RITSUMEIKAN

暗号化消去と鍵管理

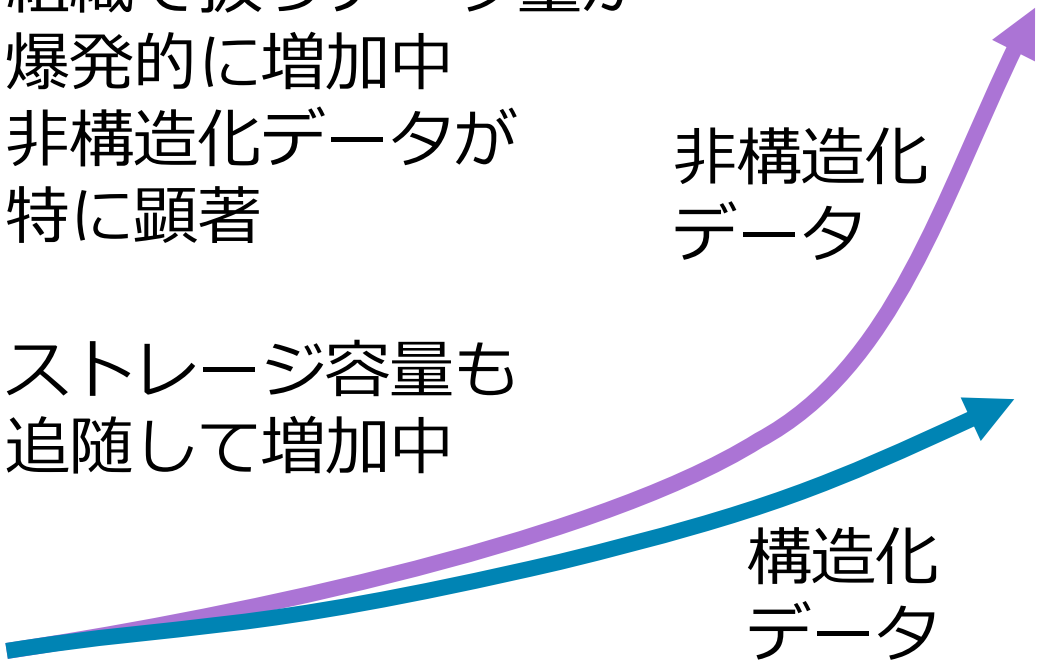
立命館大学 情報理工学部　上原 哲太郎

Beyond Borders

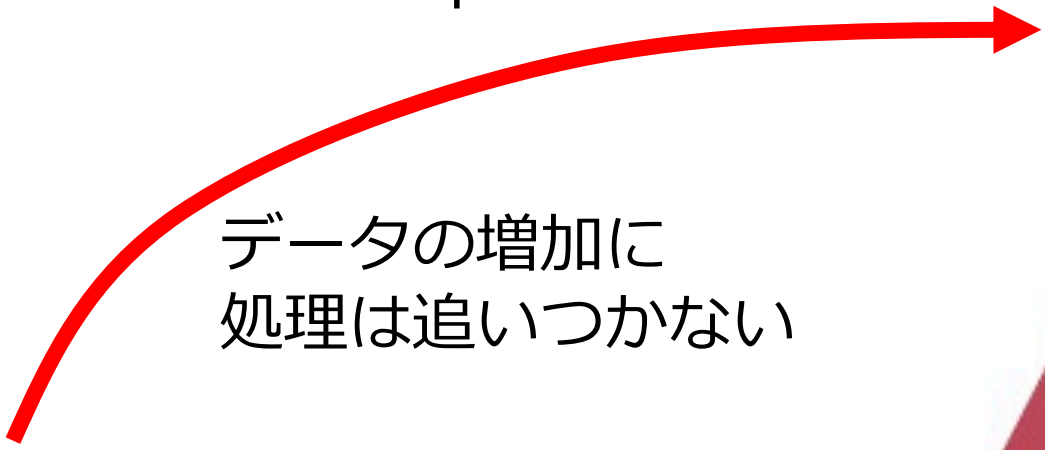
ビッグデータの時代 vs ポストムーア時代

組織で扱うデータ量が
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

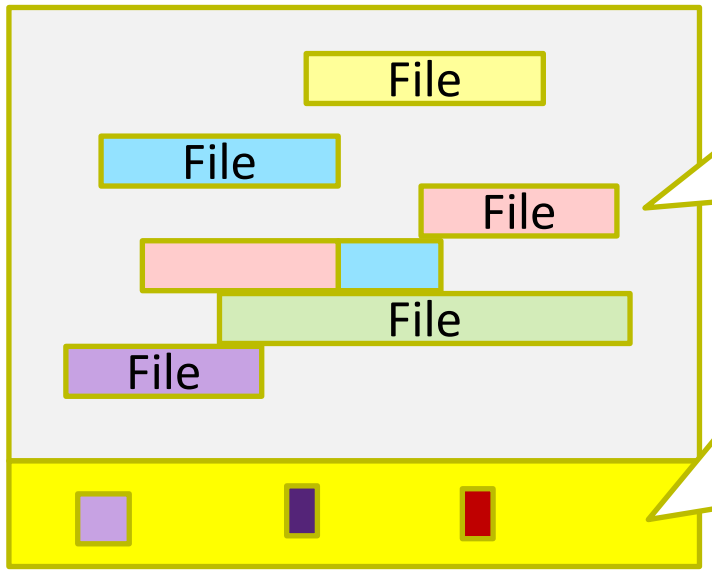


データの増加に
処理は追いつかない

ストレージの内容を「完全に消す」困難

- システム撤去・廃棄時にデータ漏洩を防ぐために「データを完全に消そう」とするとなかなか困難

HDD

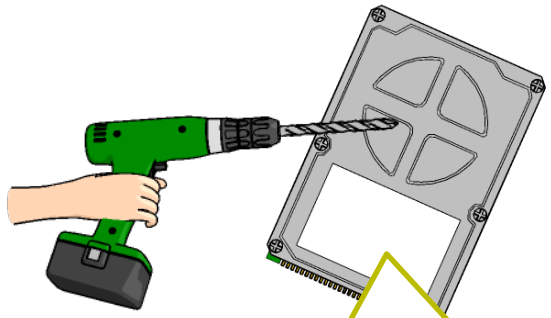


通常領域内のデータは上書き消去可

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

情報システム撤去・廃棄時の情報漏洩を防ぐ
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

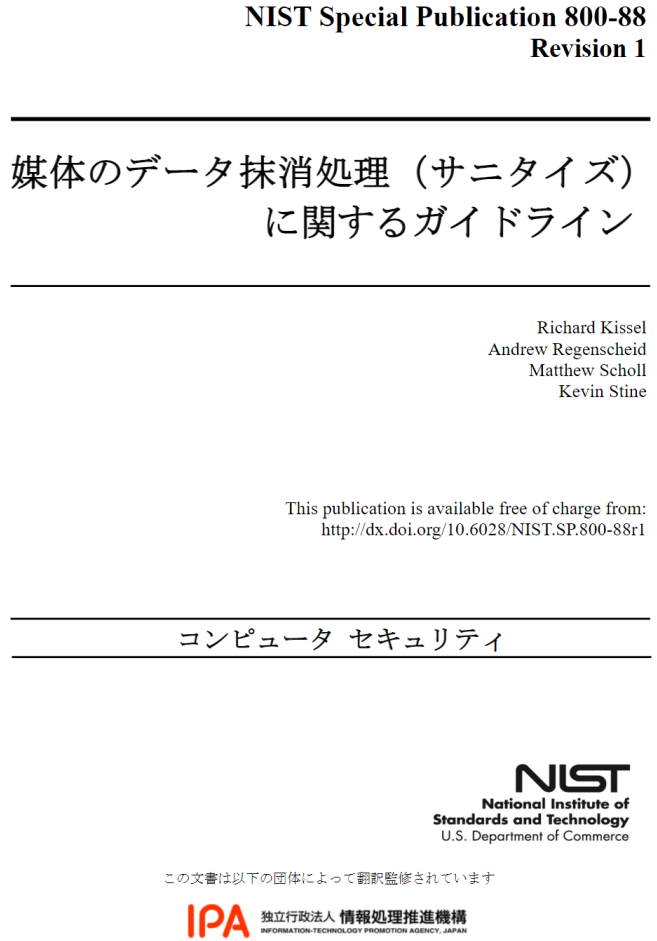
Supplemental Material:
None available

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

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

3段階の抹消処理：消去・除去・破壊

NIST SP 800-88 Rev. 1　　Guidelines for Media Sanitization

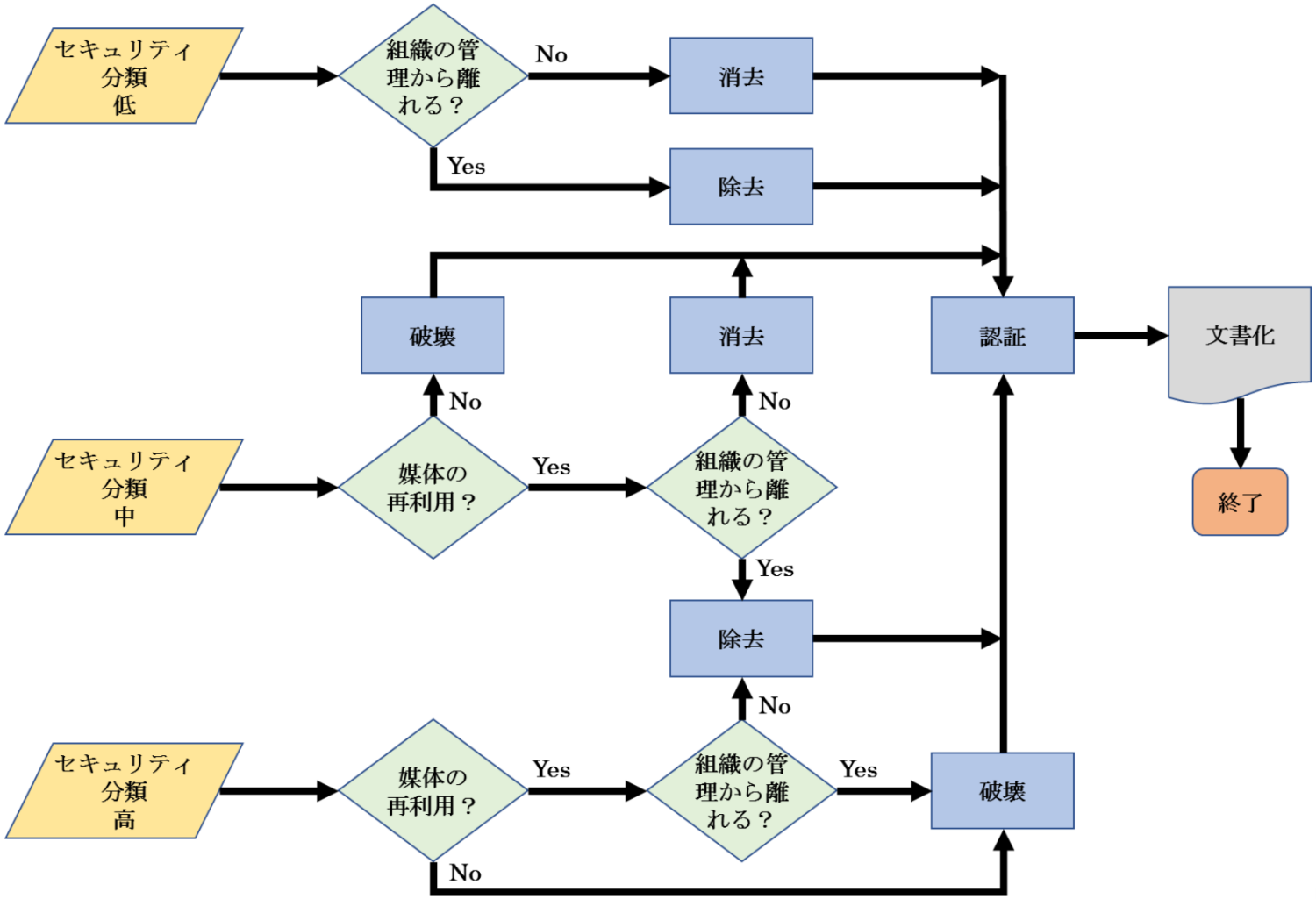
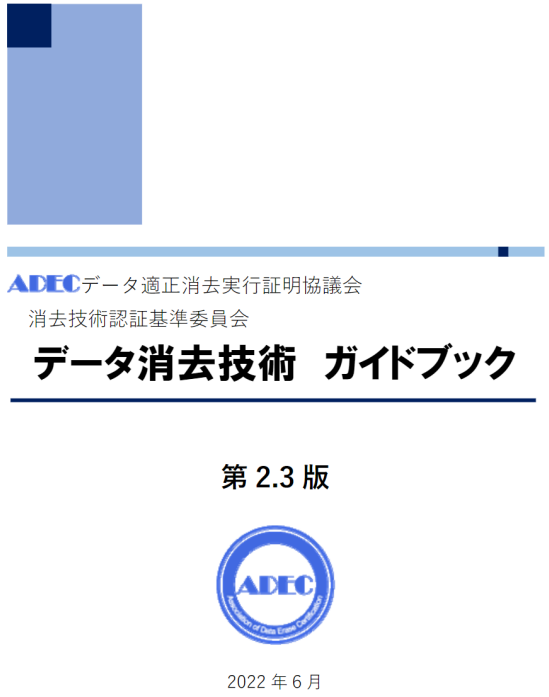


図 4-1：データ抹消処理及び廃棄の決定フロー

HDDやSSDなどのストレージでは

- 消去(Clear):
  一般的データ上書き
- 除去(Purge):
  専用コマンドでの上書き・暗号化消去
  消磁処理
- 破壊(Destroy):
  分解・粉砕・溶融・焼却による
  復元不可能処理

ADECデータ消去技術ハンドブック



- 日本語文書としては
  最も詳しく網羅的に
  消去技術を解説している

- NIST, NSAのガイドラインや
  日本の公的ガイドラインにも
  言及

HDD消去の現実

- 現在HDDの消去は1回上書きだけでも
  1TBあたり2～4時間必要
- ガイドラインは3回程度の複数上書きを求めている

- 一方、システム撤去時のストレージ容量は膨大
- クラウドなど「上書き消去」がそもそもできない
  ストレージも存在する

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

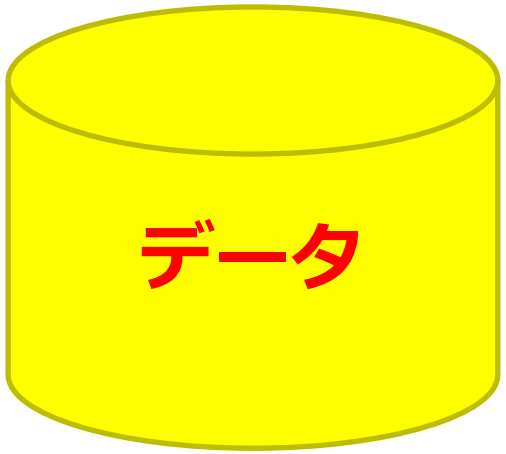
廃棄業者

従業員が
持ち出し
転売(18台)

ネット
オークション

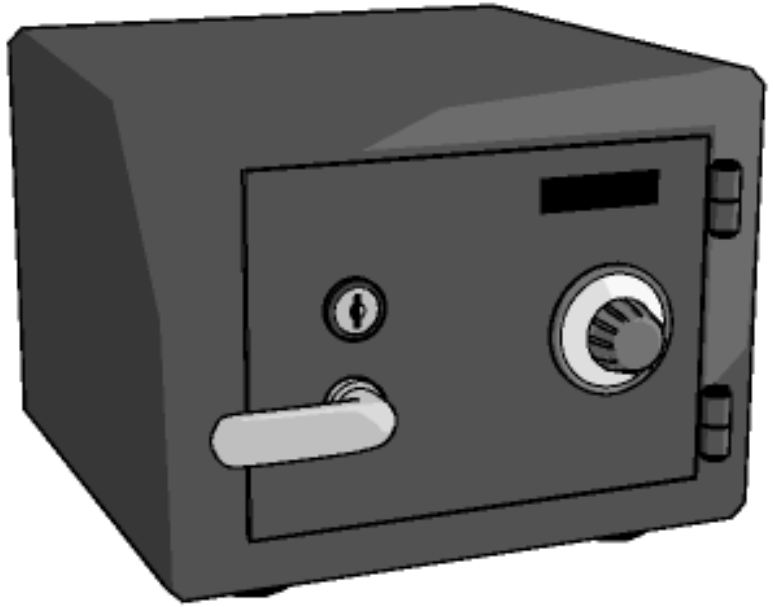
流出発覚

そこで暗号化＝管理対象を変える技術



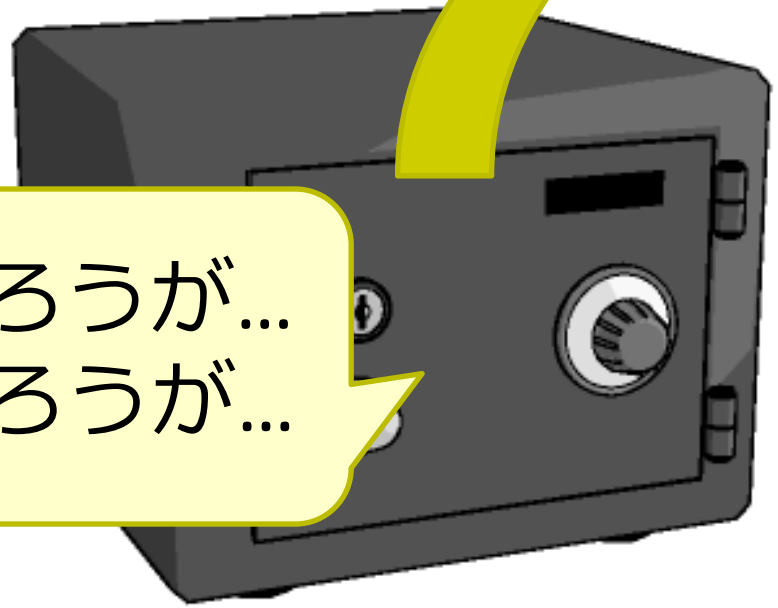
そこで暗号化＝管理対象を変える技術

暗号化



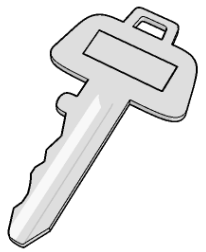
そこで暗号化＝管理対象を変える技術

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

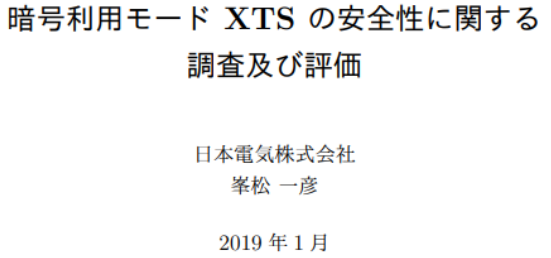
さまざまな粒度で
高速かつ簡便な
「除去」が可能

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
  - CRYPTREC暗号
- 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
  - 暗号鍵管理ガイドライン
- 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…

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

- 多くの暗号利用モードは
  ランダムアクセス向きでない
- ランダムアクセス可能な
  ブロック単位で処理する
  暗号利用モードとしてXTSが提案される
  - Windows10のBitLocker
    macOSのFileVault2
  - AESでの利用はIEEE P1619-2007で標準化
    NISTもSP800-38Eで規定
  - CRYPTREC暗号リストにも掲載

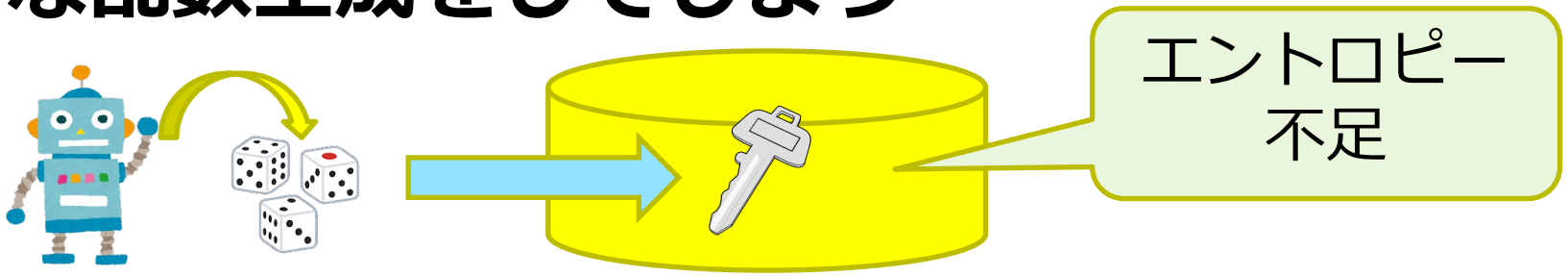
XTSの安全性評価と運用上の注意

- 2011年 Philip Rogawayによる評価[1]により
  XTSに明確な安全性定義がないとされる
  - 特にデータの終端部、最終2ブロックに端数処理として
    Ciphertext Stealing (CTS)処理が入るが
    この部分の安全性の定義が困難
- 2019年峯松一彦による評価[2]により…
  - CTSはストレージ暗号化利用である限り致命的問題はない
  - 鍵を変えずに2^(n/2)ブロック（nはブロックサイズ）以上
    利用した場合に鍵回復攻撃が可能
    →64bitブロック暗号では脅威だがAESでは脅威にならない

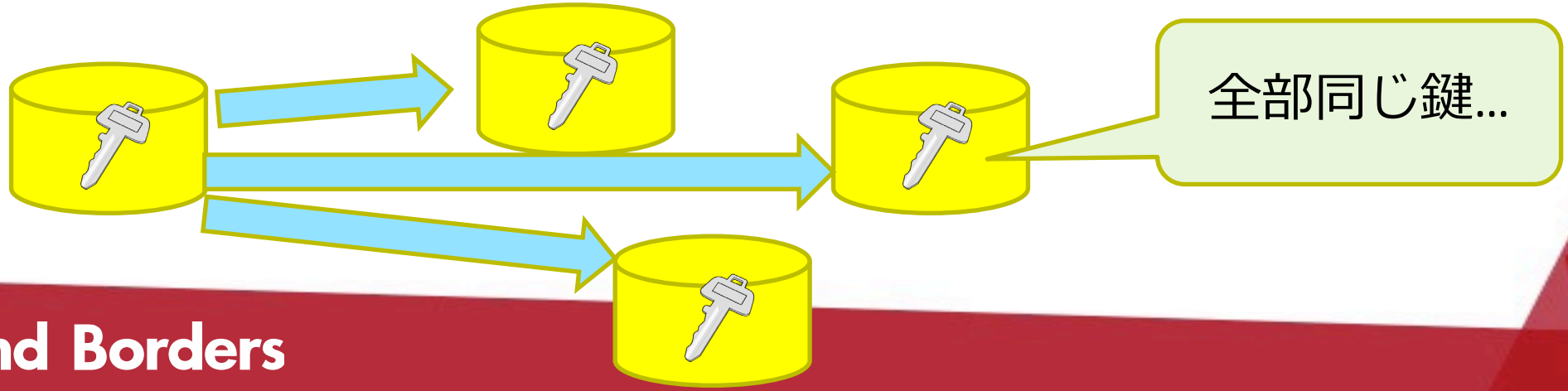
[1] P.Rogaway: Evaluation of Some Blockcipher Modes of Operation
[2] 峯松一彦:暗号利用モードXTSの安全性に関する調査及び評価

鍵管理の問題

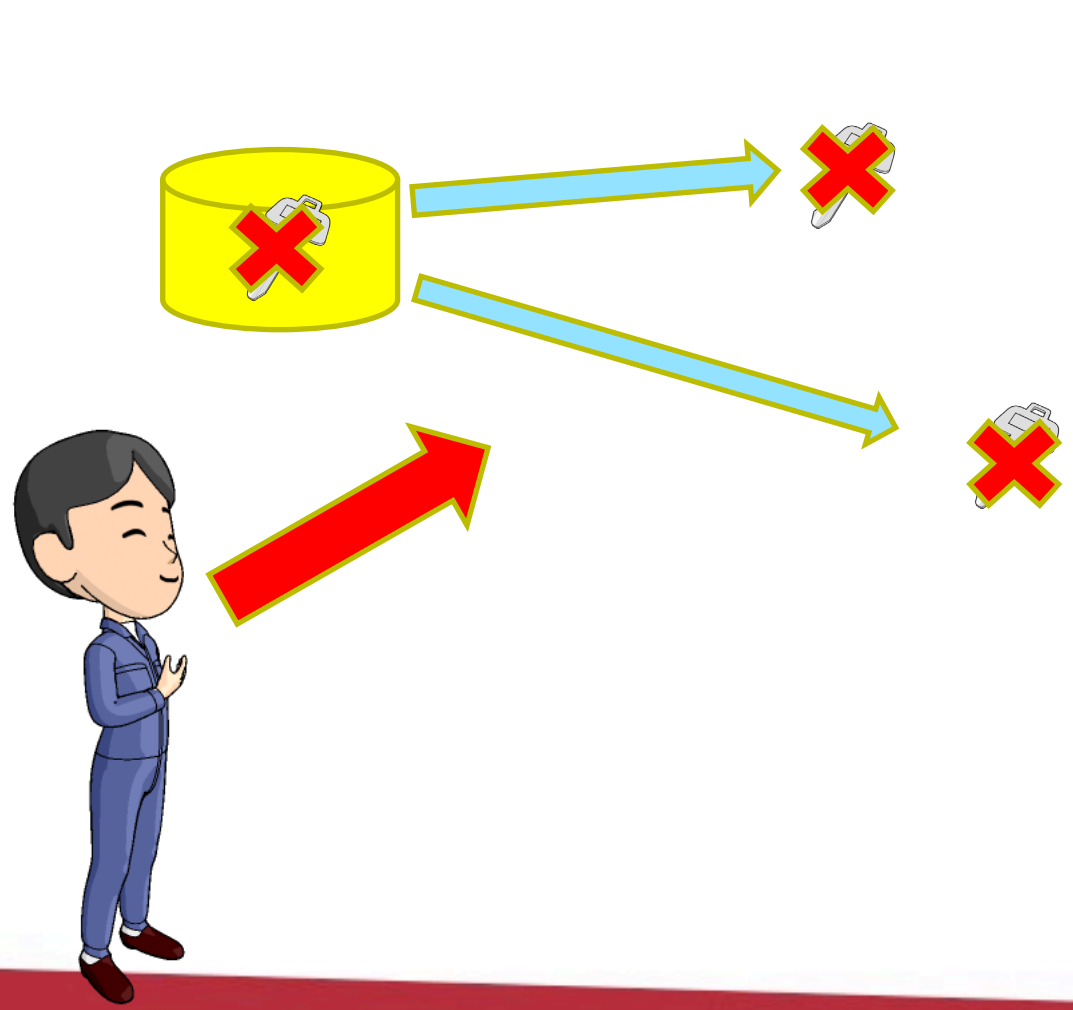
- 脆弱な乱数生成をしてしまう



- 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



鍵のバックアップ問題（合鍵問題）



システム管理上
データ滅失は脅威なので
鍵のバックアップは
多く取られがち
→鍵管理が重要

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?

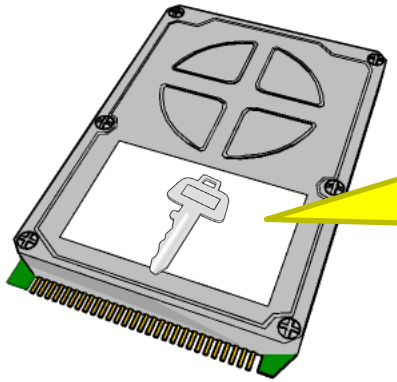
鍵管理を楽にする方法は
物理媒体に鍵を閉じ込め取り出せなくする

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

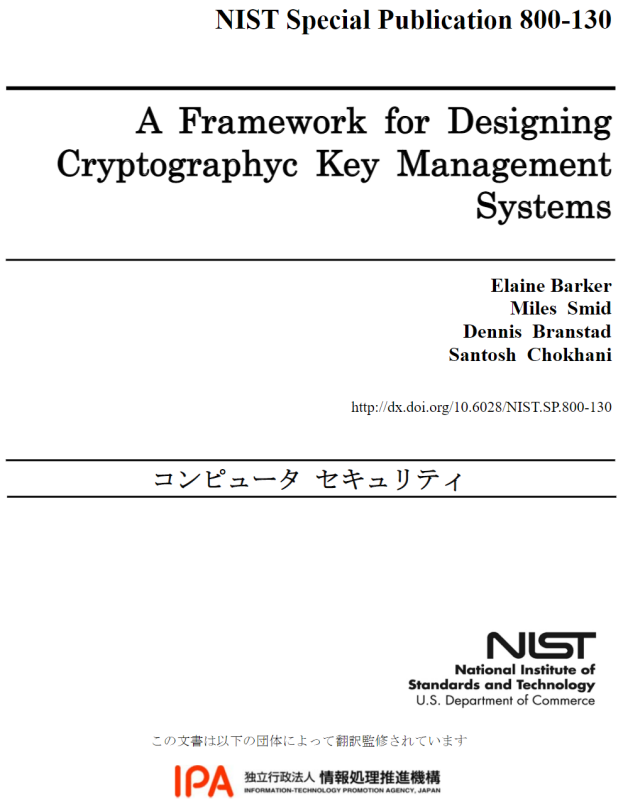
政府機関等のサイバーセキュリティ対策

- 政府機関等の対策基準策定のためのガイドライン（令和３年度版）
  - 基本対策事項3.1.1(7)-1「返却時の情報の抹消方法」について返却時の情報の抹消方法として暗号化消去を採用する場合は、**OSやハードウェアの機能により、電磁的記録媒体へ書き込まれる情報が自動的に暗号化されるように設定された端末やサーバ装置等を導入し、運用の全期間を通じて暗号化**することが前提となる。

残る問題は鍵管理

- 基本対策事項3.1.1(7)-1続き：
  また、暗号化された情報の復号に用いる鍵については、遵守事項6.1.5(1)(b)(エ)で策定を求めている管理手順に従って適切に管理するとともに、暗号化消去を行う際にはバックアップも含め鍵を確実に消去することが重要である。
- 遵守事項6.1.5(1)(b)(エ)「管理手順を定めること」について暗号化された情報の復号又は電子署名の付与に用いる鍵（以降本条において「鍵」という。）の管理手順として、**CRYPTRECが発行している「暗号鍵管理システム設計指針（基本編）」**を参照しつつ、以下の視点を含む鍵のライフサイクルを考慮した管理手順を策定するとよい。

暗号鍵管理のガイドライン


NIST Special Publication 800-130

A Framework for Designing Cryptographyc Key Management Systems

Elaine Barker
Miles Smid
Dennis Branstad
Santosh Chokhani

http://dx.doi.org/10.6028/NIST.SP.800-130

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

NIST SP800-130は
暗号鍵管理システムの
設計書に指定すべき
ことを包括的に記した
フレームワーク

暗号鍵管理システム
設計指針（基本編）は
このSP800-130の
解説書

暗号化消去と暗号鍵管理システム

- 「鍵のライフサイクル管理」の一部を使う
  （非活性化・一時停止は不要）
- 「失効リスト」
  （危殆化した鍵のリスト）
  なども不要

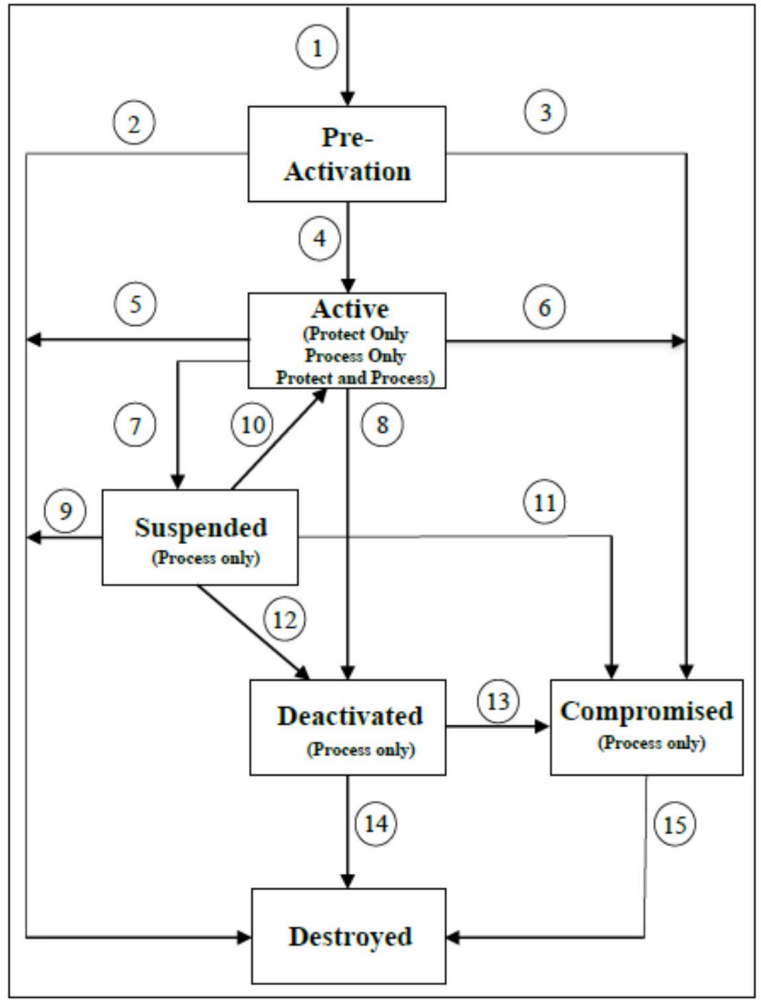
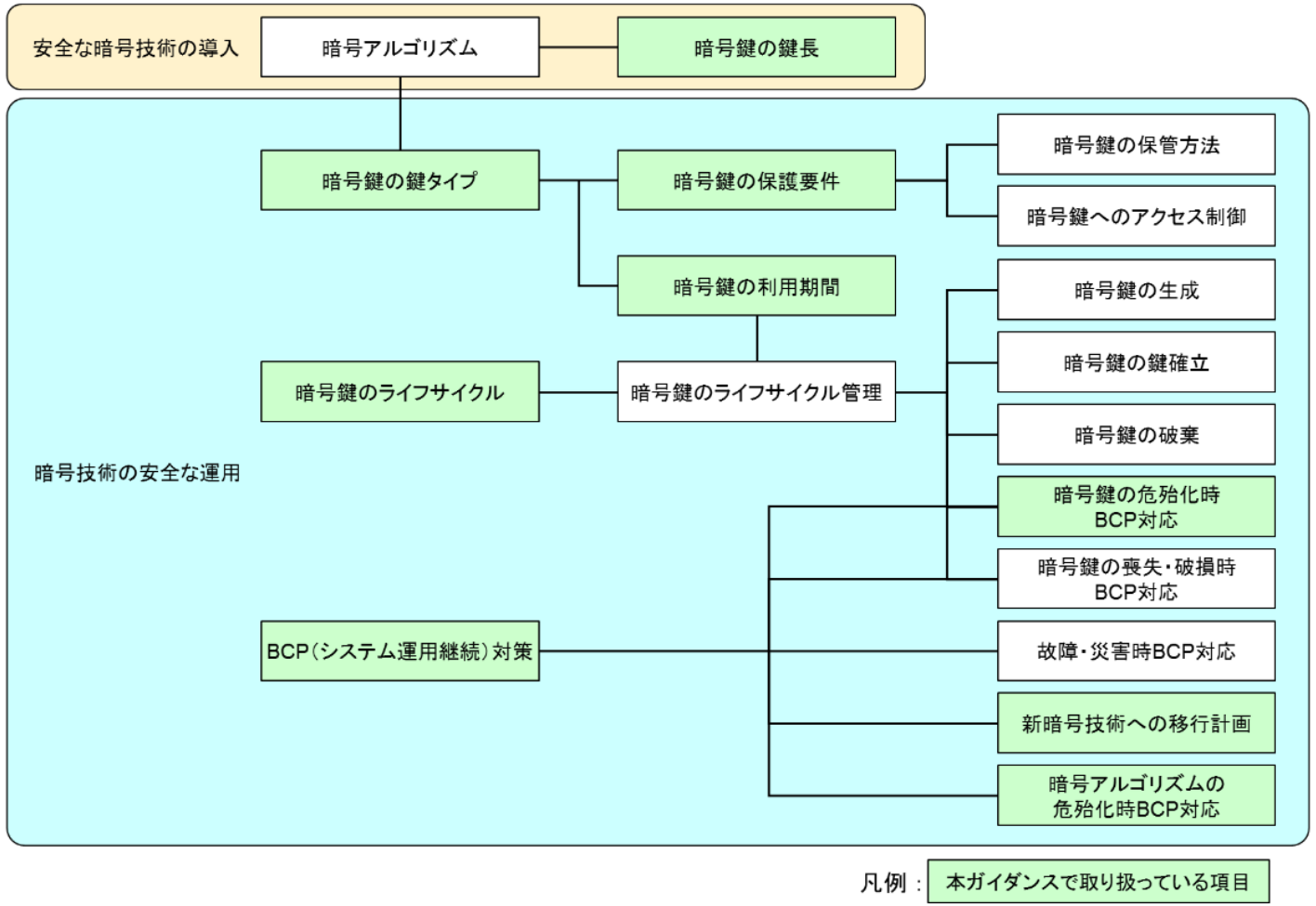


図 5-1　鍵状態及び遷移の例（SP800-57 Part 1 revision 5 より引用）

暗号鍵設定ガイダンスと暗号化消去

- **CRYPTRECGL-3003-1.0「暗号鍵設定ガイダンス」**



- 鍵長選択
- 鍵のライフサイクル
- 鍵の利用期間
- 鍵の保護

について
ポイントを
まとめたもの
SP800-57も
簡単に解説

運用上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

残る問題は何か

- 暗号鍵がなくなっても
  データ自体が長く残る可能性

- 量子耐性
- 将来の新技術へのリスク

終わりに

- 運用上暗号化消去は必然になっている
  - ストレージの容量問題
  - クラウドの問題
- しかしNIST SP800-88rev.1にいう「破壊」(Destroy)同等とまでは認められていない
- 今後運用上どのように位置づけるか？
  その安全性をどう担保するか？