第2回 鍵管理勉強会 資料

FUJITSU
shaping tomorrow with you

# TCG*関連から見る鍵管理
## - Opal HDD(暗号化ディスク)
## - 欧米における個人情報扱い/考え方

*TCG：Trusted Computing Group

2012年7月3日

富士通(株)　インテリジェントサービス本部
戦略企画統括部　小谷誠剛
TCG常任理事、組込系WGおよび日本支部共同議長

TRUSTED COMPUTING GROUP™

# Trusted Computing Group (TCG)とは

FUJITSU

- 信頼できるプラットフォーム/インフラを構築するため、ハードウェア、ソフトウェアの業界標準、統合的仕様の開発、普及を目的とする

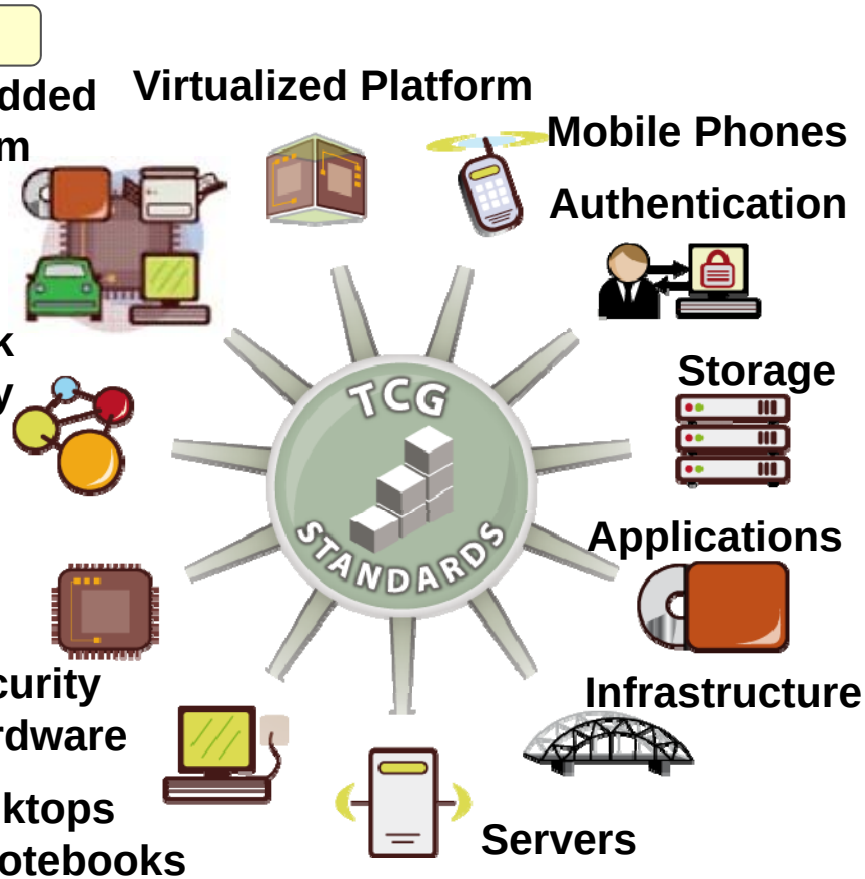
  http://www.trustedcomputinggroup.org/, http://www.trustedcomputinggroup.org/jp (日本支部)

- 2003年発足のNPO
  - HP, IBM, Intel, MSが設立した団体(TCPA, 1999年)を改組
  - 理事11社(上記およびAMD, Cisco, Fujitsu, Juniper, Infineon, Lenovo, Wave)

新加盟:トヨタ(3月)、Cisco(5月)

- 世界115社加盟
  - 多数国家機関(日,米,英,独,仏,中,印,加)多数の大学がリエゾンとして参画
  - 米国/EUの政府調達要件盛込み済(1/'06~)、日本は検討中

相手状況把握、完遂確認: HW信頼基点
証拠(ログ)保存(免責): 第三者検証可能



# OPAL HDD

FUJITSU

## TCG公式公開サイト内ストレージ関連

http://www.trustedcomputinggroup.org/developers/storage

## TCG日本支部第二回公開ワークショップ(2010.11.4)

「安全なモバイルコンピューティングを実現 - ディスク暗号化標準技術（TCG/OPAL）」

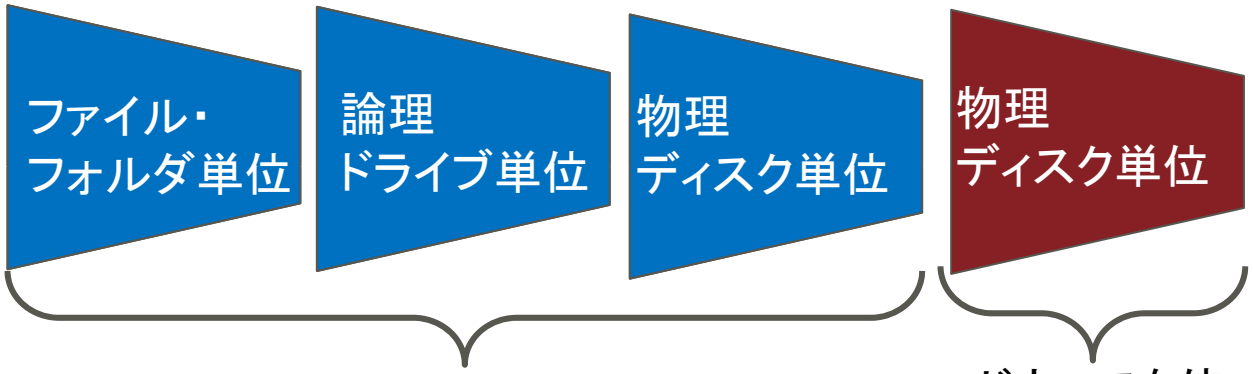
http://www.trustedcomputinggroup.org/jp/jrfworkshop/pastworkshop2

# HDD暗号化

FUJITSU

- モバイルコンピューティングの普及 (1990～)
  - ネットワークの発達により、電子的なインフラが発達し、さまざまな情報がノートパソコン上に蓄積されるように。

- 盗難・紛失、廃棄PCからのデータ漏えい (2000～)
  - 盗難・紛失、廃棄されたPCから、そのPCに蓄積されたデータが漏えいする事例が多数発生し、社会的問題に。
  - ノートパソコンのセキュリティ、とりわけHDD単体でのセキュリティ強化が求められ、さまざまな暗号化手法が導入され始めた。

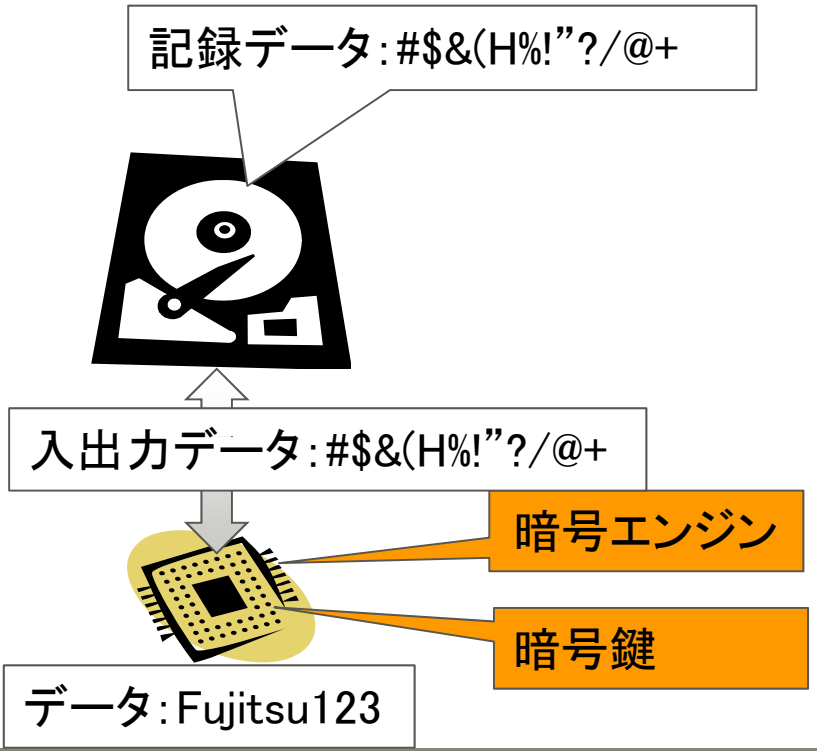


# 暗号化手法

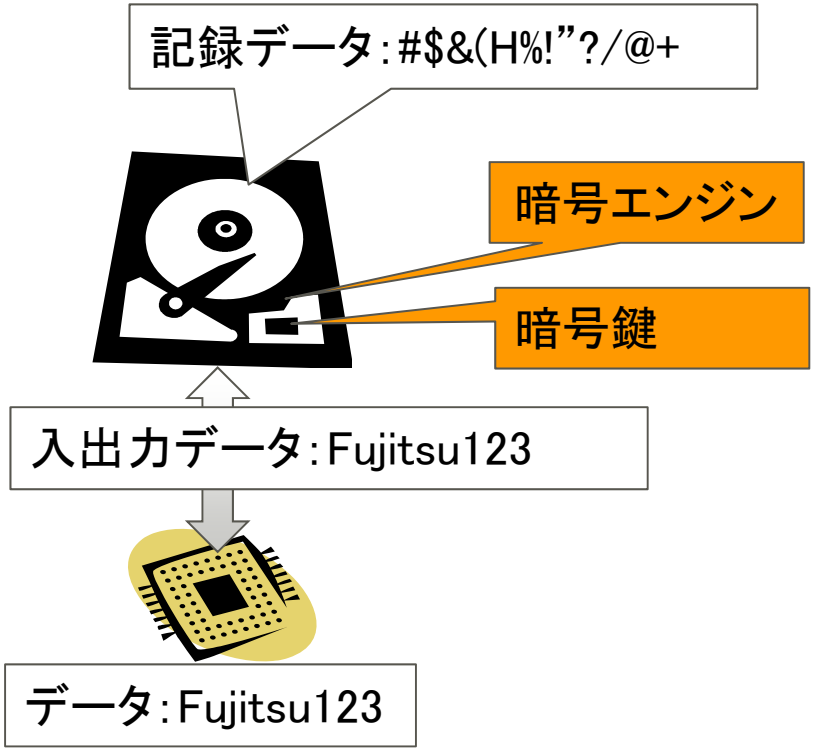
FUJITSU

- 大きく分けて、2つの方式。データの暗号処理/暗号鍵管理をソフトウェアが担うのか、ハードウェアが担うのかで異なる。
- 暗号鍵を瞬時に書き換え、データ無効化という共通の特徴

## [ソフトウェア方式]

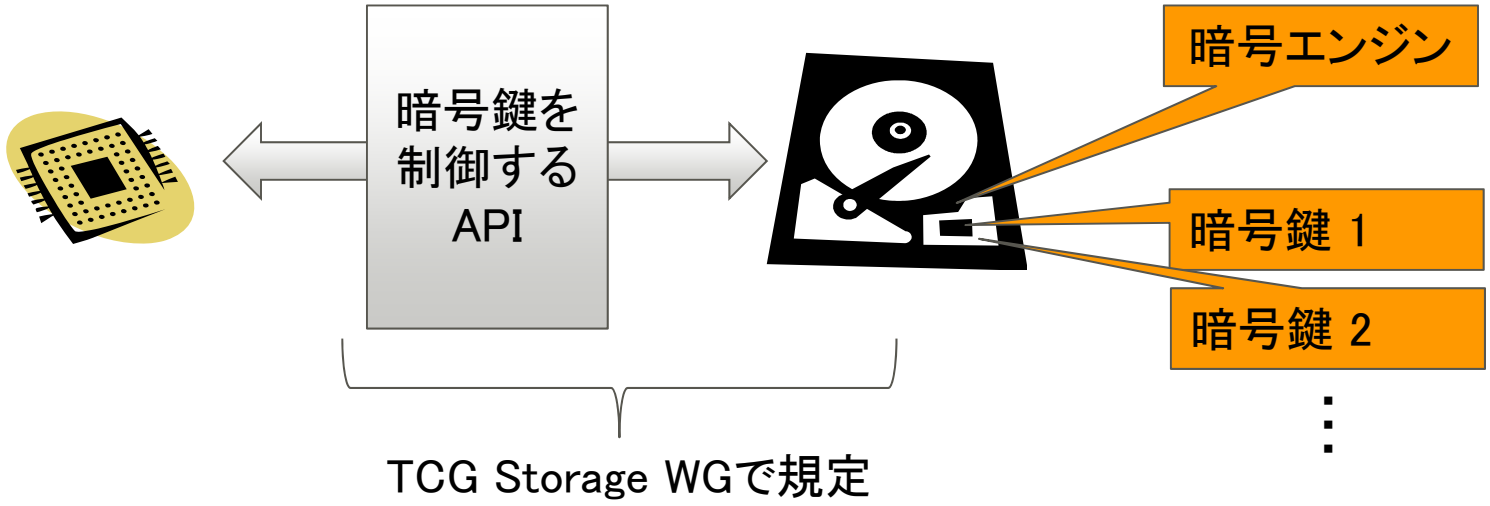



## [ハードウェア方式]



# Opal HDDとは

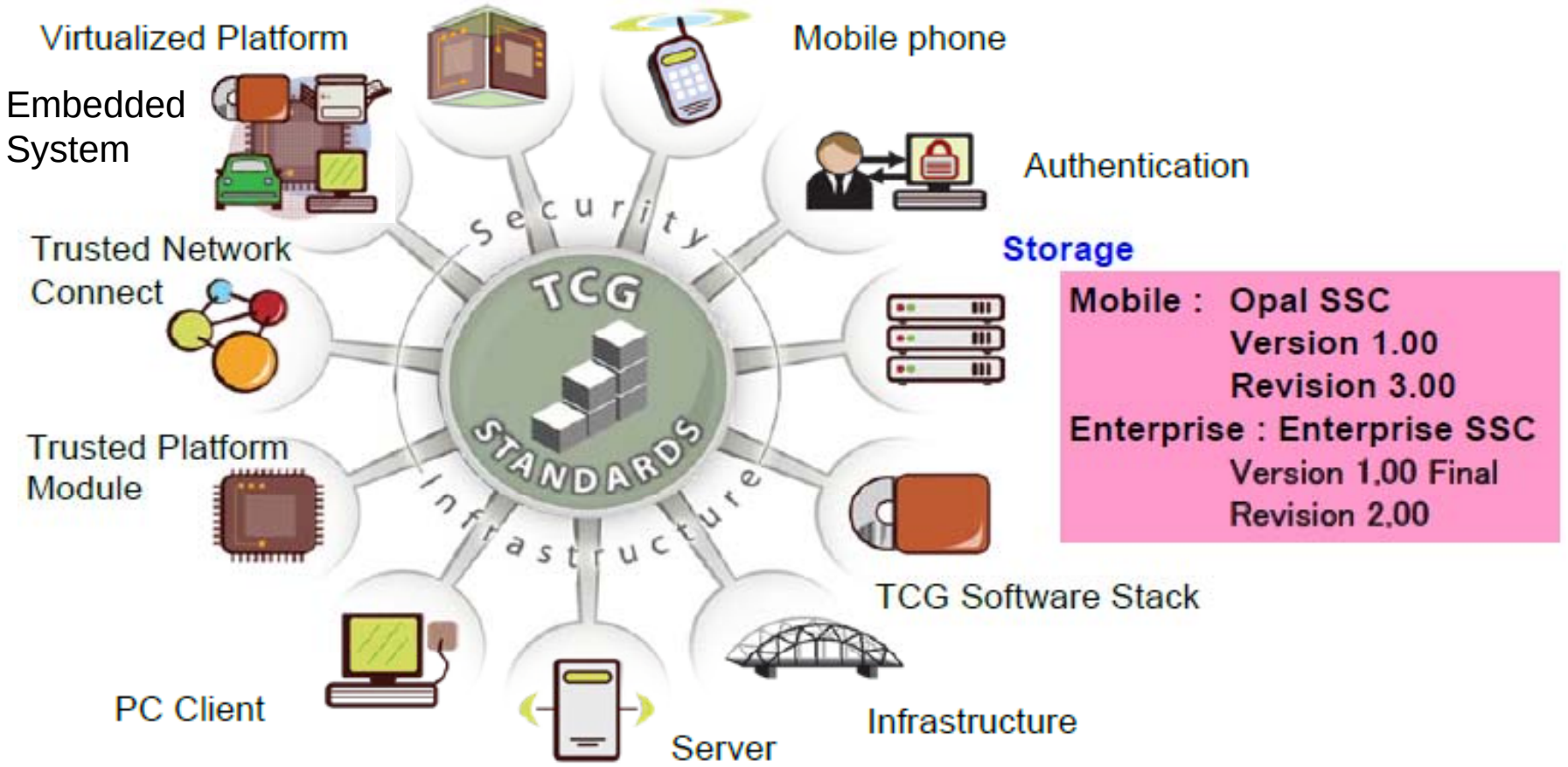
- ハードウェア方式をベースに、ソフトウェア方式のメリット(暗号鍵の外部制御、データ単位での暗号)を取り込んだのがOpal HDD
- 特徴
  - 暗号鍵の外部制御
    - 暗号鍵をwrappingするWrapping keyの生成、有効、書き換えをするAPIが用意
  - データ単位での暗号
    - 複数の暗号鍵をもち、その暗号範囲はLBA(Logical Block Address)を用いて指定
  - 消去に関する規定



# TCGの中での位置づけ

FUJITSU

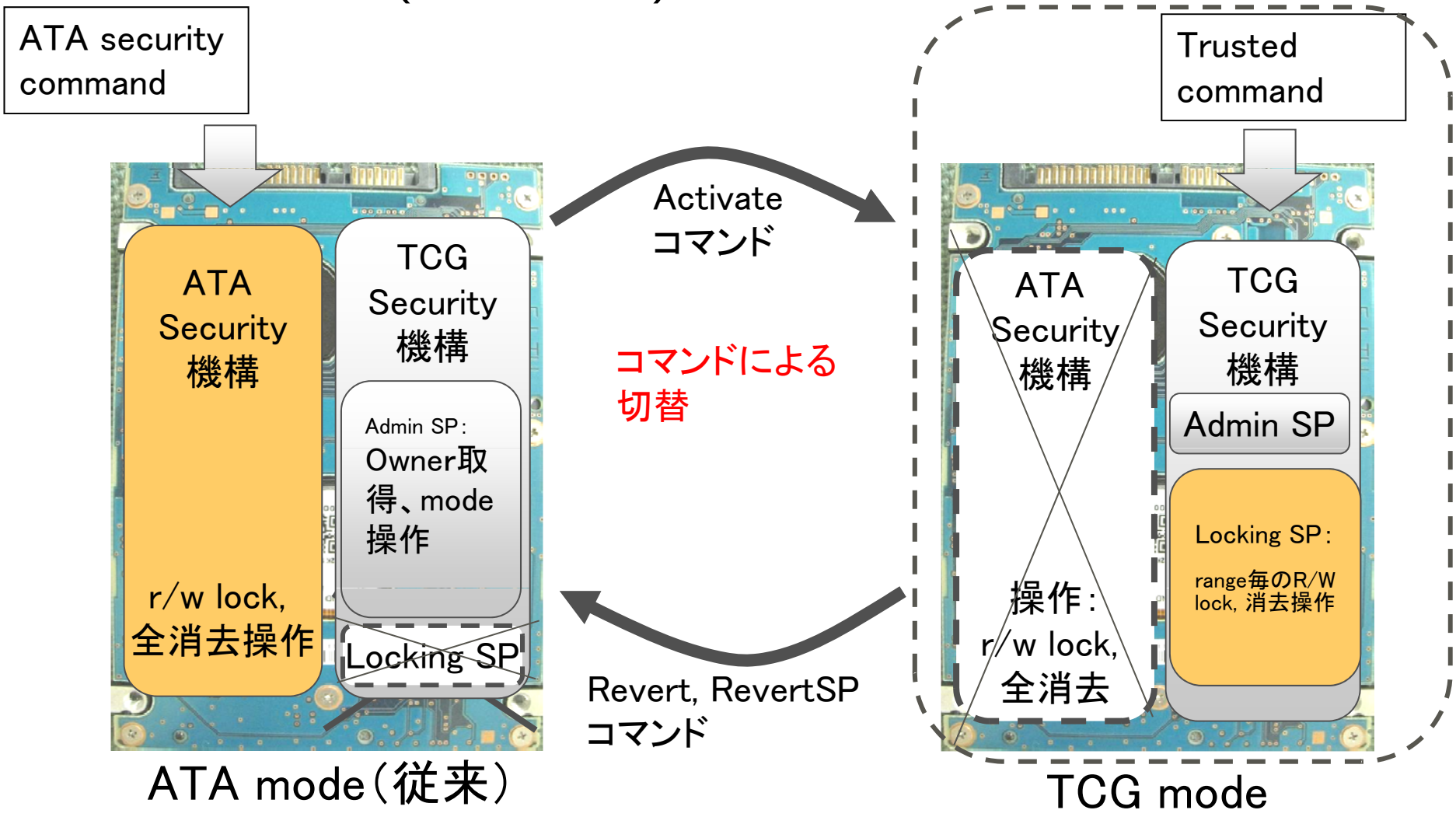
- Opal HDDは、TCG Storage WGで仕様策定
- 仕様は、
  - Enterprise/Opal　共通仕様をまとめたCORE仕様、用途ごとにCORE仕様をベースにまとめたOpal SSC /Enterprise SSCがある。



# Opal HDDの基本動作(その1)

FUJITSU

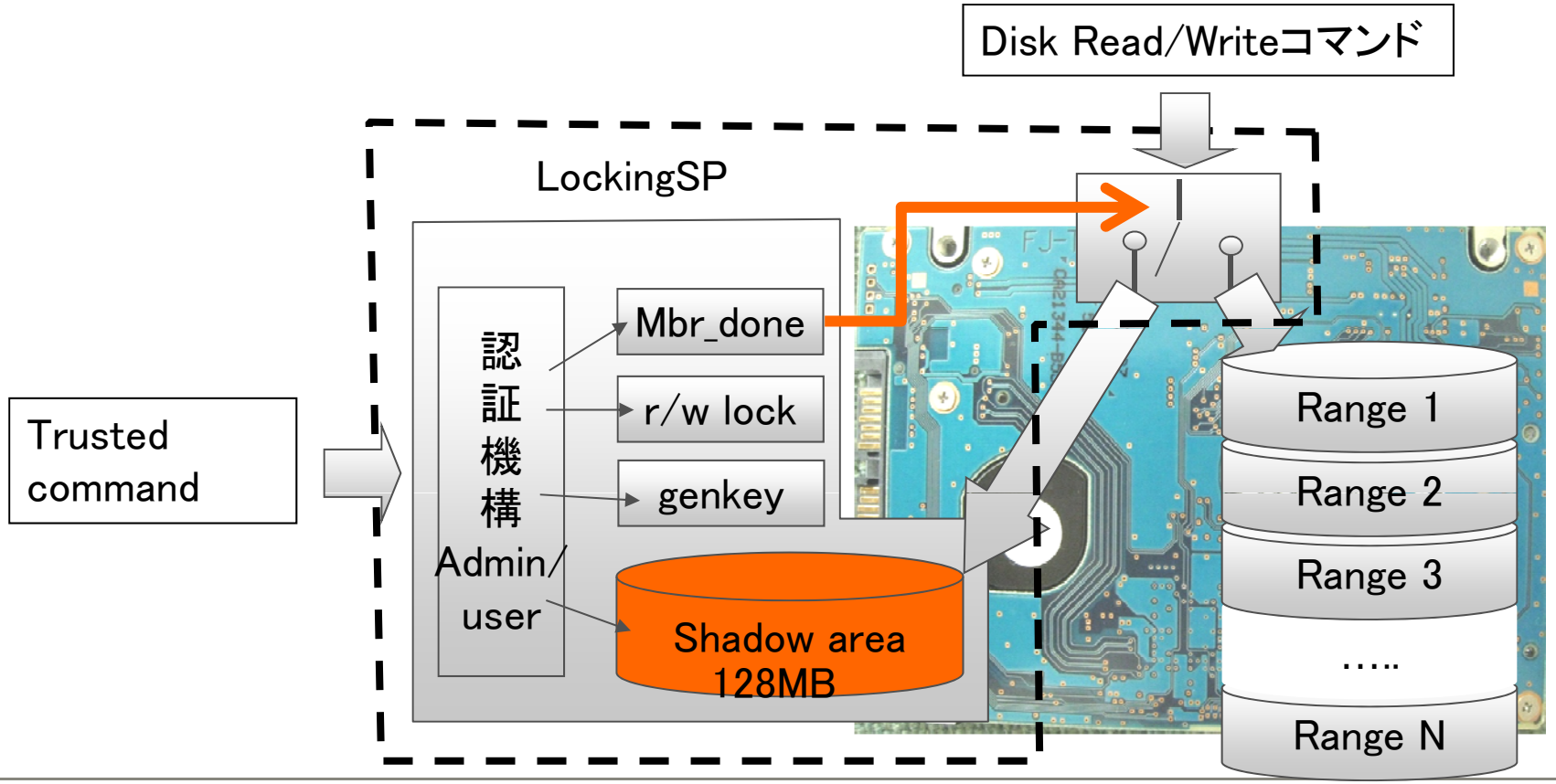
- 従来のハードウェア方式での動作（下位互換性）と、Opal 仕様で規定された動作(TCG mode)を兼ね備えている。



# Opal HDDの基本動作(その2)

FUJITSU

- TCG modeにおける動作
  - HDD内部に、複数ユーザ(ex. Admin1～4, user1～8) アカウントをもち、そのアカウントによるアクセス制御が行われる。
  - HDD領域のLock/Unlockは、上記アカウントによって操作される。
  - OSへ変更を加えることなく、Pre-OS認証が追加できる「Shadow MBR機能」

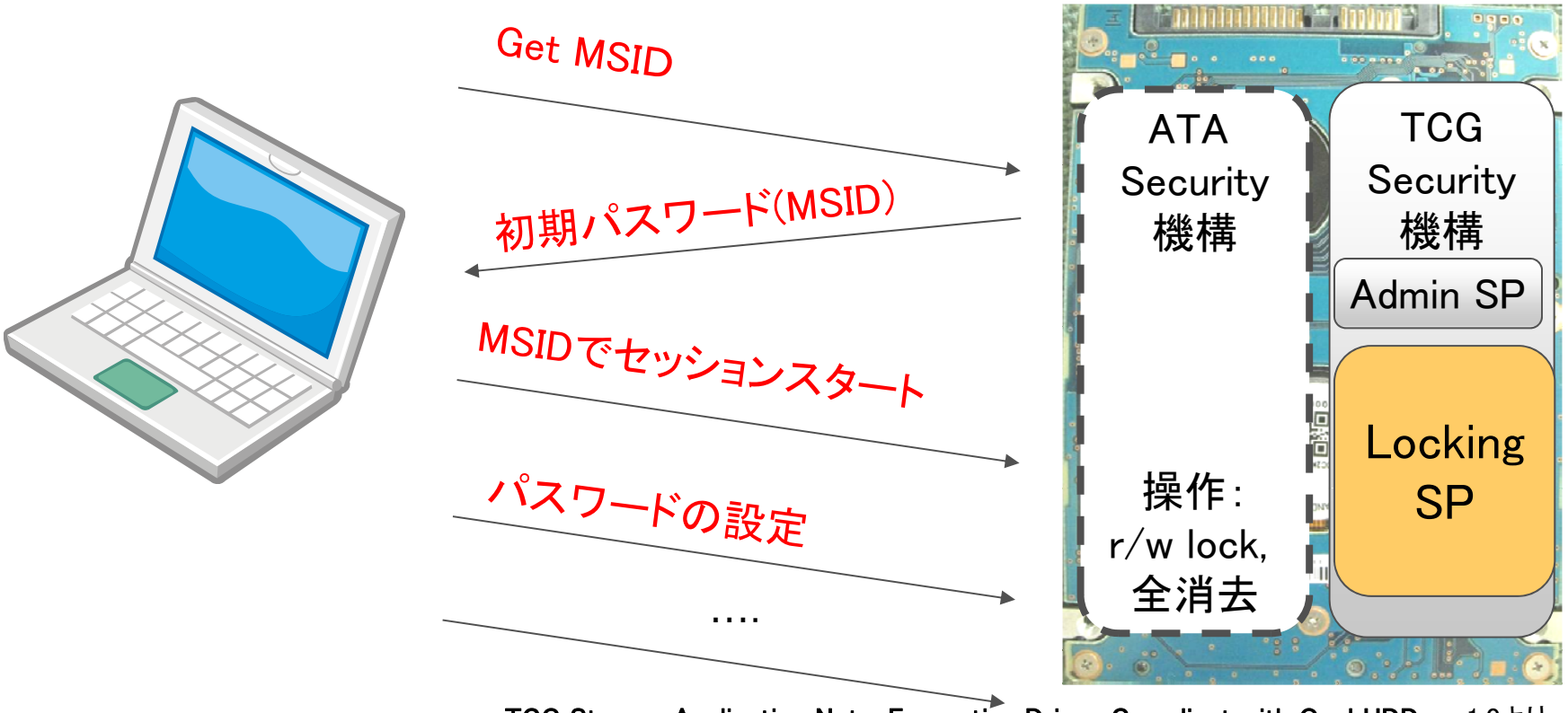


# Opal HDD の設定(その1)

FUJITSU

## Opal HDDの初期設定

1）アカウントの設定。Opal HDDの初期パスワードを読み出し、その初期パスワードを用いて、Adminアカウントの設定。




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

2）パスワードが設定されると、MSIDアカウントは無効化され、初期化が完了。

# Opal HDD の設定(その2)

FUJITSU

- Adminアカウントを用いて、Locking SP の中にある、ACL Tableを“ソリューション”にあわせて編集。

1) Adminパスワードを用いて、各ユーザのPINを設定

【Admin SP】

| UID | Name | CommonName | PIN | CharSet | TryLimit | Tries | Persistence |
|---|---|---|---|---|---|---|---|
| 00 00 00 0B 00 01 00 01 | "C_PIN_Admin1" | | SID or MSID[1] | Null | 0 | 0 | FALSE |
| 00 00 00 0B 00 01 00 00 (+XX XX) (O) | "C_PIN_AdminXXXX" | | "" | Null | 0 | 0 | FALSE |
| 00 00 00 0B 00 03 00 01 | "C_PIN_User1" | | "" | Null | 0 | 0 | FALSE |
| 00 00 00 0B 00 03 00 00 (+MM MM) (O) | "C_PIN_UserMMMM" | | "" | Null | 0 | 0 | FALSE |

2) ACL Tableの中のBooleanExprを編集。

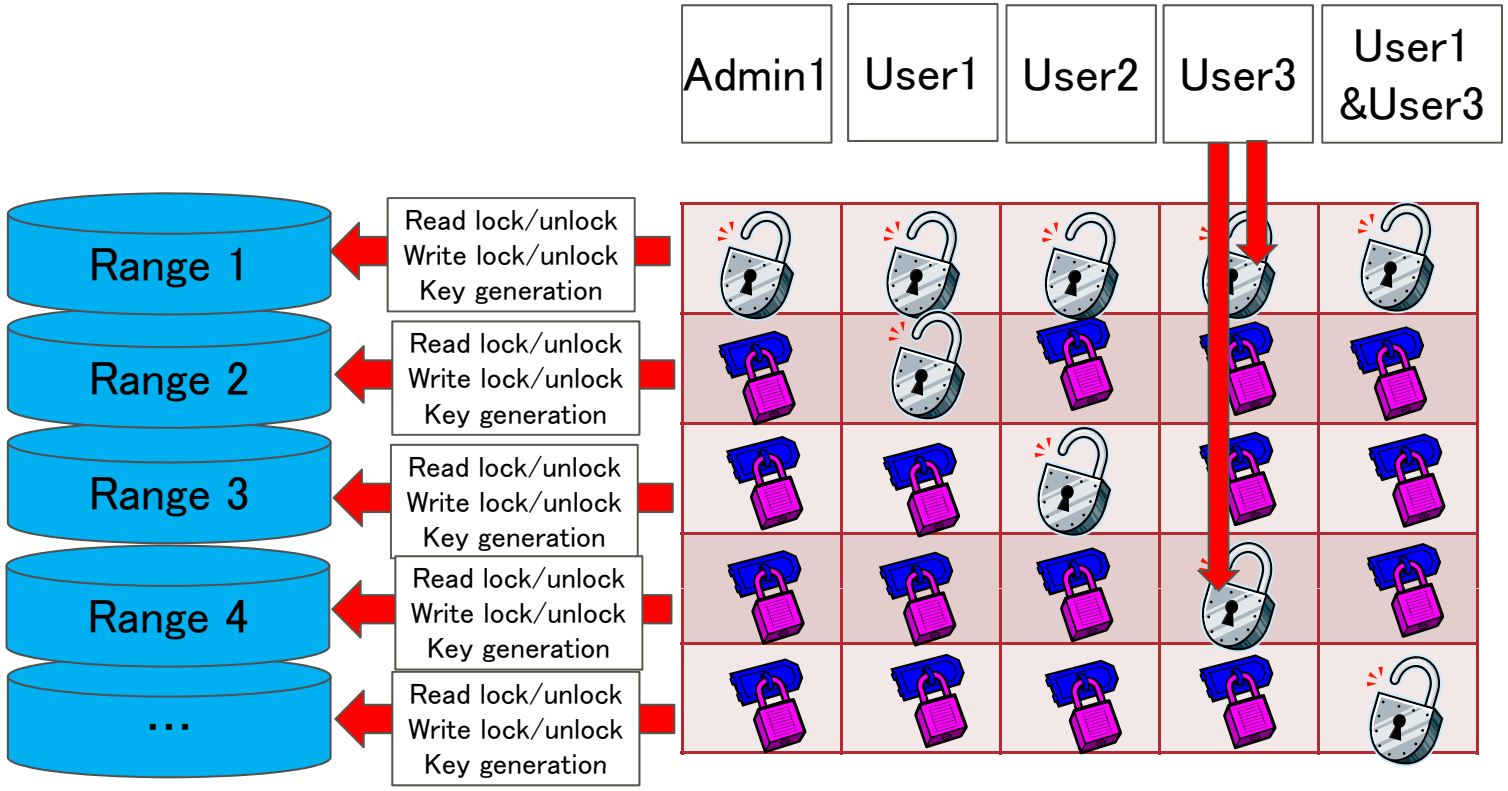
【Locking SP】

| UID | Name | CommonName | BooleanExpr | Columns |
|---|---|---|---|---|
| 00 00 00 08 00 03 E8 00 | "ACE_Locking_GlobalRange_Set_WrLocked" | | Admins | WriteLocked |
| 00 00 00 08 00 03 E8 01 | "ACE_Locking_Range1_Set_WrLocked" | | Admins | WriteLocked |
| 00 00 00 08 00 03 E8 00 (+NNNN) | "ACE_Locking_RangeNNNN_Set_WrLocked" | | Admins | WriteLocked |

# Opal HDD の設定(その3)

FUJITSU

- その結果、Opal HDDは下記のようなACL Table を保持。
  - 下記例では、User3がアクセス可能なのは、raneg1と、Range 4のみ



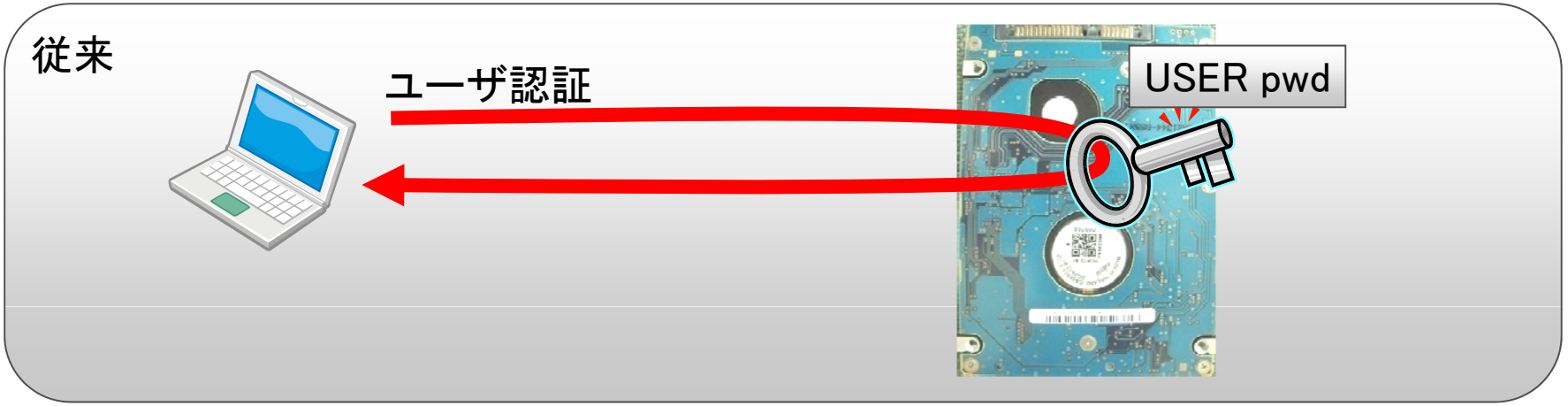
# ソリューション例

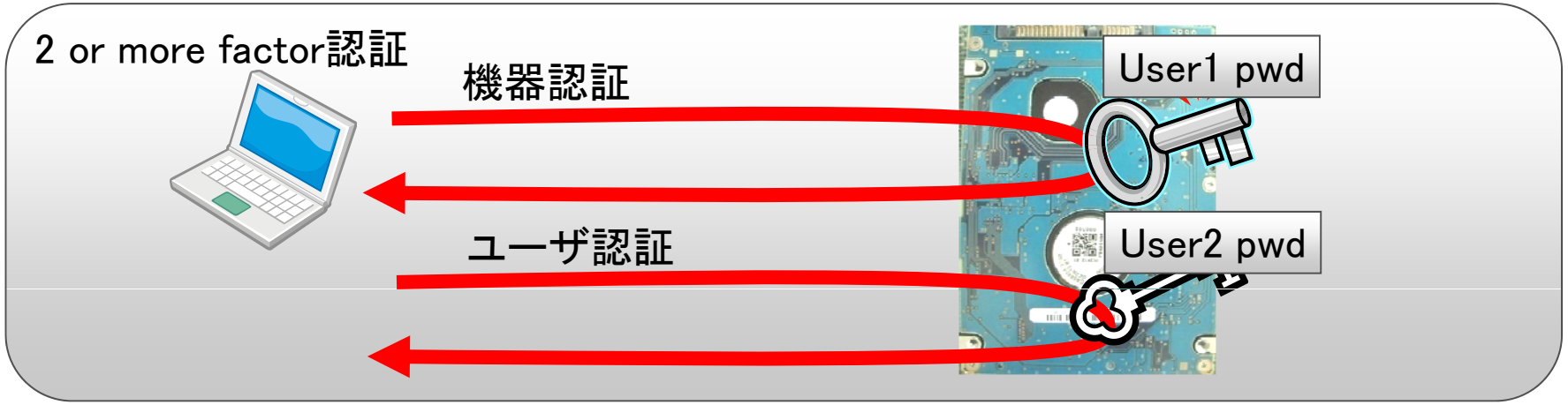
FUJITSU

# 例1：HDDの認証強化

FUJITSU

- Opal HDDが複数アカウント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。



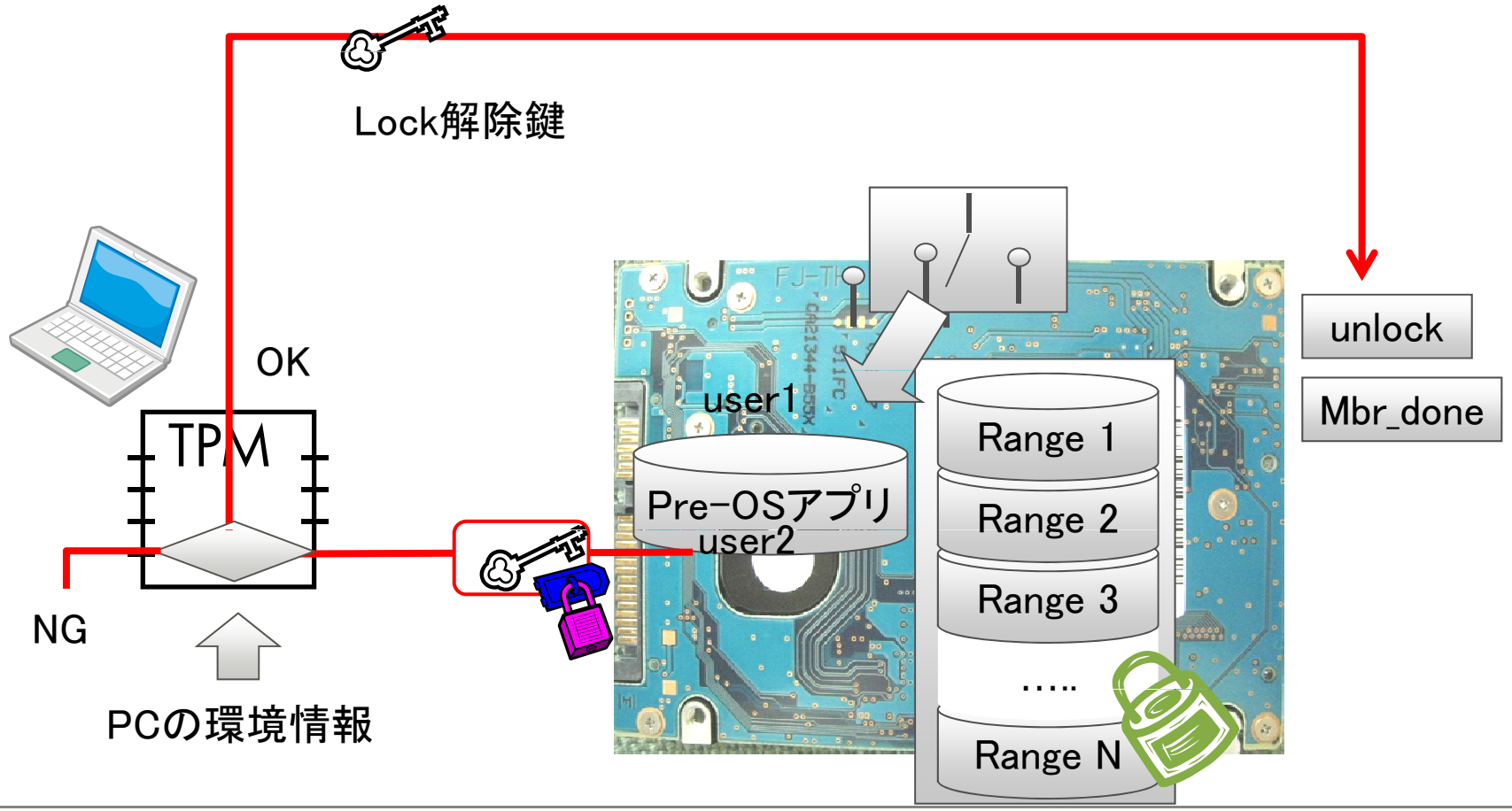



# 例1：HDDの認証強化（つづき）

FUJITSU

## ■TPMとの併用

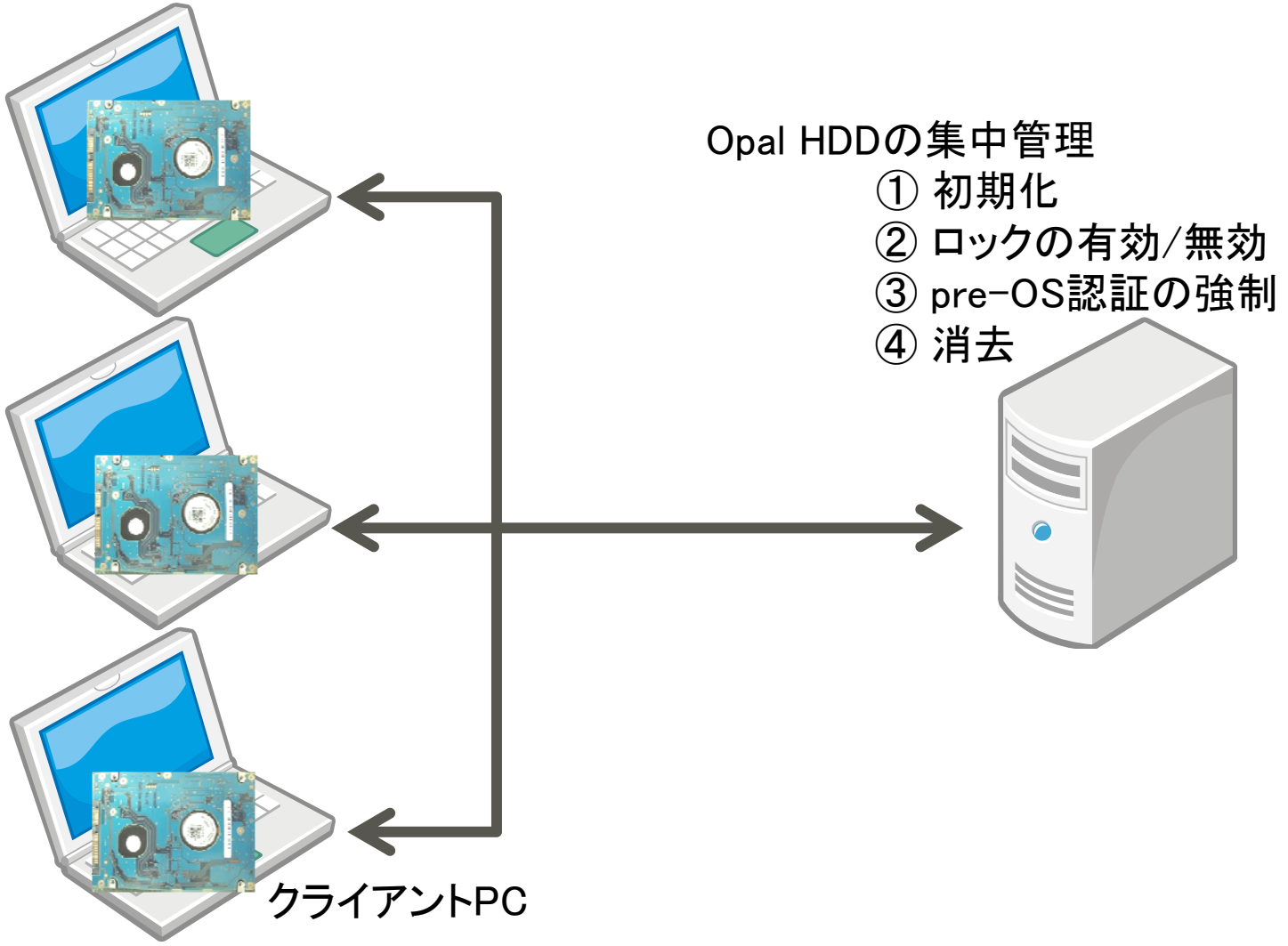
### ■HDDのlock解除鍵をTPMでwrappingして保護。TPMでの認証がOKなら、Lock解除鍵でHDDが使用可能に。



# 例2：Opal HDDの集中管理

FUJITSU

■Opal HDDの、初期化、ロック有効・無効などの集中管理



# 欧米における個人情報扱い/考え方

FUJITSU

# 松本世話役様からのお題

FUJITSU

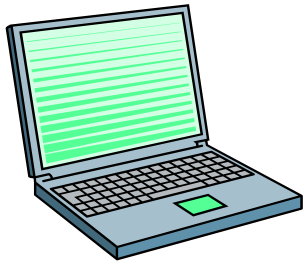
「米国および欧州における個人情報の暗号化に係る制度的な動向」

- これにお答えしようと講演内容を検討…
  しかし、到底、私の手に負えるものではなく…
  理由は様々ですが、後で述べますように、日々刻々変化し、しかも、逆戻りも日常茶飯事…
- そこで、私の得意分野であるTCGの中での話題に閉じて、お話しさせて頂こうと考えました

# TPM*のしくみ： HW信頼基点

FUJITSU

*: Trusted Platform Module, ISO化済み



- ✓BIOS
- ✓OS
- ✓Drivers
- ✓Anti-Virus SW
- ✓CPU/HDD
- ✓周辺機器
- ✓設定条件

製品

TPM

保護領域

チップが搭載されている
システム環境情報

構成情報

システム環境情報に
チップ内で署名して送出

認証鍵などを生成、格納

認証ID鍵

機密情報格納

ストレージ

機密情報暗号/復号

暗号化処理

改ざんチェック

大量の機密情報を保管する場合、
その情報を暗号化してPC内に
保存し、その鍵をチップ内の鍵で
暗号化して保存

2003年TPM仕様化完了、2004年から搭載PC出荷開始。
この際、個人情報保護の観点等から、独政府等の強い要求でTPMは出荷時オフとする事となった

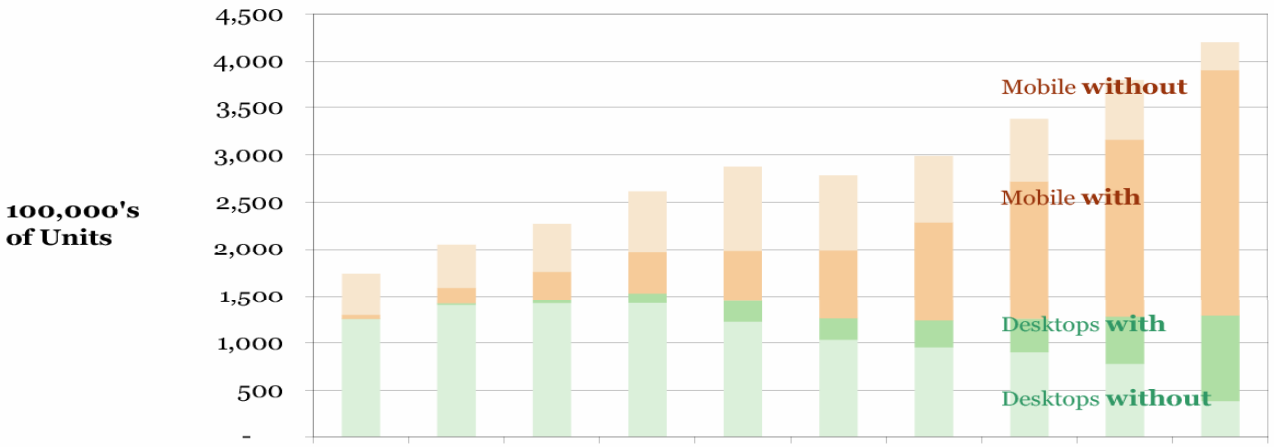
# TCG実績/予想：TPMのPCへの組込/利用状況

FUJITSU

- 2010年ノートPC 6割、デスクトップ3割（TPM総出荷数 約4億個）、2013年にはそれぞれ9割、7割にTPMが搭載されて出荷見込み

**PC Desktop and Mobile Shipments with and without TPM's from 2004 through 2013** (000,000 omitted)

IDC報告書(2009年9月)




| | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|---|---|---|---|---|---|
| Mobile without TPM | 444 | 456 | 511 | 653 | 886 | 793 | 700 | 659 | 628 | 291 |
| Mobile with TPM | 46 | 176 | 295 | 427 | 538 | 732 | 1,050 | 1,467 | 1,885 | 2,619 |
| Desktops with TPM | 3 | 16 | 43 | 113 | 228 | 226 | 284 | 351 | 497 | 902 |
| Desktops without TPM | 1,248 | 1,401 | 1,420 | 1,423 | 1,221 | 1,032 | 952 | 903 | 778 | 386 |

独政府等の要求でTPMは出荷時オフ、それ故、低稼働率。2011/6、opt-outとtransparency確保を条件に出荷時オン承認、2012年稼動率大幅アップ!

Windows8 TPM回り一括サポート発表

Windows Vista以降、BitLockerなどに標準利用⇒TPMで暗号化キーを安全に管理
Chrome OSはTPM必須で起動、ブートパス認証等を行う

携帯電話スマホでTPM必須製品計画進展中

# 個人情報扱い/考え方の将来像(小谷私見)

FUJITSU

TPM出荷時オンを勝ち取るための、5年以上に渡る各国政府機関との交渉から得た教訓

- 暗号鍵の強度は、その時点での合理的最高レベル、暗号鍵保管はソフト的にアクセス困難なハード内に。
- その上で、更に:
  システム内で何が行われているのか(個人情報がどのように扱われているのか)を知る方法を提供、Optout保証(自らの発意で、自分の情報を扱わせないよう変更可能)。

✓ *TCGは、これらの要求に答える事が可能な技術の一つ*

# ありがとうございました。ご質問対応とお願いを!

FUJITSU

個人情報保護は、当然ながら最重要課題の一つです。但し、際限無く費用、手間を掛けても100%保護出来る保証が無いのも事実です。これは悪意を持つ者の根絶が不可能で有る事から明白です。

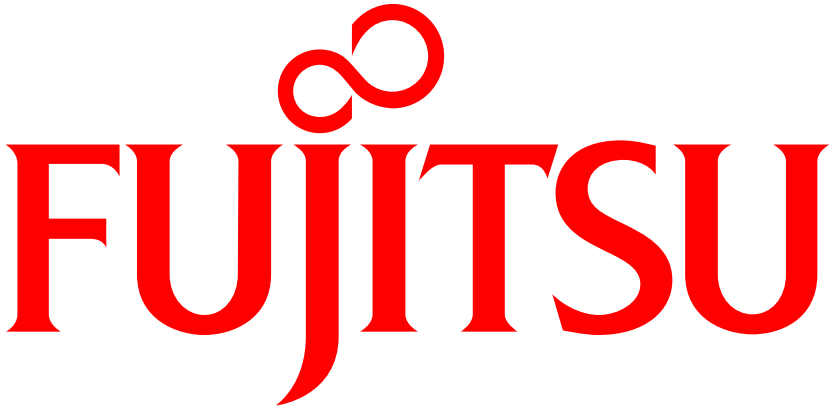
情報を扱う人口、機器の数量は著しく増大します。もはや後戻りは不可能です。

この事実、方向性を冷静に見据え、合理的な技術、費用で多くの人々が安心安全に暮らして行ける世界を創出しましょう。そのために有効なものの一つが、国際標準規格群を策定、公開しているTCGだと確信します。ハードウェア信頼基点/第三者検証性保証/証拠性保持が肝です。

日本はTCGをうまく利用する事で世界に貢献すると共に、その存在感を強く打ち出して行ける可能性が大きいと考えます。ぜひ、一緒に進みましょう！

以上、よろしくお願いします。

富士通(株)
インテリジェントサービス本部
戦略企画統括部
シニアディレクタ
TCG常任理事
小谷誠剛
skotani@jp.fujitsu.com




shaping tomorrow with you