

# TOSHIBA

Leading Innovation >>>

## TCG-JRF セミナー 講演資料 「HDD暗号のメリット、Opal SSC (Security Subsystem Class) の特徴と仕様の概要」



Copyright 2010, Toshiba Corporation.

株式会社 東芝  
ストレージプロダクツ社  
HDD事業部

Copyright 2009 , TOSHIBA CORPORATION.



東芝グループは、持続可能な  
地球の未来に貢献します。

Nov. 4. 2010

- 暗号化機能搭載HDDとは
- パフォーマンス
- データ無効化機能
- TCG と Opal HDD
- ソフトウェアサポートについて
- 安全性と互換性

# 暗号化機能搭載HDDとは?

記録データ : #\$(H%!"?!@+

暗号エンジン

暗号鍵

入出力データ : Toshiba123

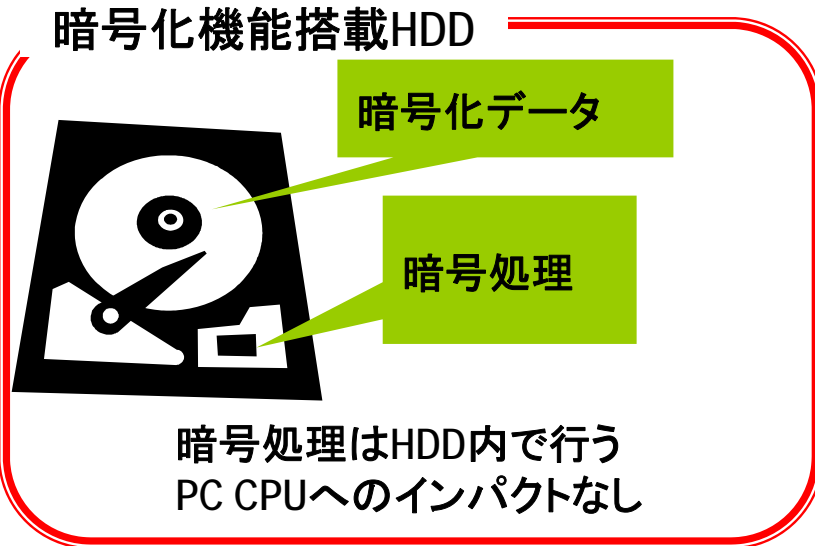
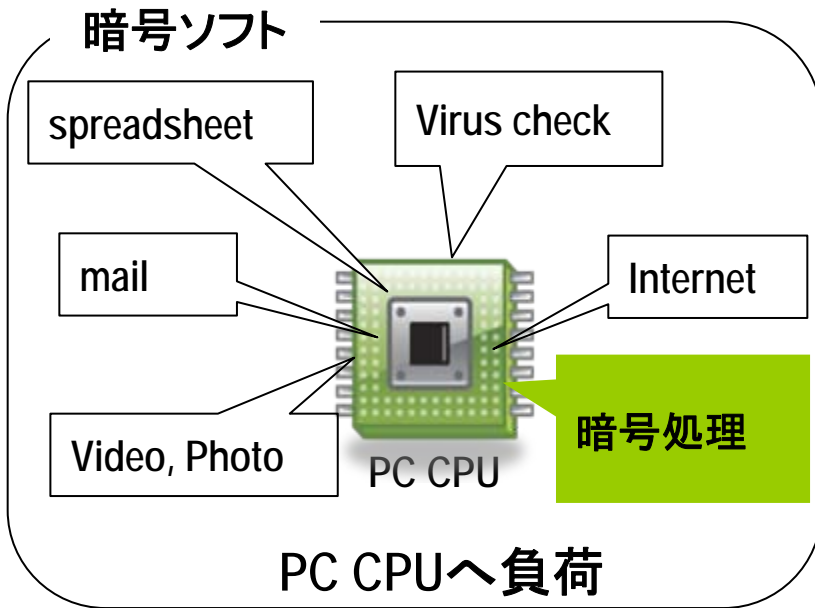
起動時にパスワード



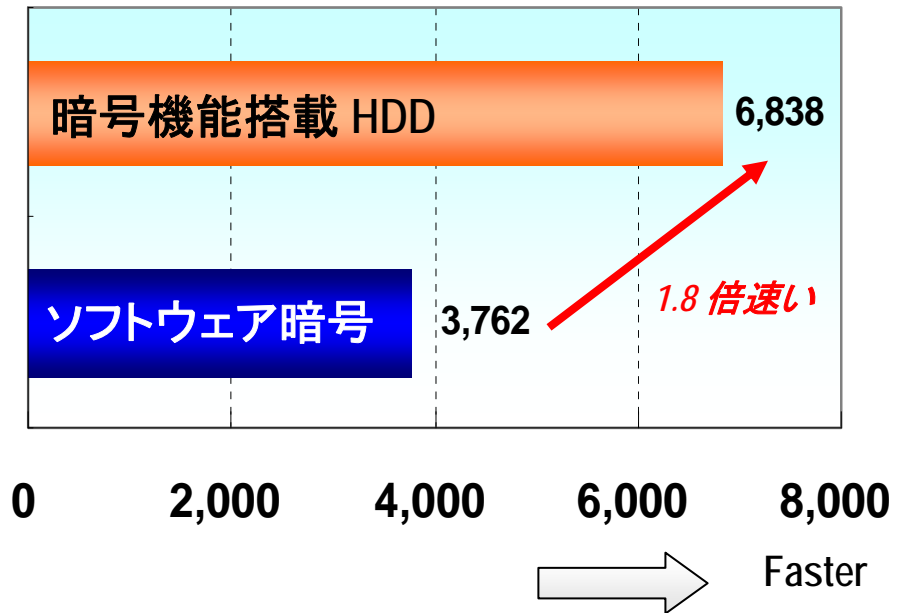
## ハードウェア暗号 盗難・紛失時のデータ漏洩防止

- インストール時の膨大な暗号処理が不要（ソフトウェア暗号の場合必要）
- 暗号処理によるパフォーマンスインパクトなし  
PC CPUへの負荷なし
- データ無効化機能
- 強固なセキュリティ  
分解解析にも耐える（媒体上のデータは暗号化されている）  
暗号鍵はHDD内部で管理され、PCメモリ上には展開しない
- プラットフォーム依存なし  
OS依存なし
- 運用へのインパクトなし  
起動時のパスワード

# パフォーマンス ソフトウェア vs. 暗号化機能搭載HDD



PCMark05 Performance Score (\*)



- HDD score test で1.8倍速い (\*)
- ウィルススキャン時には5.1 倍の速度差

# データ無効化機能

## 上書き消去ソフト

残留磁気の消去に複数回 消去が必要

トラック

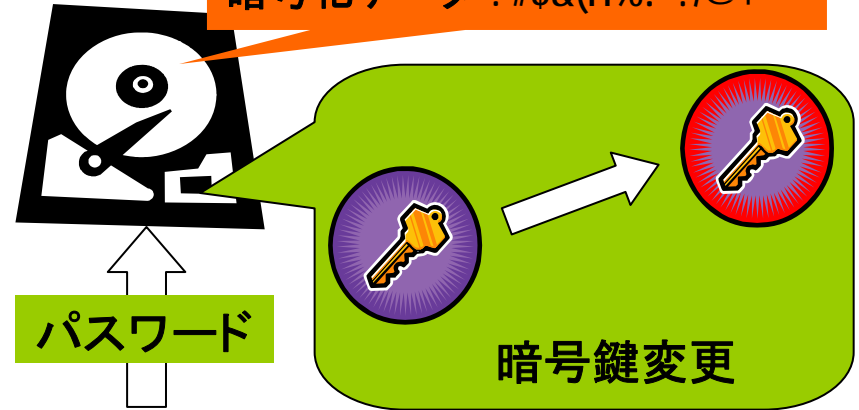
CONFIDENTIAL

消去パス

- 時間とコスト
- 320GB HDD (6億 2500万セクタ)
- 5時間 (3回消去)

## 暗号機能搭載HDD

暗号化データ : #\$(H%!"?!/@+



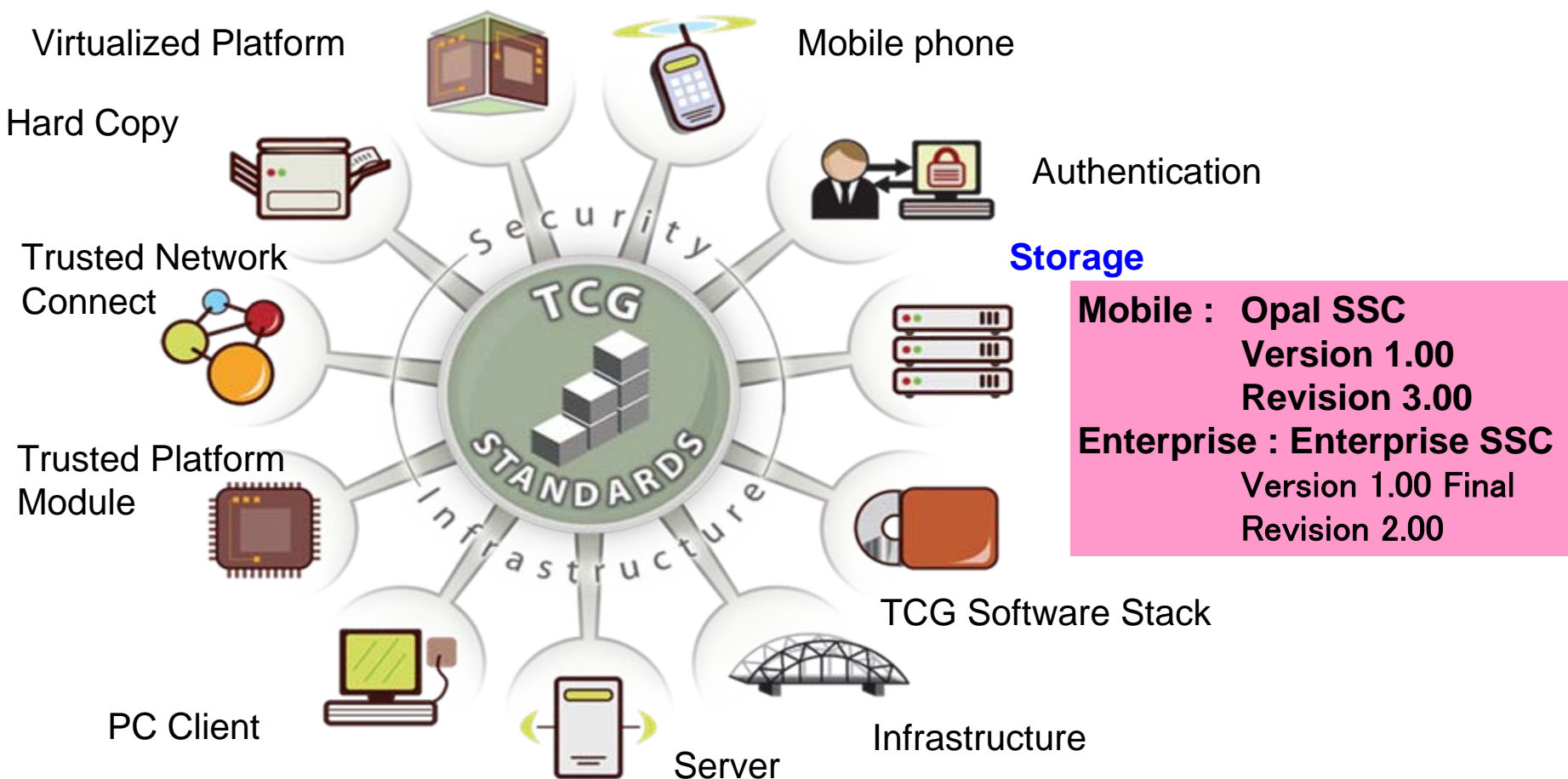
- 鍵変更後は元データの復号は不可能
- 瞬間データ無効化

PC廃棄・リサイクル時のTCO 削減に貢献

# TCGの中の位置づけ



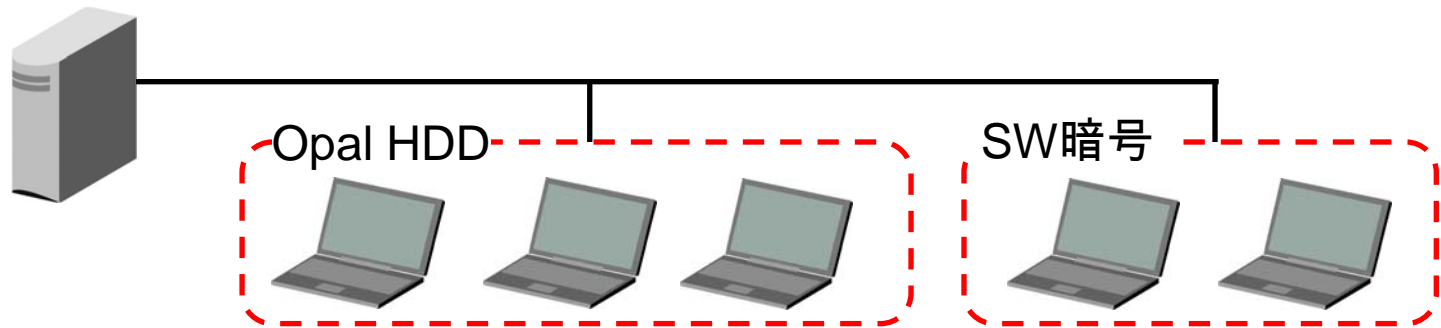
<http://www.trustedcomputinggroup.org/>



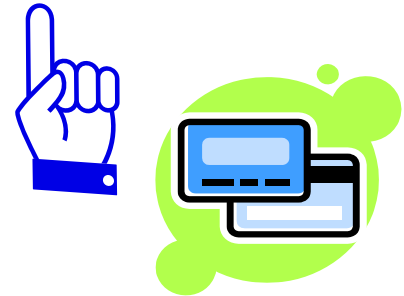
# ソフトウェアサポート

## 管理ソフト

- 一括管理 (インストールおよび、権限 - 機能管理)
  - 複数の暗号環境をシームレスに管理 (Opal HDD や ソフトウェア暗号)



- PBA (Pre Boot Authentication) 等の付加機能提供
  - 生体認証等、高度な認証方式のサポート



## ISV (Independent Software Vendor)

- Wave systems
- WinMagic
- その他

# 安全性、互換性

	ITセキュリティ評価 及び認証制度	暗号モジュール試験及び認証制度	
制度	JISEC (Japan Information Security Evaluation and Certification Scheme)	CMVP (Cryptographic Module Validation Program)	JCMVP (Japan Cryptographic Module Validation Program)
有効 範囲	日本、加盟国間で相互に認 証の効力あり	北米(米・加)	日本
規格	ISO/IEC15408 (CC:コモンク ライテリア)	FIPS140-2(米国連邦 標準規格)	JIS X19790
運用 状況	地域別の制度を1990年代に 国際標準化、日本は2003年 に加盟	1995年から運用	2007年から運用

## 暗号方式実装の安全性

NIST CAVP (Cryptographic Algorithm Verification Program), FIPS 197

## 互換性

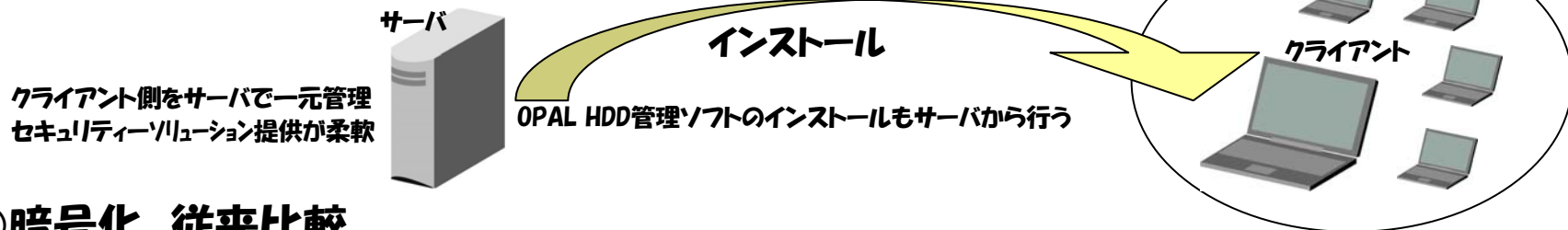
TCG Conformance subgroup においてコンプライアンステストを検討中。

# Opal HDD デモ (参考出展 協力 WinMagic社)

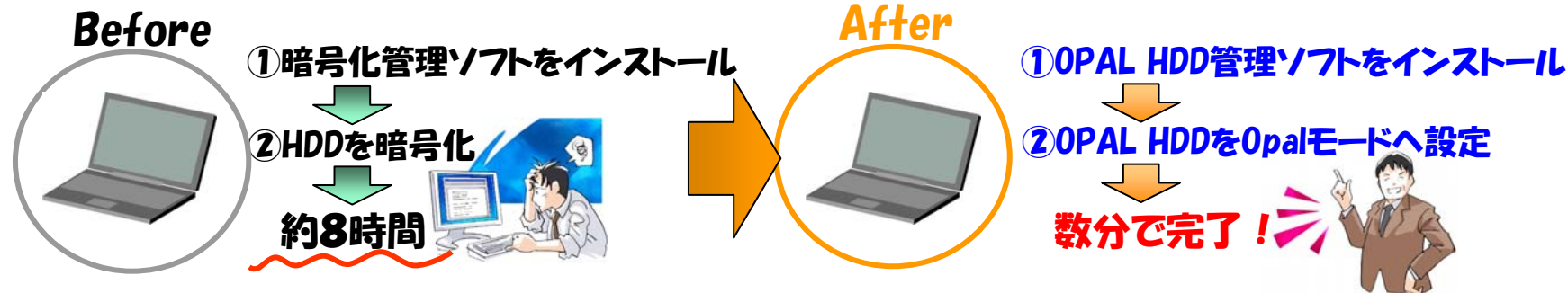
従来 暗号化に掛かっていた時間を大幅に短縮!

セキュリティ運用コスト削減、スピードアップ、システム柔軟性を向上

## ○サーバ&クライアントPC運用開始までの図 (セキュリティインテグレータの方々へ)



## ○暗号化 従来比較



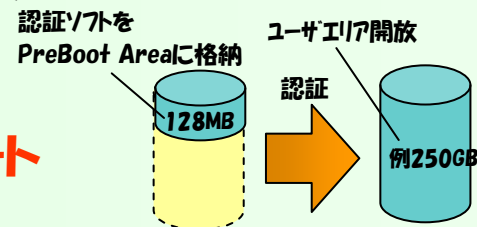
## ○PBA (Pre Boot Authentication) 機能により 高度な認証方式をサポート

Before

HDDパスワードロックのみ.....

After

生体認証、スマートカード等  
高度な認証方式をサポート



セットアップ : OPAL HDD管理ソフトでOPAL機能を有効化(数分)+PBAの書込み(数分)で運用準備完了。

廃棄・再利用時: データ無効化は暗号鍵を削除するだけで一瞬の内に完了。

# 効果 Opal HDD

運用負荷

	Opal HDD	SW encryption
初期設定	5分程度(HDD組み込み、管理ソフト設定)	数時間
設定解除(破棄・再利用)	一瞬	数時間
システムパフォーマンス	最大限	暗号復号処理オーバーヘッド
PBA領域の保護 (Pre Boot Authentication)	書き換え攻撃に対する 防御可能	書き換え攻撃に対する 防御不可能
ユーザ領域の保護(認証前)	書き換え攻撃に対する 防御可能	書き換え攻撃に対する 防御可能

セキュリティ強度

## メリット

- 暗号化機能搭載HDDは強力な情報漏えい防止ソリューションを提供します。
  - システムパフォーマンスの最大化
  - データ無効化機能
- Opal HDDは高度なセキュリティシステムの実現を可能にします。
  - PBA (Pre Boot Authentication)
  - 複数権限の設定
  - Rangeの設定
- 高いセキュリティレベルと運用負荷低減の両立を実現します。

## 普及に向けて

- 標準仕様 (Opal SSC)・コンプライアンステストの策定により、複数メーカーからの製品提供が可能となりました。
- ISVからの管理ソフト提供がスタート。

## Call to Action

- 情報漏えい防止ソリューションとしてOpal HDDをご検討ください。

**TOSHIBA**

**Leading Innovation >>>**