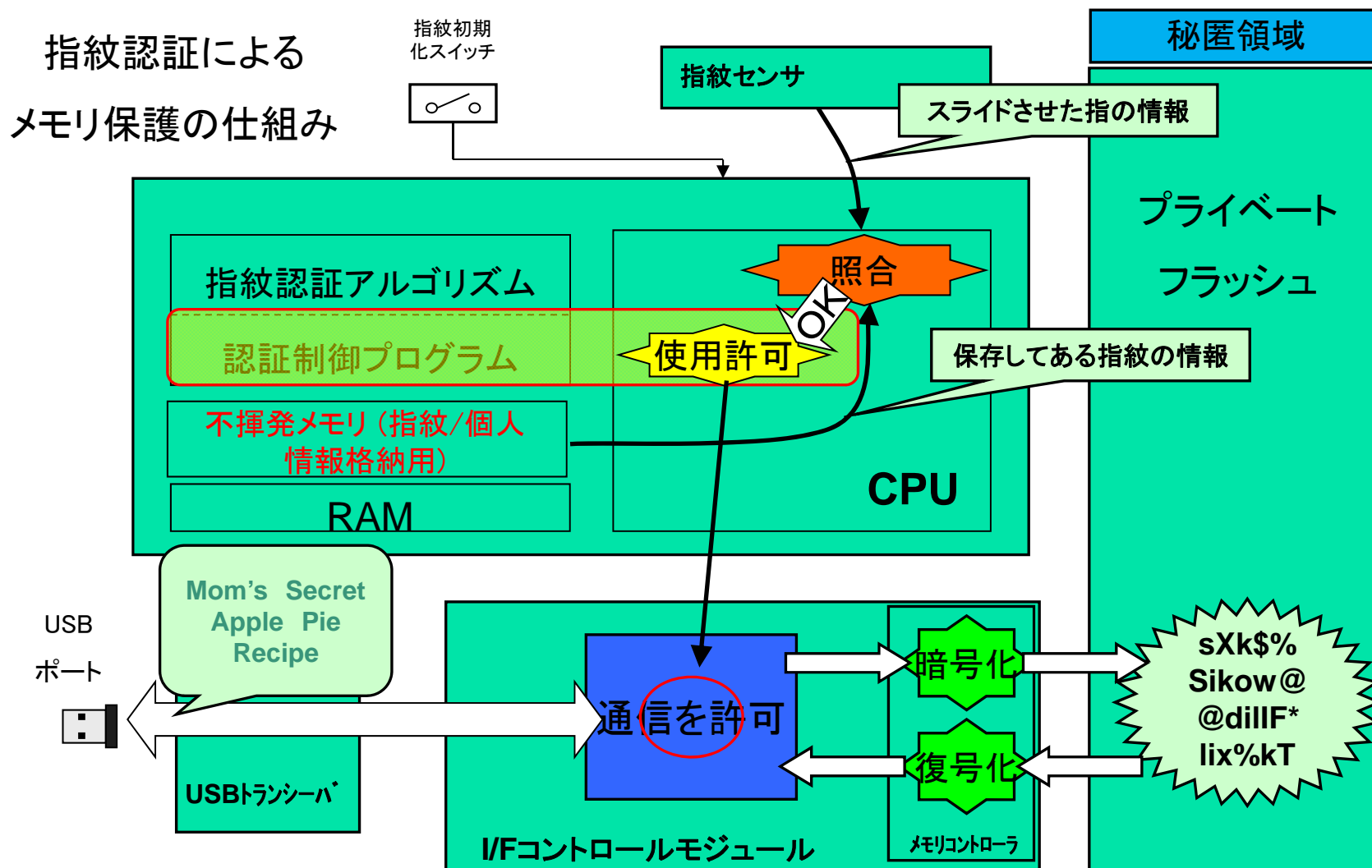
## 指紋情報独自フォーマット

- 指紋情報は画像データではなく、特徴点をベクトル化した座標情報として格納されるため、この指紋情報から画像データに戻すことは不可能です。
- 指紋特徴点情報のフォーマットはエムコマース社独自形式で、他社の指紋認証機器で処理することはできません。

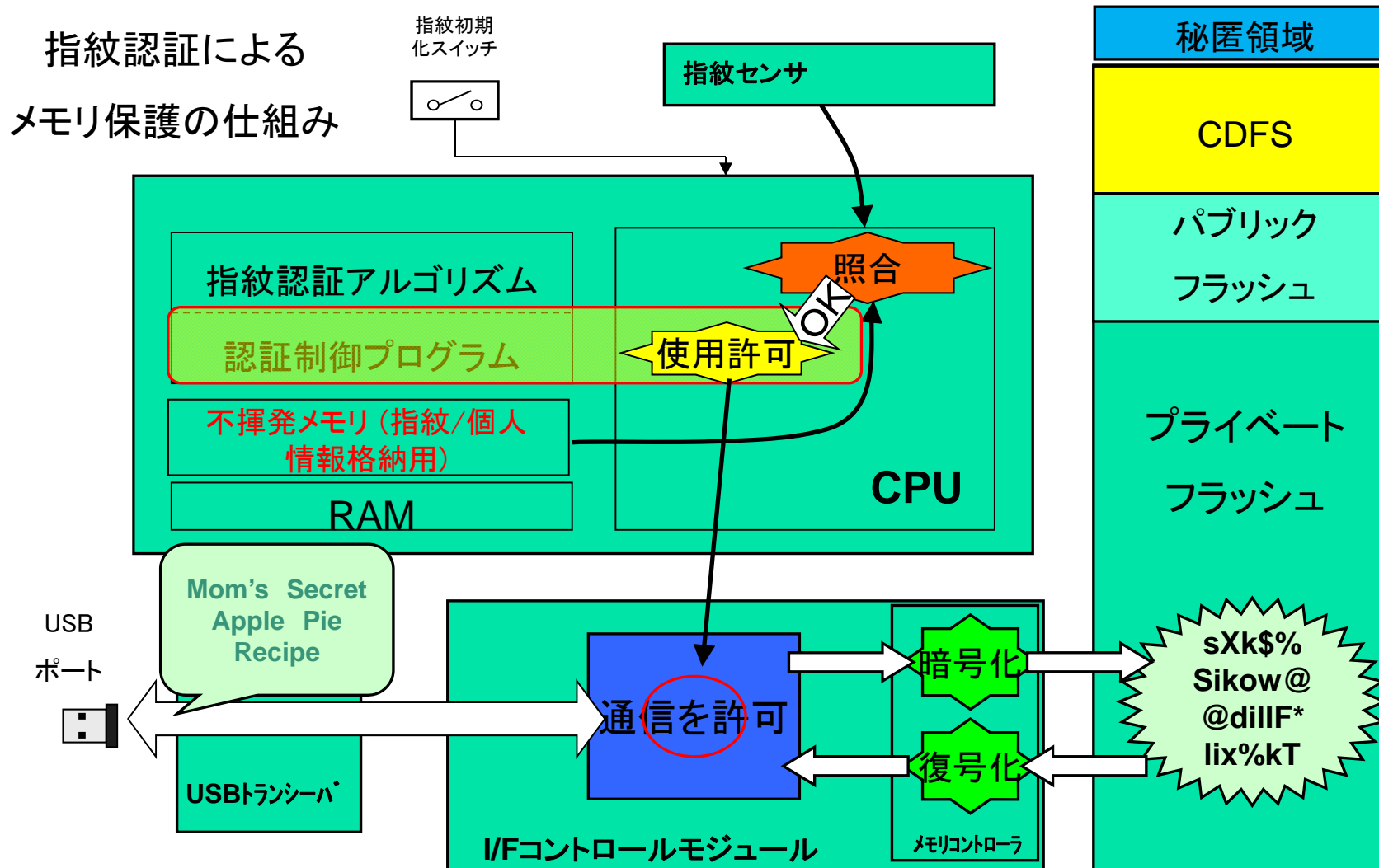
## 偽造指対策

- Biocryptodisk-ISPXは独自技術の生体検知機能を搭載しており、偽造指でのハッキングを防いでおります。

# Biocryptodisk-ISPX内部ブロック図



# Biocryptodisk-ISPX Track内部ブロック図



# Biocryptodisk-ISPXメモリ内部ダンプ

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
OBD54340	9F	62	EE	14	F5	E4	52	18	8F	4E	CF	BF	DD	D3	E4	9D
OBD54350	9F	62	EE	14	F5	E4	52	18	8F	4E	CF	BF	DD	D3	E4	9D
OBD54360	9F	62	EE	14	F5	E4	52	18	8F	4E	CF	BF	DD	D3	E4	9D
OBD54370	9F	62	EE	14	F5	E4	52	18	8F	4E	CF	BF	DD	D3	E4	9D
OBD54380	9F	62	EE	14	F5	E4	52	18	8F	4E	CF	BF	DD	D3	E4	9D
OBD54390	9F	62	EE	14	F5	E4	52	18	8F	4E	CF	BF	DD	D3	E4	9D
OBD543A0	9F	62	EE	14	F5	E4	52	18	8F	4E	CF	BF	DD	D3	E4	9D
OBD543B0	9F	62	EE	14	F5	E4	52	18	8F	4E	CF	BF	DD	D3	E4	9D
OBD543C0	9F	62	EE	14	F5	E4	52	18	8F	4E	CF	BF	DD	D3	E4	9D
OBD543D0	9F	62	EE	14	F5	E4	52	18	8F	4E	CF	BF	DD	D3	E4	9D
OBD543E0	9F	62	EE	14	F5	E4	52	18	8F	4E	CF	BF	DD	D3	E4	9D
OBD543F0	3D	98	EB	14	57	1E	57	18	2D	B4	CA	BF	7F	29	E1	9D
OBD54400	1B	BB	88	4A	DC	EC	E5	7D	41	ED	5B	36	E0	79	0D	BB
OBD54410	1B	BB	88	4A	DC	EC	E5	7D	41	ED	5B	36	E0	79	0D	BB
OBD54420	1B	BB	88	4A	DC	EC	E5	7D	41	ED	5B	36	E0	79	0D	BB
OBD54430	1B	BB	88	4A	DC	EC	E5	7D	41	ED	5B	36	E0	79	0D	BB
OBD54440	1B	BB	88	4A	DC	EC	E5	7D	41	ED	5B	36	E0	79	0D	BB
OBD54450	1B	BB	88	4A	DC	EC	E5	7D	41	ED	5B	36	E0	79	0D	BB
OBD54460	1B	BB	88	4A	DC	EC	E5	7D	41	ED	5B	36	E0	79	0D	BB
OBD54470	1B	BB	88	4A	DC	EC	E5	7D	41	ED	5B	36	E0	79	0D	BB

512バイト毎に独立した鍵で暗号化



# ご留意事項

- Biocryptodisk-ISPXにて不良が発生した際、または指紋の誤登録された場合に強制的に登録した指紋を消去し、内部のデータを復活させてほしいとのご要望に関しましてはアーキテクチャー上、登録指紋のみの消去は不可能です。弊社が行っている処置は特別のツールを使い、強制的に指紋データやフラッシュディスクの内容を初期化、工場出荷状態に戻すことしかできません。また、内部のフラッシュメモリーは個体固有の鍵を用いて暗号化されており、メモリー自身を抜き出して他の機器に載せた場合でも呼び出すことはできないため、いかなる方法を用いても内部データのみを生かすことはできません。ご了承お願い申し上げます。