FUJITSU

TCG-JRF セミナー 講演資料

PCでの活用事例:
「PC実装に必要な対応項目、ソリューション例」

2010年11月4日

(株)富士通研究所
ヒューマンセントリックシステム研究所

shaping tomorrow with you

アジェンダ

- Opal HDD採用のモチベーション
- Opal HDDの特徴
- PC搭載
  - Opal HDDの初期設定
  - Shadow Area開発における注意点
  - Opal HDDの具体的なアクセス方法
- Opal HDDを用いたソリューション
- まとめ

Opal HDD採用のモチベーション

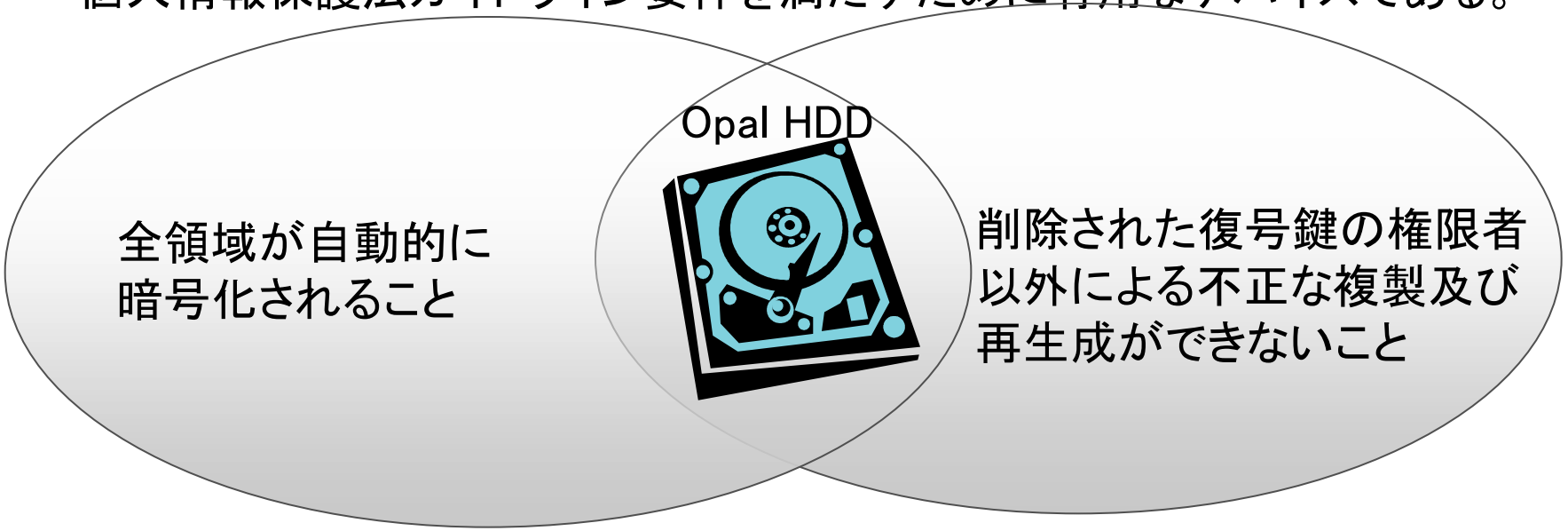
FUJITSU

業界標準

- 暗号化機能付きHDDは、現状HDDベンダ毎に仕様が異なる。Opal HDDによりPCベンダが採用判断基準を持たないといけない問題が解消される。

コンプライアンス

- 個人情報保護法ガイドライン要件を満たすために有用なデバイスである。



電気通信事業における個人情報保護に関するガイドライン(総務省)
2010.7. 改訂

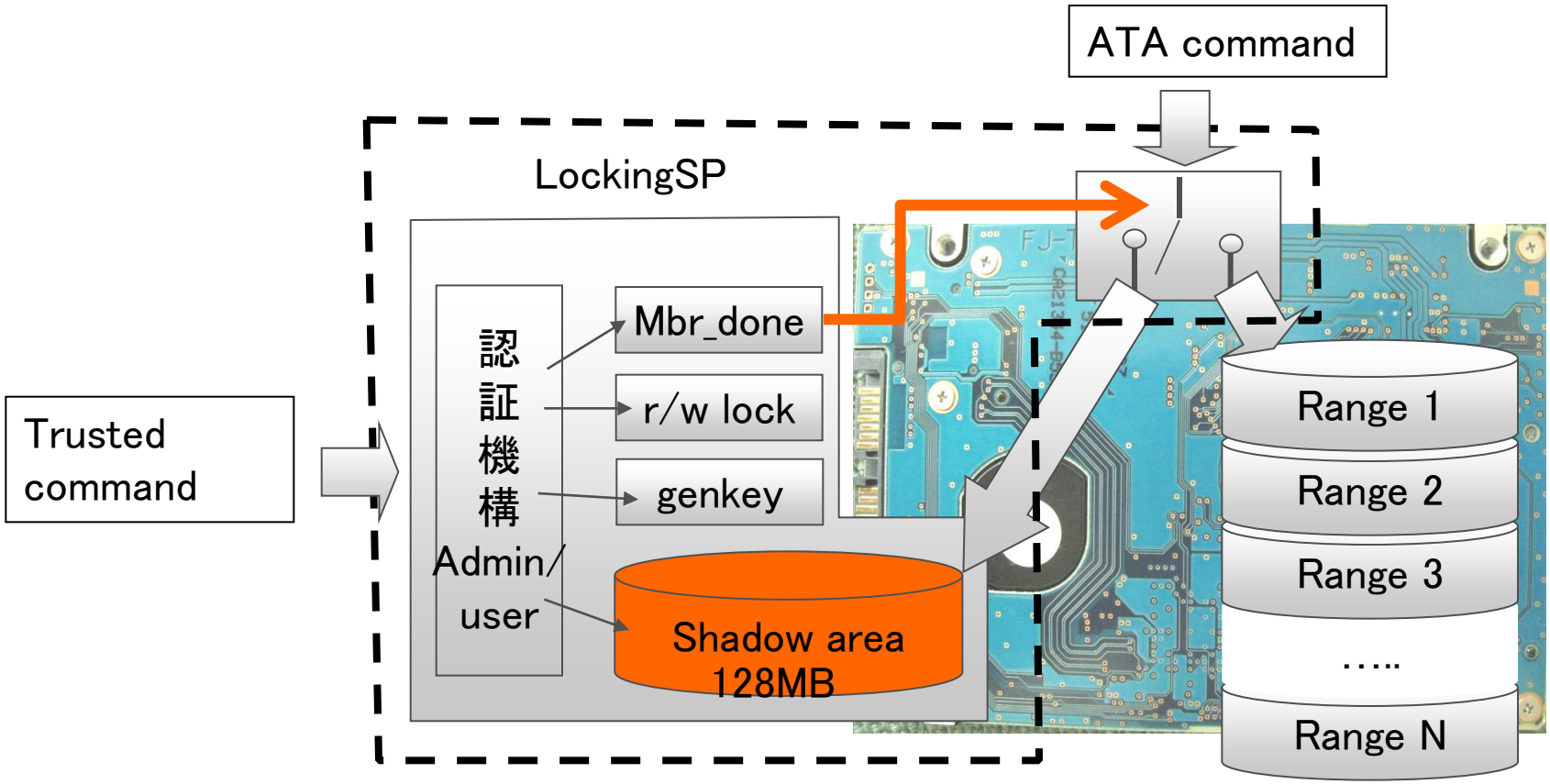
- Opal HDD採用のモチベーション
- Opal HDDの特徴
- PC搭載
  - Opal HDDの初期設定
  - Shadow Area開発における注意点
  - Opal HDDの具体的なアクセス方法
- Opal HDDを用いたソリューション
- まとめ

Opal HDDの特徴

- Opal HDDには、ATAとTCGの2つのmodeがある。

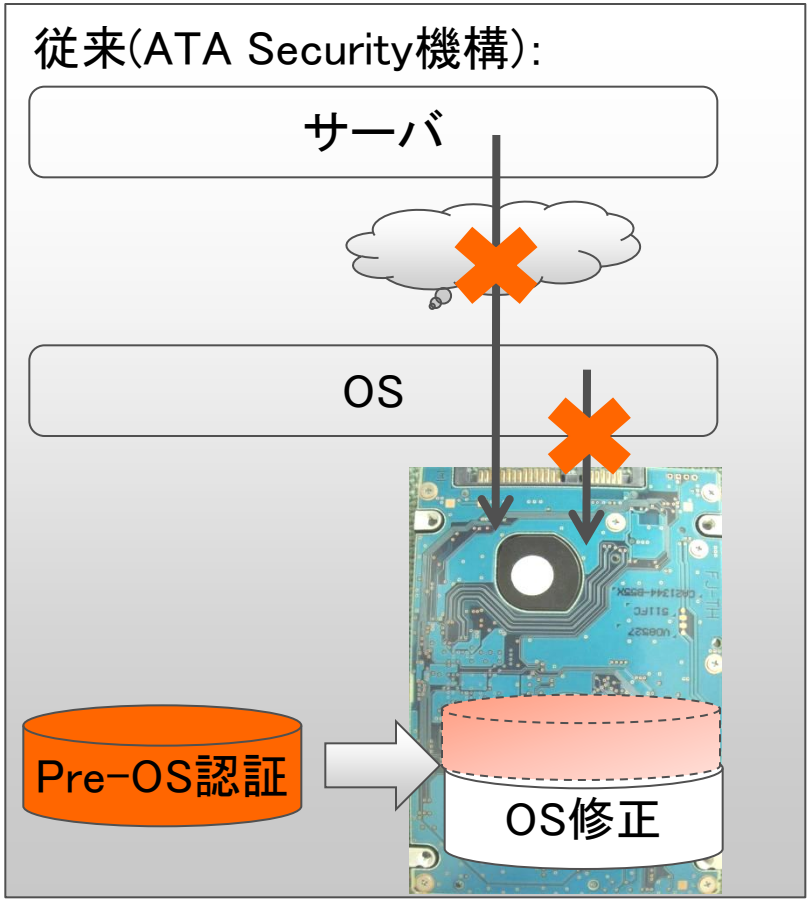
Opal HDDの特徴(つづき)

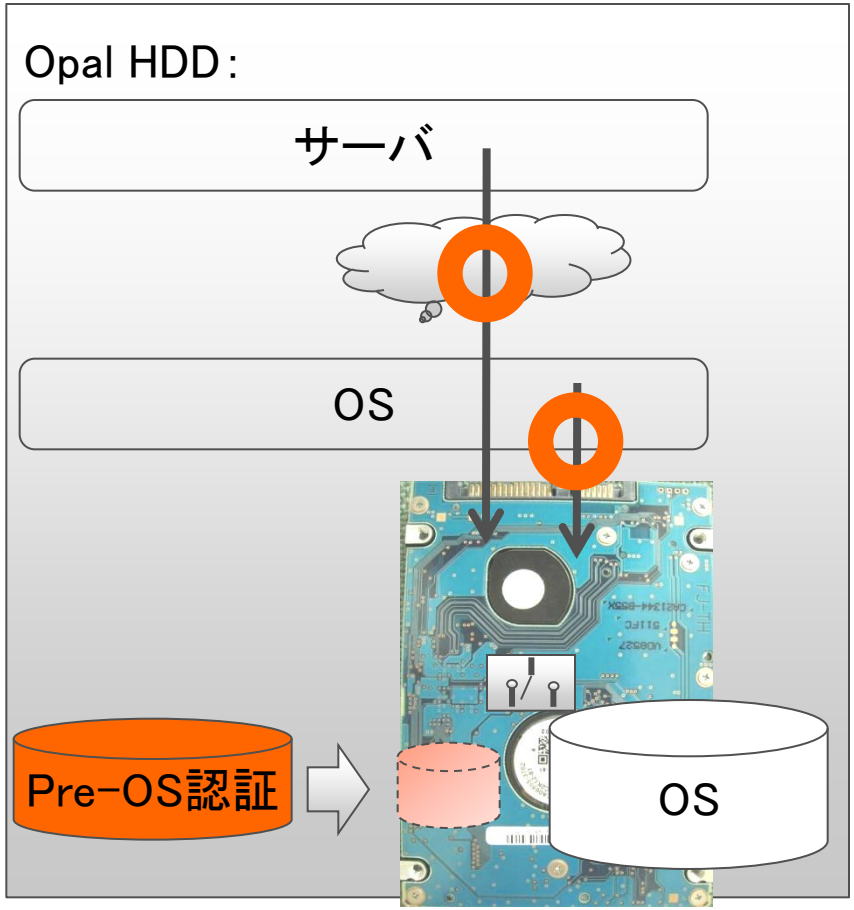
- Locking SPの特徴
  - 複数ユーザ(ex. Admin1～4, user1～8) アカウントが設定可能
  - HDD領域を複数Rangeにわけ、部分的に「read/write lock」,「消去」が可能
  - HDD先頭領域をShadowする、「Shadow MBR機能」を設定可能



- Opal HDD採用のモチベーション
- Opal HDDの特徴
- PC搭載
  - Opal HDDの初期設定
  - Shadow Area開発における注意点
  - Opal HDDの具体的なアクセス方法
- Opal HDDを用いたソリューション
- まとめ

PC搭載におけるメリットは？





- メリット:
  - OS起動後も、外部からr/w lock, 消去、アカウント設定などのリモートコントロールが可能
  - OSのブートローダーなど修正せずに、pre-OS認証を導入できる

- Opal HDD採用のモチベーション
- Opal HDDの特徴
- PC搭載
  - Opal HDDの初期設定
  - Shadow Area開発における注意点
  - Opal HDDの具体的なアクセス方法
- Opal HDDを用いたソリューション
- まとめ

外部からコントロールするための注意点

FUJITSU

Opal HDDの初期設定

- Opal HDDを制御したいソフトウェアは、Opal HDDとの間で共通パスワードをshareする必要がある。

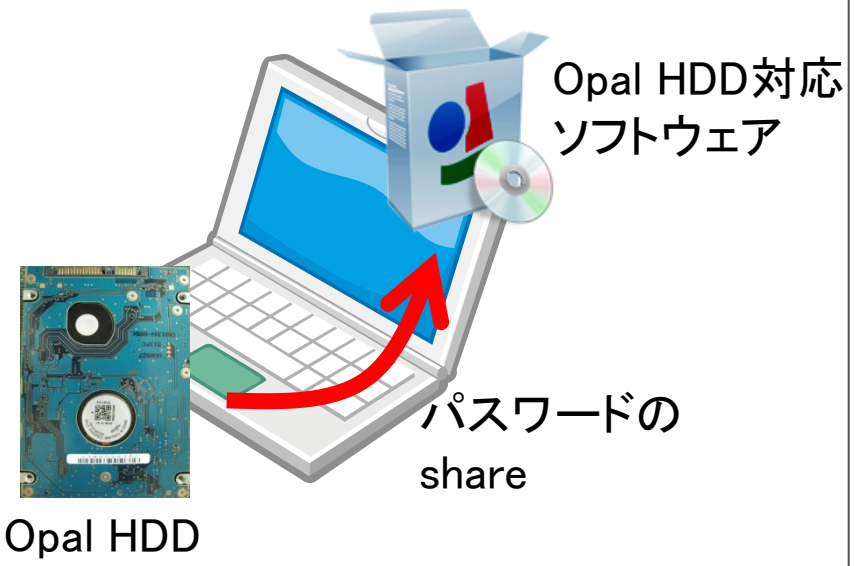
TCG Storage Application Note: Encrypting Drives Compliant with Opal HDD rev1.0より

共通パスワードが設定されると、初期パスワードでのコマンド発行は無効化され、初期化が完了。

初期設定の実装

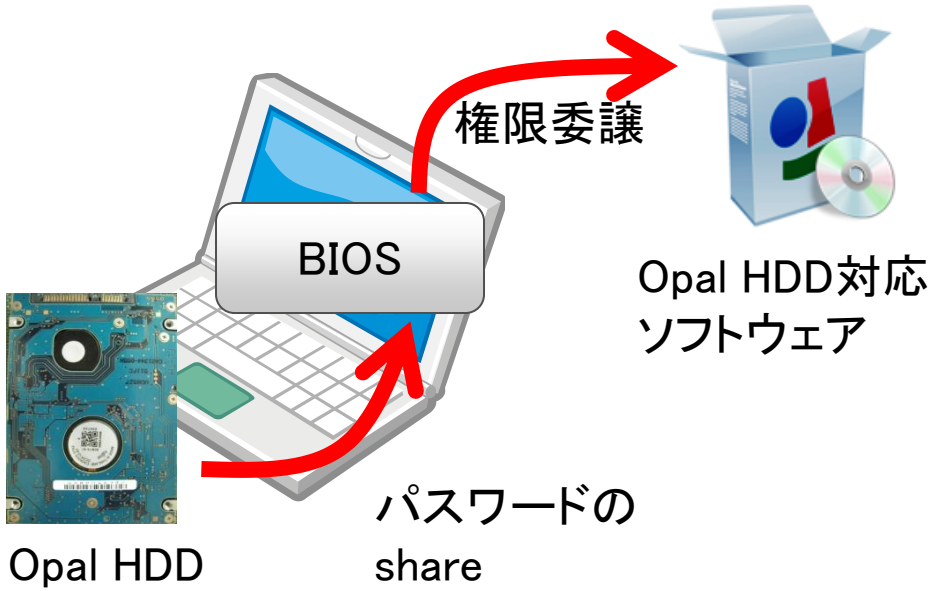
- 実装方法は2つある。

[実装1] プレインストールソフトで管理



PC開封時に、Opal HDD対応ソフトウェアがOpal HDD間との間で、共通パスワードをシェアする実装

[実装2] BIOSで管理



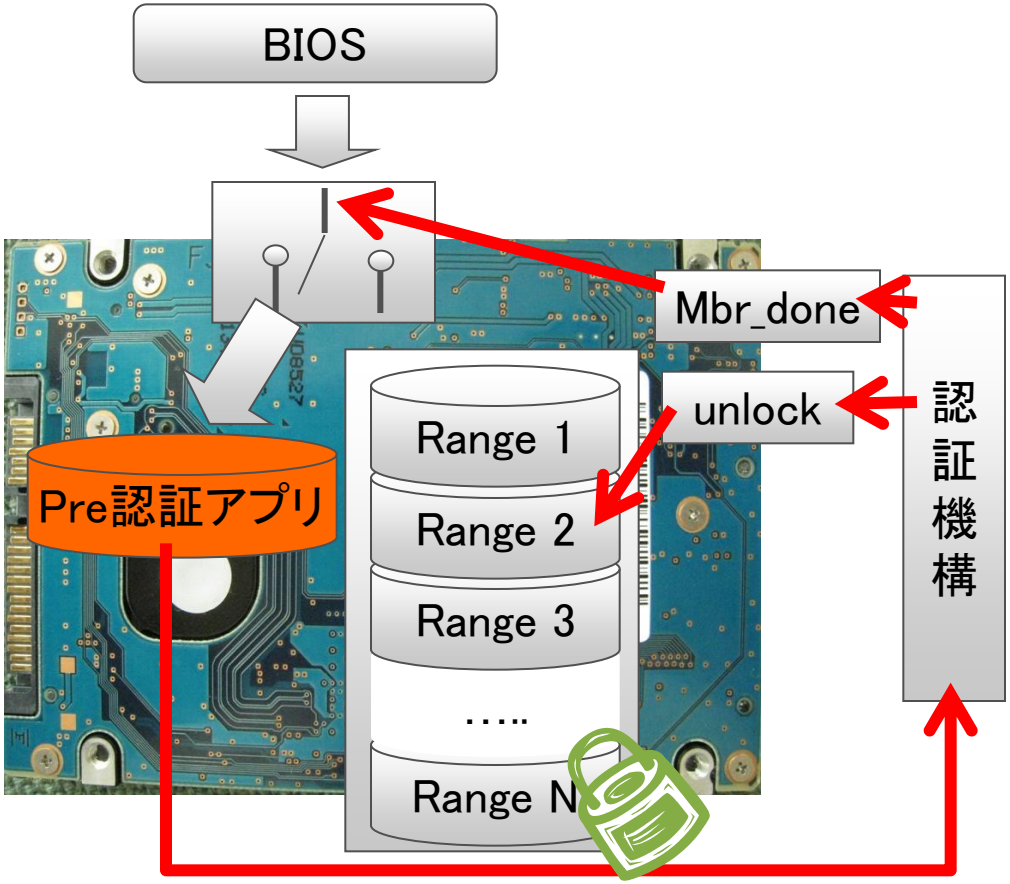
PC出荷時に、BIOSとOpal HDD間で共通パスワードをシェアする。その後ユーザがOpal HDD対応ソフトウェアを使用する際に、そのパスワードをOpal HDD対応ソフトウェアに教える実装

- Opal HDD採用のモチベーション
- Opal HDDの特徴
- PC搭載
  - Opal HDDの初期設定
  - Shadow Area開発における注意点
  - Opal HDDの具体的なアクセス方法
- Opal HDDを用いたソリューション
- まとめ

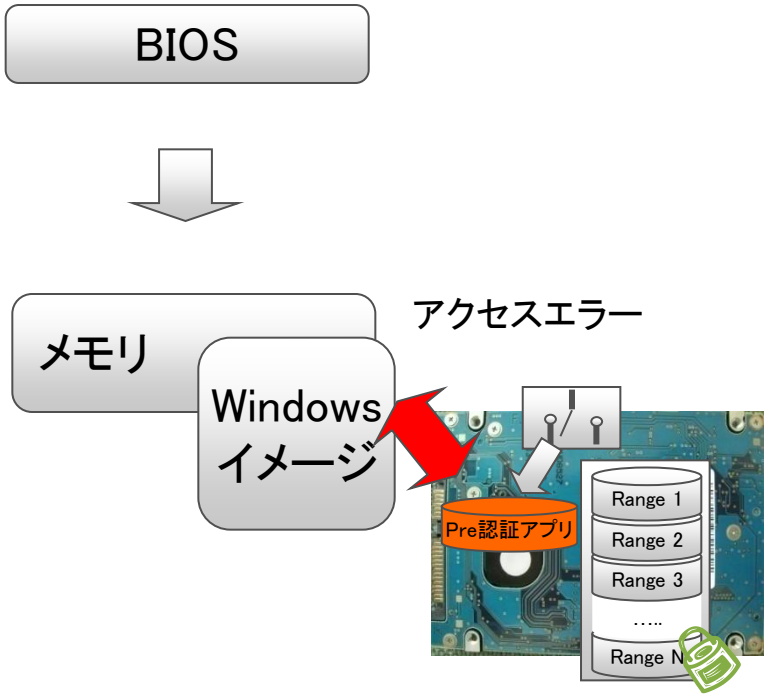
Shadow Area開発における注意点

- Power/Off/休止状態からのブート時は、Pre認証アプリがHDDのロックを解除。
- スリープからのブート時は、Pre認証アプリがよばれないので、HDDロックを解除する仕組みを追加する必要。

Power off/休止状態からのブート



スリープからのブート

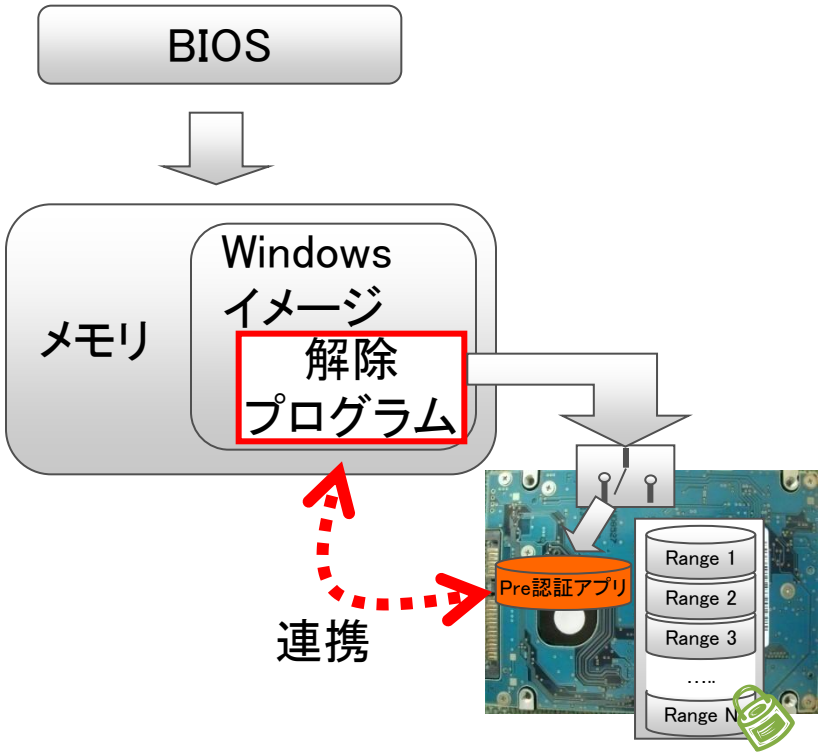


スリープからの復帰方法に関する実装

FUJITSU

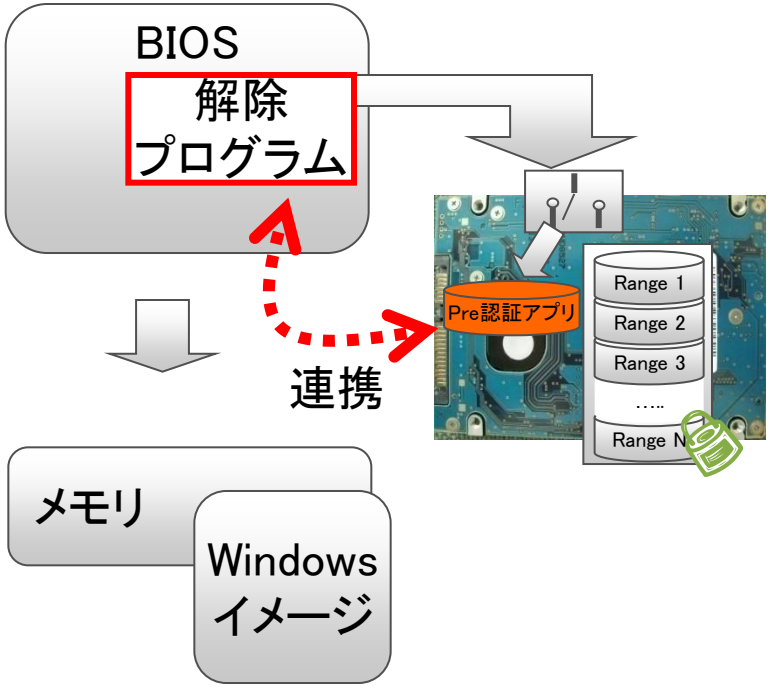
- 実装方法は2つある。

[実装1] Windowsドライバで解除



ソフトウェア暗号と同じく、windowsドライバでOpal HDDの状態をハンドリングし、ロックされた状態を解除する実装

[実装2] BIOSで解除



BIOSでOpal HDDの状態をハンドリングし、ロックされた状態を解除する実装

- Opal HDD採用のモチベーション
- Opal HDDの特徴
- PC搭載
  - Opal HDDの初期設定
  - Shadow Area開発における注意点
  - Opal HDDの具体的なアクセス方法
- Opal HDDを用いたソリューション
- まとめ

Opal HDDのアクセス方法

FUJITSU

- Trusted commandの送受信

Feature	Security Protocol	01h
Count	Transfer Length(7:0)	00h
LBA	23:8 SP Specific	0001h
	7:0 Transfer Length(15:8)	00h
Command	Trusted command	5Ch

① Discovery0

② ComID

Feature	01h
Count	01h
LBA	comID
	00h
Command	5Eh

data	Tcg defined packet (Startsession)

③ Trusted send command (start session)

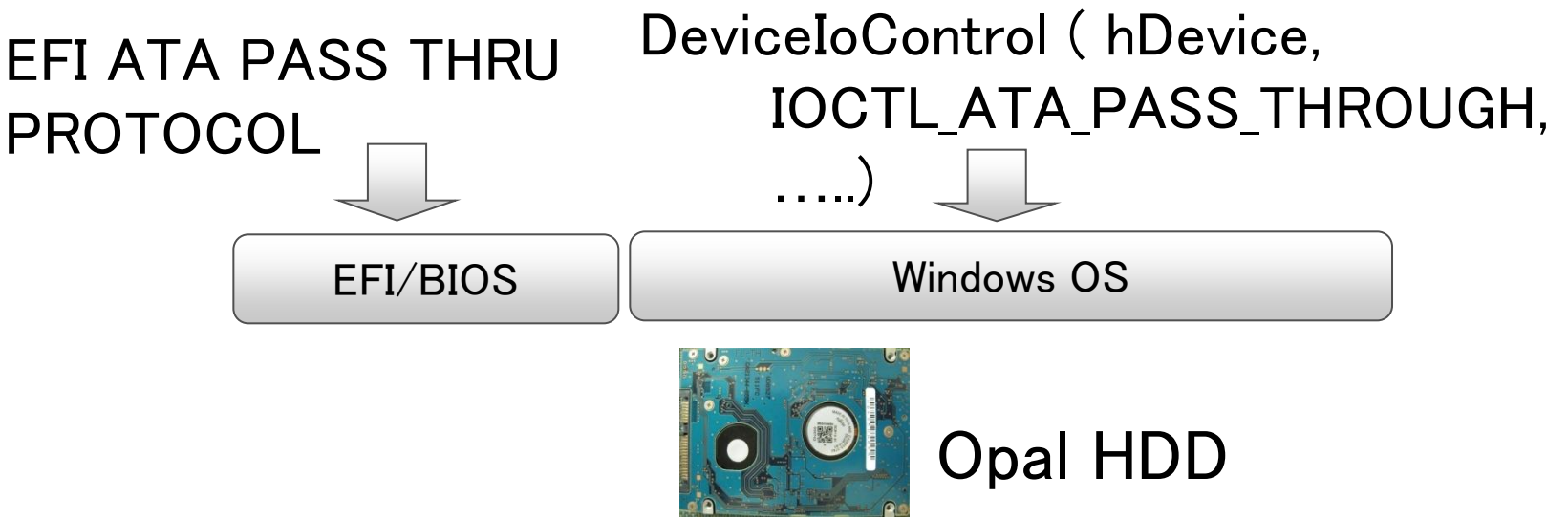
ATA/ATAPI Command Set (ATA8-ACS) T13/1699-D

TCG Storage Interface Interactions Specification (Jan.27, 2009)

Opal HDDのアクセス方法(つづき)

FUJITSU

- アクセスするためのAPI
  - WindowsアプリからTrusted commandを発行するのに利用できるAPIは、ATA PASS THROU、SCSI PASS THROU
- HDDベンダ間の差異に関して
  - 通信に必要な情報：Discovery0,Discovery1による取得
  - サポートしている機能一覧：管理するtableに対してnext methodを発行することで取得



- Opal HDD採用のモチベーション
- Opal HDDの特徴
- PC搭載
  - Opal HDDの初期設定
  - Shadow Area開発における注意点
  - Opal HDDの具体的なアクセス方法
- Opal HDDを用いたソリューション
- まとめ

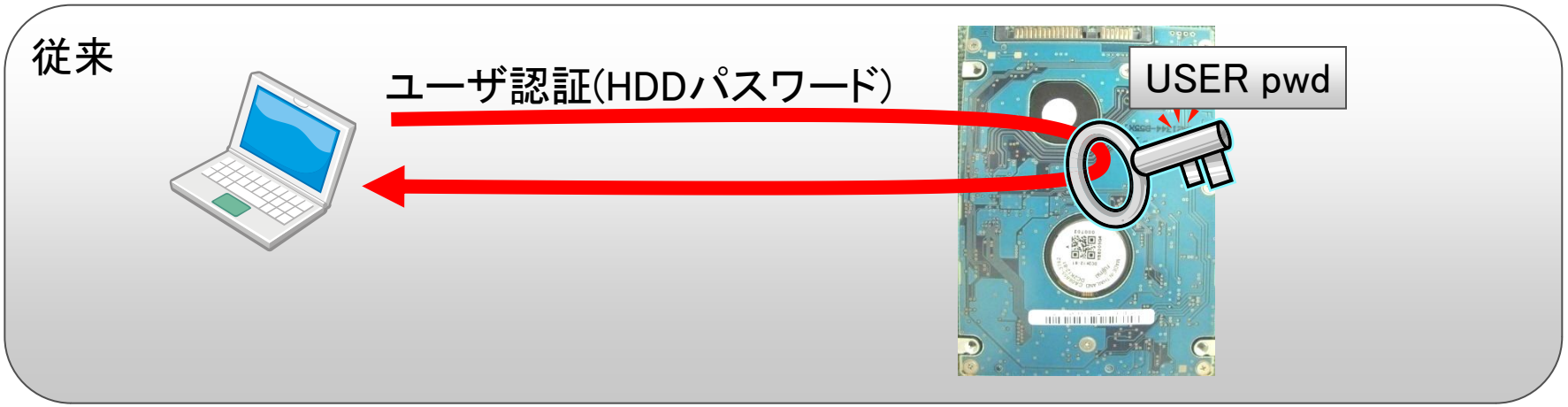
Opal HDDを用いたソリューション

FUJITSU

- 例1：HDDの認証強化
- 例2：データへのアクセス保護強化

例1：HDDの認証強化

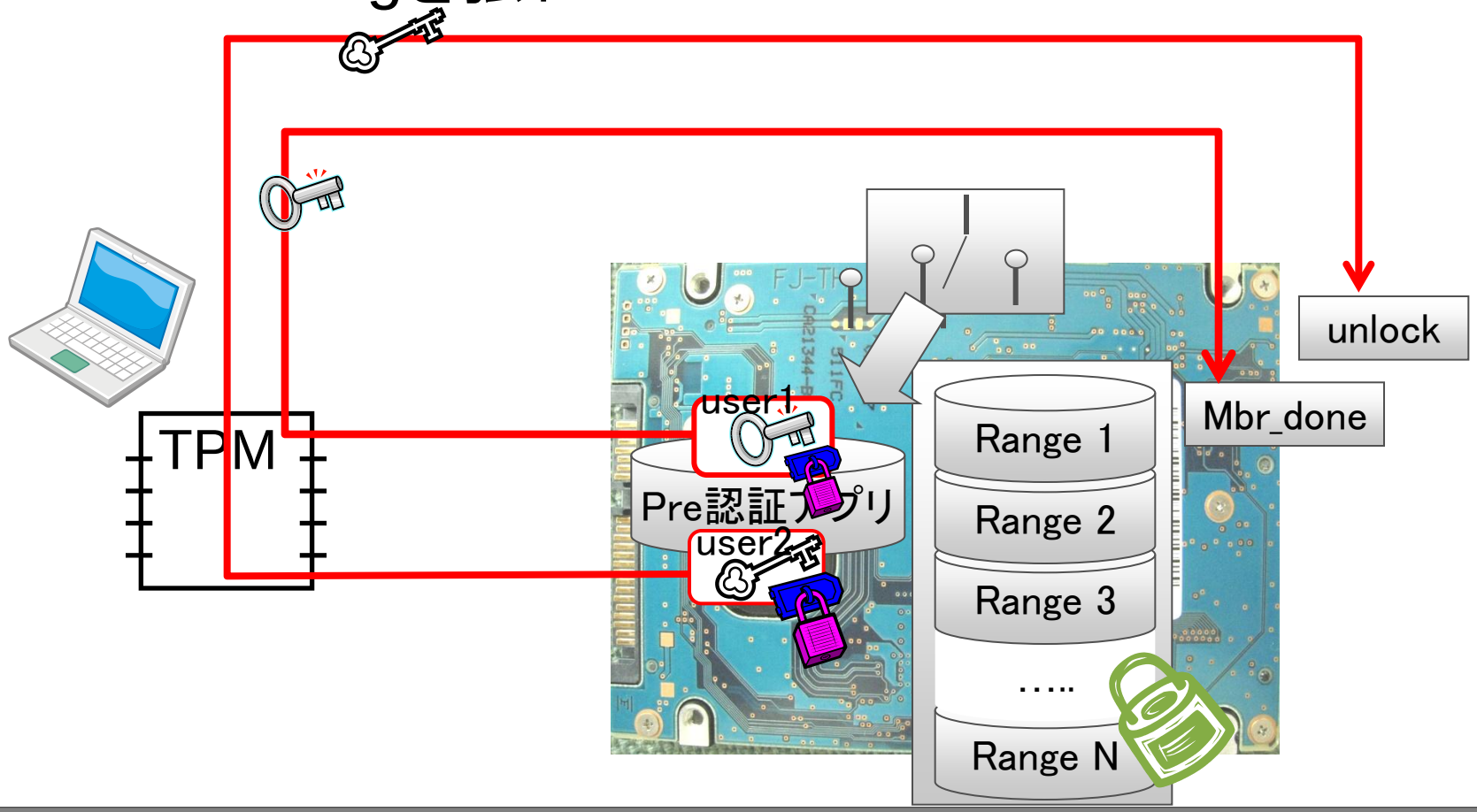
- Opal HDDが複数ユーザをもてることを利用して、PCとのBindingを強化したソリューション。



例1：HDDの認証強化（つづき）

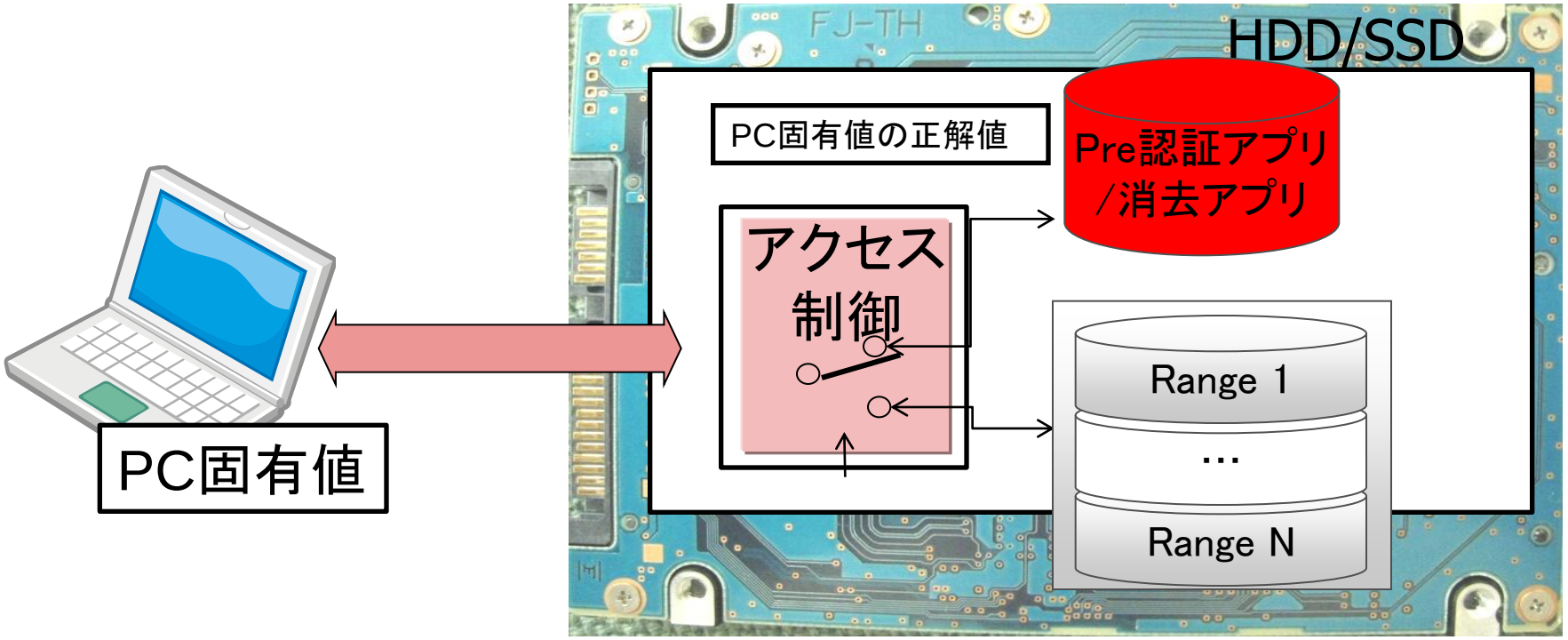
FUJITSU

- TPMの利用
  - Pre認証アプリがもつ秘密情報を保護
  - PCとのbindingを強化



例1:データ漏洩保護

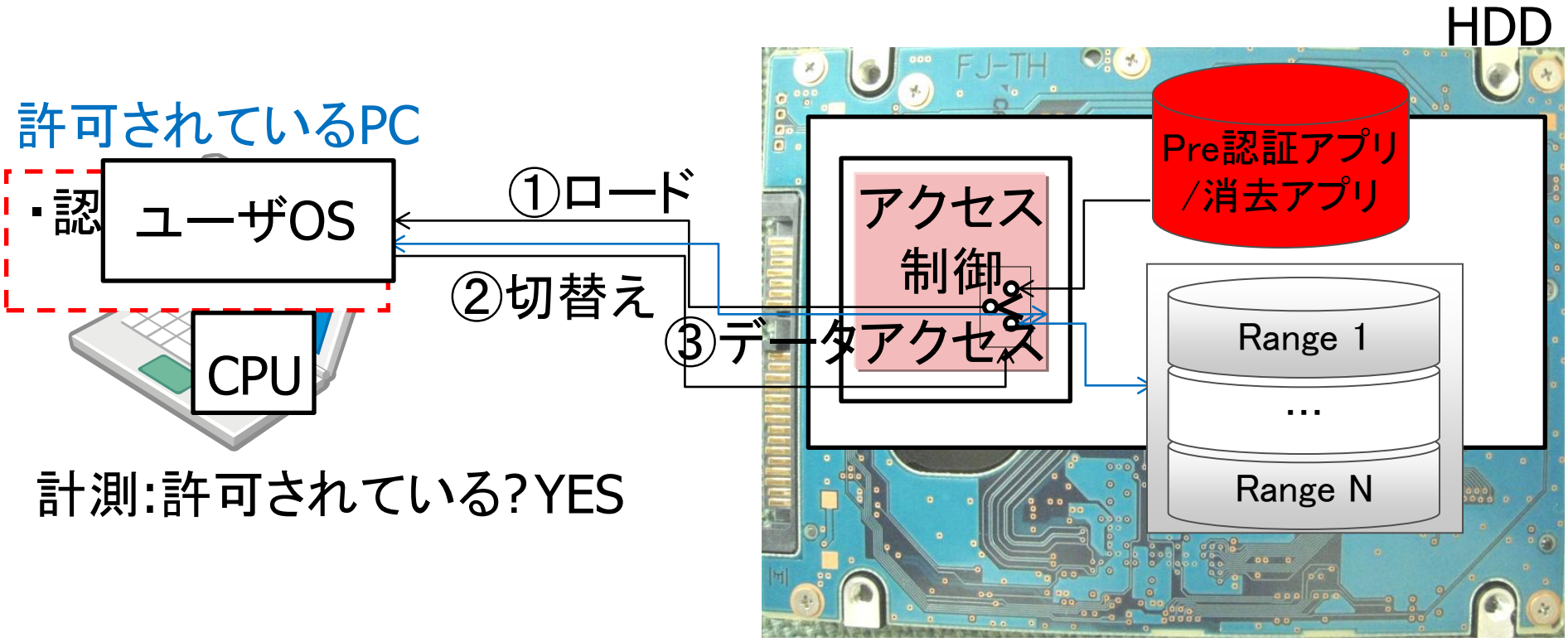
- Opal HDDのpre認証アプリ内に、HDD内データを消去する機能を実装してデータ漏洩保護



例1:データ漏洩保護の動作:登録されたPC

FUJITSU

- 既存の動作と変わらないPC起動
  - 登録されたPCで使う場合には、認証/消去App動作後、自動的にユーザOSを駆動

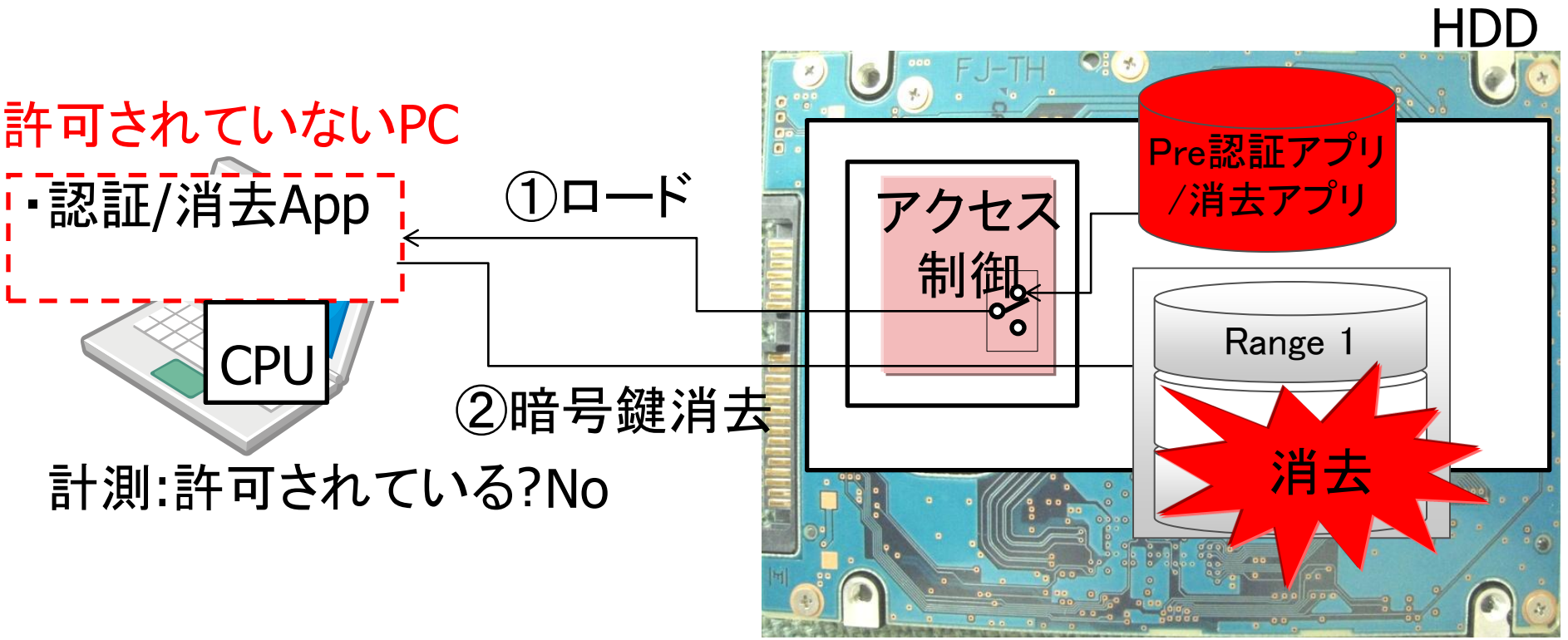


計測:許可されている?YES

例1:データ漏洩保護の動作:登録外PC

FUJITSU

- データ消去機能の実現
  - HDDを許可されていないPCで使用した場合、ユーザOSを含めたデータを消去する



Opal HDDを用いたソリューション

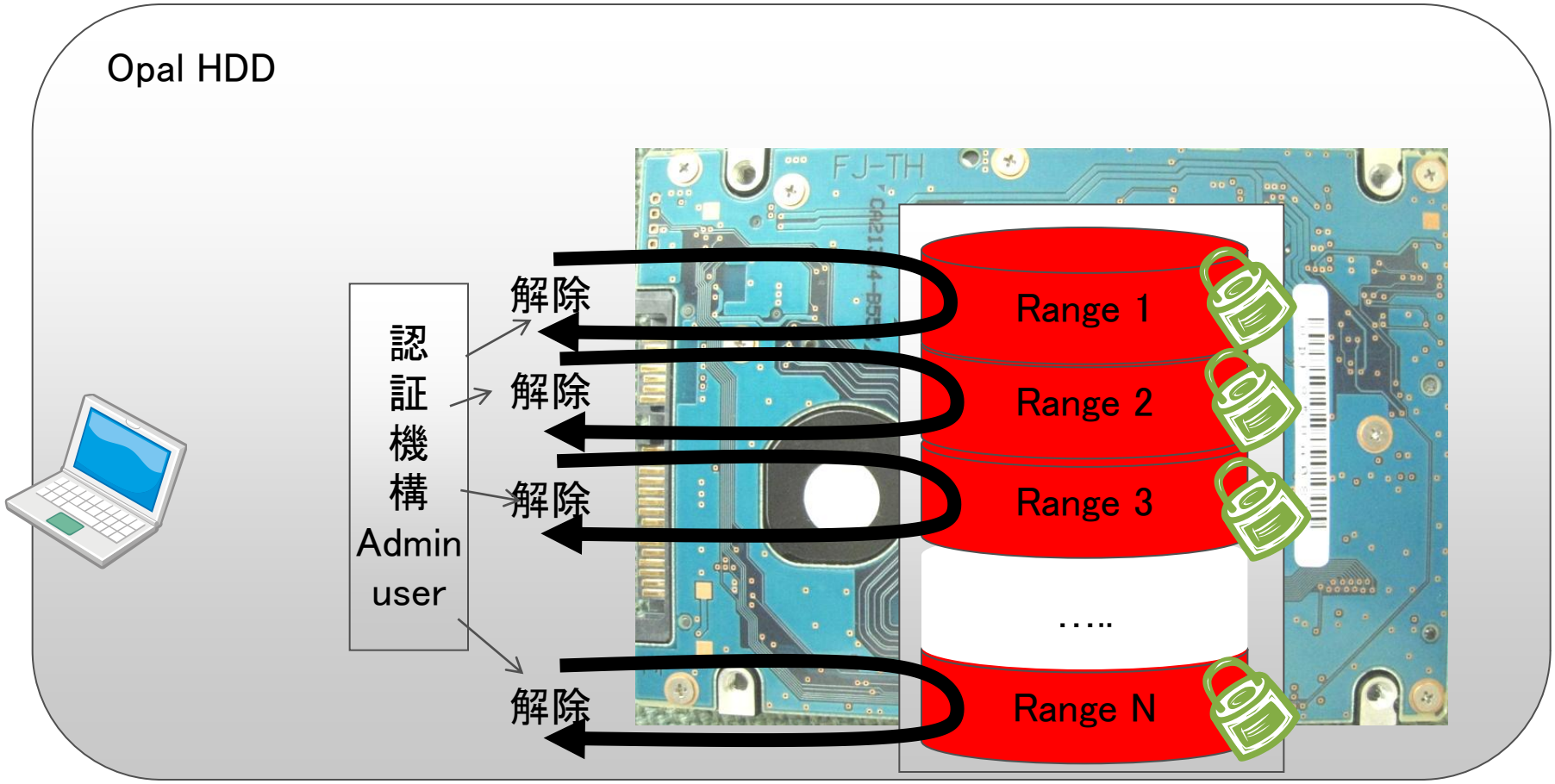
FUJITSU

- 例1：HDDの認証強化

- 例2：データへのアクセス保護強化

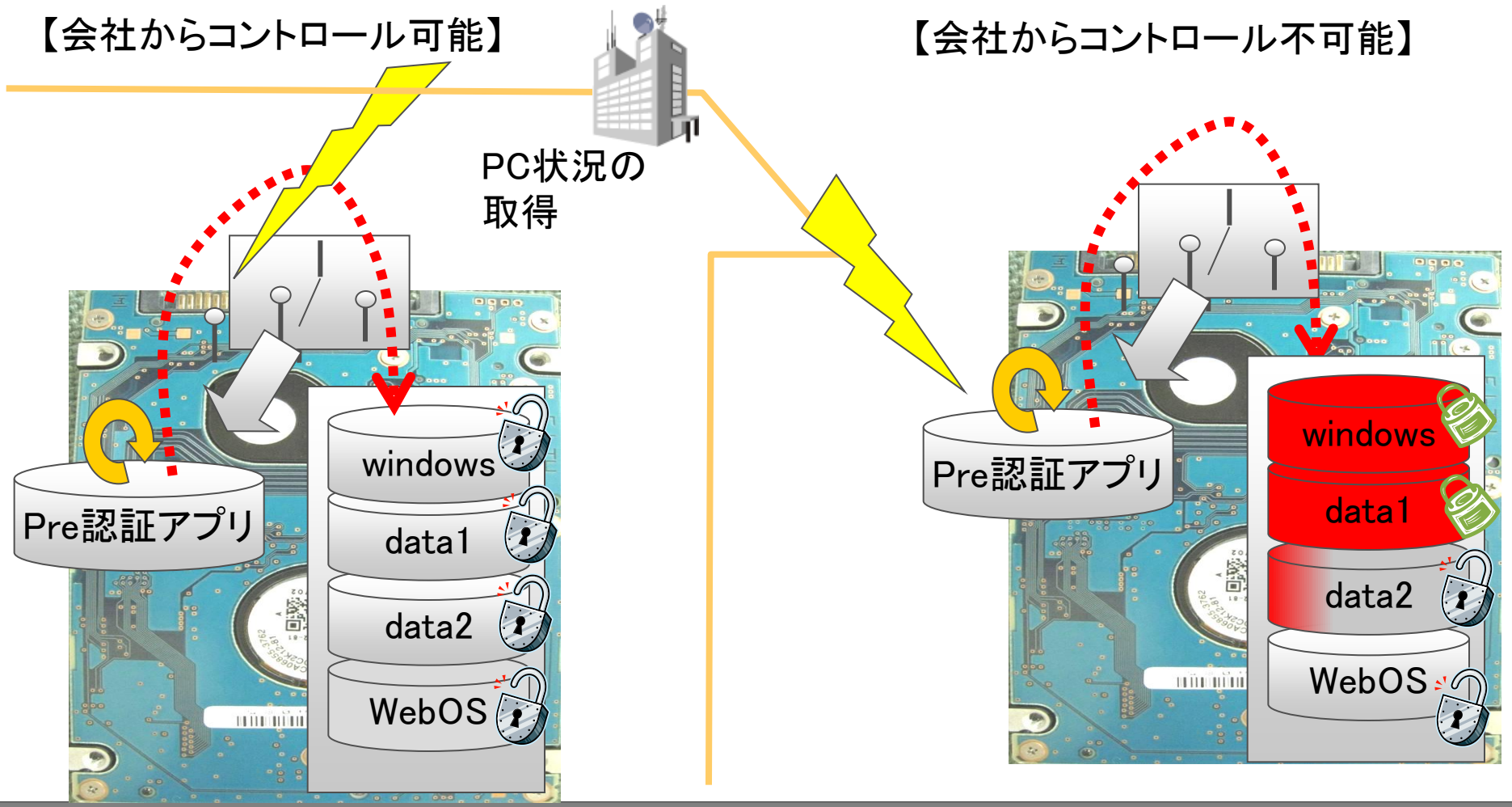
例2：データアクセス保護強化

- Opal HDDのrange機能を用いた、データへのアクセス保護強化
  - データそのものへのread/Writeアクセス制限



例2：PC状況に応じたHDDの部分lock

- PC状況(位置、ネットワーク認証など)に応じて、range解除する部分をコントロールして、データアクセスできる範囲を制限する。

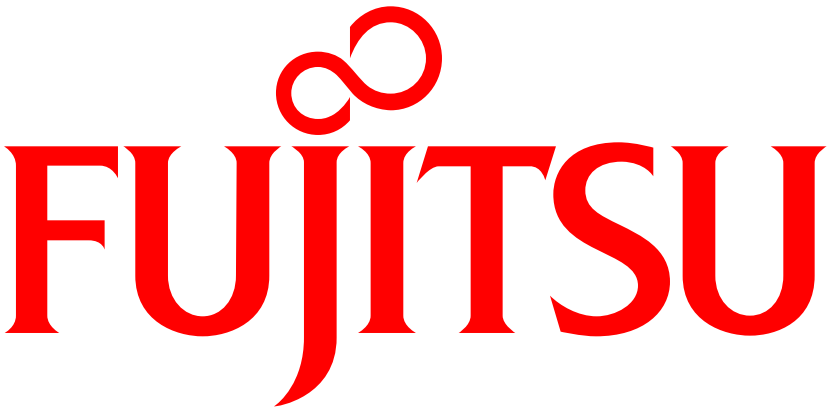


- Opal HDD採用のモチベーション
- Opal HDDの特徴
- PC搭載
  - Opal HDDの初期設定
  - Shadow Area開発における注意点
  - Opal HDDの具体的なアクセス方法
- Opal HDDを用いたソリューション
- まとめ

まとめ

FUJITSU

- Opal HDDは、標準暗号化HDD仕様、リモートコントロール、Pre-OS開発を容易にする新しい機能をもつ
- PC適用においては、ソフトウェア開発の観点から、いくつかの注意点があることを示し、それらに対する実装方法を紹介した
- PCのセキュリティ機能を強化することが可能な、いくつかのソリューションを紹介した



shaping tomorrow with you