

The Lenovo logo is displayed in white lowercase letters on a dark blue background.

NEW WORLD. NEW THINKING.

Trusted Computing Group - Japan Regional Forum

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) ～

ノートブック PC におけるセキュリティ・ソリューション

～ その歴史と今後の展望 ～

Y. Miyaguchi

Storage Dev Eng, Notebook Development

Yamato R&D, Lenovo Japan

November 04, 2010

A solid orange horizontal bar is located at the bottom of the slide.

目次

1. ノートブック PC におけるセキュリティ面の要求
2. セキュリティ・ソリューションにおける歴史的考察
 - a) Full Disk Encryption (FDE) の適用による長所と課題
 - b) Trust Security の提案と問題点
 - c) Software Encryption の適用と課題
 - d) TCG Opal 採用における展望と期待
3. ノートブック PC における TCG Opal の適用範囲と課題
4. TCG Opal における発展性
 - a) サーバー・アプリケーション
 - b) その他のアプリケーション (組込型?)
5. HDD/SSD Device 開発の現状
6. TCG Opal における今後の課題

スピーカーの紹介

◆ 連絡先

レノボジャパン(株) ノートブック開発研究所

サブシステム技術 機構・ストレージ技術

宮口 康宏 Yasuhiro Miyaguchi

Address : 神奈川県大和市下鶴間 162-14

Phone : 046-408-3615 , email : ymiya@lenovo.com

◆ 略歴

- 日本アイ・ビー・エム(株) 野洲事業所 メインフレーム・生産技術開発
- ディ스플레이・テクノロジー(株) LCD 設備開発、セル技術
- 日本アイビーエム(株) 藤沢事業所 2.5” HDD 開発チーム
- (株)日立グローバルストレージテクノロジーズ 2.5” HDD 開発チーム
- (株)サムスン横浜研究所 ストレージチーム
- 日本シーゲイト(株) System Integration Engineering 部
- レノボジャパン(株) < 現職 >

ノートブック PC におけるセキュリティ面の要求 (1)

◆ ノートブック PC における要求

- ノートブック PC 固有の要求
 - ➔ 盗難に対する安全性

- モバイル環境に対するセキュリティ
 - ➔ 紛失、盗難に対する安全性
 - 外出、出張時の不測の事態に対する安全性

- ネットワーク接続におけるセキュリティ
 - ➔ 接続認証、侵入防止に対する安全性

- データに対するセキュリティ
 - ➔ 個人情報等データの安全、アクセス制御に対する安全性

ノートブック PC におけるセキュリティ面の要求 (2)

◆ 社会的、企業的な要求

- 個人情報の安全な管理
 - ➔ 個人情報の管理と漏洩防止
万一の際に備えた仕組み

- 社会的、企業的信頼
 - ➔ 軍需、警備、コンサルティング、金融、保険、
認可要件とペナルティ

- 企業におけるセキュリティ・システムの構築
 - ➔ 社員教育よりも、システムの整備 (特に US, EMEA)

- 情報公開と問題の共有化
 - ➔ 社会的問題の公開と、対策の実施

セキュリティ・ソリューションにおける歴史的考察

- (1) 旧来のセキュリティ管理手法
- (2) FDE (Full Disk Encryption) HDD/SSD の適用
- (3) Trust Security の提案
- (4) Software Encryption の提案
- (5) TCG Opal 採用における展望と期待

セキュリティ・ソリューションにおける歴史的考察 (1)

◆ 旧来のセキュリティ管理手法

- BIOS におけるログイン・パスワードの管理
- BIOS における HDD パスワードの管理

- セキュリティ面の課題
 - データそのものは Readable なまま、Encrypt 機能無し
 - パスワード・ハッキングに対する耐性の不足
 - ATA Bus におけるセキュリティ未適用
 - PC レベルのみの安全性

セキュリティ・ソリューションにおける歴史的考察 (2)

- ◆ FDE (Full Disk Encryption) HDD/SSD の適用と課題
 - HDD/SSD 内部における Self Encryption 機能
 - ➔ AES128 が主流での HDD/SSD 内部データのセキュリティ Encryption Key の管理 (+ BIOS/ストレージ パスワード)

 - HDD/SSD 内部データのセキュリティ
 - ➔ 盗難、紛失に対する安全性
 - 廃棄における容易性

 - セキュリティ面の課題
 - ハッキングに対する耐性の不足
 - ATA Bus におけるセキュリティ未適用
 - PC レベルのみの安全性

セキュリティ・ソリューションにおける歴史的考察 (3)

◆ Trust Security の提案

- Seagate Technology 独自のセキュリティ提案
 - ➔ Full Disk Encryption を基本
 - Wave systems, Secudo 2社の Software との共同開発

- 3 Phases Solution の提唱 (TCG Opal の原案)
 - ➔ I : Full Disk Encryption
 - II : ATA Bus を含めたセキュリティ
 - III : Partitioning/Multi Users 対応セキュリティ

- セキュリティ面の課題
 - ISV Software の未成熟と性急過ぎた提案
 - 1社供給による購買的制約 ➔ **Standard 化の必要性**

セキュリティ・ソリューションにおける歴史的考察 (4)

◆ Software Encryption の提案と課題

□ Security Application Software による Encryption

➔ パスワードのサーバー管理

PC へのログイン認証

ネットワーク・ログインの認証

□ HDD 内部データのフォーマット必要 *事前準備の時間的課題

□ セキュリティ面の課題

➢ ソフトウェアのみによるセキュリティ対応

➢ ハードウェアとの組合せ対策として、全ての問題を Software で吸収

➢ Seagate Technology のみ Trust Security での対応可

セキュリティ・ソリューションにおける歴史的考察 (5)

◆ TCG Opal 採用における展望と期待

- 世界レベルでの標準規格に即した共通ソリューション
- Storage Device と Application Software をキーにした総合的セキュリティ・ソリューション ~ 特に、Enterprise 環境での効果を期待
- Encryption HDD/SSD の採用
 - HDD/SSD 内部データの暗号化 と 紛失、盗難時のデータ保護
 - 廃棄時の安易性
- Security Application Software との Collaboration
 - ログイン認証の適用
 - ネットワーク認証の適用
 - セキュリティ・キー情報のネットワーク・サーバー管理

ノートブック PC における TCG Opal の適用と課題

◆ TCG Opal の適用

- 世界的標準規格
- ログイン認証とネットワーク認証
- ユーザー情報のサーバー管理
- HDD/SSD 内における Self Encryption によるデータの安全
- ATA Bus におけるセキュリティ化
- Software におけるパーソナル版とエンタープライズ版の提供

◆ TCG Opal の課題

- 現行の Standard では S3 機能使用時に Security Hole
→ Application Software により S4 に適用変更
- Reset に関する Issue の可能性残存
- HDD/SSD と Application Software の総合的機能検証
- 一部の機能はノートブック PC では未使用

セキュリティ・ソリューションにおける歴史的まとめ

効果 セキュリティ の進化	パスワード・ セキュリティ	データの 暗号化	インストー ルと準備	ATA バス の安全性	標準化	盗難紛失 廃棄管理	ログイン 認証	ネットワー ク認証
ATA パスワード	○	X	△	X	X	X	X	X
FDE HDD/SSD	○	◎	○	X	△	◎	X	X
Trust Security	○	◎	○	△	X	◎	○	○
Software Encryption	○	○	X	◎	△	○	◎	◎
TCG Opal	○	◎	○	◎	◎	◎	◎	◎

TCG Opal における発展性 (1)

◆ TCG Opal によるサーバー・システムへの適用

- TCG Opal 採用ノートブック PC との組合せによる高度なセキュリティ
- ログイン、ネットワーク認証による企業規模の管理
- Multi User による個別セキュリティの管理
- Storage Partition における User/Group 管理

◆ TCG Opal における課題

- エンタープライズ・サーバー環境における検証の不足
- システム・インテグレーション的ソリューション提案の不足
→ 今後の成長における発展的解消を期待

TCG Opal における発展性 (2)

◆ PC, サーバー以外への適用可能例の提言

- プリンター複合機
- ATM 等の金融端末
- 金融システム
- 保険システム
- 医療システム
- 地方自治向け個人情報システム

◆ TCG Opal における課題

- Application Software の 拡張性
- ソリューション提供分野の拡大

HDD/SSD Device 開発の現状 (1)

◆ TCG Standard Test の実践と完成

現在の進捗度

□ TCG Standard の Firmware への適用

△ → ○

□ TCG Standard Test の実施

△ → ○

□ Application Software の検証

△ ~ X

➢ インストールの検証

△ ~ X

➢ 認証の検証

△ ~ X

➢ Windows Boot の検証

△ ~ X

➢ サーバー環境の検証

X

➢ Multi Partition の検証

X

➢ Multi Users の検証

X

TCG Opal における今後の課題 (1)

1) TCG Standard における課題

- TCG Standard の改訂による S3 制約の解決
- Reset Issue の明確化と解決
- Standard における定義分野の発展的成長

2) HDD/SSD Supplier における課題

- TCG Standard に対する Firmware 検証
- Application Software との相互的な組合せ検証

3) Application Software における課題

- Application Software におけるニーズの明確化
- HDD/SSD Supplier との相互的な組合せ検証
- Software の Revision 管理の明確化

TCG Opal における今後の課題 (2)

4) PC Supplier における課題

- HDD/SSD Firmware Update の仕組み
- エンドユーザー・ニーズの取り込み
- ソリューションとしての提供

5) 社会的環境における課題

- 法人、企業におけるシステム導入の動機付け
- ペナルティ等の施策と社会的責任の奨励
- セキュリティ面の格付けへの反映

6) TCG JRF における課題

- **世界に誇れる、日本でのビジネス成功モデルの確立**

thank you grazie **merci** danke **grazias** 謝謝 СПАСИБО
gracias **obrigado** ありがとう **dank** takk **bedankt** dakujem

lenovo
NEW WORLD. NEW THINKING.