

TCG JRF Opal Seminar



TCG Opalの 特徴と仕様の概要

Yoshiju Watanabe

Firmware Common Engineering Group
Firmware Development Department

Hitachi Global Storage Technologies

November 4, 2010

I. Opal SSCの概要

1. Opal SSCの主な機能と特徴
2. Opal Storageの構成
3. Opal Storageの効果
4. アクセス・コントロール
5. MBR Shadowing機能
6. SPのライフサイクル
7. インターフェース
8. セッションの実行

II. TCG Opal SSC HDDデモ

9. Opal SSC HDDデモ

*1. TCG: [T](#)rusted [C](#)omputing [G](#)roup の略

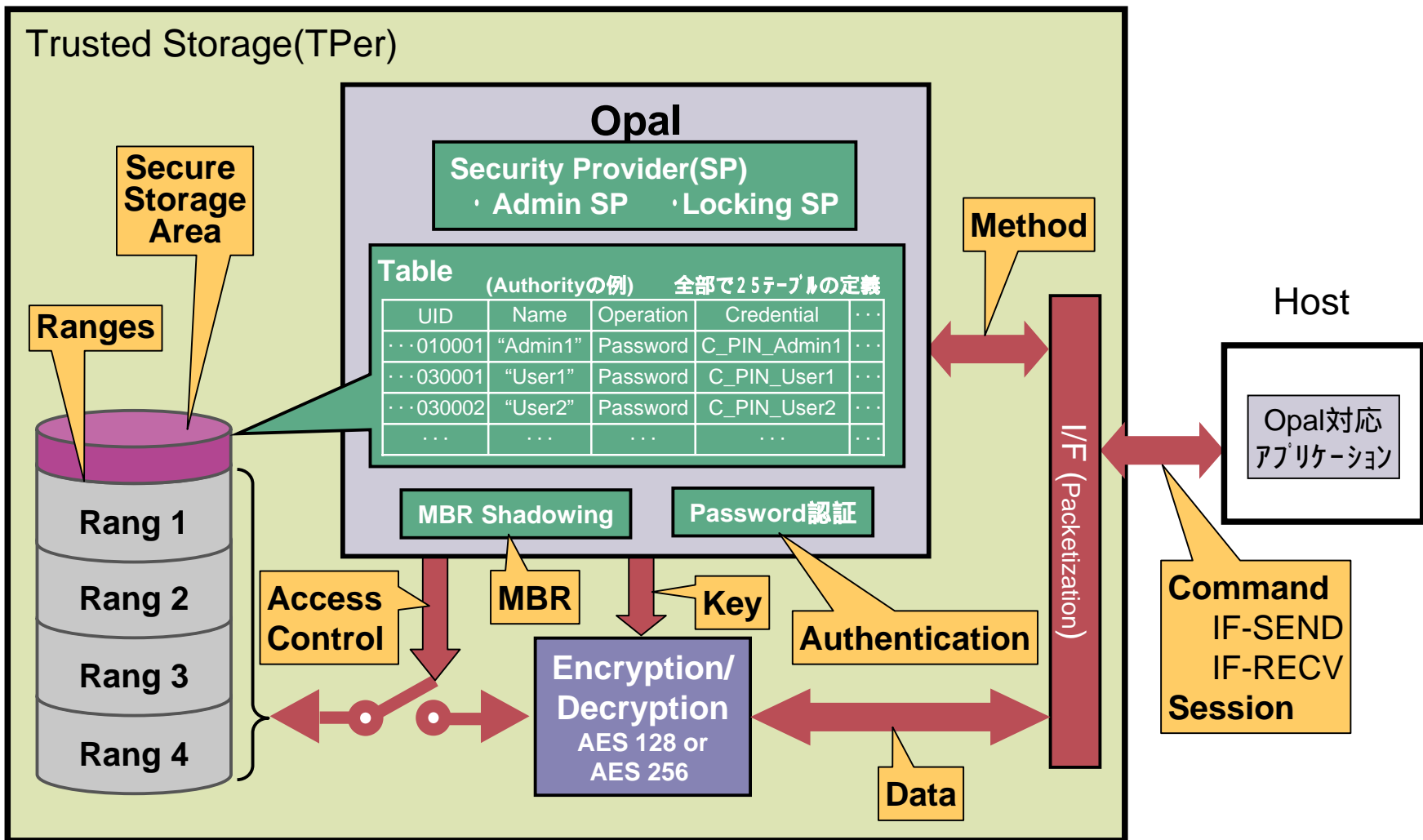
*2. TCGは、Trusted Computing Groupの米国、および、その他の国における商標です。

*3. Opal SSC: Opal [S](#)ecurity [S](#)ubsystem [C](#)lass

1. Opal SSCの主な機能と特徴

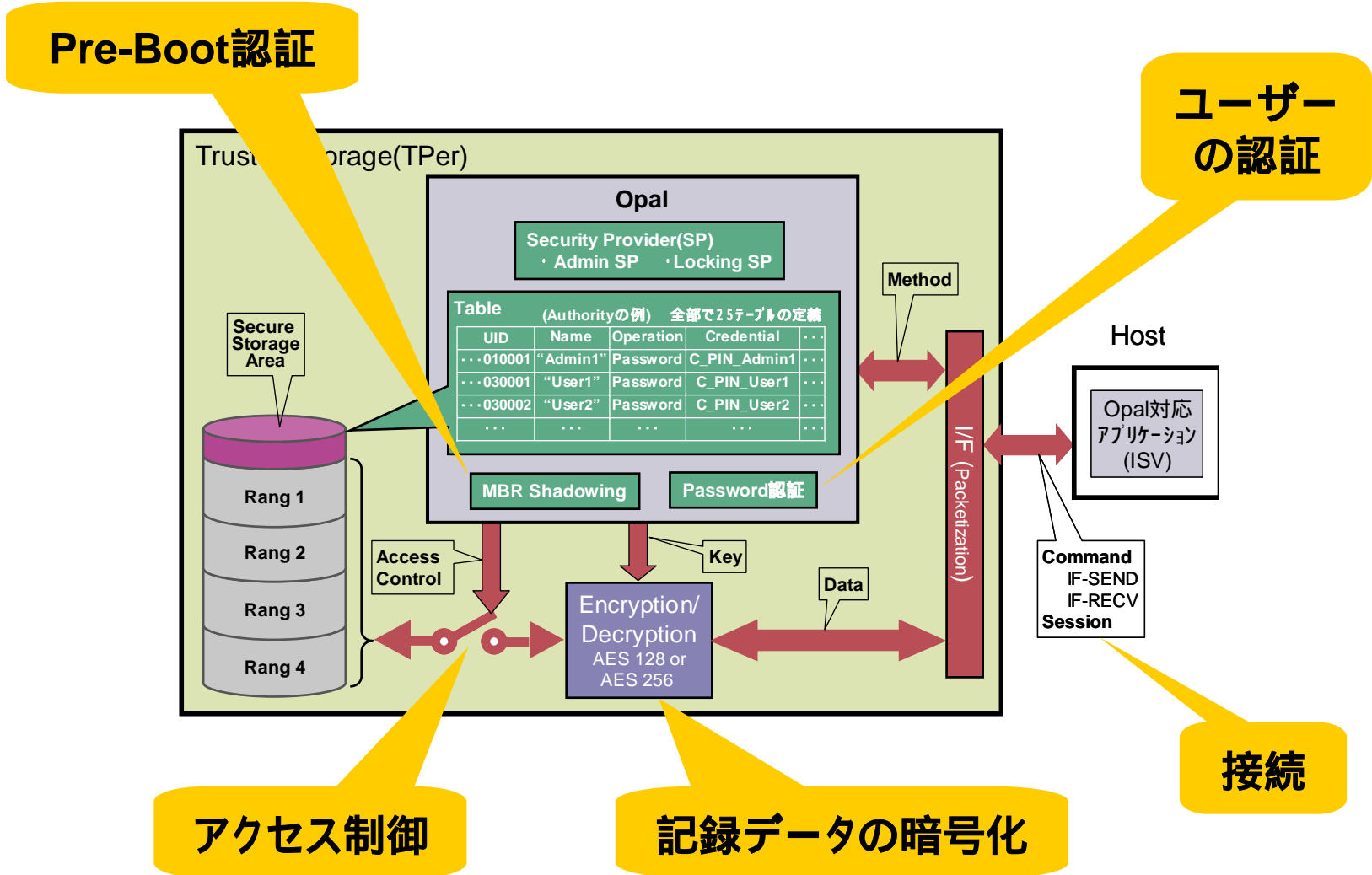
- **個別の暗号鍵で暗号化されたLBA Ranges (最小4)**
 - ・ LBA Rangeは、Administratorによって構成できる
 - ・ LBA RangeはStart LBAとSizeで指定
- **きめ細かなアクセス制御が可能**
 - ・ PINによる管理者 (1 Administrator (min))、使用者 (4 Users (min)) の設定
 - ・ AdministratorによるLocking機能のEnable/Disable設定
 - ・ 個々のLBA Rangeのアクセス制御 (Read/WriteのLocking/Unlocking) が可能
 - ・ 個々のLBA rangeの暗号鍵が変更可能 (Secure Erase)
- **MBR Shadowing実現のための共通プラットフォームの提供**
 - ・ MBR Shadowing のための領域 (PBAプログラム格納) を提供 (128MB)
 - ・ Administratorによる、MBR Shadow 領域への書き込み、Enable/Disable設定
 - ・ MBR ShadowingのUnlockingの権限の設定
- **セキュアなデータ領域 (Data Store Table: 1KB以上) の提供**
 - アクセスコントロールの設定が可能
- **ライフサイクル制御**
 - ・ LBA Range設定、Locking設定を工場出荷状態へ戻せる

2. Opal Storageの構成



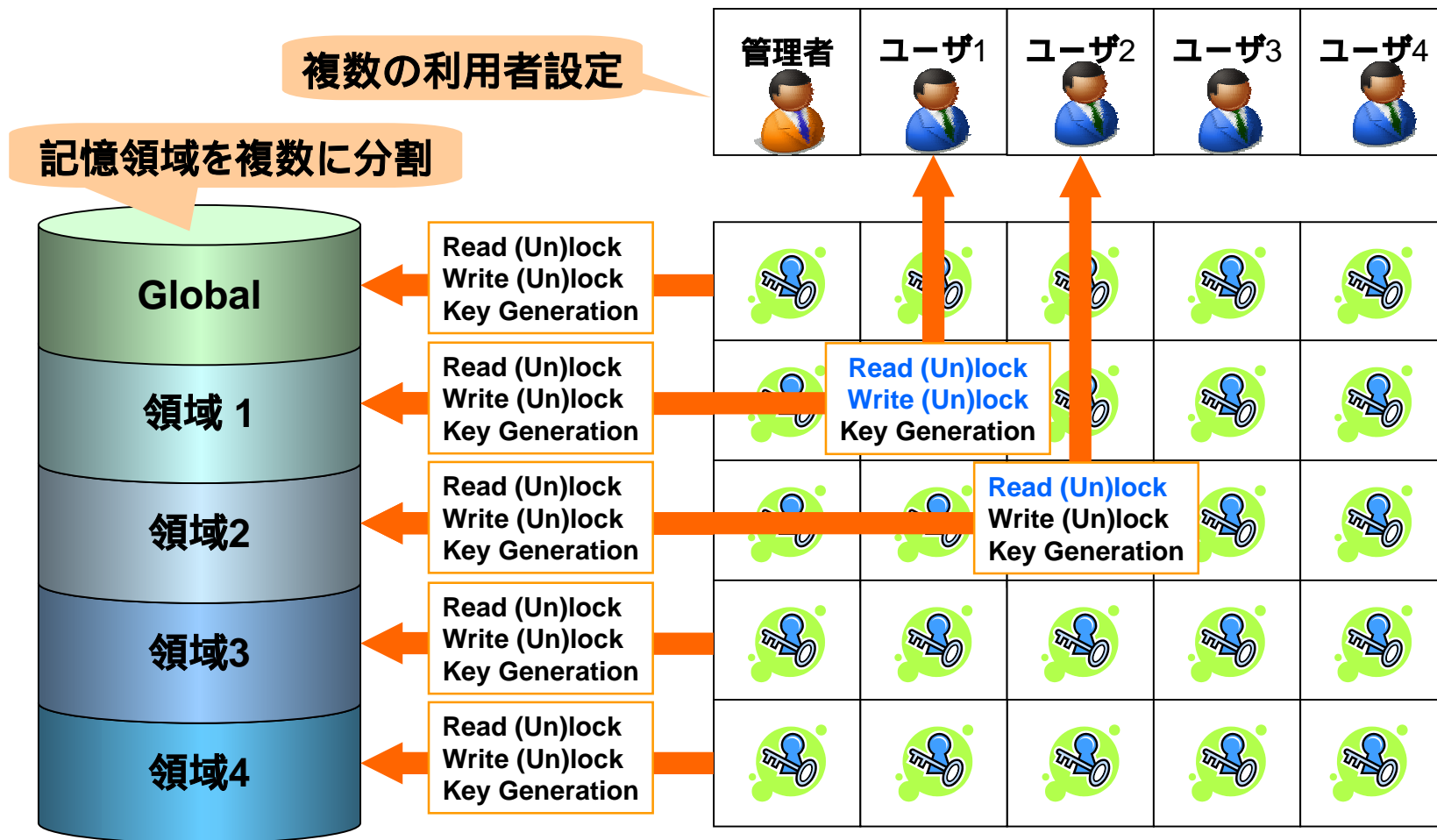
MBR: Master Boot Record

3. Opal Storageの効果

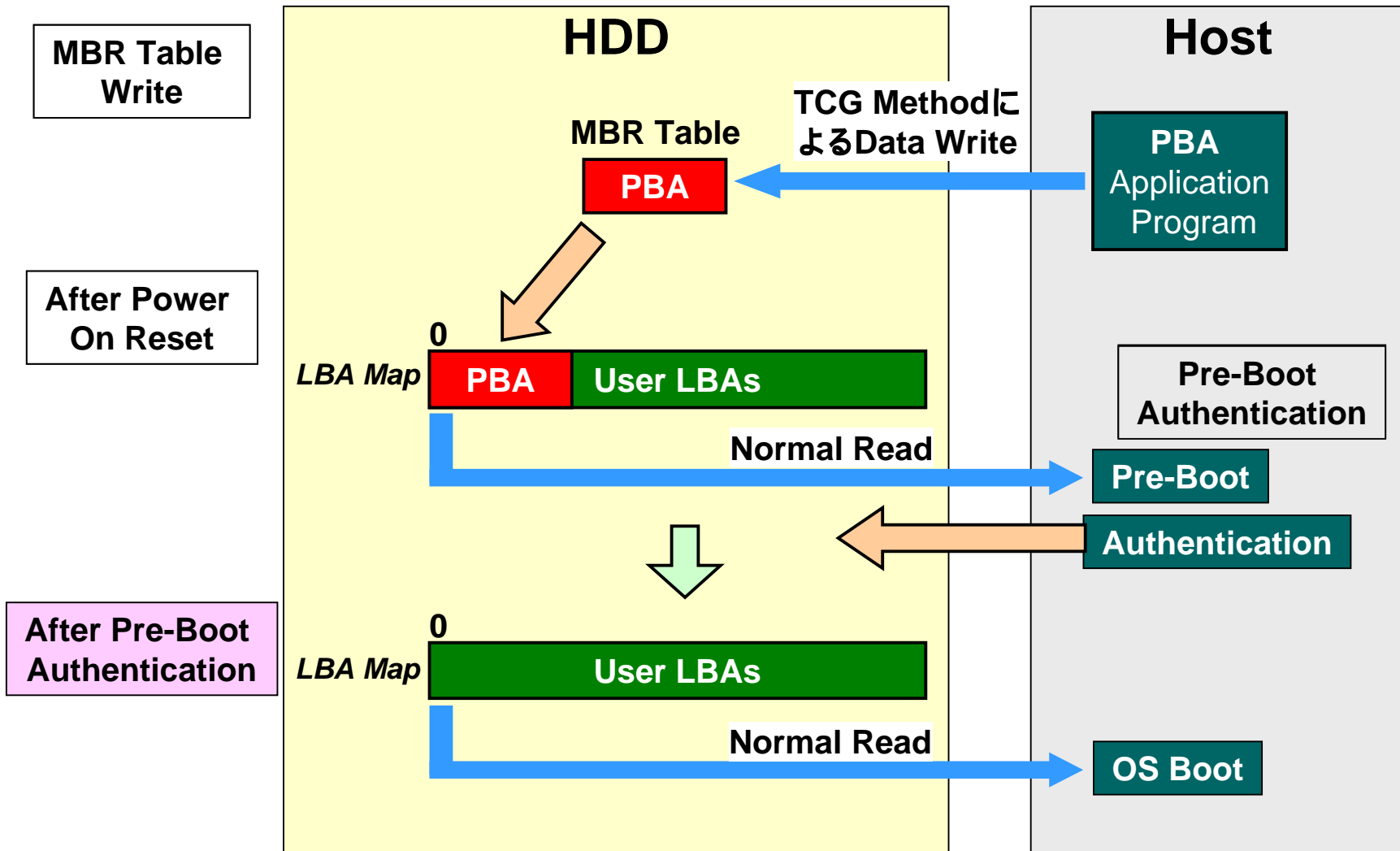


4. アクセス・コントロール

- 個々の組み合わせでアクセス管理を設定できる (Read / Write / Key)

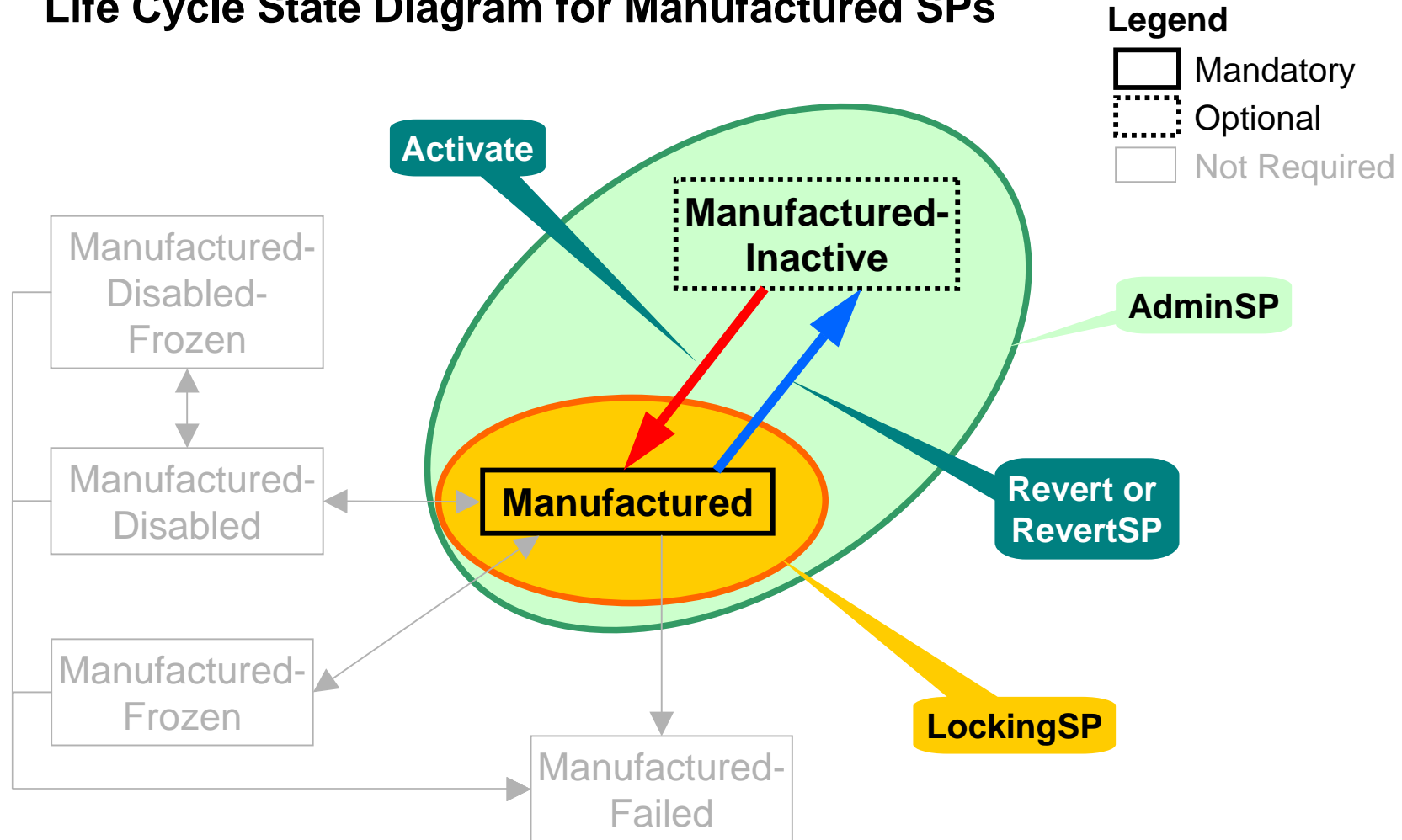


5. MBR Shadowing機能



PBA : Pre-boot authentication

Life Cycle State Diagram for Manufactured SPs

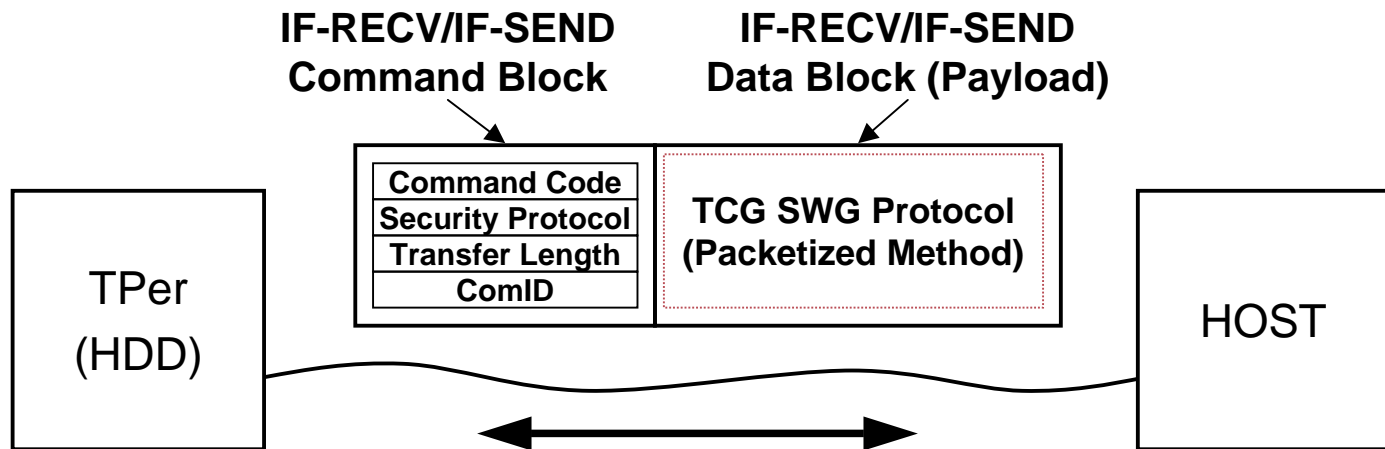


■ ATA Command Operation Codes

- Trusted Receive : 5Ch, 5Dh
- Trusted Send: 5Eh, 5Fh

■ SCSI Command Operation Codes

- SECURITY PROTOCOL IN: A2h
- SECURITY PROTOCOL OUT: B5h



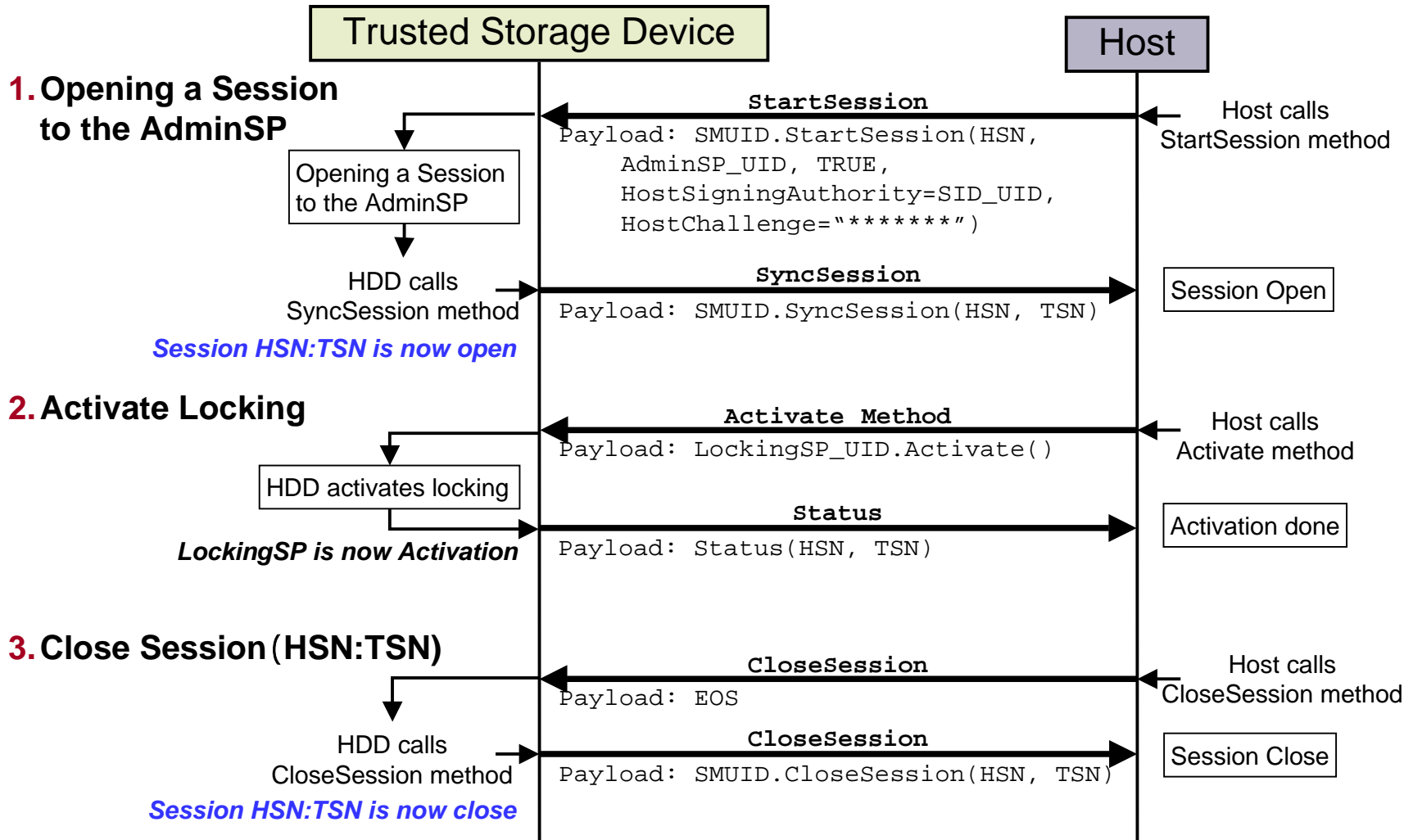
Payload Example (Set Method Call Encoding Stream)

Call Authority MethodID(Set)

```

F8 A8 00 00 00 09 00 00 00 00 A8 00 00 00 06 00
00 00 07 F0 F2 A4 4E 61 6D 65 A8 00 00 00 05 00
00 02 0B A5 41 6C 69 63 65 F3 F2 AA 43 6F 6D 6D
6F 6E 4E 61 6D 65 A8 00 00 00 05 00 00 .. .. ..
    
```

■ Locking SP をActivationする例



■ デモ画面の説明

The screenshot shows a management interface for Opal SSC HDD. It features a grid of controls for different ranges (Range1, Range2, Global Range) and users (User1, User2). Each cell contains icons for Read (Rd), Write (Wr), and Erase (Er) permissions, along with a lock icon. A legend on the right defines the icons: Rd (Read), Wr (Write), Er (Erase), and a key icon for '権限なし' (No permission). Callouts point to various UI elements: '操作ボタン' (Operation buttons), '操作タブ' (Operation tabs), '各ユーザーの各レンジでのアクセス権限の状態' (Access permission status for each user and range), '領域' (Range), 'ユーザー' (User), 'ロッキング状態 アクセス制限有 (認証要)' (Locked state, access restrictions apply, authentication required), 'コマンド処理表示' (Command processing display), '暗号鍵変更可能' (Encryption key change possible), '実行可能' (Executable), and '権限なし' (No permission).

操作ボタン

操作タブ

各ユーザーの各レンジでのアクセス権限の状態

領域

ユーザー

**ロッキング状態
アクセス制限有
(認証要)**

**コマンド
処理表示**

**暗号鍵
変更可能**

実行可能

権限なし

Legend:
 Rd: 読取り権限 (Read permission)
 Wr: 書込み権限 (Write permission)
 Er: 鍵変更権限 (Erase permission)

本資料は、将来のハードディスク需要、および、ハードディスク業界の売上げ見通し、日立の将来の製品ポートフォリオ、民生機器の将来需要に関わる文言、すなわち、米国の「連邦有価証券法」の意味する範囲内での将来予測の文言を含みます。これらの予測は、弊社の製品の需要変動の可能性、新製品の開発またはマーケティング上の遅れ、競合他社による新製品の投入、または、新しい競合相手の市場参入や法的な争いの可能性を含んでおり、これらのリスク、不確実性により、実際の業績等の結果が見通しと異なることがあります。上記以外のリスクや不確実性は、(株)日立製作所から米国証券取引委員会へ提出されている最新の資料および、報告に含まれません。(株)日立製作所と日立グローバルストレージテクノロジーズは、本資料発表の後に起きた出来事や、状況を反映するためにこの将来予測を更新するいかなる責務も負いません。

HITACHI
Inspire the Next 