ADEC「データ消去ガイドブック」とは？

DoD（3回上書き）からNISTへ
～グローバル標準の採用～

2022年12月6日

ADEC（データ適正消去実行証明協議会）技術顧問

沼田 理

ADEC：Association of Data Erase Certification

https://www.adec-cert.jp

講師自己紹介

- 氏名：沼田　理　（ぬまた　まこと）
- 経歴
  - 電子部品、オーディオ関連企業、オランダPHILIPS社などで技術開発業務に従事。
  - 1986年より（株）ワイ・イー・データに於いて、FDD、HDD、テープドライブなど磁気記憶装置の設計開発に携わる。
  - 2001年：データ復旧のパイオニア、オントラック事業部に異動、
    2006年：事業部長。
  - 2010年～日本データ復旧協会事務局長、データ復旧関連複数社の顧問を歴任。
    技術情報、Web原稿の提供、
    IDF（デジタル・フォレンジック研究会）データ消去分科会メンバー
  - 2019年～ADEC（データ適正消去実行証明協議会）技術顧問
    KLDiscovery Ontrack社　技術担当広報
    （旧 Kroll Ontrack）

はじめに

2019年12月に発生した神奈川県の「HDD流出事件」に対応した、総務省の**「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改訂（2020年12月28日）**では、IT機器の廃棄時等に必要とされるデータの抹消方法を、従来の「データが復元できない状態にする」等の漠然とした表現から、「情報の機密度や媒体の種類など」によって「データの抹消方法」の適切な手段を選択・採用するように変更される等　データ抹消手段の基準として、**「NIST　SP800-88 Rev.1」準拠**の方法が明確に記載され、ADECの**「データ消去技術ガイドブック第2版」が技術的見解に関する参照資料とされました。**

また、来年に予定されているNISC（内閣サイバーセキュリティセンター）による「政府統一基準」の改訂にも協力しています。

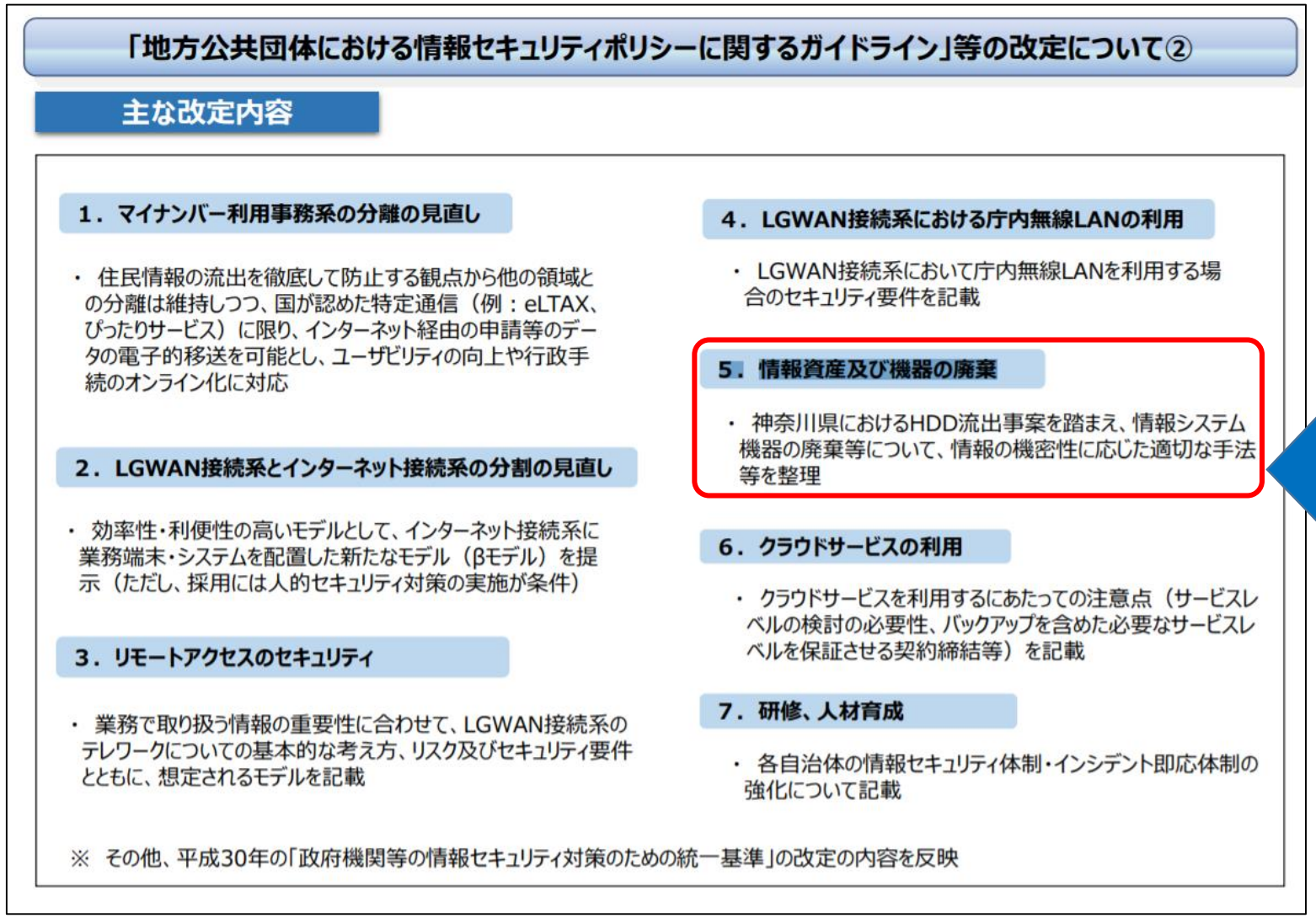
更に、2020年6月のISMAP管理規定に引き続き、2021年7月7日改訂の「政府統一基準（第3版）」で、クラウド環境に於ける情報セキュリティの手段として「暗号化消去」が記載されました。これも、ADECが基準としている「NIST SP800-88 Rev.1」に準拠したものです。

データ消去技術認証基準委員会は、周回遅れ状態にある日本の情報セキュリティ対策を、これからも牽引して行きます。

DoD（米国国防総省規格：3回上書き）からNIST（Purge）へ
総務省 地方公共団体向けガイドライン改訂
改訂の伏線（上原 哲太郎教授の2019・12・11 Twitter）

DoD（米国国防総省規格：3回上書き）からNIST（Purge）へ

地方公共団体向けガイドライン（総務省　2020･12･28）の改訂のポイント



神奈川県におけるHDD流出事案を踏まえ、情報システム機器の廃棄等について、情報の機密性に応じた適切な手法等を整理

DoDからNISTへ （総行情第 77 号）

NISTに従い

ADEC

ガイドライン改訂　機密レベルと抹消方法を3分類（令和2年5月22日）

総 行 情 第 ７７号
令和２年５月２２日

各都道府県情報セキュリティ担当部長
各指定都市情報セキュリティ担当部長　殿

総務省自治行政局地域情報政策室長
（　公　印　省　略　）

情報システム機器の廃棄等時におけるセキュリティの確保について

平素より、当室の業務に格段のご理解・ご協力をいただき誠にありがとうございます。

「地方公共団体における情報セキュリティポリシーに関するガイドライン」においては、情報システム機器を廃棄、リース返却等（以下「廃棄等」という。）をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置（以下「抹消措置」という。）を講じなければならないとされているところです。

先般、神奈川県において、リース契約等により返却した物品からの情報流出事案が発生致しましたことを踏まえ、「情報システム機器の廃棄等時におけるセキュリティの確保について」（令和元年12月６日総務省自治行政局地域情報政策室長）を発出し、住民情報等の重要情報が大量に保存された機器内部の記憶装置に係る抹消措置の具体的な方法に関して当面の措置を要請したところです。

その後、総務省においては、有識者も参画した「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会ワーキンググループ」の議論の結果等も踏まえ、改めて情報システム機器の廃棄等について、以下のとおりと致しましたので、各地方公共団体におかれては、適切な取扱いをお願い致します。

併せて、貴都道府県におかれては、貴都道府県内の市区町村（指定都市を除く。）及び一部事務組合等にも、この旨周知されるようお願いします。

記

1　基本的な考え方

情報システム機器を廃棄等する場合、機器内部の記憶装置からの情報漏えいのリスクを軽減する観点から、情報を復元困難な状態にする措置を徹底する必要があること。この場合、一般的に入手可能な復元ツールの利用によっても復元が困難な状態とすることが重要であり、ＯＳの初期化、および記憶装置の初期化（フォーマット等）による方法は、ＨＤＤの記憶演算子にはデータの記憶が残った状態となるため、適当でないことに留意が必要である。

2　取り扱う情報の機密性に応じた機器の廃棄等の方法について

機器の廃棄時における措置にあたっては、当該機器内部の記憶装置に記録される

情報の機密性に応じて、原則として、以下を参考に適切な廃棄等の方法を検討するとともに、作業を外部委託する場合（リース企業に行わせる場合も含む。）は、確実な履行を担保する方法を検討すること。

分類	機器の廃棄等の方法	確実な履行を担保する方法
（１）マイナンバー利用事務系の領域において住民情報を保存する記憶媒体 ※　マイナンバー利用事務系：[illegible]	当該媒体を分解・[illegible]・溶解・焼却・細断などによ[illegible]に破壊し、確実に復元[illegible]とすること[illegible]が適当である。 なお、対象と[illegible]について、リース契約によ[illegible]場合においても、リース契約終了後、当該機器の記憶媒[illegible]については[illegible]に破壊[illegible]に明記のうえ、機器の廃棄[illegible]約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述（３）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行[illegible]る。当該完了証明書については、破壊の[illegible]とが望ましい。
（２）機密性２以上に該当する情報を保存する記憶媒体（上記（１）に該当するものを除く。）	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃から[illegible]レベルで抹消を行う[illegible]である。 具体的には、[illegible]物理的な方法による破壊、②磁気的な方法による破壊、③ＯＳ等から[illegible]が不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェ[illegible]による上書き消去、④ブロック[illegible]、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	庁舎内において後述（３）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
（３）機密性１に該当する情報を保存する記憶媒体	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。 具体的には、（２）[illegible]した方法①～⑤のほか[illegible]からアクセス可能な全ての[illegible]領域をデータ消去装置又は[illegible]消去ソフトウェアによ[illegible]消去する方法がある。 ＯＳの初期化、および記憶装置の[illegible]ＨＤＤの記憶演算子[illegible]記憶が残った状態となるため、適当ではない。	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。

① マイナンバー利用事務系
機密度3：デストロイ（破壊）

② 機密性2：パージ（除去）

③ 機密性1：クリア（消去）

3　補足事項

①　データの消去方法の選択に当たっては、コンピュータ技術の変化にも留意する必要がある。例えば、SSD については、製造者のみが管理する領域等が存在することから、消去のコマンドが期待どおりに実行されるかは、製造者との信頼と保証に頼らざるを得ないとの指摘がされている点に留意が必要である。

②　マイナンバー利用事務系の情報を扱う基幹系システム等については、いわゆる自治体クラウド等、クラウドを利用している場合であっても、その情報資産を廃棄する場合は、原則として当該情報資産が取り扱われる機器を原則として物理的に破壊することが適切である。（現状の自治体クラウドにおいては、ハウジングのケースが多く、サーバ等の機器を管理する区域が明確な場合も多いと想定され、サービス提供終了後に機器を物理的に破壊することも可能と考えられるが、それ以外のサービス利用形態等におけるサービス利用終了後のデータの抹消について、物理的な破壊が困難な場合のデータの抹消の在り方については、別途検討が必要。）

4　「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会ワーキンググループ」における検討の概要や関係ガイドライン等を別紙のとおりまとめているため、適宜参考とされたい。

連絡先：自治行政局地域情報政策室
安達、権藤、池田、西口
ＴＥＬ：03-5253-5525（直通）
ＦＡＸ：03-5253-5530
E-mail：lg-security@soumu.go.jp

DoDからNISTへ

NISTに従い

ガイドライン改訂　媒体により区別

【参考】ハードディスク装置とSSDによる消去方法等の相違

	Clear(消去)※1	Purge(除去)※1	Destroy(破壊)※1
ハードディスク装置（HDD） **HDD**	データ消去装置、データ消去ソフトウェアを利用してOS等からアクセス可能な全てのディスク領域を上書き消去する	データ消去ソフトウェアやデバイス専用のコマンド（Secure Erase）を使用して上書き消去（OS等からのアクセスが不可能な領域※2も含めて上書き消去）・暗号化消去する。または、磁気消去を行う。	物理的破壊装置により、再使用不可能になるように破壊する。
SSD **SSD**	データ消去装置、データ消去ソフトウェア、デバイス専用のコマンドを使用してOS等からアクセス可能な全ての領域を上書き消去する	デバイス専用のコマンドやデータ消去ソフトを使用してブロック消去（データが残される領域等含め）する。	物理的破壊装置により、再使用不可能になるように粉砕・破壊する。

※1 データ抹消方法の定義（NIST SP800-88Rev.1）
・「Clear(消去)」：一般的に入手できるツールを利用した攻撃に対して耐えられること。
・「Purge(除去)」：研究所レベルの攻撃に対して耐えられること。
・「Destroy(破壊)」：媒体の再生（再組立等）に対して耐えられること。
※2 OS等からのアクセスが不可能な領域：
ユーザデータ領域（リカバリ領域、クリップ領域）及び再割り当て済みセクタにデータが残存している場合。ソフトウェアでは読みだし不可能であるが、データ復旧やデジタル・フォレンジックを行う機器等を用いることによりデータにアクセスすることは可能。

上記の消去方法の技術的な見解に関する参照資料
・「データ消去技術 ガイドブック 第2版」データ適正消去実行証明議会
https://adec-cert.jp/guidebook/index.html

4

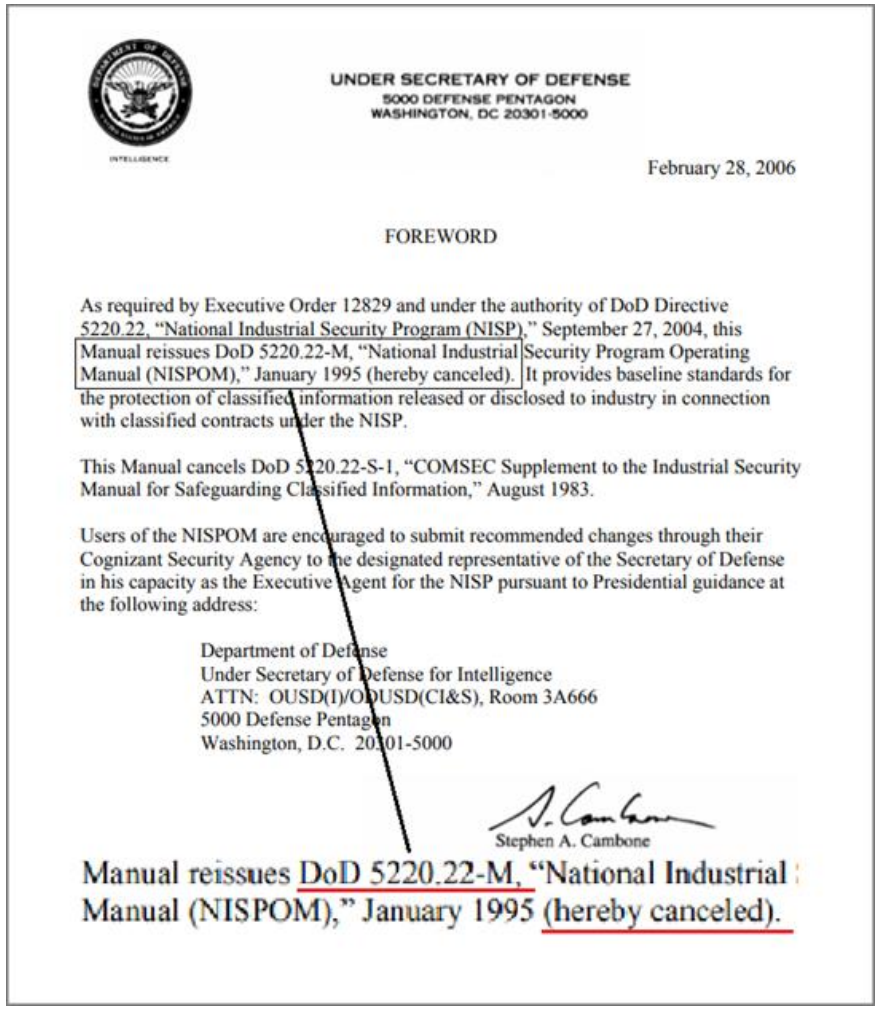
データ抹消方法は
NIST SP800-88rev.1
を参照して媒体種類別に定義

ADECの
「消去技術ガイドブック」を
技術的見解の参照資料として紹介

DoDからNIST SP800-88Rev.1へ

（IDFデータ消去分科会のレポートから）

DoD（米国国防総省：3回上書き）は過去の物！



UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

February 28, 2006

FOREWORD

As required by Executive Order 12829 and under the authority of DoD Directive 5220.22, "National Industrial Security Program (NISP)," September 27, 2004, this Manual reissues DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," January 1995 (hereby canceled). It provides baseline standards for the protection of classified information released or disclosed to industry in connection with classified contracts under the NISP.

This Manual cancels DoD 5220.22-S-1, "COMSEC Supplement to the Industrial Security Manual for Safeguarding Classified Information," August 1983.

Users of the NISPOM are encouraged to submit recommended changes through their Cognizant Security Agency to the designated representative of the Secretary of Defense in his capacity as the Executive Agent for the NISP pursuant to Presidential guidance at the following address:

Department of Defense
Under Secretary of Defense for Intelligence
ATTN: OUSD(I)/ODUSD(CI&S), Room 3A666
5000 Defense Pentagon
Washington, D.C. 20301-5000

Stephen A. Cambone

Manual reissues DoD 5220.22-M, "National Industrial
Manual (NISPOM)," January 1995 (hereby canceled).

出典：National Industrial Security Program Operating Manual　DoD 5200.28-M 2006年Feb.26

1973年：

現在においての標準的とも言える、
「DoD 5200.28-M」3回上書き方式を提唱

1995年：

上書3回（固定値、補数、乱数、その後検証を実施）方式を発表

2006年2月：

データ消去の具体的な
方法等の記載を取り消し。

NIST SP800-88

2006年　NIST SP800-88（初版）

- **「2001年以降に製造された15GB 以上のATAディスクに対し、上書き抹消を行う場合の上書き回数は1 回で十分」**と、明記。

  理由：大容量化による下層データのはみだし幅の微小化）

  参考：1TB/プラッタの物理的寸法（TDKヘッド工場による）

  トラック間隔：70nm、書込み幅：55nm、ビット長：約10nm

  読み出し幅　：35nm、トラッキング要求精度：8nm

- **ATAコマンドの「Secure Erase」を、HDDの全領域の消去が可能であり最高機密の機密情報に対する抹消手段として容認。**

NIST SP800-88Rev.1

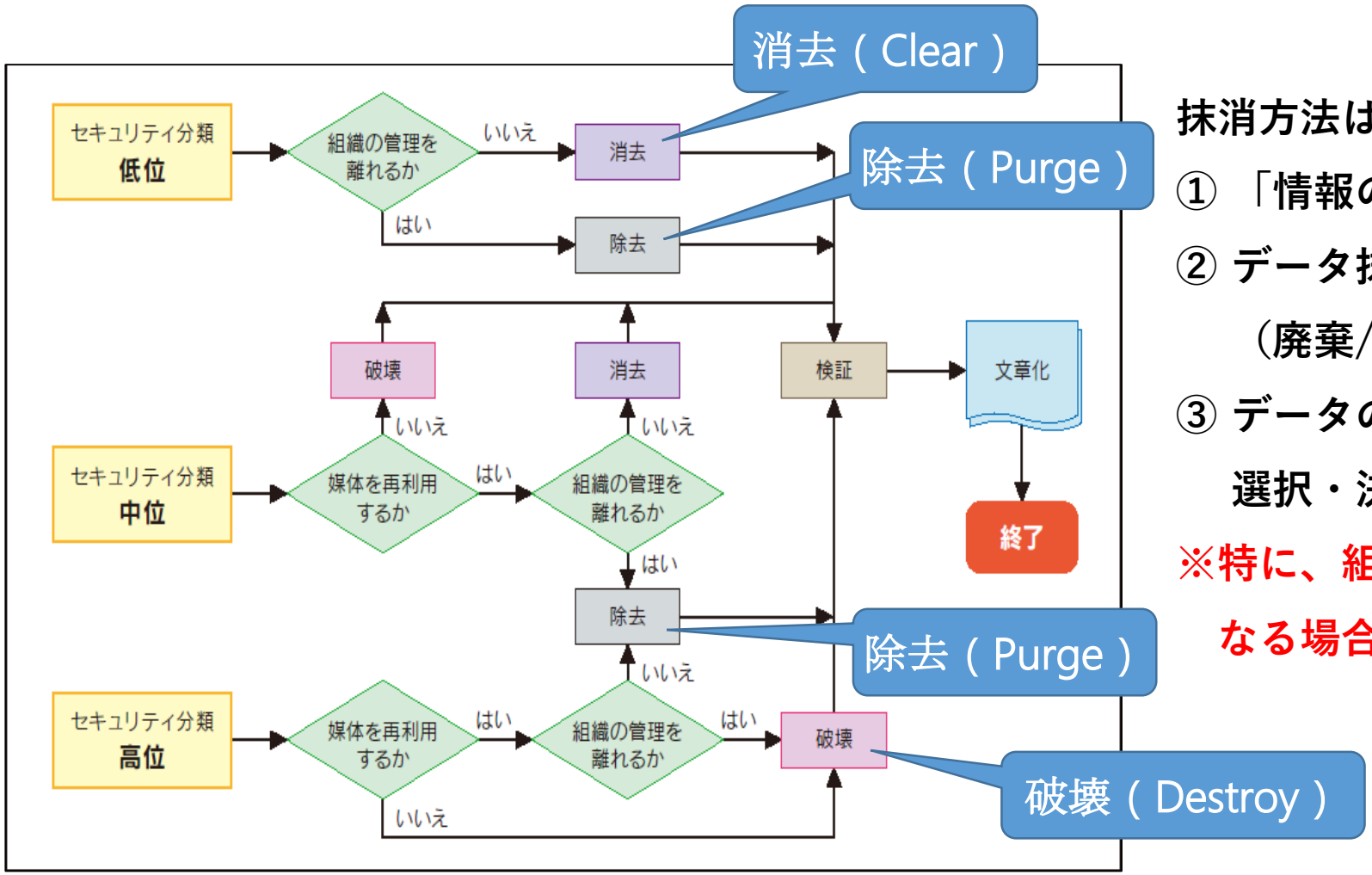
2014年12月　SP800-88rev.1（最新版）

・ **Secure Eraseを含む上書き消去を**、電子記憶媒体には製造者のみが管理可能な領域が存在し、その領域に対するアクセス手段は存在しないことを理由に、**最高機密に対する抹消手段から除外**。

・**暗号化消去（Cryptographic Erase：CE）**、SSD、**スマホ等**を追加

2021年11月24日にIPAが和訳を公開！
https://www.ipa.go.jp/files/000094547.pdf

NIST SP800-88Rev.1
リスク判定と抹消手段の選択基準



抹消方法は、

① 「情報の機密度」と、

② データ抹消後の「記憶媒体の管理（廃棄/再利用）」を勘案して、

③ データの所有者・管理者の責任で選択・決定する。

※特に、組織の管理が行き届かなくなる場合に注意する。

注：米国政府・行政機関向けの判断基準を示す。

出典：NIST「SP800-88 Rev.1 Guidelines for Media Sanitization」、「Sanitization and Disposition Decision Flow」

NIST SP800-88Rev.1
3段階の情報の機密レベル

①. 高度：情報が漏えいした場合、危機的・致命的な悪影響を及ぼすレベル
・総務省：地方公共団体向け情報セキュリティポリシーガイドライン
機密性3：マイナンバー利用事務系に関する情報システム及びデータ
（社会保障、地方税、防災、戸籍事務等）

②. 中度：情報が漏えいした場合、重大な悪影響を及ぼすレベル
・総務省：地方公共団体向け情報セキュリティポリシーガイドライン
機密性2：行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、
直ちに一般に公表することを前提としていない情報資産

③. 低度：情報が漏えいした場合の影響は限定的なレベル
・総務省：地方公共団体向け情報セキュリティポリシーガイドライン
機密性1：機密性2またはマイナンバー利用事務系の情報資産以外の情報資産、公開情報

SP800-88Rev.1による抹消方法：Clear（消去）

・記憶媒体上の「OSが認識できる領域」のデータを抹消。

HDD：OS上で無意味なデータを1回以上の上書き（**DoD 5200.28-M**）、など。

SSD：HDDと同一の上書きが代表例だが、SSDのデータ書込みは、書込み可能なページにデータを書き込み、LBAを後から割り当てる方法（リマップ）であるため、**ファームウェアで設定された動作上の都合で、一部にデータが残存してしまう現象が見受けられる**ため、**上書きを複数回とすることが必要**。（**ADECのソフトウェア検証作業で確認済**）

注：SATAの場合は、Secure Eraseコマンドを使用する。（Enhancedモード以外のSecure Eraseでは、オーバ・プロビジョニング等にデータが残存することを認めているので、NISTではSSDに対するPurgeに適合するコマンドとしては認めていない）

LBA（論理アドレス）を持たない、システム動作で使用する領域

SP800-88Rev.1による抹消方法：Purge（除去）

・記憶媒体上の「あらゆる領域に書き込まれたユーザデータ」を抹消。

HDD：指定されたインターフェイス規格に従った**コマンドによる消去。**

外部から磁界を印加する**磁気消去装置**の利用、**暗号化消去。**

SSD：指定されたインターフェイス規格に従ったデータ抹消専用**コマンドによる消去。暗号化消去。**

注：SSDに対する磁気消去は全く有効ではない。

	SATA	SAS/SCSI	NVMe
SSD	Block Erase	SCSI SANITIZE	NVMe Format NVMe SANITIZE
HDD	Enhanced Secure Erase	SCSI SANITIZE	――

Purgeでも、特殊な設備と特殊な技能があってようやくデータのカケラが見つかるか見つからないか程度であり、狙ったデータの窃取につながることはない。

上原 哲太郎

2014には存在しなかった「NVMe SANITIZE」も同等の機能を持っている。

SP800-88による抹消方法：Destroy（破壊）

- **記憶媒体を破壊し、あらゆる領域の、あらゆるデータを抹消する。**

HDD：手段：物理的な破壊を行う。

注：磁気的な消去（上書きを含む）を伴わない場合にプラッタ（磁気円盤）から直接データを読み出す技術は存在する。　**但し、データ復旧やデジタルフォレンジックを目的に、そのようなサービスを提供している業者は世界中でも存在しない。NSA/CSS POLICY MANUAL 9-12**では、**磁気的な処置を伴わない場合、プラッタを2mm角以下にする事を求めている。**（２mm角は上記規格を決定した時点でのプラッタ上の1セクタ（512Bytes）の物理的長さ）

SSD：手段：物理的な破壊を行う。

注１：**HDDに対する、穿孔、V字折曲げ等はSSDに対して全く無効。**（基板からメモリICを取り外し、専用の読出し装置を使用するとデータは読み出すことができる）個々の**ICを全て通電動作不能になるまで破壊する**。

注２：NAND型フラッシュメモリは、ICの封止樹脂を取り除き、IC上に存在する記憶素子であるセルに書き込まれているデータをビットレベルで読み出す技術は存在する。**但し、データ復旧やデジタルフォレンジックを目的に、そのようなサービスを提供している業者は世界中でも存在しない。**
NSA/CSS POLICY MANUAL 9-12では、2mm角以下の寸法にする事を求めている。

Destroyつまり物理破壊は、軍事機密のような、どんなにコストをかけてでもデータを取り出したいような相手がいる状況での基準。

上原 哲太郎

物理的破壊に対するガイドライン

物理的な破壊、外部磁気等による国家機密レベルのデータ抹消の規定として、アメリカのNSA/CSS（National Security Agency：国家安全保障局/ Central Security Service 中央保安部）による POLICY MANUAL 9-12が存在する。

注：（2006年のDoDの取り消し、NIST SP800-88の発表と同時に設定されている）

最新版：

- Storage Device Sanitization and Destruction Manual, December 2020
- NSA EPL Hard Disk Drive Destruction Devices, Oct. 2022
- NSA EPL Magnetic Degaussers, Oct. 2022
- NSA EPL Optical Destruction Devices, Oct. 2022
- NSA EPL Paper Disintegrators, Oct. 2022
- NSA EPL Paper Shredders, Oct. 2022
- NSA EPL Punched Tape Disintegrators, Oct. 2022
- NSA EPL Solid State Disintegrators, Oct. 2022

※ https://www.nsa.gov/Resources/Media-Destruction-Guidance/NSA-Evaluated-Products-Lists-EPLs/からダウンロード可能

物理的破壊及び磁気消磁装置のガイドライン NSA/CSS 9-12 の要点

1. NSA EPL Hard Disk Drive Destruction Devices より抜粋

- ハードディスクドライブ破壊装置は単独で使用した場合、磁気ストレージ機器に対するデータ抹消には相当しません。**磁気消磁装置と組み合わせて使用した場合にのみハードディスクドライブのデータ抹消として認められます。**
- **粉砕は、NSA / CSSの9-12ストレージデバイスのデータ抹消マニュアルの指示に従い、プラッタが2ミリメートル角以下のサイズを達成することが無ければ、データ抹消には相当しません。**

2. NSA EPL Magnetic Degaussersより抜粋

- すべてのハードディスクドライブ内の**プラッタを変形させる物理的な破壊を併用することを強く推奨**します。
- **機器の継続的な性能は保証されません。**製造元に従って、またはNSA / CSS承認済みの磁場検証装置を使用して、機器を再テストする必要があります。

3. NSA EPL Solid State Disintegratorsより抜粋

- 機器の評価は、**粉砕後の長辺の最大値が2㎜以下**であることを条件としています。

物理破壊上の注意

HDDには、そのHDD自体が使用するファームウェア等を収納しているシステムエリア（SA）と、更に製造元のみがアクセス可能な、余剰な領域が存在する。それらに対する（上書き）消去は不可能であり、この部分を含めすべての領域に対する抹消は、技術論的にも読み出しを不可能にすることを目的とする。
物理破壊＝裁断・粉砕・溶解（NIST SP800-88Rev.1）

注意点１．上書き消去が1回で良いとされている理由は、上書きされた部分から以前に書き込まれたデータのはみ出す可能性を持つ幅が、現在の技術では読み出し不可能な程狭いことが理由であり、**上書きが行われていない場合は、**プラッタが物理的な損傷を受け、破砕されても、その**破片から現在存在する技術で読み出すことが出来る**ことを否定していない。これにより、**完全なデータの抹消を求めるのであれば、物理破壊・破砕においても事前処理として、外部磁界による消去や、上書き消去を行なうことが必要**である。

注意点２．製品（HDD）によっては、**3.5インチの筐体に2.5 インチのプラッタ（円盤）を組み込んでいるものも存在**する、またそうでないものに於いても穴の場所（破壊の方法）によってはプラッタ（記録円盤）に損傷を与えることが出来ない可能性や、**複数枚の最下層（現時点では10枚）まで破壊出来ない可能性**が存在し、**外観だけで確実な処理が実行されたという判定が困難**である。

SSDの物理破壊（最近の事例） on Twitter！

外装難ありSSDが入荷！！
フォーマット済み
とりあえず動いてます。

激安価格！数量限定！無保証！
128GB 1,380円
256GB 2,480円
512GB 3,780円
など他の容量もございます。

なくなり次第終了です。
購入はお一人様2個まで
レジカウンターにお尋ね下さい。

SSDにはSSD専用の物理破壊機が必要です。（ICチップの破壊が必要）

外部磁気消去は？

１）十分な外部磁界が印加されたのか否かの判定が不可能である。

外部磁界の印加によって機器自体（スピンドルモータ、磁気ヘッド）が動作不能になってしまうことが多く、また、動作する場合に於いても、プラッタ上のデータが、現存するあらゆる技術を用いても全く**読み出し不能な状態に消去されたのか否かを容易に確認することはほぼ不可能**である。

２）印加磁界に変動要因が存在する

①磁界を発生させるための電磁石の**コイルの銅線の抵抗は、1℃当たり約0.4%の割合で上昇**するため、仮に**20℃から60℃まで上昇した場合には約16%磁界が減少**するので、機器（コイル内部）の温度管理等も必要である。

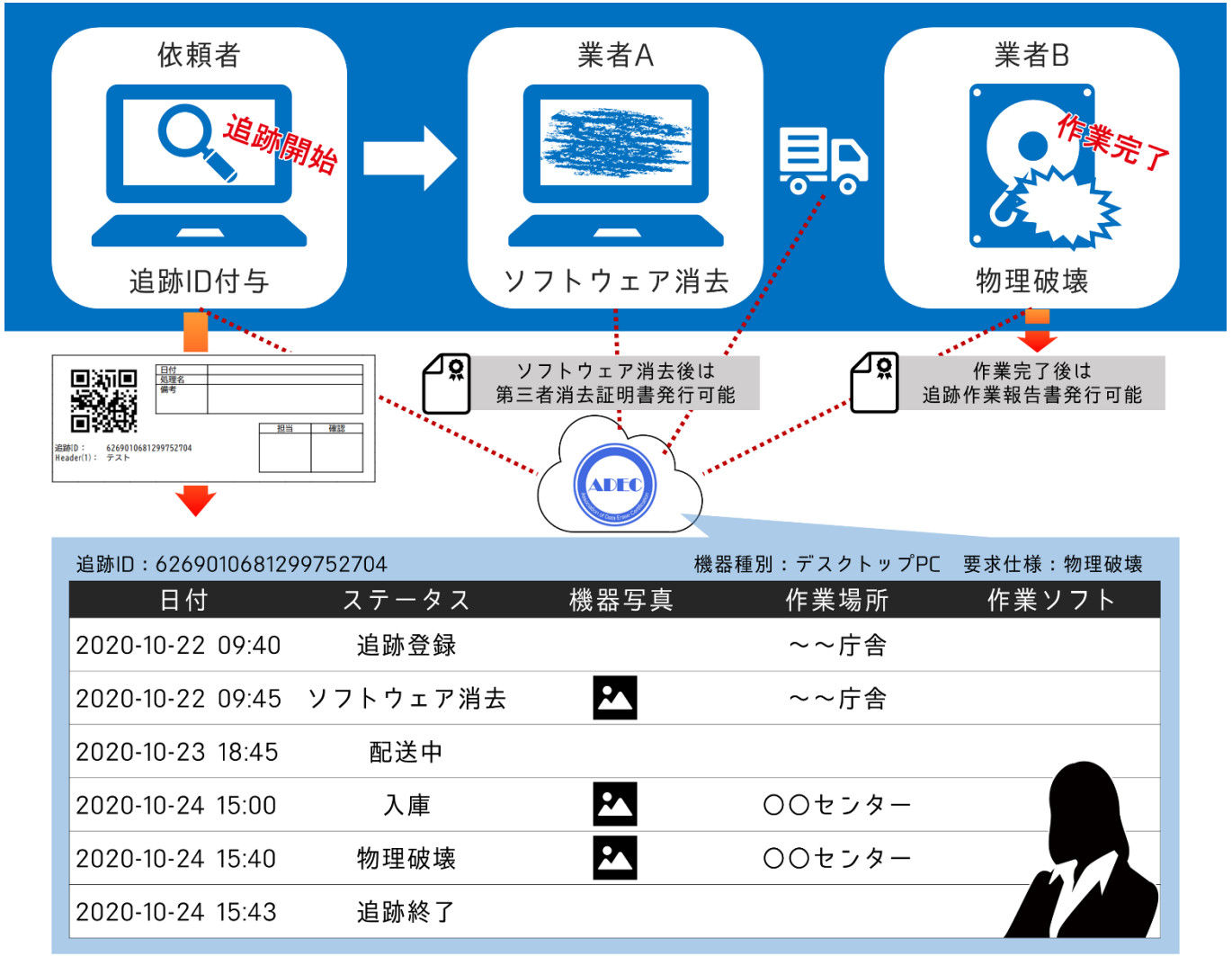
②コンデンサに対する充電時間の確保機能
パルス印加等の方式を採用している場合が多く、高電圧を必要とするため内部の昇圧回路を利用してコンデンサに充電をしているので、充電時間（放電エネルギー）管理が必要である。

③**コンデンサは、構造上急速な充放電による劣化が激しい**ので、定期的な性能の確認検査が行われていなければ性能の保証は出来ない。

上記により、**印可磁界の管理が必須**であり、また**十分にマージンを有する設計性能が要求され、信頼できる組織によって最新のHDDのデータ抹消に対する有効性を認められている機器が稀（日本製のNSA認証済み機器は、１社、1機種のみ）**であり、機器の信頼性に欠ける。

注：最近サンプル出荷されている、「20TBを超えるエネルギーアシスト型HDD」やSSDには役に立ちません。

総務省ガイドラインに従った
ADECの一元管理システム：ETTMS（エトムス）



情報機器を廃棄する際の対応として、適切な【廃棄措置（データ抹消）】と【廃棄手順の記録・管理】を行うことが推奨されていますが、現状、このガイドラインに則った運用体制にするにはいくつかの課題が発生します。

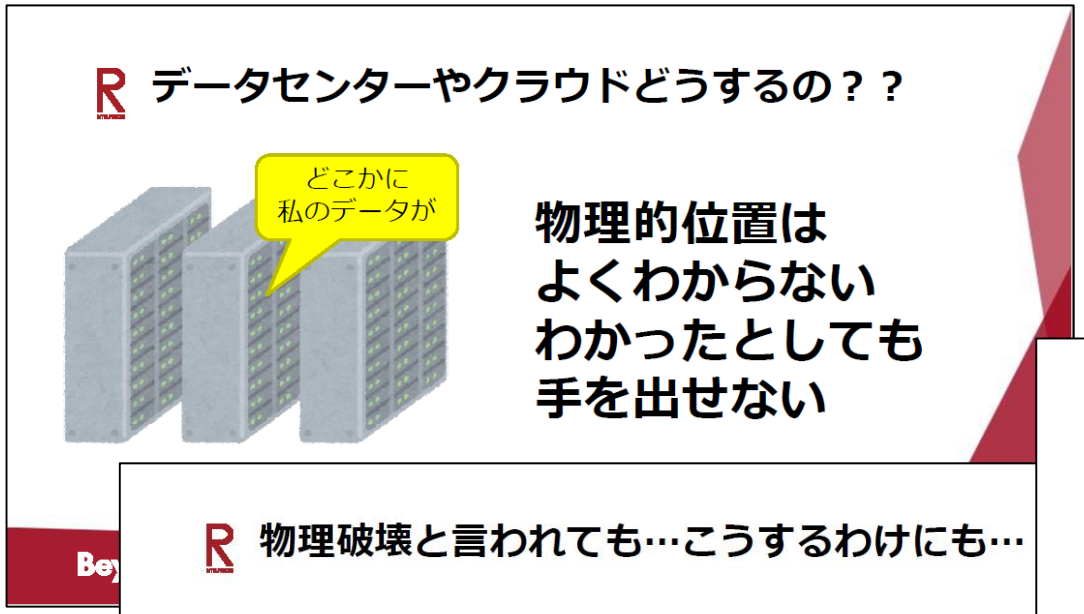
ADECでは、PCが手元を離れた時から廃棄処理が完了するまで、すべての作業工程をの管理する事のできるシステムを準備しています。

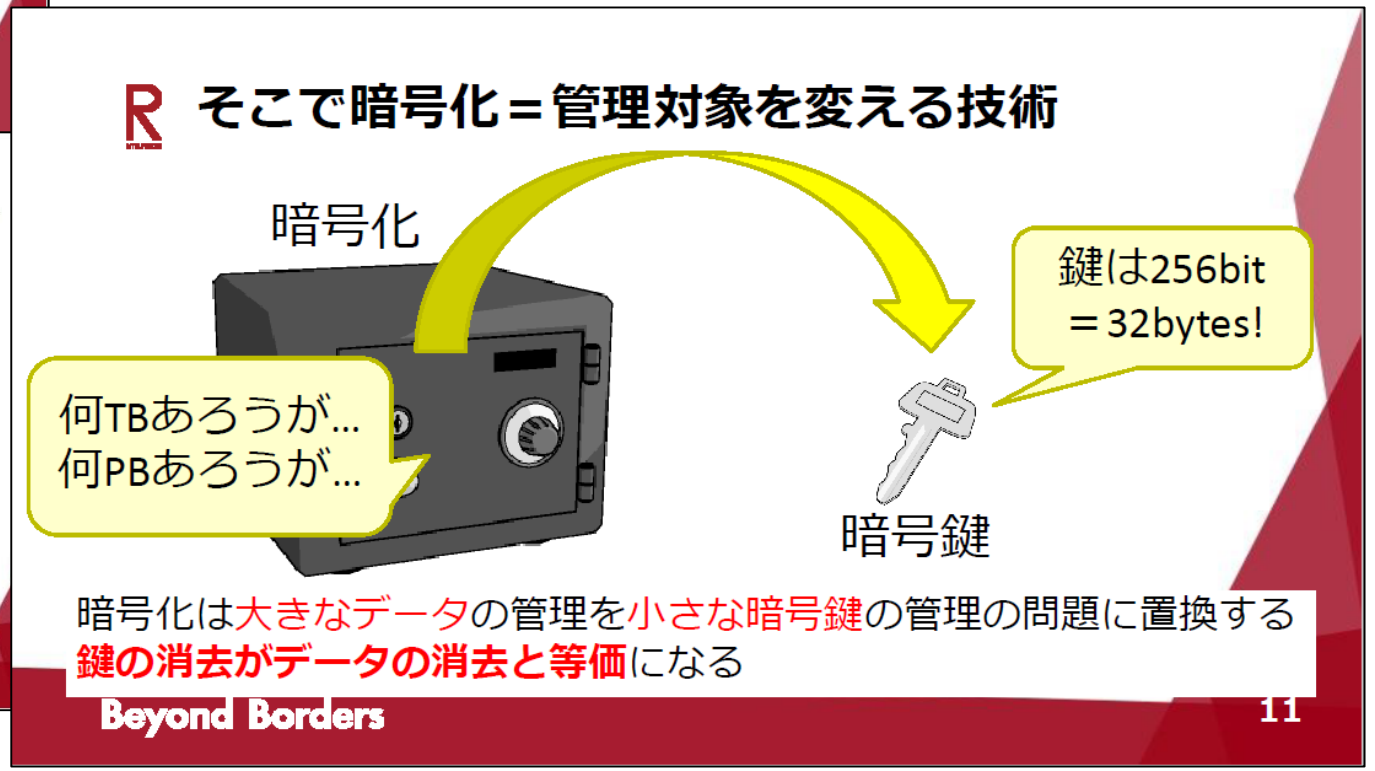
本システムを使用することにより、消去依頼をした機器情報を一括で　管理する事が可能になります。

追跡IDを使ってリアルタイムに機器情報を追跡できるため、今まで以上に安心して消去依頼を委託することができます。

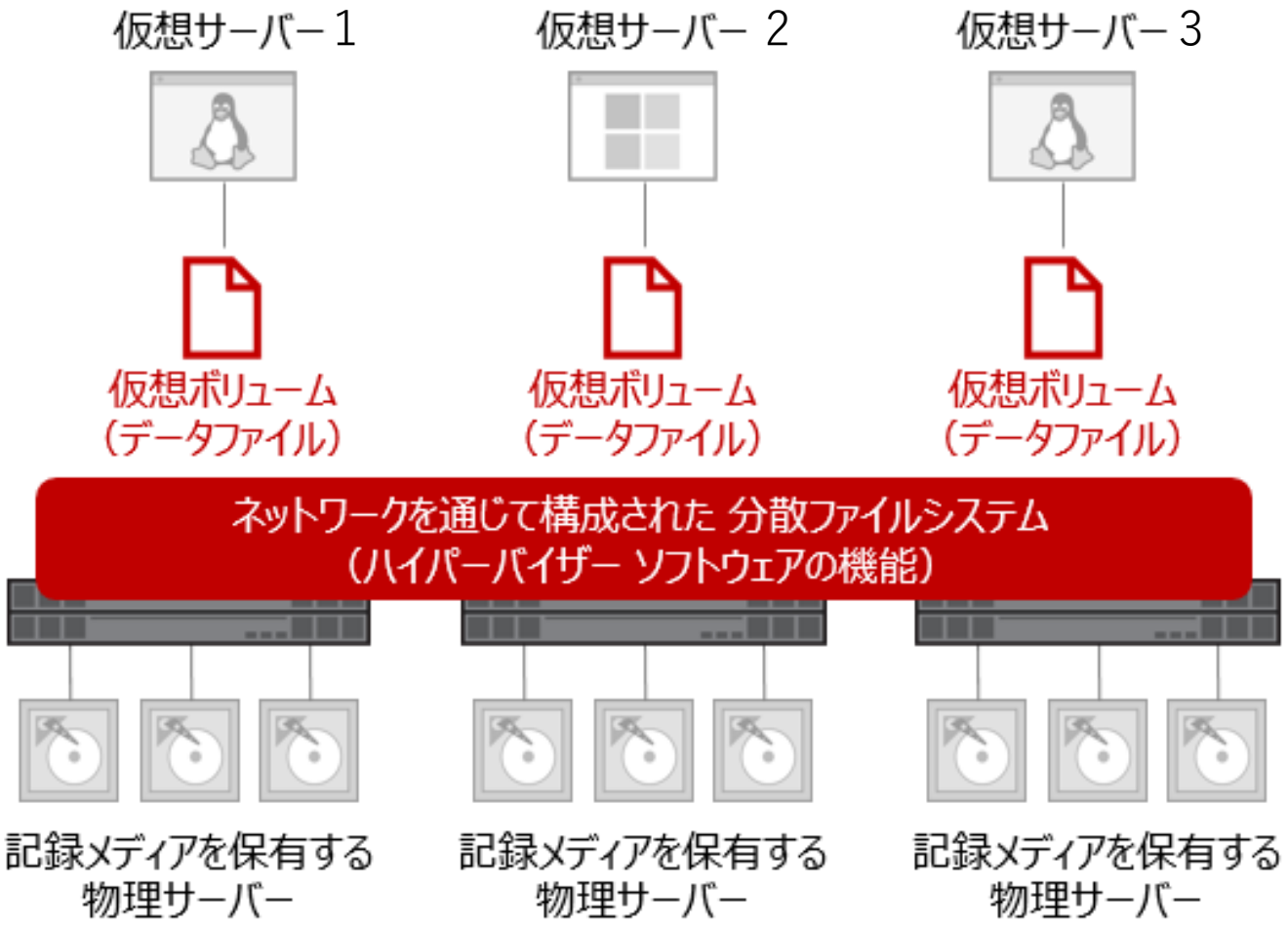
クラウドやデータセンターのデータ抹消
クラウド・バイ・デフォルト原則やISMAPはどうする？

2022年6月16日 DBSC 春のセミナー
「クラウドデータベースの完全消去を考える」
「暗号化消去の原理とリスク」
　　上原哲太郎氏プレゼン資料より抜粋





クラウドやデータセンターのデータ抹消
仮想ボリュームの構造

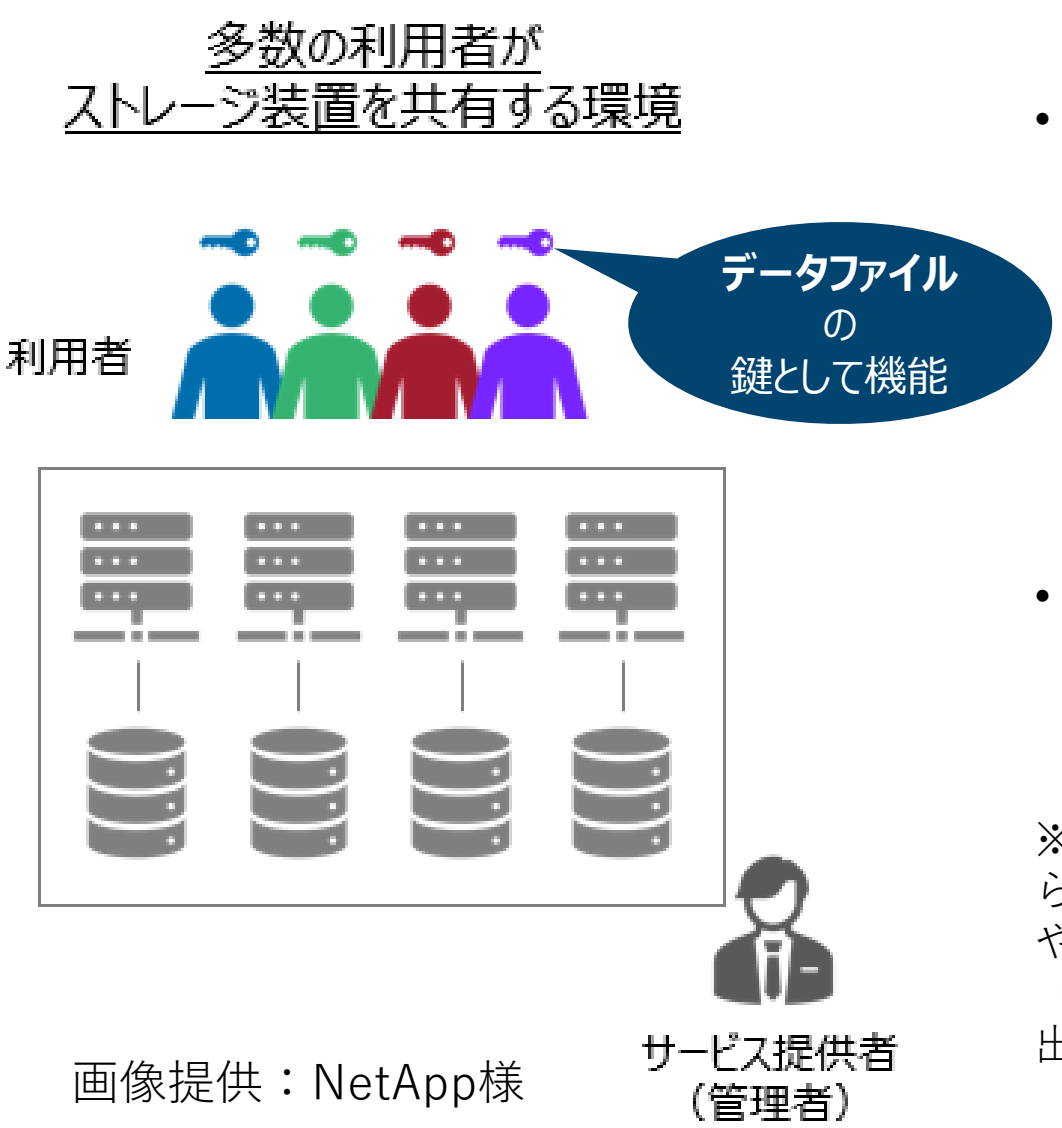


画像提供：NetApp様

•仮想ボリューム

- サーバー ハードウェアの性能向上に伴い、 1台の物理的なサーバーを、 ソフトウェア（ハイパーバイザーとゲスト）により仮想的に複数のサーバーに分割して利用することが一般的です。（仮想環境）
- **仮想ボリュームは、ハイパーバイザ上に構成された「データファイル」**です。
- Purge（除去）レベルのデータ抹消を実現する場合は、バッドセクタ処理等により、OS経由でアクセス不能となった領域に存在するデータの抹消も要求されるため、全ての記録媒体を取り外し、個別にPurge対応のデータ抹消作業を行うことが必要です。

クラウドやデータセンターのデータ抹消（解決策）



画像提供：NetApp様

「暗号化消去」がベストソリューション！

- 「暗号化消去」とは、「データの暗号化と復号のための暗号鍵の廃棄」、という方法で、論理ボリュームや仮想ボリュームに格納されるデータ全てを、予め暗号鍵を用いた暗号化を行い、仮想ボリュームが不要となった場合に、暗号鍵だけを抹消・廃棄することにより、**記録媒体上のOSでは認識できない領域も含む、あらゆる暗号化データの復号を非現実的なものとし、実質的なデータ抹消の効果を得る**ものです。
- **暗号鍵の抹消だけで済むため、仮想サーバ毎（管理単位毎）に暗号鍵を設定すれば、同一物理サーバ内の隣接する仮想サーバ相互での（ハッキング等を含め）影響も受けません。**

※OS経由では認識できない領域とは：最近の大容量HDDで用いられている**SMR**（Shingled Magnetic Recording：瓦記録）方式や、**SSD**で用いられている**システム動作専用のデータキャッシュ（スプール）領域（オーバ・プロビジョニング）**や、使用中に検出された障害によって**LBAを失った再割り当て済みセクタ**等。

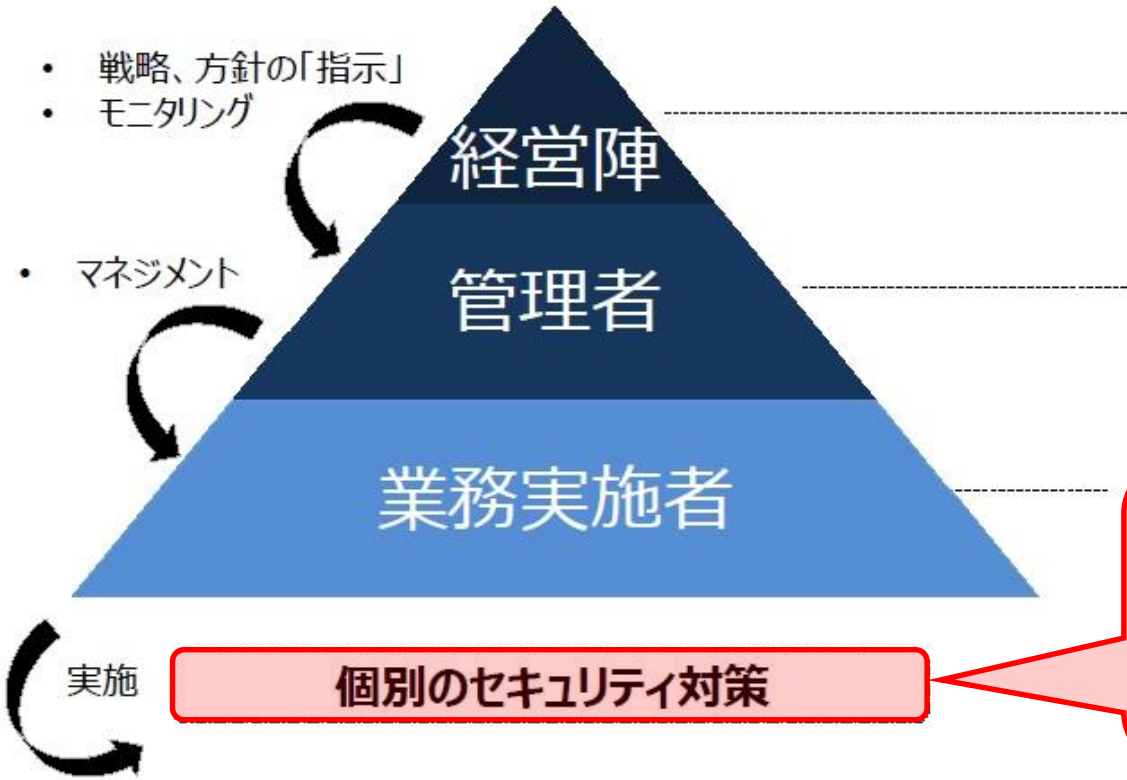
ISMAP管理基準の構成 I

ADEC

■ ①CSPの「経営陣」が管理者層に対して、セキュリティに関する意思決定や指示等を継続的に実施し、②これを受けたクラウドサービスの「管理者」が的確にマネジメントを実施し、③クラウドサービスの「業務実施者」が実際にセキュリティ対策を実施していることを確認する。

■ 上記①～③のそれぞれに対して基準を設け、確認するため、管理基準は①ガバナンス基準、②マネジメント基準、③管理策基準の３種類から構成される。

クラウドサービスプロバイダ（CSP）



①ガバナンス基準

例）

✓ 経営陣は、情報セキュリティの戦略及び方針を
(ア)経営陣は、管理者に、情報セキュリティの戦
実施させる。
(イ)経営陣は、管理者に、情報セキュリティの目
せて調整させる。

②マネジメント基準

例）

✓ 情報セキュリティマネジメントの確立
✓ 情報セキュリティマネジメントの運用
✓ 情報セキュリティマネジメントの維持及び改善

③管理策基準

例）

✓ アクセス制御に対する業務上の要求事項
✓ 媒体の取扱い
✓ 暗号による管理策
✓ マルウェアからの保護
✓ ログ取得及び監視
✓ 冗長性

自己申告で良いのか？

具体的な指定は？
例：データ抹消処置
“Purge”、“Destroy”等

検証・判定は監査団体で可能なのか？

第三者認証が必要では？

暗号・暗号鍵管理について

ＩＳＭＡＰ管理基準によるクラウドの要件（抜粋）

８資産の管理
８.1 資産に対する責任
８.1.2.目録の中で維持される資産は、管理する。

8.1.2.7 ＰＢクラウドサービス事業者は、クラウドサービス利用者に対し、当該利用者の資産（バックアップを含む）を管理するため、次のいずれかを提供する。

（ａ）当該利用者の管理する資産を、記録媒体に記録（バックアップを含む）する前に暗号化し、当該利用者が暗号鍵を管理し消去する機能

（ｂ）当該利用者が、当該利用者の管理する資産を記録媒体に記録（バックアップを含む）する前に暗号化し、暗号鍵を管理し消去する機能を実装するために必要となる情報

暗号鍵の管理はユーザが原則

8.1.5 Ｐクラウドサービス事業者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時期を失せずに返却又は除去する。

FedRAMPやSP800-53を引用した文言であれば、SP800-88によるPurge（除去）を意味する。

Ｐ：クラウドサービスに特有なものとして、クラウドサービス事業者が特に考慮すべき管理策に対する表記
Ｂ：管理策を実装するための単なる選択肢ではなく、それ自体が基本言明要件である管理策に対する表記
ＰＢ：その両方の意味を示す

暗号化消去の詳細
NIST SP800-88Rev.1 より、抜粋・再編

1）CEをデータ抹消手段として有効に利用するための条件

- CEを必要とするすべてのデータがメディアに書き込まれる前に暗号化されている場合。
- 暗号化キーが格納されている媒体上の場所（ターゲットデータの暗号化キーまたは関連するラッピングキー）が判明しており、適切な媒体固有のデータ抹消手法を使用してその領域を抹消することが可能な場合。
- CEを実行するための、機器に依存するコマンドを確実に使用することが可能な場合。

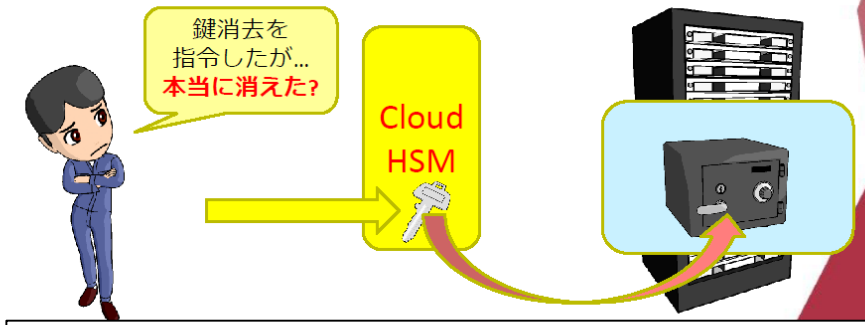
2）ソフトウェアによる暗号化消去の利用に対する留意点

- 紛失したモバイル機器の迅速なリモートワイプの実行などを目的とする場合、CEを使用することが適切かつ有利ですが、**暗号化キーが機器の外部に格納される場合（バックアップまたは外部預託）は、復号のために将来そのキーが使用される可能性があるため、「Purge(除去)」には相当しません。**
  ソフトウェアによる暗号化消去ソリューションは、信頼できる暗号化キーの保護と管理の上で成り立ちます。

- **暗号技術を利用した情報セキュリティ製品やシステムの安全性を確保するためには、暗号アルゴリズム（暗号化をするための手順）をハードウェア、ソフトウェア等で実現しているFIPS 140-2適合認定暗号モジュールの採用等によって安全性の確保が行われていることが重要です。**

クラウドやデータセンターのデータ抹消
クラウド・バイ・デフォルト原則やISMAPはどうする？

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

Beyond Borders 27

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

Beyond Borders 29

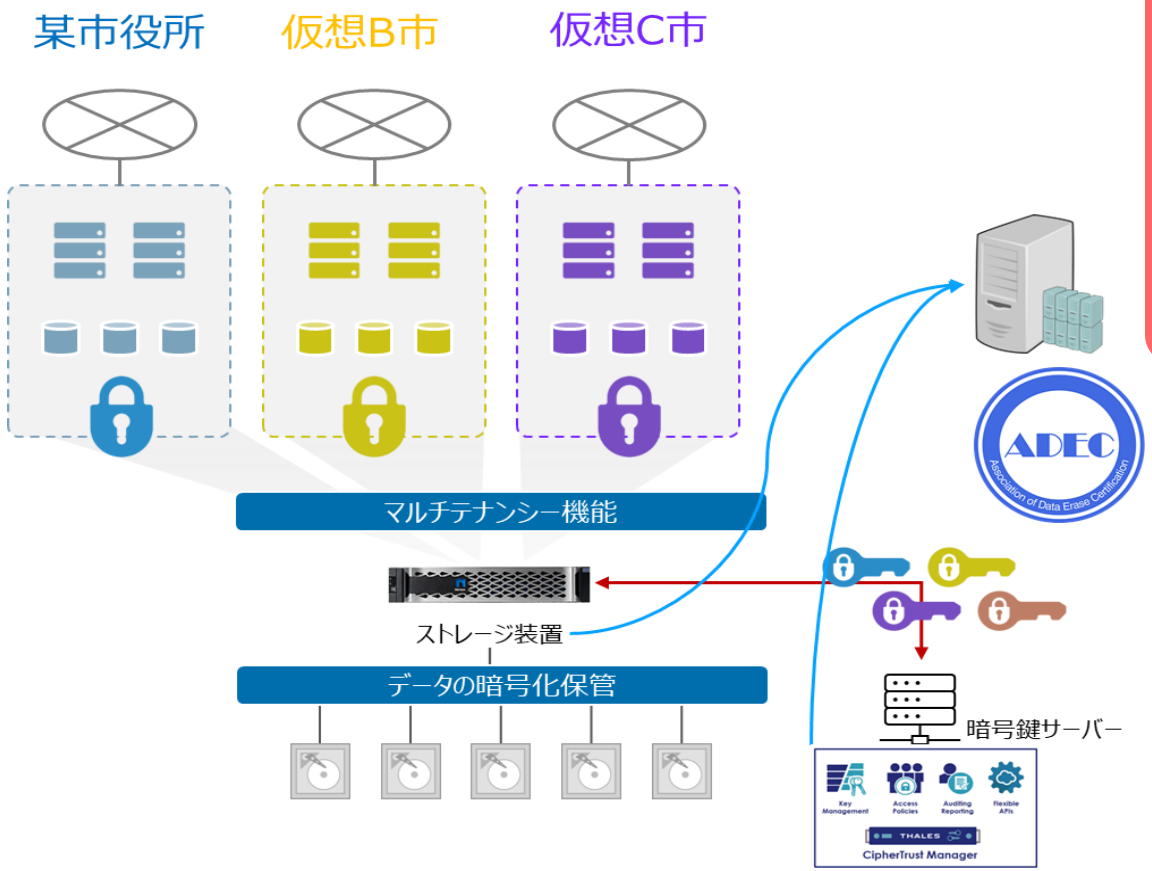
HSM(Hardware Security Module)

2022年6月16日 DBSC 春のセミナー
「クラウドデータベースの完全消去を考える」
「暗号化消去の原理とリスク」
上原哲太郎氏プレゼン資料より抜粋

暗号化消去実証実験：
某自治体様の仮想住民データ等を利用し、
マルチテナント(仮想B市データ含む)にて暗号化消去の実証実験を2022年11月に実施

【実証実験環境】

・システム共同利用DCに検証ストレージを設置
・マルチテナントの環境を構築
・某自治体様の仮想データ、仮想B市等行政データを暗号化書き込み
・暗号鍵管理、消去



画像提供：NetApp様

(1) シスログ転送
(2) ログから鍵の生成を検知
(3) ログサーバ上のログに出力される鍵の名前を使い、その鍵に紐づくストレージ情報をKMIPサーバから取得（ksctlコマンドでKMIPサーバと通信）（KMIP：Key Management Interoperability Protocol）
- クラスタ名、クラスタUUID
- SVM名、SVM ID、SVM UUID
- Volume名、Volume UUID
- Key_ID

(4) KMIPサーバに作成された鍵とそれに紐づく対象のストレージに対して、暗号化消去の証明を発行

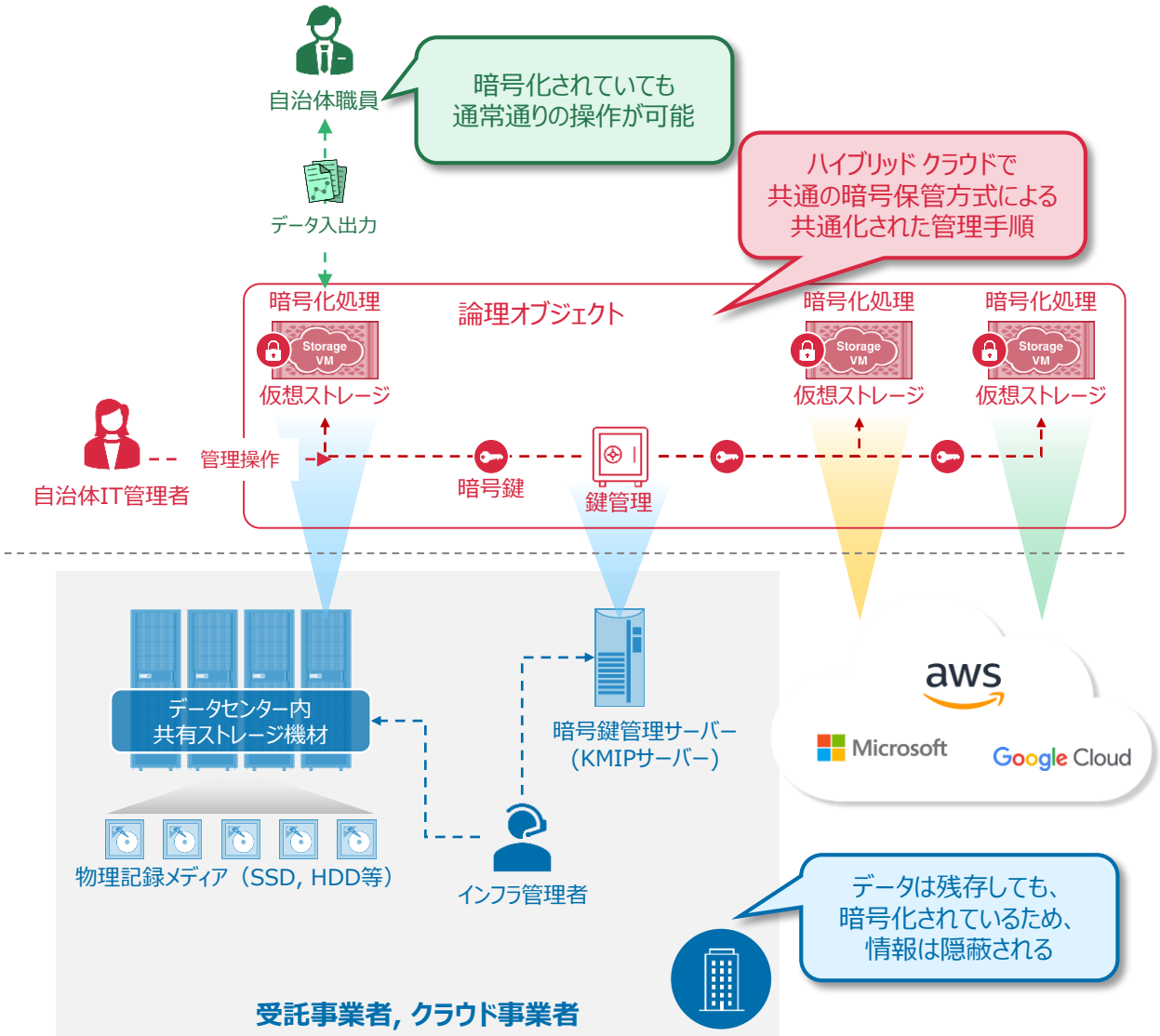
FIPS140等で規定される暗号鍵の適正な管理方法との併用により、
「NIST SP800-88 Rev.1」で規定される【暗号化消去】の基準に適合している事が示された。


データ消去検証調査報告書（案３）
「NetApp社製 暗号化クラウドストレージ」

表題の件につき、次のとおりご報告申し上げます。

第１ 調査概要
１ 調査番号：ＥＶ２０２２１０２８－０１
２ 調査依頼者：データ適正消去実行証明協議会（ADEC）
３ 調査目的
NetApp社製の暗号化クラウドストレージ搭載媒体の記録情報をバイナリレベルで解析することにより、仮想ドライブのデータ消去性能を調べること。
４ 検証対象媒体
計４点の検証対象媒体の概要及び識別情報は次の通りである。
（１）媒体番号：ＥＶ２０２２１０２８－０１－㊀（以下、Disk㊀）
・機能等：SASドライブ 2.5型
・品番等：SAMSUNG MZ-6ER4000/0G3
・Ｓ／Ｎ：S182NEAF701051
・WWN：5002538454704183
・容　量：4,096,339,839,360バイト
（２）媒体番号：ＥＶ２０２２１０２８－０１－㊁（以下、Disk㊁）
・機能等：SASドライブ 2.5型
・品番等：SAMSUNG MZ-6ER4000/0G3
・Ｓ／Ｎ：S182NEAF700890
・WWN：5002538454703743
・容　量：4,096,339,839,360バイト
（３）媒体番号：ＥＶ２０２２１０２８－０１－㊂（以下、Disk㊂）
・機能等：SASドライブ 2.5型
・品番等：SAMSUNG MZ-6ER4000/0G3
・Ｓ／Ｎ：S182NEAF700087
・WWN：5002538454700573
・容　量：4,096,339,839,360バイト
（４）媒体番号：ＥＶ２０２２１０２８－０１－㊃（以下、Disk㊃）
・機能等：SASドライブ 2.5型
・品番等：SAMSUNG MZ-6ER4000/0G3
・Ｓ／Ｎ：S182NEAF700053
・WWN：5002538454700353
・容　量：4,096,339,839,360バイト
５ 対象機器の受領
・受領日：２０２２年１１月１３日
・宅配便：ヤマト運輸（3941-2286-3632）
６ 調査責任者
・下垣内 太（代表取締役）
７ 調査場所
・アイフォレンセ日本データ復旧研究所（株）大阪データ復旧
８ 調査期間
・着手：２０２２年１１月１３日
・完了：２０２２年１１月２４日
９ 調査結果
暗号化Volumeに書き込まれたユーザデータは暗号化されており、なおかつその領域の記録はVolumeの削除及び暗号鍵の抹消による一切の影響を受けないことを認めた。
このことはすなわち、FIPS140等で規定される、暗号鍵の適正な管理方法との併用により、「NIST SP800-88 Rev.1」で規定される「暗号化消去」の基準に適合したことを示している。

セキュアなデータ連携基盤実現に向けた リファレンス アーキテクチャ と ロールモデルの提唱



■ ハイブリッド マルチクラウド環境における情報漏洩対策

- 暗号化保管方式の現実的なリファレンス アーキテクチャの策定
- 運用時における 現実的なロールモデルの策定

■ 自治体 IT管理者様の観点では・・・

- 受託事業者、国内クラウド事業者、パブリッククラウド事業者に関わらず 共通して利用できる 暗号化保管方式
- 標準化・共通化することで、住民の資産である情報の漏洩を防止

■ 受託事業者・クラウド事業者の観点では・・・

- お客様のデータが残っていても「情報」は隠蔽される
- 安心 且つ シンプルな運用により 安定稼働を実現

画像提供：NetApp様

最後に！

ADEC（データ適正消去実行証明協議会）は、
「消去技術認証基準委員会」において、
データ消去技術に関するガイドブックを公開しております。

データ消去技術 ガイドブック第2.3版
https://adec-cert.jp/guidebook/pdf/DATAWIPEGUIDEBOOK.pdf
【別冊】データ消去技術 ガイドブック 暗号化消去技術編
https://adec-cert.jp/guidebook/pdf/DATAWIPEGUIDEBOOK_extra.pdf

暗号化消去技術編の作成は、
右記の参加者にご協力を頂
いております。

主査：東京電機大学　佐々木良一様
参加者（五十音順）：
さくらインターネット株式会社
独立行政法人情報処理推進機構（IPA）
日本マイクロソフト株式会社
ネットアップ合同会社
ワンビ株式会社

その他データ抹消に関する参考資料：
データ抹消に関する米国文書（規格）及びHDD、SSD の技術解説
https://digitalforensic.jp/wp-content/uploads/2016/02/technical-aspect.pdf