JEITA 社団法人　電子情報技術産業協会
Japan Electronics and Information Technology Industries Association

暗号化機能：必要性と優位性
テープストレージの活用

2009年9月

社団法人　電子情報技術産業協会
情報・産業社会システム部会
技術企画・標準委員会
テープストレージ専門委員会
（旧　磁気記録媒体標準化専門委員会）

テープストレージ専門委員会
Tape Storage Technical Committee

資料の目的

- テープストレージの啓蒙のひとつとして、テープドライブの持つ暗号化機能の必要性・有用性を理解していただくために作成した資料です
- 最新のテープテクノロジーをご理解いただき、長期的視点に立った皆さまの業務やシステムの改善や拡張の参考としていただければ幸いです

データの保管と機密性の要請

- 保管データの機密性 / 長期データ保管 / 迅速な参照性 / 罰則規定[1]

日本国内における例

- 個人情報保護法（第20条）[2]
- e-文書法[3] ⇒具体的文書及びそのデータ保管期限は251の関連法で定められている
- 会社法[4] ⇒「内部統制システム構築の義務化」（大会社）
- 金融商品取引法（日本版SOX法）[5] ⇒内部統制

アメリカ合衆国における例

- SOX法[6] ⇒データ保管期間7年：US公開企業・その他連結対象子会社
- SEC ルール 17a-4[7] ⇒データ保管期間6年：金融業界
- HIPAA[8] ⇒データ保管期間6年：医療業界
- カリフォルニア州個人情報取扱法（California SB1386）[9]

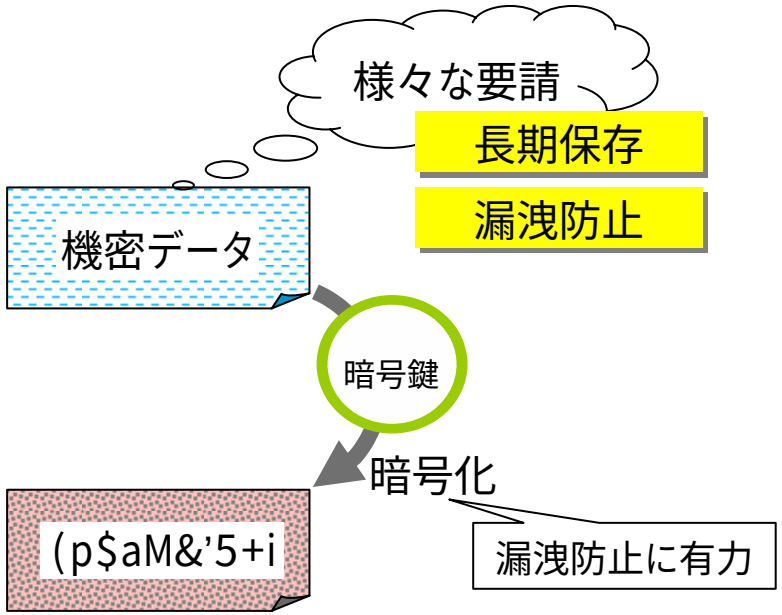
欧州連合における例

- データ保護指令 European Data Protection Directive[10]

その他

- クレジットカード業界のデータセキュリティ基準 PCI DSS[11]

保存データの暗号化にはテープストレージ！



- テープストレージには数多くの特徴があります

- 記憶容量
  カートリッジ単位の容量も大きく、カートリッジの追加により更に増大
- 転送速度
  高速 (例：120MB/s @ LTO4, 非圧縮時)
- ビット単価
  低い
- 消費電力
  容量あたりの消費電力が低い
- 長期保存性
  長期保存性に優れる
- データ圧縮
  テープドライブによるデータ圧縮が可能
- WORM機能
  専用カートリッジにより可能
- 可搬性
  カートリッジは可搬が容易

テープドライブでは暗号化機能をサポート

☆ LTO Ultrium4
☆ IBM TS1120, TS1130
☆ Sun StorageTek T10000, T9840D

暗号化機能が実装されているテープドライブ（2009年9月現在）

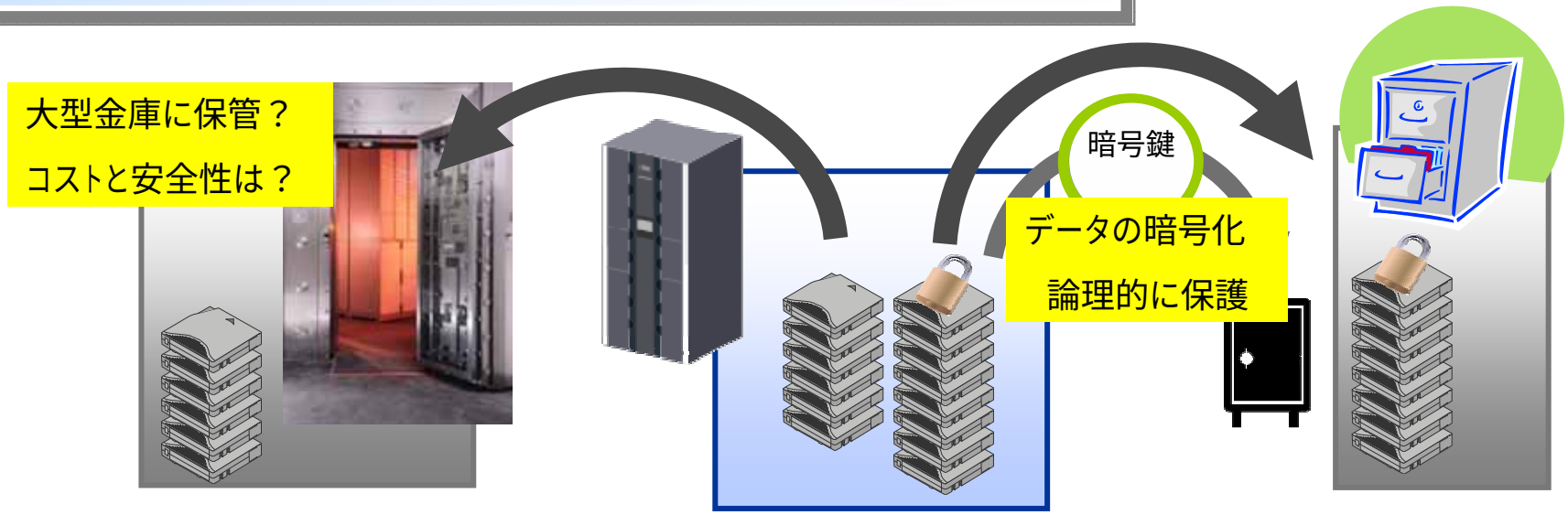
参考資料: [1],[12]

データの暗号化の必要性　(例①)

- 顧客データを保管 (アーカイブ・バックアップ) する場合

- 物理的な対策:　保管庫への入出や保管データへのアクセスを厳格・厳重に規制
  - テープにデータをそのまま書き込み、金庫にしまい、物理的にデータを保護
    (例)　銀行の大型金庫と同じレベルの物理的な対策の実施
  - ⇒ 厳格・厳重性を追求するほど、かかるコストも膨大
- 論理的な対策:　テープに暗号化して書き込み、保管　(論理的にデータを保護)

- データを暗号化することで比較的安価にデータを保護できます



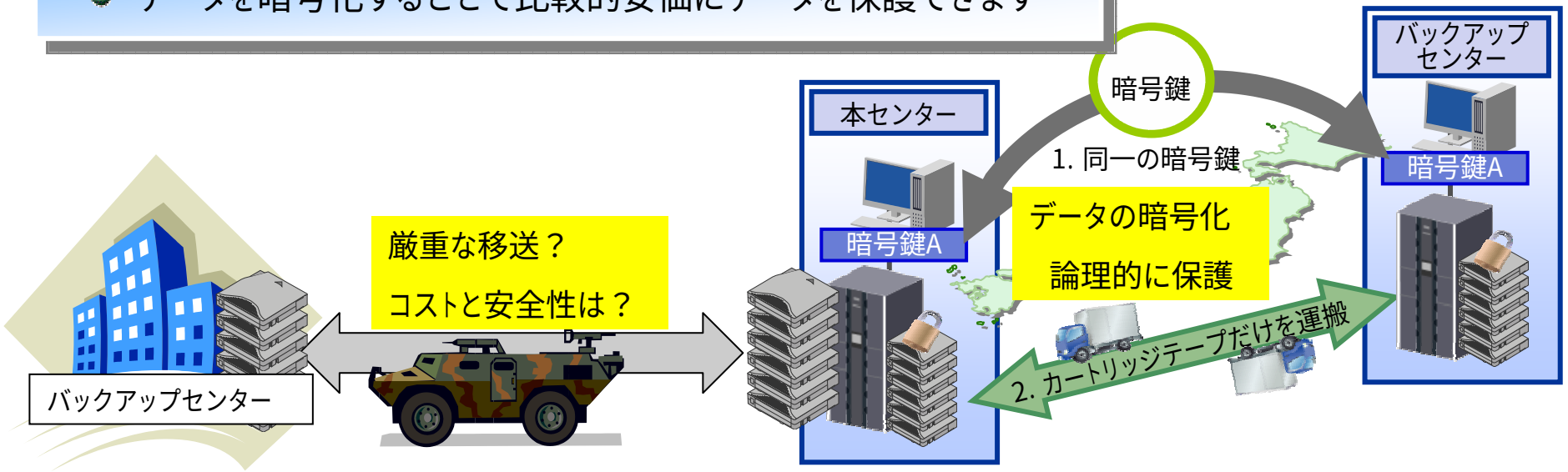
データの暗号化の必要性　(例②)

- 遠隔地にデータ保管庫 (またはバックアップセンター) を設け、データを大量に移送する場合

- 物理的な対策：　テープ媒体を厳重な金庫に入れて移送
  - 万一、移送中にテープが紛失または盗難事故にあった場合、どれほど厳重な金庫でもテープのデータの機密性が確保されていたのかを第三者が判断することは困難
  - ⇒　厳重性を求めるほど、かかるコストも膨大
- 論理的な対策：　データを暗号化した上でテープを移送
  - 事故が発生した場合に第三者によるデータの解読が困難であると容易に判断

(注)　解読：　正規の鍵を持たない者が鍵を類推するなどの方法により、正しいデータを得ること

- データを暗号化することで比較的安価にデータを保護できます



データ（個人情報）が漏洩した場合の影響

- 万一、個人情報が漏洩した場合の影響は？

被害者に対する損害賠償

- 一人あたりの平均想定損害賠償額は4万円以上
- 一件あたりの平均想定損害賠償額は1億8千万円以上

（NPO 日本ネットワークセキュリティ協会の調査結果より[13]）

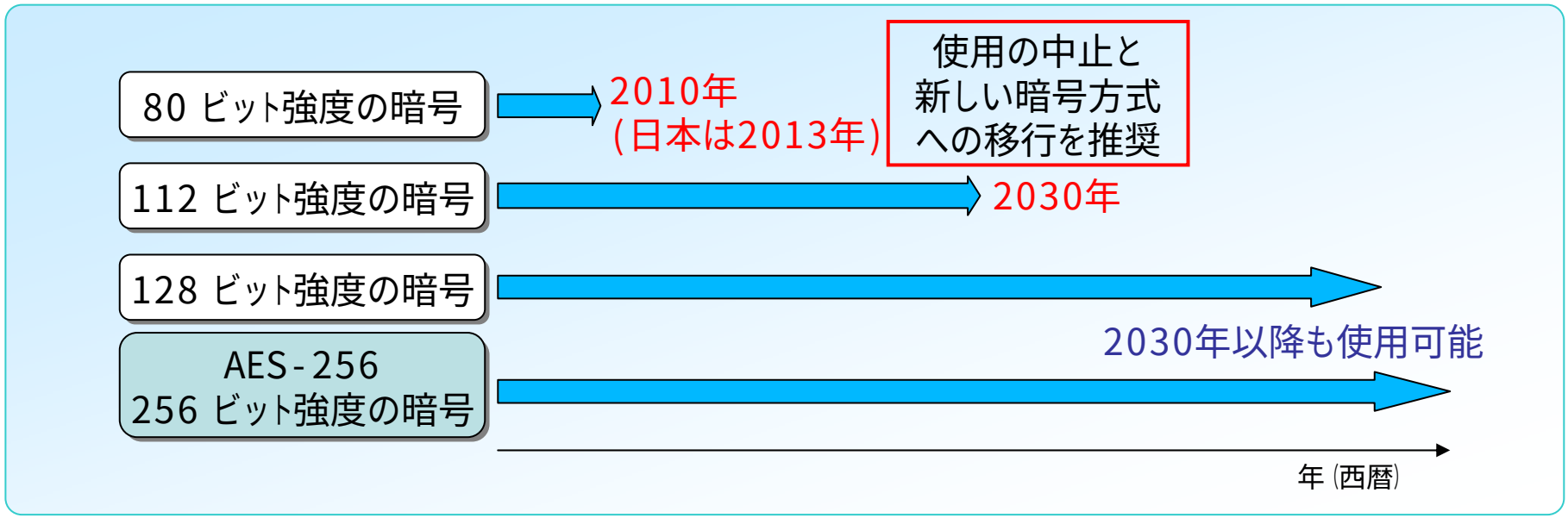
上記以外のさまざまな影響

- 漏洩の原因と被害の範囲を特定するための調査とその対策費用
- 被害者や株主代表から損害賠償の裁判を起された場合の作業費用
- 企業ブランドの信用性に対する毀損 ➡ 営業活動への悪影響
- 法令の罰則規定への対応、など

- 事故後の対応では膨大なコスト負担と悪影響があるため、適切な事前対策が望まれます

国際標準AES 256ビット暗号化方式の安全性

- コンピュータの演算能力の向上にともない、使用する暗号化方式への配慮が必要

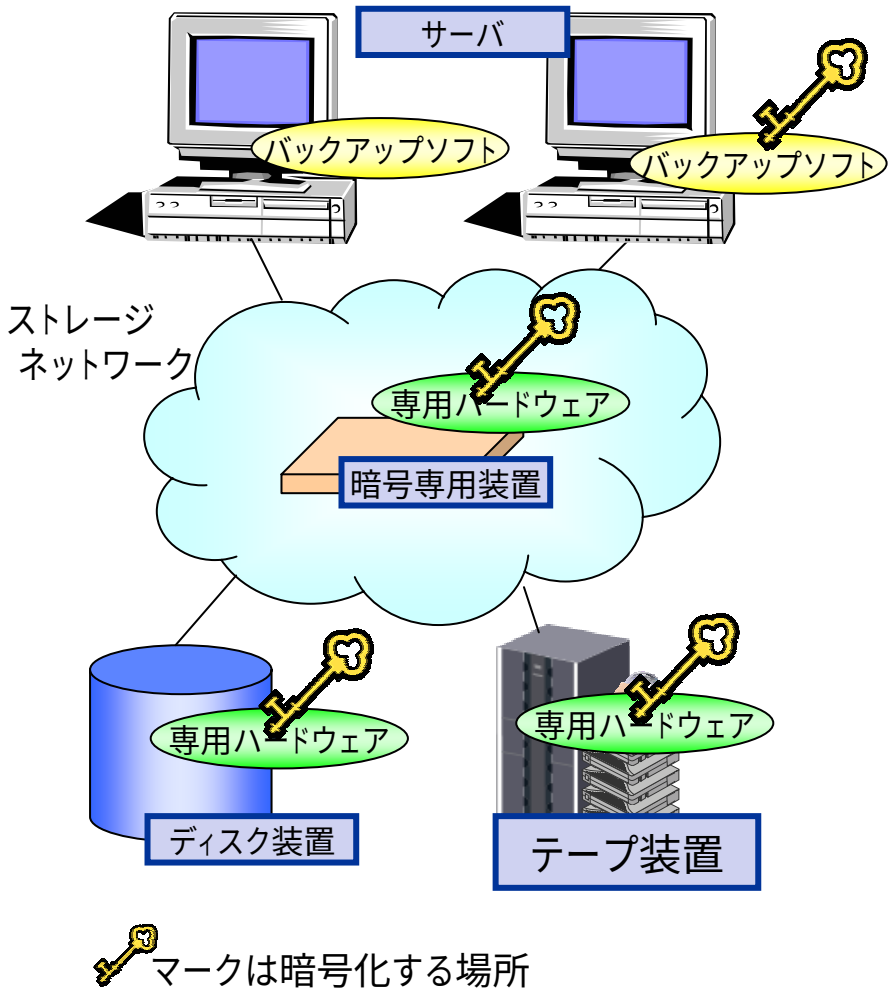


- テープドライブが採用している国際標準AES 256ビット暗号化方式は長期にわたる使用が可能

(参考)
各ビット強度の暗号化方式の例:
- 80 ビット強度: 2-key Triple DES, RSA-1024
- 112 ビット強度: 3-key Triple DES, RSA-2048
- 128 ビット強度: AES-128
- 256 ビット強度: AES-256

参考資料: [14],[15]

バックアップシステムと暗号化機能



サーバ

暗号のJOB管理が容易であるが、サーバのCPUに負荷を与え、処理能力はサーバの性能に依存

暗号専用装置

高価な専用装置の追加導入が必要で、転送性能にも影響

ディスク装置

ディスクで暗号化したデータのままではテープ装置にバックアップが出来ない
(サーバ読取り時、復号しないとサーバ側でデータを認識しない)
(他にも、長期保管や消費電力の観点で不利)

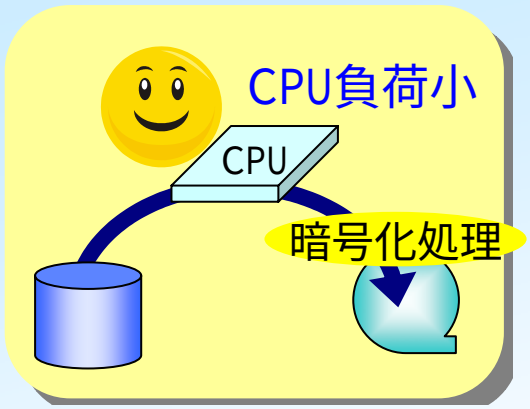
テープ装置

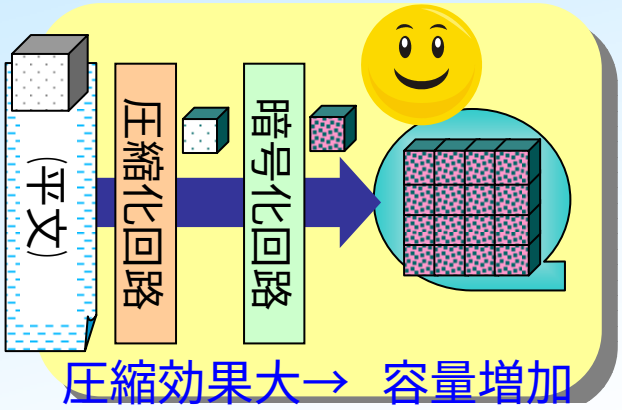
標準機能として実装されている専用ハードウェアを利用するため高速かつ安価

暗号化前にデータ圧縮が可能なので圧縮効率が低下しない

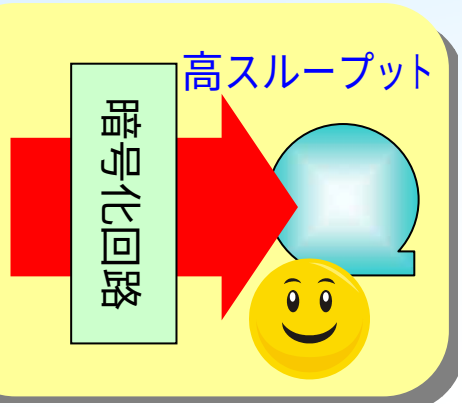
テープドライブでの暗号化処理の優位性

テープ装置の暗号

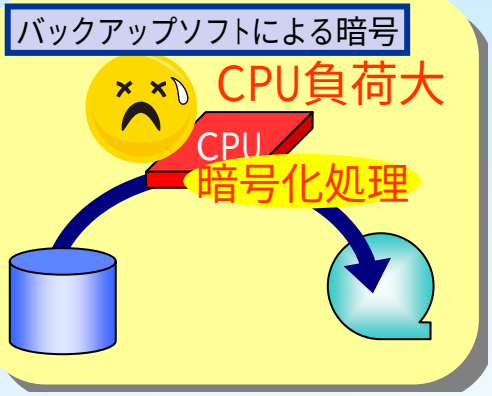




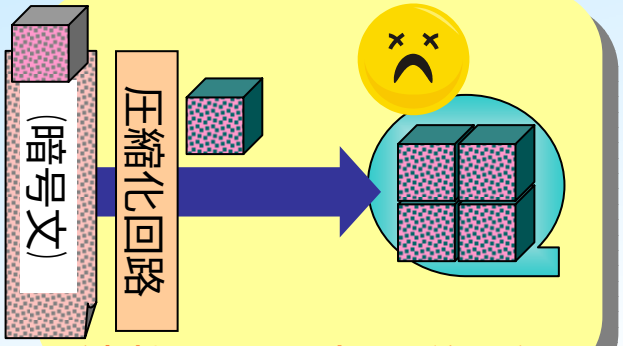
圧縮効果大→ 容量増加



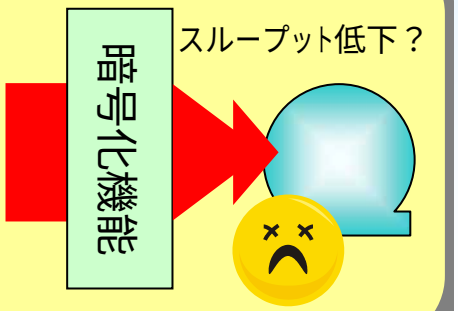
テープ装置以外の暗号



暗号化処理でCPU負荷大



圧縮効果小→容量増加無し
暗号化の後の圧縮は効果がない



暗号化機能のオーバーベッドにより
高スループットでの暗号化は難しい

まとめ

- テープストレージは、データの保管と機密性の要請に応えるのに適したストレージです

  - テープストレージでのデータ暗号化は導入が容易
  - 転送性能への影響が少ない
  - 他のリソース（CPUなど）に負荷を与えない
  - 暗号化前にデータ圧縮が可能なので圧縮効率が低下しない

  など、多くの特徴があります

- 是非、最新テープドライブの暗号化機能を活用ください！

参考資料（#1）

[1] データ保管法制･規制への対応 / テープストレージの活用，2008年版（JEITA 磁気記録媒体標準化専門委員会）
http://home.jeita.or.jp/is/committee/tech-std/std/com02.html

[2] 個人情報保護法令
http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html
http://www5.cao.go.jp/seikatsu/kojin/gimon-kaitou.html

[3] e-文書法
http://www.kantei.go.jp/jp/singi/it2/others/e-bunsyou.html

[4]会社法
http://www.moj.go.jp/HOUAN/houan33.html

[5]金融商品取引法（日本版SOX法）
http://www.fsa.go.jp/policy/kinyusyohin/index.html

[6] 米SOX法（Sarbanes-Oxley act）
http://www.sec.gov/about/laws/soa2002.pdf
http://www.sec.gov/spotlight/sarbanes-oxley.htm

[7] SEC（Securities Exchange Commission）Rule
http://www.sec.gov/about/laws.shtml

[8] HIPAA（Health Insurance Portability and Accountability Act of 1996）
http://www.hhs.gov/ocr/hipaa/

[9] カリフォルニア州上院法案 SB1386
http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

参考資料 (#2)

[10] データ保護指令 European Data Protection Directive
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

[11] PCI DSS (PCI Data Security Standard)
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

[12] テープストレージの製品動向, 2008年版 (JEITA 磁気記録媒体標準化専門委員会)
http://home.jeita.or.jp/is/committee/tech-std/std/com02.html

[13] 2008年度 情報セキュリティインシデントに関する調査報告書, Ver. 1.2 (NPO 日本ネットワークセキュリティ協会)
http://www.jnsa.org/result/2008/surv/incident/index.html

[14] Recommendation for Key Management, 米NIST Special Publication 800-57, 2007
http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

[15] 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」の決定について, 内閣官房情報セキュリティセンター (NISC)
http://www.nisc.go.jp/conference/seisaku/dai17/pdf/17siryou0101.pdf