RITSUMEIKAN

暗号化消去の原理とリスク

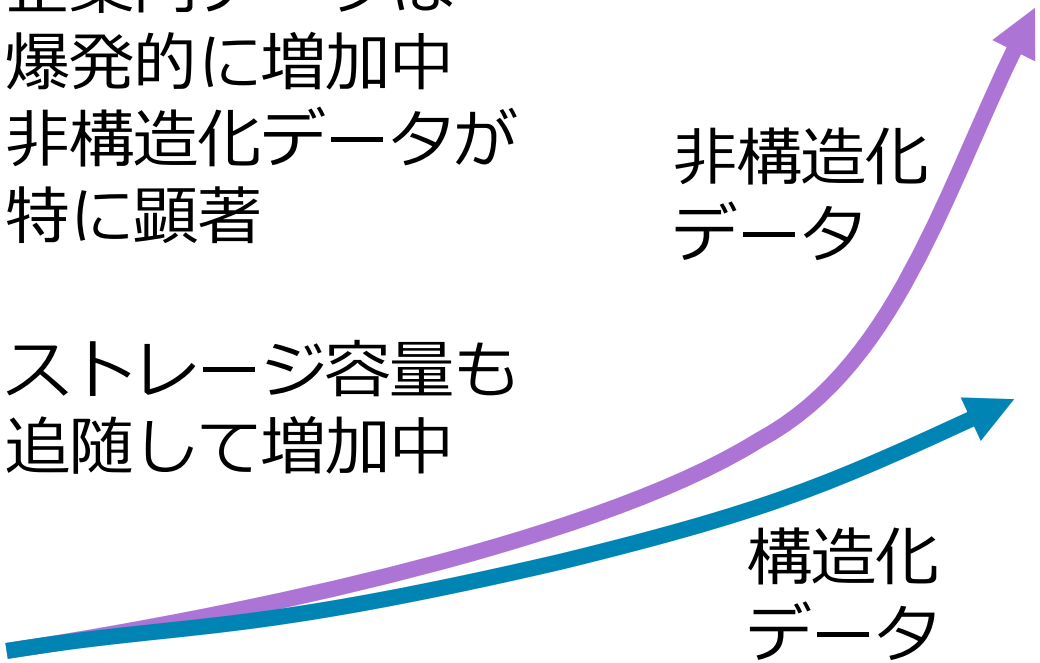
データベース・セキュリティ・コンソーシアム 会長
立命館大学 情報理工学部　上原 哲太郎

Beyond Borders

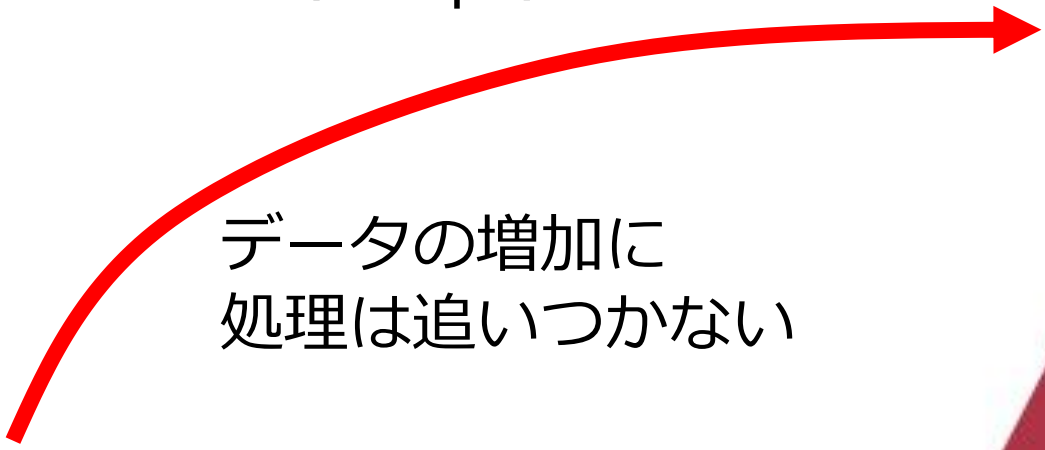
ビッグデータの時代 vs ポストムーア時代

企業内データは
爆発的に増加中
非構造化データが
特に顕著

ストレージ容量も
追随して増加中



CPUは5GHzで停滞
ネットワークは10GbEで停滞
インターフェース転送速度は
SATA III（6Gbps）で停滞

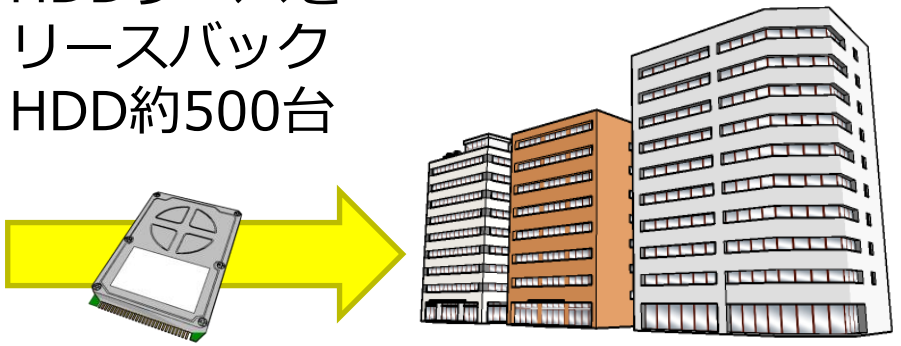


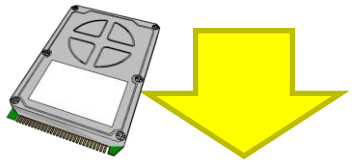
データの増加に
処理は追いつかない

神奈川県事件が明らかにした HDD消去の難しさ

HDDサーバを
リースバック
HDD約500台

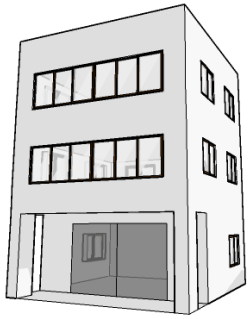
リース会社





廃棄のため
転売

従業員が
持ち出し
転売(18台)



廃棄業者

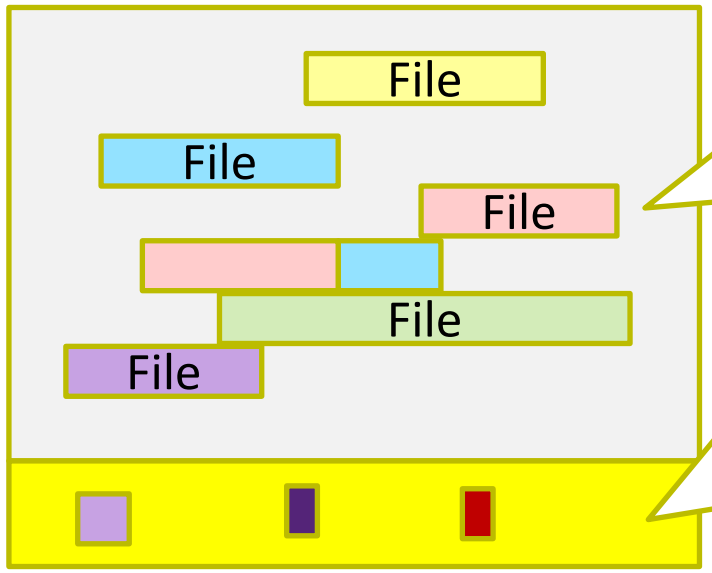
ネット
オークション

流出発覚

ストレージの内容を「完全に消す」困難

- 壊れるときは簡単なのに
  「データを完全に消そう」とするとなかなか困難

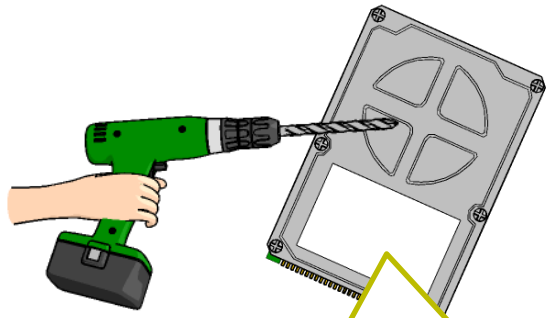
HDD



通常領域内の
データは
上書き消去可

代替セクタ内に
残ったデータ断片は
上書き困難

Enhanced Secure Erase
などを行う必要
消えたかどうか
確認はどうする？！



物理破壊しても
メディア上の
データ断片は
残存する

NIST SP800-88Rev.1


NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

CSRC

PUBLICATIONS

SP 800-88 Rev. 1

Guidelines for Media Sanitization

Date Published: December 2014

Supersedes: SP 800-88 (09/01/2006)

Author(s)

Richard Kissel (NIST), Andrew Regenscheid (NIST), Matthew Scholl (NIST), Kevin Stine (NIST)

Abstract

Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.

Keywords

media sanitization; ensuring confidentiality; sanitization tools and methods; media types; mobile devices with storage; crypto erase; secure erase

Control Families

DOCUMENTATION

Publication:
SP 800-88 Rev. 1 (DOI)
Local Download

Supplemental Material:
None available

TOPICS

Security and Privacy
general security & privacy; maintenance; risk assessment

Technologies
storage

Laws and Regulations


NIST Special Publication 800-88
Revision 1

媒体のデータ抹消処理（サニタイズ）に関するガイドライン

Richard Kissel
Andrew Regenscheid
Matthew Scholl
Kevin Stine

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

コンピュータ セキュリティ

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

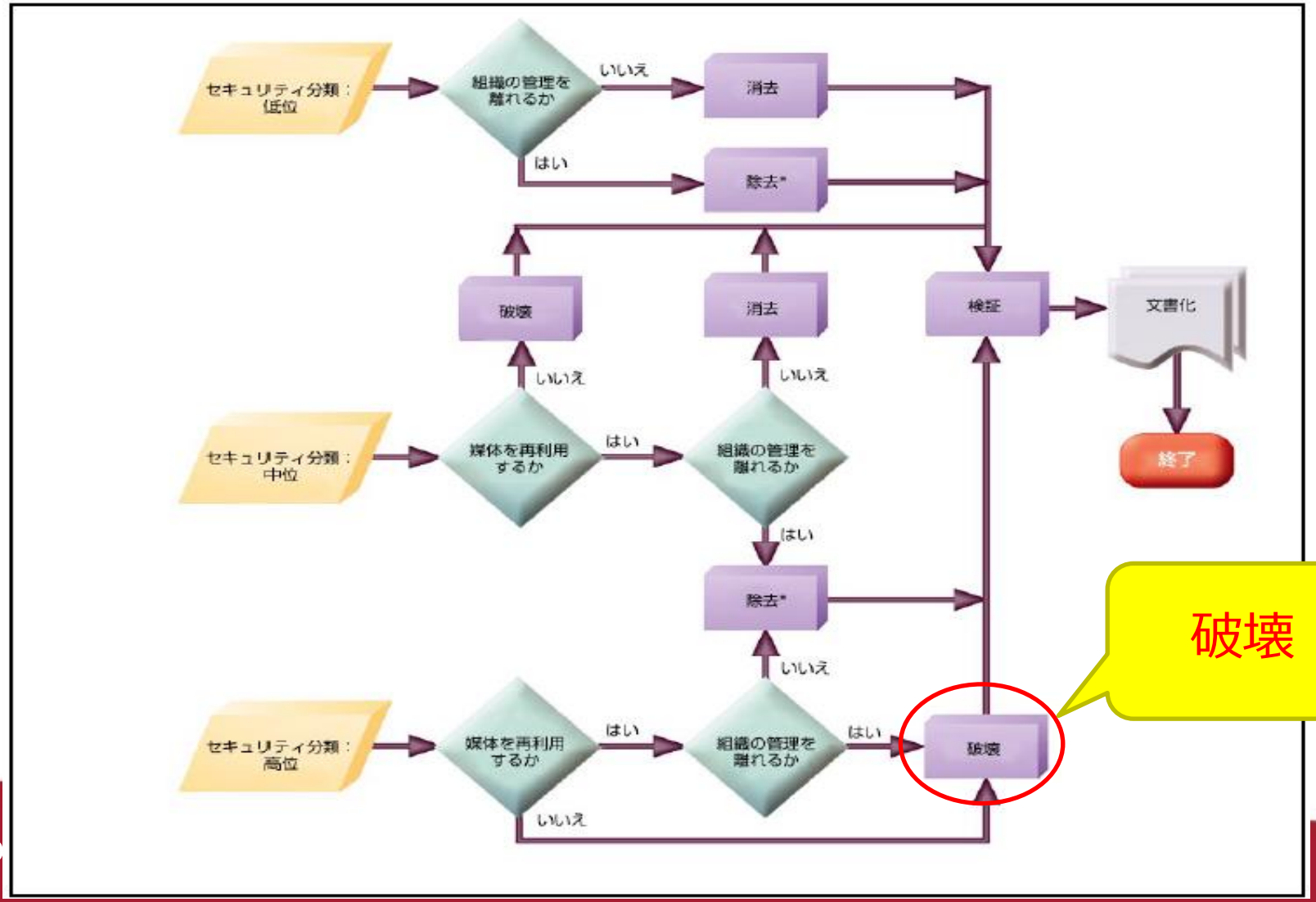
この文書は以下の団体によって翻訳監修されています

IPA 独立行政法人 情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

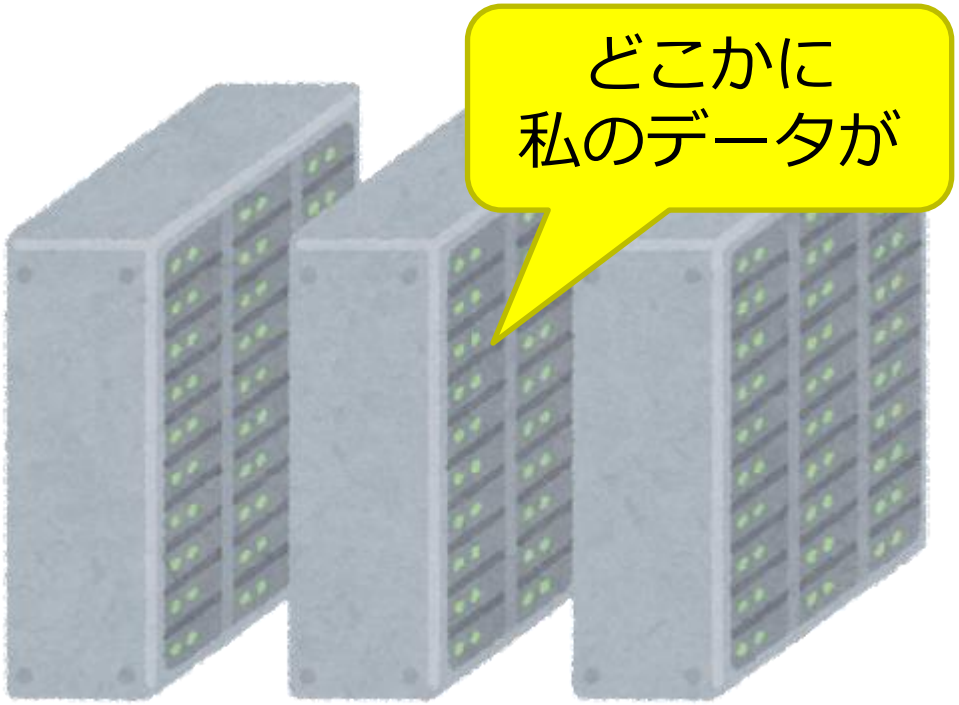
Beyond Borders

https://www.ipa.go.jp/security/publications/nist/index.html

高機密な情報が入った媒体が組織を離れる場合は「破壊」一択

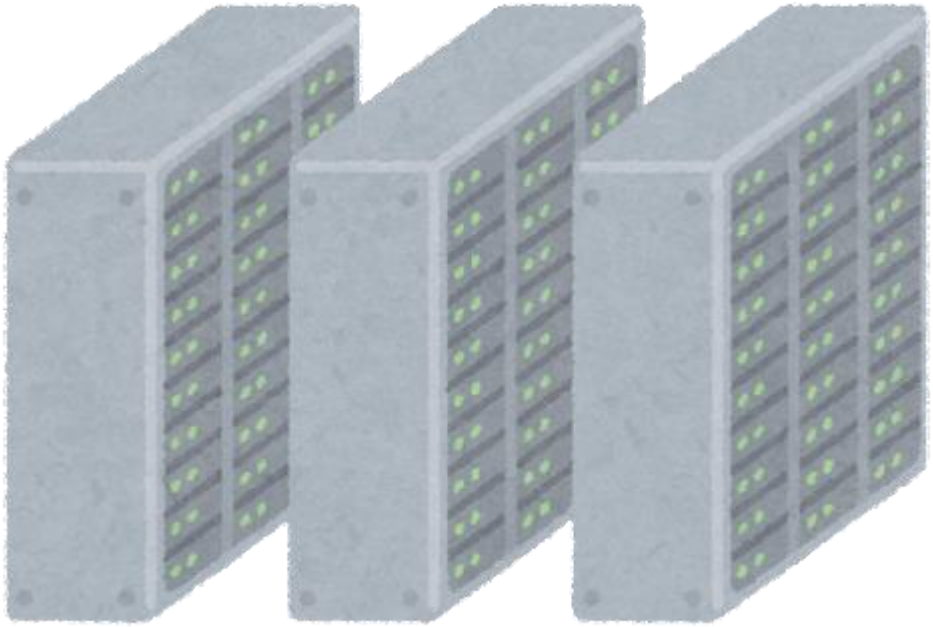


データセンターやクラウドどうするの？？

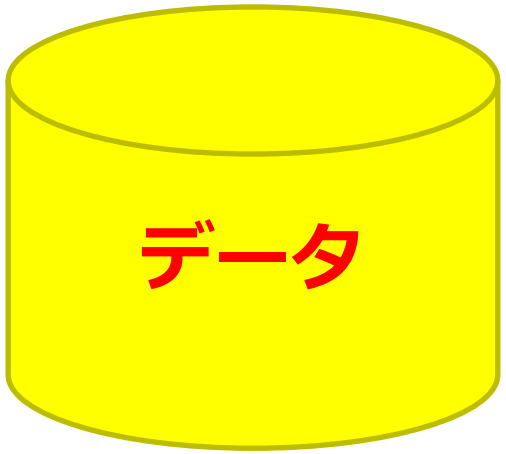


物理的位置は
よくわからない
わかったとしても
手を出せない

物理破壊と言われても…こうするわけにも…

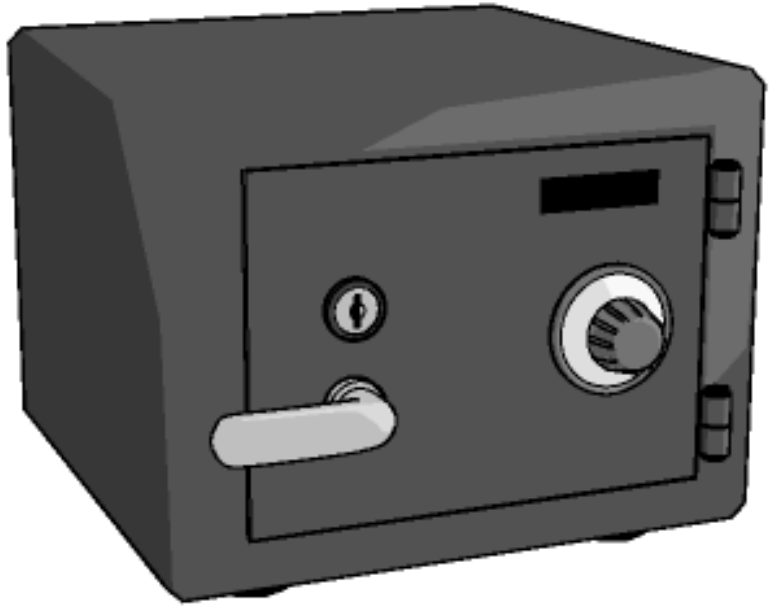


そこで暗号化＝管理対象を変える技術



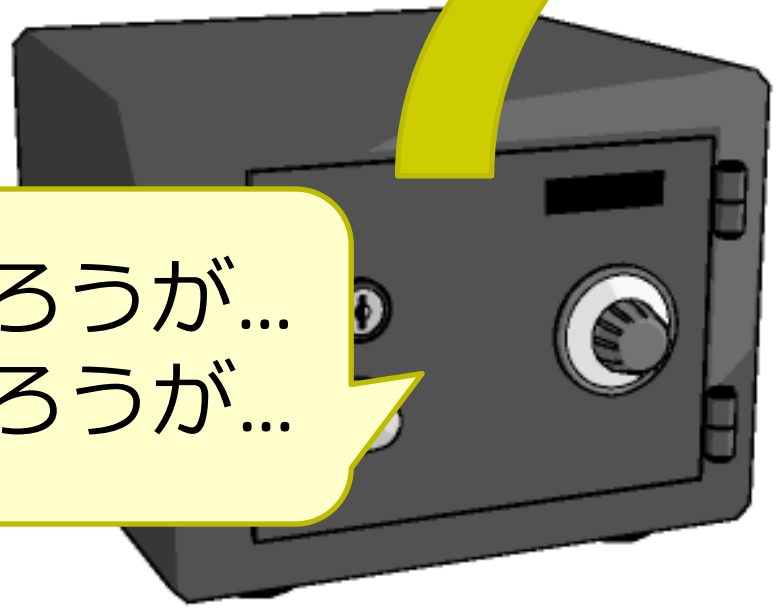
そこで暗号化＝管理対象を変える技術

暗号化



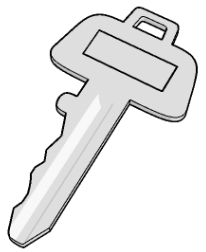
そこで暗号化＝管理対象を変える技術

暗号化



何TBあろうが…
何PBあろうが…

鍵は256bit
＝32bytes!



暗号鍵

暗号化は大きなデータの管理を小さな暗号鍵の管理の問題に置換する
鍵の消去がデータの消去と等価になる

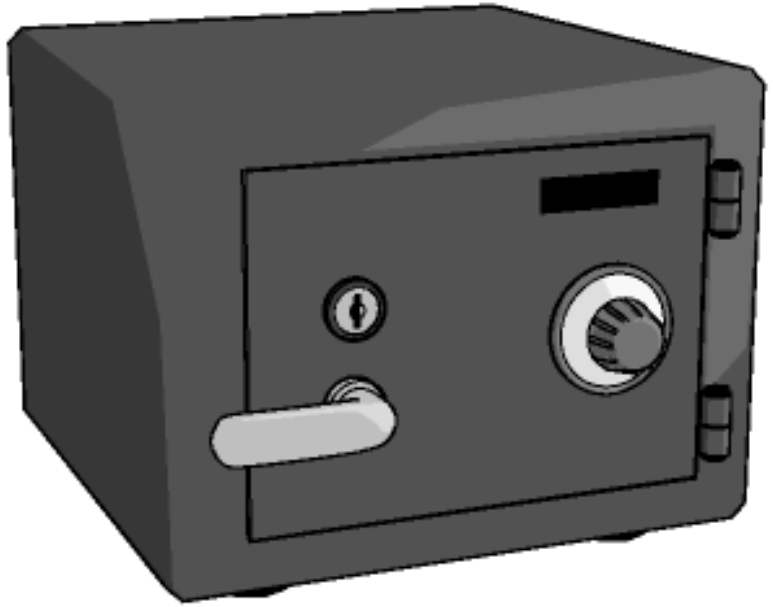
暗号化消去は対象範囲が広い

- システム単位 (例：BitLocker)
  - 暗号鍵をTPMなどマザーボード側に持つことで
    ストレージデバイスとシステムを不可分にした暗号化
- ストレージデバイス単位（例：自己暗号化ドライブ）
  - ストレージ全体をストレージ内の鍵で暗号化
- ファイルシステム単位（例：NTFS等の暗号化ドライブ）
- ファイル単位
- データベースのテーブル単位etc

さまざまな粒度で
高速かつ簡便な
「消去」が可能

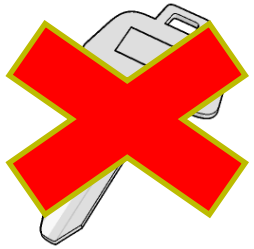
でも不安になりますよね

暗号化されたデータ



鍵は本当に開かないの？

暗号化されたままの
データが残ってるよね
それ「消去」なの？



暗号鍵
消去

暗号化消去がうまく働く条件

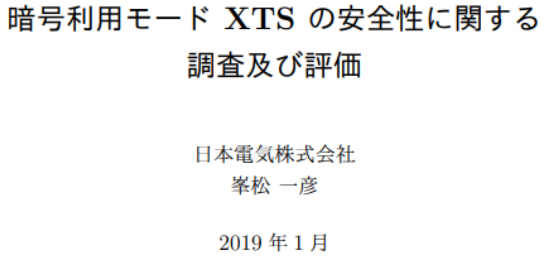
- 「**ちゃんとした暗号**」が使われること
  - 最近はこれはだいたい大丈夫
- **暗号化鍵の管理**がきちんとしており鍵の消去が確認できること
  - 特に「鍵のバックアップ」問題
- **使用開始時から暗号化**されていること
  - 途中で暗号化すると問題が複雑に

全部大切だが特に…

よく聞かれること

- 暗号はいつか解かれる？
  - 平文が「鍵なしで」回復できることは考えがたい
  - 量子コンピュータを使っても平文回復は大変
- 「ちゃんとした暗号」の残存リスク（他は問題ないとして）
  - ストレージ暗号化は「超長期間」データが残存する可能性があるので万年単位だとわからない
    - ただ1万年後解読される心配をする必要があるのか？
  - 実装の誤り・運用の誤り（特に鍵）

暗号利用モード（運用モード）XTS


暗号利用モード XTS の安全性に関する
調査及び評価

日本電気株式会社
峯松 一彦

2019 年 1 月

- CBC等の従来普及した
  ブロック暗号利用モードは
  ランダムアクセス向きでない
- ストレージ向け暗号利用モードとして
  XTSが提案され普及が進む
  - Windows10のBitLocker
    macOSのFileVault2
  - IEEE P1619-2007で標準化
    NISTもSP800-38Eで規定
  - 日本でもすでにCRYPTREC暗号リスト掲載
  - 注：AESの利用が前提
    安全性確保のためには鍵更新頻度に条件あり
    →実装が重要

CRYPTREC暗号リストに載れば JCMVPによる実装の認証が可能に

暗号モジュール試験及び認証制度 (JCMVP)

最終更新日：2020年12月1日

Japan Cryptographic Module Validation Program

本制度は、電子政府推奨暗号リスト等に記載されている暗号化機能、ハッシュ機能、署名機能等の承認されたセキュリティ機能を実装したハードウェア、ソフトウェア等から構成される暗号モジュールが、その内部に格納するセキュリティ機能並びに暗号鍵及びパスワード等の重要情報を適切に保護していることを、第三者による試験及び認証を組織的に実施することにより、暗号モジュールの利用者が、暗号モジュールのセキュリティ機能等に関する正確で詳細な情報を把握できるようにするために設置されます。

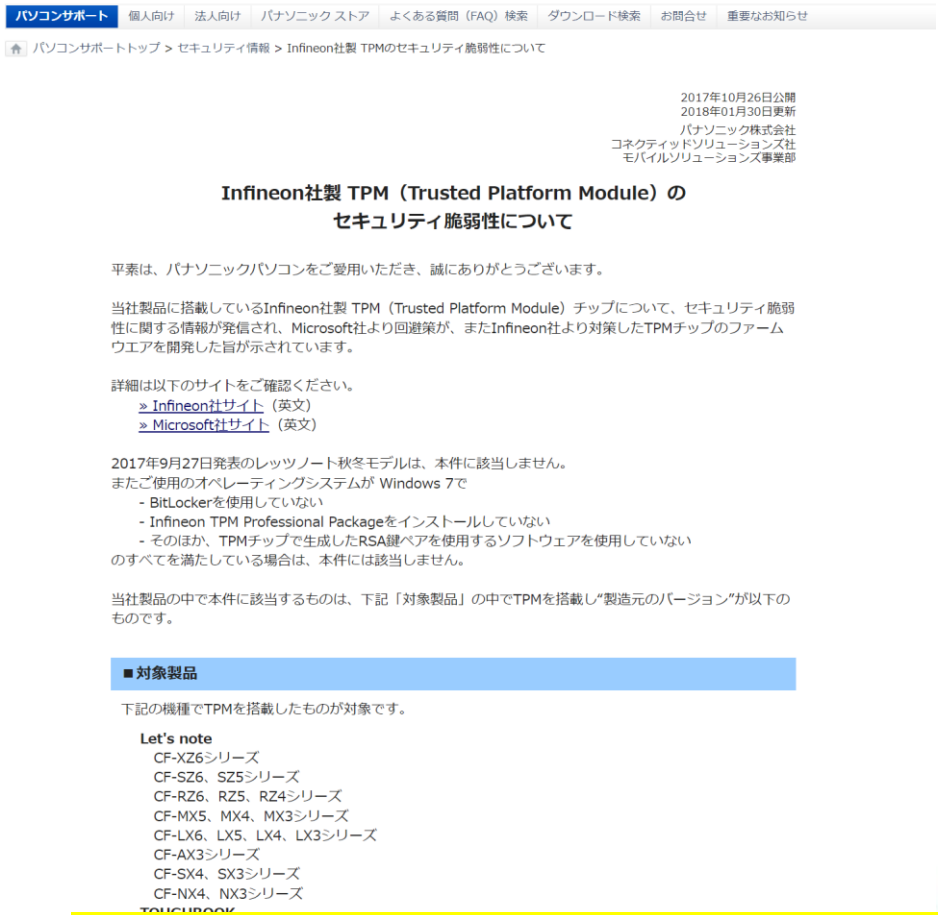
また、内閣サイバーセキュリティセンターによる「政府機関等の対策基準策定のためのガイドライン (平成30年度版)」に基づき、政府機関向けセキュリティシステムの調達に際して、供給者は、本制度に基づく認証を取得することにより、選択された暗号アルゴリズムが適切に実装され、鍵等の重要情報のセキュリティが確保された暗号モジュールであることをアピールできます。

これで解決?!

- 運用中のシステムを暗号化すると
  暗号化前のデータの断片が残る
  - その断片はフォレンジック可能？！
  - 大事な情報がたまたま載るリスク
  - だから「**運用開始時点で暗号化**」は重要
- 鍵は**「ちゃんと」生成**されてる？
- 運用後は鍵の消失は
  データロストに繋がるので
  どうしても「バックアップ」したくなる…
  鍵の複製を把握しきれる？

暗号実装の問題で頻発する鍵生成の「エントロピー不足」

2008年 DebianのOpenSSL実装に問題



2017年 Infineon製TPMのファームウェア実装に問題

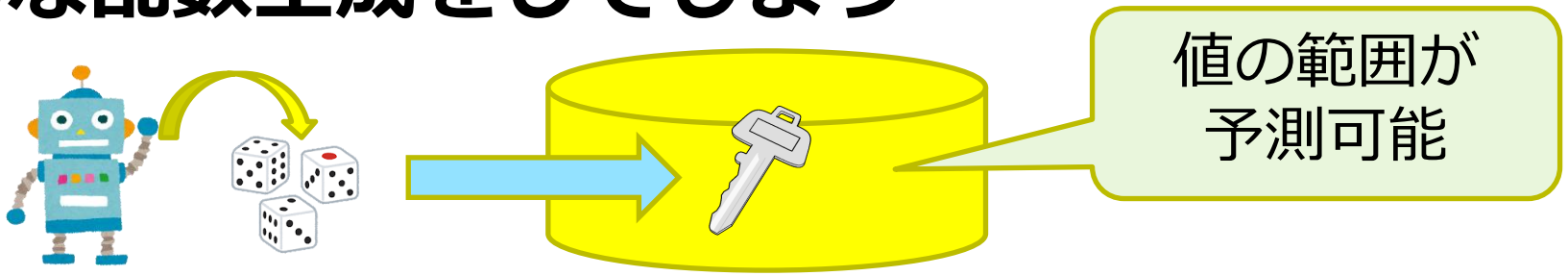
結構深刻な「鍵の使いまわし問題」

- 2012年 SSL/TLSやSSHで使われる公開鍵がネット上で重複している例が多々あることをLenstraらとHeningerらが独立に報告
  - http://eprint.iacr.org/2012/064
  - https://www.usenix.org/conference/usenixsecurity12/mining-your-ps-and-qs-detection-widespread-weak-keys-embedded-devices
- Heningerらはネット上の公開鍵の6割が他の公開鍵の使いまわし？！と指摘

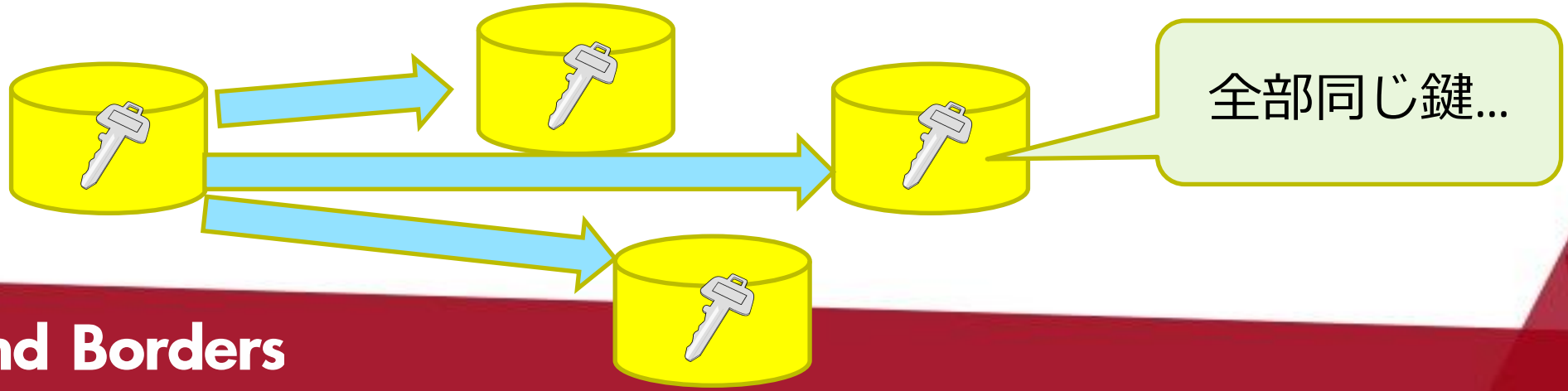
参考：https://sect.iij.ad.jp/blog/2012/08/public-key/

暗号化消去の場合にもそのリスクは高い…

- 脆弱な乱数生成をしてしまう



- クラウド等でテンプレートをそのまま複製して
  暗号化ストレージのインスタンスを作ってしまう



BitLocker 回復キーを探す

Windows 10

BitLocker は Windows のデバイスの暗号化機能です。デバイスで BitLocker 回復キーの入力を求めるメッセージが表示された場合は、次の情報を参照して、デバイスのロックを解除するために必要な 48 桁のキーを見つけることができます。このキーがすぐに利用可能でない場合は、以下の場所を確認してキーを見つけることができます。

Microsoft アカウントに保存した場合: 別のデバイスで Microsoft アカウントにサインインして回復キーを探します。他のユーザーがデバイス上のアカウントを持っている場合は、各自の Microsoft アカウントにサインインして、キーがあるかどうかを確認してもらうことができます。

印刷した場合: 回復キーは、BitLocker がアクティブ化されたときに保存された印刷出力に記載されている可能性があります。コンピューターに関連する重要な書類を保管してある場所を探します。

USB フラッシュ ドライブに保存した場合: ロックされた PC に USB フラッシュ ドライブを接続し、指示に従って操作します。キーをテキスト ファイルとしてフラッシュ ドライブに保存した場合は、別のコンピューターを使ってテキスト ファイルの内容を確認します。

Azure Active Directory アカウントの場合: デバイスが職場または学校のメール アカウントを使用して組織にサインインしたことがある場合は、デバイスに関連付けられているその組織の Azure AD アカウントに、回復キーが保存されている可能性があります。直接アクセスできる場合もあれば、回復キーにアクセスするためにシステム管理者に問い合わせる必要がある場合もあります。

システム管理者によって保持されている場合: デバイスがドメイン (通常、職場または学校のデバイス) に接続されている場合は、システム管理者に問い合わせて回復キーを入手します。

BitLocker 回復キーに関する詳細情報

デバイスの暗号化の詳細

鍵がどこに残っている?

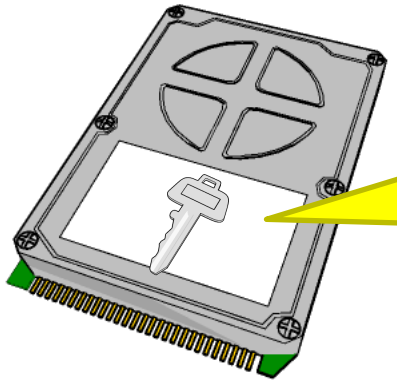
鍵管理を楽にする方法は
物理媒体に鍵を閉じ込め取り出せなくする

耐タンパ性のある
ICカードで鍵管理
（公的個人認証）

耐タンパ性のある
USBキーで鍵管理
（FIDO U2F認証）

PC等で内蔵される
Trusted Platform Module
(TPM)はBitLocker等で使用
Windows11では必須化
（最近はソフトウェア実装も）

自己暗号化ドライブ
Self Encryption Drive (SED)



暗号化機能と
耐タンパな鍵ストアが
一体化したドライブ

様々な提案があったが
現在は
Trusted Computing Group(TCG)のOpal SSCが中心的役割

他にMicrosoftのeDrive
ドライブ各社独自規格
など

クラウド上の Hardware Security Module (HSM)

Cloud HSM

クラウド上のHSM
直接は触れられないが
中の鍵の管理権限は
利用者が独占

AWS CloudHSM の概要

PDF | RSS

AWS CloudHSM では、AWS クラウドにハードウェアセキュリティモジュールが搭載されています。ハードウェアセキュリティモジュール (HSM) は、暗号化オペレーションを処理し、暗号化キーの安全なストレージを提供するコンピューティングデバイスです。

AWS CloudHSM から HSM を使用すると、さまざまな暗号化タスクを実行することができます。

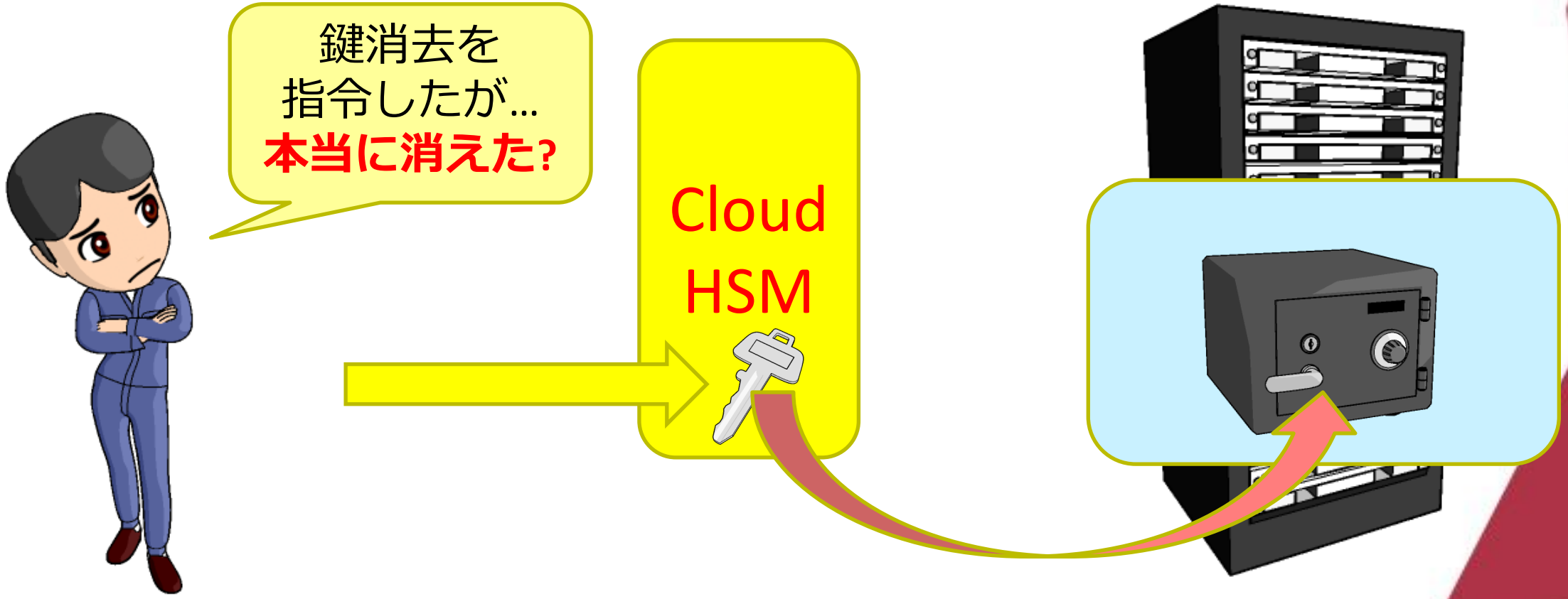
- 対称キーと非対称キーペアを含む暗号化キーの生成、保存、インポート、エクスポート、および管理。
- 対象および非対称アルゴリズムを使用した、データの暗号化および復号化。
- 暗号化ハッシュ関数を使用した、メッセージダイジェストおよびハッシュベースのメッセージ認証コード (HMAC) の計算。
- 暗号化された、データの署名 (コード署名を含む) および署名の検証。
- 暗号化された安全なランダムデータの生成。

データの暗号化キーを作成および管理するマネージド型サービスは欲しいが、独自の HSM を運用したくないまたは不要である場合、の使用を検討してください。AWS Key Management Service。

AWS CloudHSM でできることの詳細については、以下のトピックを参照してください。AWS CloudHSM の使用を始める準備ができたら、「使用スタート方法」を参照してください。

AWSの例

最後の最後に残る問題は…？！



重要になるのは消去の「監査」

- どのようにして「消去」したことを示すのか
  - 特に「鍵の複製」がないことをどのように示すのか
    - 不存在の証明＝「悪魔の証明」問題
    - そのためにもHSMなど「ハードウェア内の鍵」は重要
- そのためにも鍵管理が重要
  - 鍵管理システムを作って証跡を残していく
  - IPAはNIST SP800-130「鍵管理における推奨事項」を翻訳これを利用するための手引書として「暗号鍵管理システム設計指針」をCRYPTRECでまとめて公表

始めるより終える方が難しい
始めるときに終わりを考えるべき

始めるより終える方が難しい
始めるときに終わりを考えるべき

運用開始時点で暗号化

鍵管理を徹底=HSM

廃棄時鍵をちゃんと消す
それを確認する手段を