仮想化サーバにおける暗号化消去について
DoD（3回上書き）からNISTへ
周回遅れを解消？

2021年12月7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（20年4月～一時帰休中）
    （旧 Kroll Ontrack）

はじめに

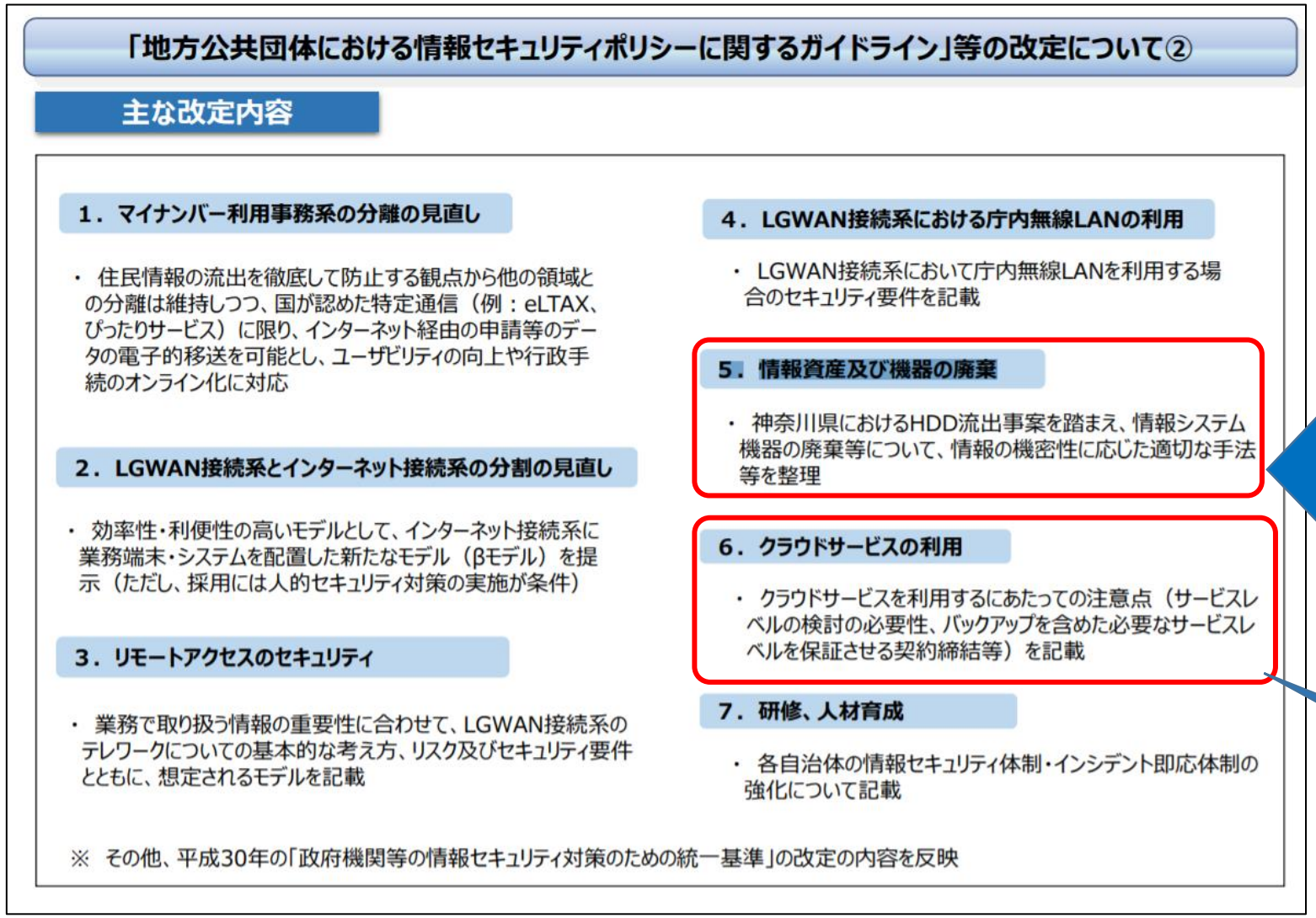
２０２０年６月のISMAP管理規定に引き続き、７月７日改訂の「政府統一基準（第3版）」で、クラウド環境に於ける情報セキュリティの手法として**「暗号化消去」**が記載されました。

これは、「データ消去分科会」が２０１６年４月に発表した「証拠保全先媒体のデータ抹消に関する報告書」中の「データ抹消に関する米国文書（規格）及びHDD、SSD の技術解説」で触れた「NIST SP800-88 Rev.1」に規定されているものであり、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がDoD 5200.28-Mの３回上書きから「NIST SP800-88 Rev.1」準拠へと、周回遅れが解消される方向となりました。

この流れと、**クラウド環境（仮想サーバ）に於ける「暗号化消去」の詳細と優位性**について解説します。

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

2022年度へ
課題を残す

DoDからNISTへ （総行情第 77 号）

NISTに従い

ガイドライン改訂　機密レベルと抹消方法を3分類

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：社会保障、税、防災、災害等に関する情報システム及びデータ	当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元が不可能とすることが適当である。 なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については物理的に破壊すること。この場合、あらかじめ仕様書に明記のうえ、機器の廃棄方法を契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い、委託事業者等が物理的な破壊を実施したことを当該破壊の作業工程の証明書により確認する。当該完了証明書については、破壊前後の写真が添付されていることなど、その提出方法についても明記されていることが望ましい。
（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も解読されるレベルで抹消を行うことが適当である。 具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③ＯＳ等から全ての領域へのアクセス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アによる上書き消去、④ブロックイレース、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）で記述した方法①～⑤のほかの方法によりアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより消去する方法がある。 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。

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

①マイナンバー利用事務系：物理破壊

②機密性2：パージ（除去）

③機密性1：クリア（消去）

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

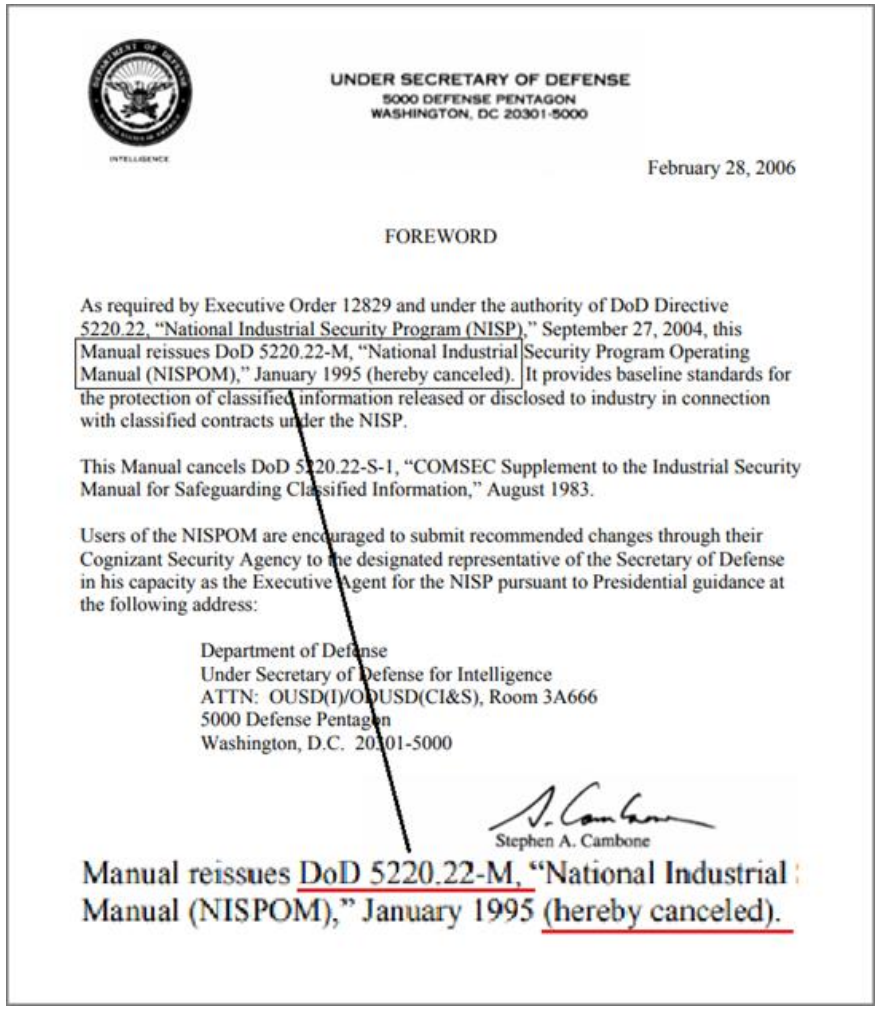
ADECの
「消去技術ガイドブック」を
技術的見解の参照資料として紹介

DoD（米国国防総省規格：3回上書き）からNIST（Purge）へ

ガイドライン改訂　改訂内容の伏線（上原 哲太郎会長の2019・12・11 Twitter）

DoDからNIST SP800-88Rev.1へ（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

  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

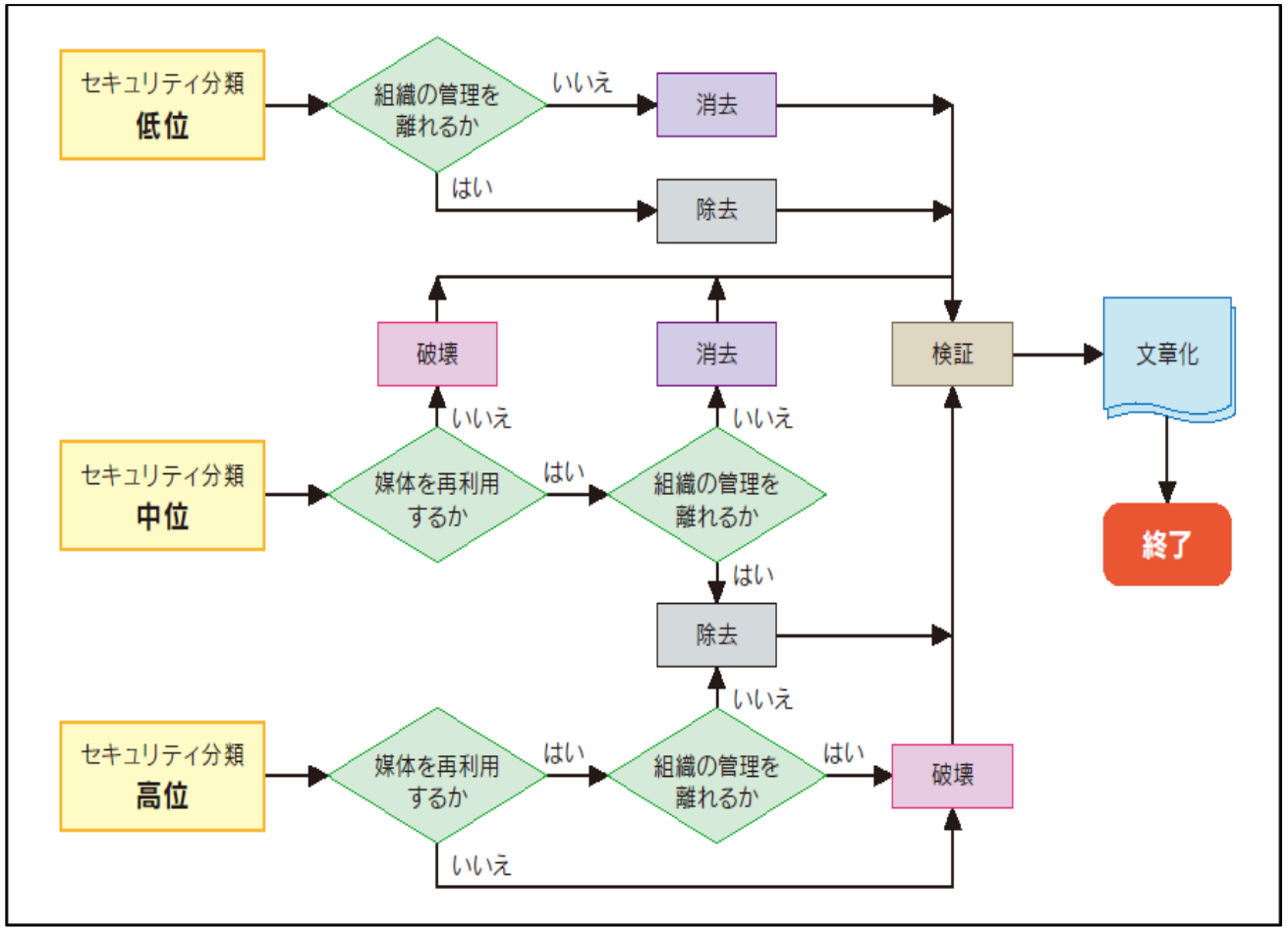
2014年12月　SP800-88rev.1（最新版）

・ **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

11月24日にIPAから和訳が公開されました！

NIST SP800-88Rev.1
リスク判定と抹消手段の選択基準



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」

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。

NIST SP800-88Rev.1
3段階の情報の機密レベル

①．低度：情報が漏えいした場合の影響は限定的なレベル

（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）

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

（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．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

（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）

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）

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
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**ことが必要。

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

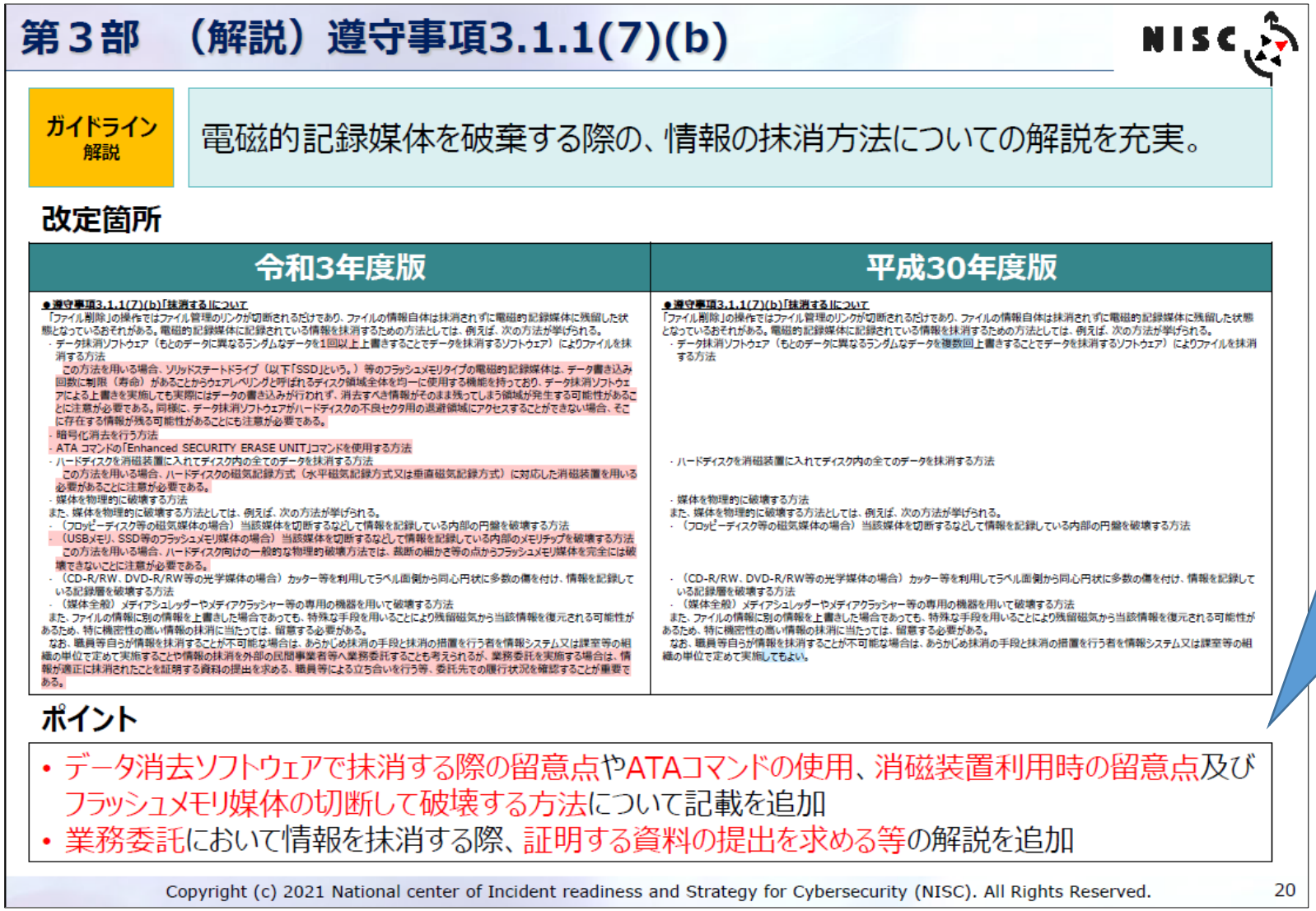
SSDの物理破壊（最近の事例） From Twitter！

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。

統一基準（令和3年7月7日）の改訂（情報の抹消）



第３部　（解説）遵守事項3.1.1(7)(b)

NISC

ガイドライン解説

電磁的記録媒体を破棄する際の、情報の抹消方法についての解説を充実。

改定箇所

令和3年度版	平成30年度版
●遵守事項3.1.1(7)(b)「抹消する」について 「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。電磁的記録媒体に記録されている情報を抹消するための方法としては、例えば、次の方法が挙げられる。 ・データ抹消ソフトウェア（もとのデータに異なるランダムなデータを1回以上上書きすることでデータを抹消するソフトウェア）によりファイルを抹消する方法 この方法を用いる場合、ソリッドステートドライブ（以下「SSD」という。）等のフラッシュメモリタイプの電磁的記録媒体は、データ書き込み回数に制限（寿命）があることからウェアレベリングと呼ばれるディスク領域全体を均一に使用する機能を持っており、データ抹消ソフトウェアによる上書きを実施しても実際にはデータの書き込みが行われず、消去すべき情報がそのまま残ってしまう領域が発生する可能性があることに注意が必要である。同様に、データ抹消ソフトウェアがハードディスクの不良セクタ用の退避領域にアクセスすることができない場合、そこに存在する情報が残る可能性があることにも注意が必要である。 ・暗号化消去を行う方法 ・ATA コマンドの「Enhanced SECURITY ERASE UNIT」コマンドを使用する方法 ・ハードディスクを消磁装置に入れてディスク内の全てのデータを抹消する方法 この方法を用いる場合、ハードディスクの磁気記録方式（水平磁気記録方式又は垂直磁気記録方式）に対応した消磁装置を用いる必要があることに注意が必要である。 ・媒体を物理的に破壊する方法 また、媒体を物理的に破壊する方法としては、例えば、次の方法が挙げられる。 ・（フロッピーディスク等の磁気媒体の場合）当該媒体を切断するなどして情報を記録している内部の円盤を破壊する方法 ・（USBメモリ、SSD等のフラッシュメモリ媒体の場合）当該媒体を切断するなどして情報を記録している内部のメモリチップを破壊する方法 この方法を用いる場合、ハードディスク向けの一般的な物理的破壊方法では、裁断の細かさ等の点からフラッシュメモリ媒体を完全には破壊できないことに注意が必要である。 ・（CD-R/RW、DVD-R/RW等の光学媒体の場合）カッター等を利用してラベル面側から同心円状に多数の傷を付け、情報を記録している記録層を破壊する方法 ・（媒体全般）メディアシュレッダーやメディアクラッシャー等の専用の機器を用いて破壊する方法 また、ファイルの情報に別の情報を上書きした場合であっても、特殊な手段を用いることにより残留磁気から当該情報を復元される可能性があるため、特に機密性の高い情報の抹消に当たっては、留意する必要がある。 なお、職員等自らが情報を抹消することが不可能な場合は、あらかじめ抹消の手段と抹消の措置を行う者を情報システム又は課室等の組織の単位で定めて実施することや情報の抹消を外部の民間事業者等へ業務委託することも考えられるが、業務委託を実施する場合は、情報が適正に抹消されたことを証明する資料の提出を求める、職員等による立ち合いを行う等、委託先での履行状況を確認することが重要である。	●遵守事項3.1.1(7)(b)「抹消する」について 「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。電磁的記録媒体に記録されている情報を抹消するための方法としては、例えば、次の方法が挙げられる。 ・データ抹消ソフトウェア（もとのデータに異なるランダムなデータを複数回上書きすることでデータを抹消するソフトウェア）によりファイルを抹消する方法 ・ハードディスクを消磁装置に入れてディスク内の全てのデータを抹消する方法 ・媒体を物理的に破壊する方法 また、媒体を物理的に破壊する方法としては、例えば、次の方法が挙げられる。 ・（フロッピーディスク等の磁気媒体の場合）当該媒体を切断するなどして情報を記録している内部の円盤を破壊する方法 ・（CD-R/RW、DVD-R/RW等の光学媒体の場合）カッター等を利用してラベル面側から同心円状に多数の傷を付け、情報を記録している記録層を破壊する方法 ・（媒体全般）メディアシュレッダーやメディアクラッシャー等の専用の機器を用いて破壊する方法 また、ファイルの情報に別の情報を上書きした場合であっても、特殊な手段を用いることにより残留磁気から当該情報を復元される可能性があるため、特に機密性の高い情報の抹消に当たっては、留意する必要がある。 なお、職員等自らが情報を抹消することが不可能な場合は、あらかじめ抹消の手段と抹消の措置を行う者を情報システム又は課室等の組織の単位で定めて実施してもよい。

ポイント

- データ消去ソフトウェアで抹消する際の留意点やATAコマンドの使用、消磁装置利用時の留意点及びフラッシュメモリ媒体の切断して破壊する方法について記載を追加
- 業務委託において情報を抹消する際、証明する資料の提出を求める等の解説を追加

地方公共団体向けガイドライン（2020/12月/28日）に続きSP800-88Rev.1を採用

https://www.nisc.go.jp/active/general/pdf/guider3.pdf

統一基準（令和3年7月7日）の改訂（暗号化消去も登場）

第３部　（解説）基本対策事項3.1.1(7)-1

NISC

統一基準
ガイドライン

暗号化消去に関する解説及び暗号化消去を採用する場合の留意点を追加。

改定箇所

令和3年度版	平成30年度版
1.3/1.5(3) 用語定義 ● 「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（WindowsのBitLocker等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。 ●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。 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。	規定なし

ポイント

- 暗号化消去とは、暗号化して記録した情報に対して復号に用いる鍵を抹消することで消去する方法である解説を追加。
- 暗号化消去を採用する場合は、運用の全期間を通じて暗号化することが前提となる記載を追加。

注：統一基準に記載されるためには、基本的にある程度知名度・実績を必要とされる。

暗号化消去については、2020年6月20日に、ISMAP（政府情報システムのためのセキュリティ評価制度：クラウドサービスが対象）の規定類の公開により記載されたものと推定する。

統一基準（令和3年7月7日）上の記載

NISC（National center of Incident readiness and Strategy for Cybersecurity：内閣サイバーセキュリティセンター）の、
「政府機関等のサイバーセキュリティ対策のための統一基準」（令和３年度版）

●1.3/1.5(3) 用語定義
「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、**ソフトウェアによる暗号化（WindowsのBitLocker等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。**

●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。
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

暗号化消去の詳細
NIST SP800-88Rev.1 より、抜粋・再編

- **Cryptographic Erase（暗号化消去：CE）の解説**
  - CEは、**データが媒体に書き込まれる時点で暗号化が実行されている場合に使うことができる抹消手法**であり、データの抹消は、書き込まれたデータを物理的に抹消するのではなく、データの暗号化に使用される**暗号化キーを抹消する**ことによって行われます。
  - CEは非常に高速にデータの抹消を実現することができ、部分的な抹消、例えば記憶媒体の限定された一部の領域に対するデータの抹消にも利用することができます。部分的な抹消は、選択的抹消とも呼ばれ、**クラウドコンピューティングシステム**や**スマートフォンやタブレット型端末**などのモバイルデバイスに対しても有効なデータ抹消の方法です。
  - 通常、ストレージデバイスが大きくなると、他のデータ抹消方法ではその大きさに比例して時間が必要となりますが、CEは数分の1秒で実行することが可能です。これは特に重要なことです。また、 CEは他の抹消方法の補助として使用することもできます
  - **暗号化キーの管理について高い信頼が存在しない限り、CEを使用したデータ抹消は、暗号化キーをバックアップまたは預託した機器では信頼することができません。**

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。**

暗号化消去の詳細
NIST SP800-88Rev.1 より、抜粋・再編

3）暗号化の規定（FIPS 140について）

NISTとCSEC（Communications Security Establishment Canada：カナダ通信保安局）は1995年からCMVP（Cryptographic Module Validation Program：**暗号モジュール**認証プログラム)の共同取り組みを行い、暗号モジュールのセキュリティ要件標準(FIPS 140) および関連するSP文書に従って、米国政府標準暗号及び暗号鍵などの重要情報の保護機能が適切に実現されていることを客観的な試験によって認証しています。

注１：日本では、CMVPとほぼ同じスキームで、IPAがJCMVP（Japan Cryptographic Module Validation Program：日本版**暗号モジュール**認証プログラム)を2007年から運用しています。CMVPとの大きな違いは、**電子政府推奨暗号リスト**等に掲載されている暗号アルゴリズムを主な対象にしている点です。

注２：FIPS 140は、140-1（1994年1月11日発行）、140-2（2001年5月25日発行）、最新版は140-3(2019年３月22日発行)となっています。これに伴い、FIPS140-3認証への移行計画が進行しており、FIPS140-2の認証申請受付は2021年9月22日に終了、現在はFIPS140-3の認証申請受付になっています。また、FIPS140-2認証の有効期限についても、認証取得後原則5年となっていますが、最長でも2026年9月21日までに制限されます。

暗号モジュールとは？

非常に表現が難しいが、
「暗号化および復号、鍵管理等、備えるべきセキュリティ機能を定義した国際規格などの認定を取得している、ICチップ搭載型ICカードやUSBトークンなどの物理的な部品だけでなく、ソフトウェア等も含む製品を指す。」
と解釈すれば良さそう。

ISMAP管理基準によるクラウドの要件（抜粋）

ISMAP（Information system Security Management and Assessment Program：政府情報システムのためのセキュリティ評価制度：

**　米国の連邦情報セキュリティ管理法（FISMA）に基づいて標準化されたクラウドソリューションの導入を目的に設立された、FedRAMP（Federal Risk and Authorization Management Program：米国連邦リスク承認管理プログラム）と、管理基準であるSP800-53Rev.5を参考に、IPA（Information-technology Promotion Agency, Japan：独立行政法人情報処理推進機構）が2020年に作成・発行した。2021年11月14日現在20件クラウドサービスが登録されている。**

1.3.14 消去(もしくは抹消)
消去には、媒体を物理的に破壊する物理的消去、媒体を消磁装置により抹消する電磁的消去に加え、論理的消去も含む。論理的消去とは、元のデータを暗号化した後、暗号鍵を消去し、元のデータの復号を不可能にする方法を指す。

1.3.15 暗号
暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された**電子政府推奨暗号、又はそれと同等以上の安全性を有する暗号**を指す。

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

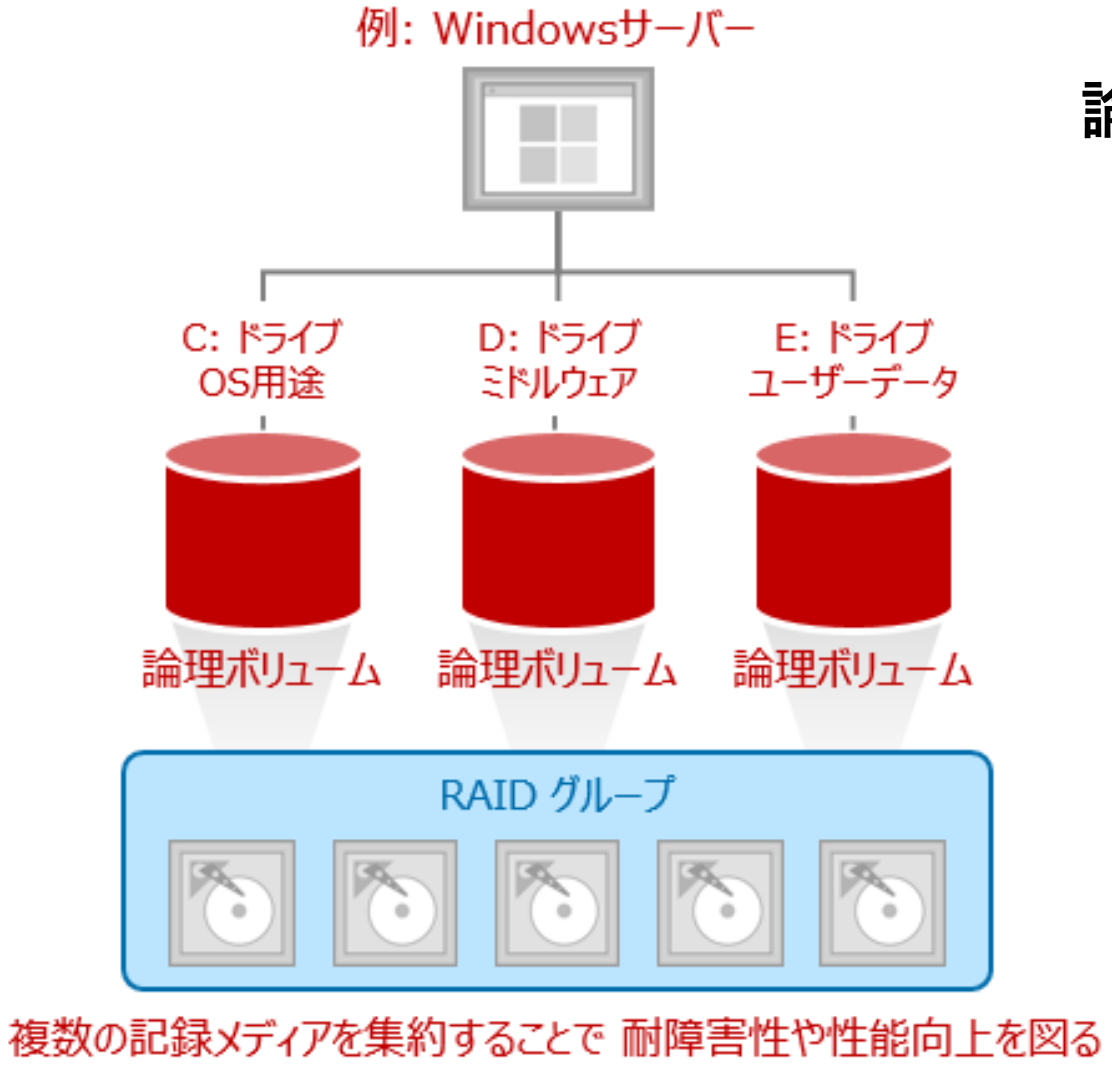
（ｂ）当該利用者が、当該利用者の管理する資産を記録媒体に記録（バックアップを含む）する前に暗号化し、暗号鍵を管理し消去する機能を実装するために必要となる情報

暗号鍵の管理はユーザが原則と読める。

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。

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

サーバの物理・論理構造（論理ボリューム）

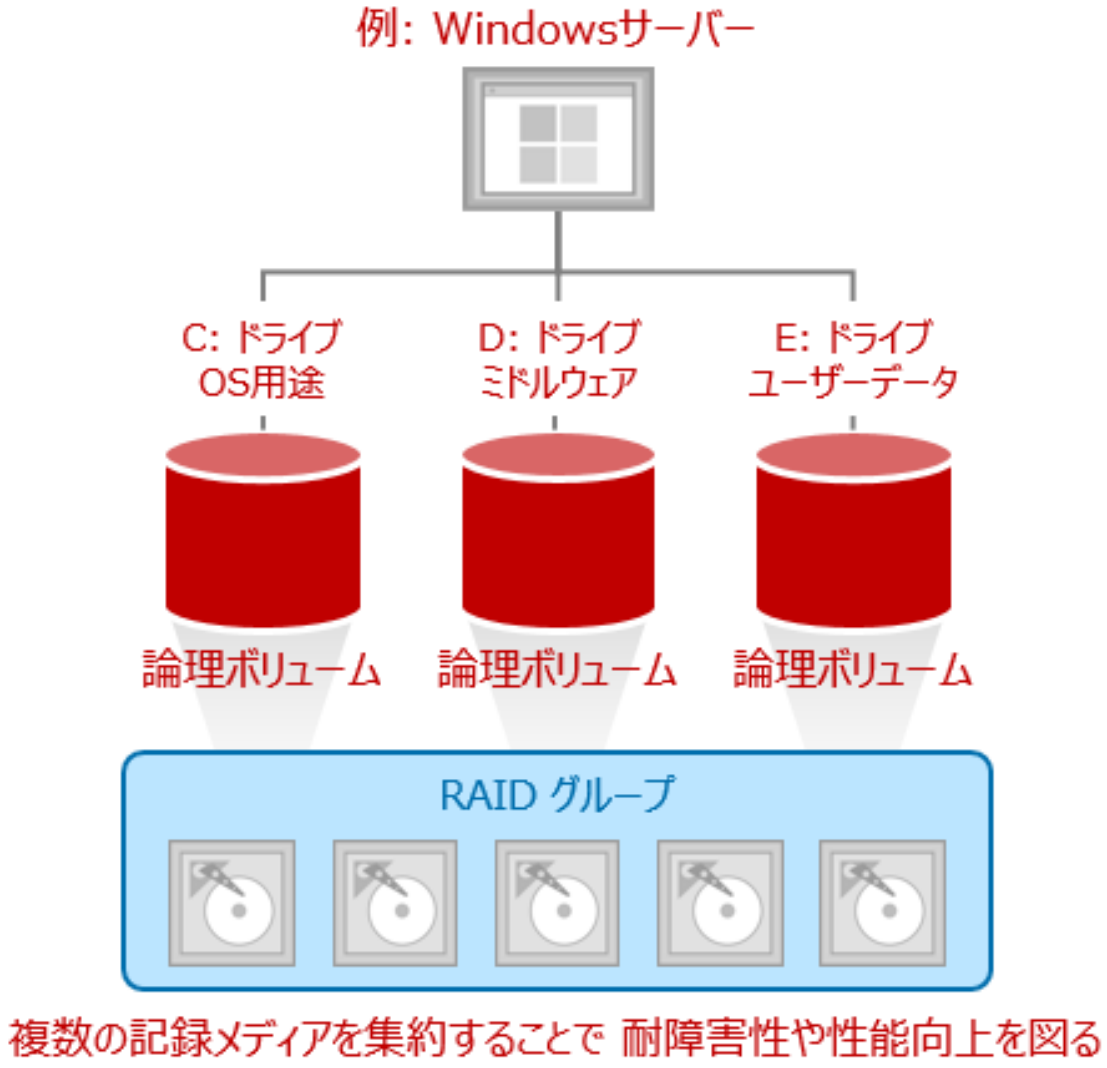


画像提供：NetApp様

論理ボリューム

サーバーでは、記録媒体の物理的な故障からデータを保護するために、複数の記録媒体を集約し、論理的な記録媒体である「論理ボリューム」を構成することが一般的であり、従来から利用されている代表的な技術としてRAID（Redundant Arrays of Inexpensive Disks）技術があります。
集約された複数の記録媒体は、RAIDグループと呼ばれ、RAIDグループを、個別のデータの格納先となる論理ボリューム（LBAを指定・分割したパーティション）を必要に応じて設定します。この論理ボリュームは、OSからは物理的な記録メディア（ドライブ）として認識されます。

サーバのデータ抹消　論理ボリュームの場合

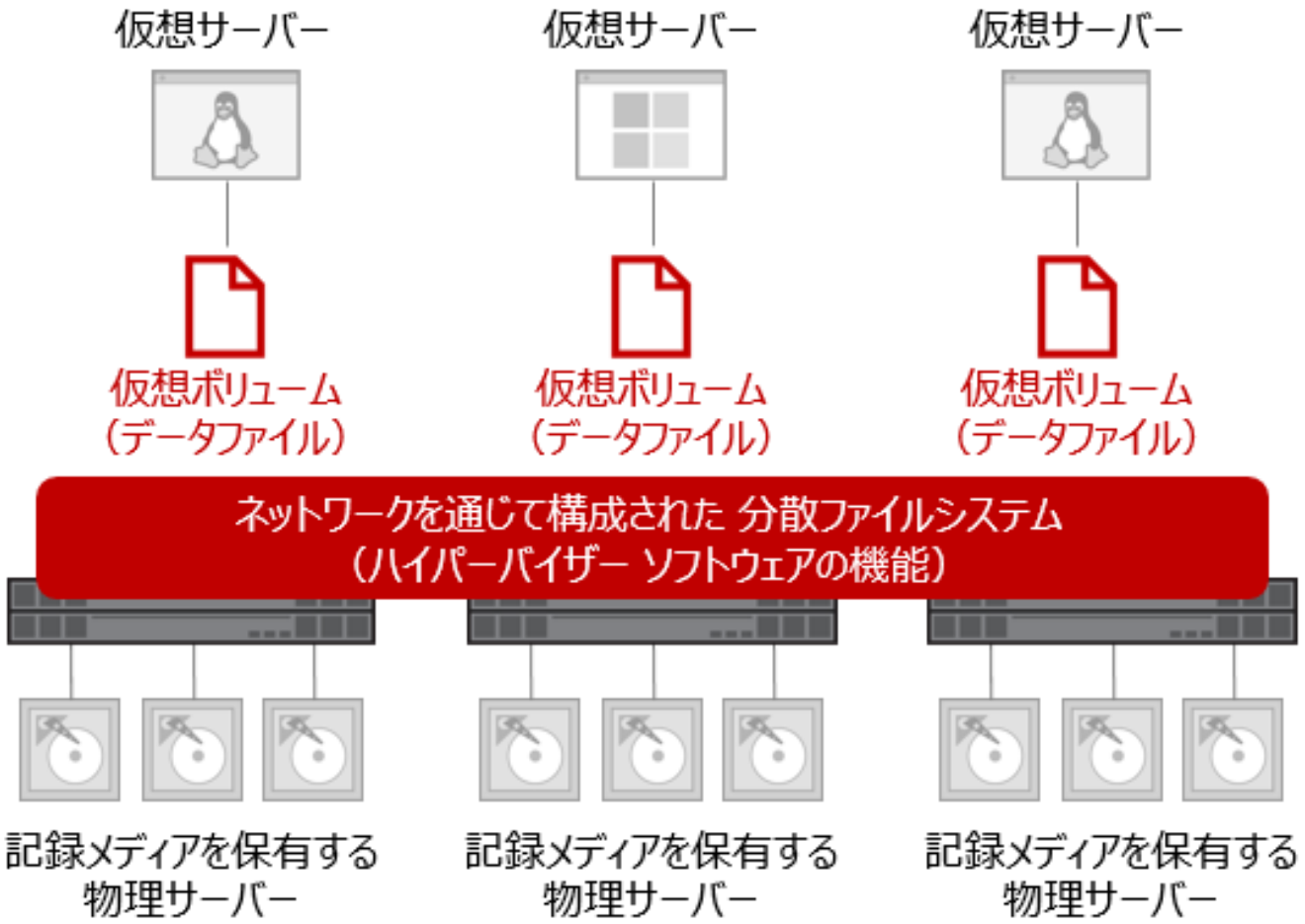


画像提供：NetApp様

例：Eドライブのユーザデータが不要になり、**Purge（除去）レベル**のデータ抹消を実行する場合、全ての記録媒体に分散記録されているため、RAIDグループを構成している**全ての記録媒体を取り外し**、然るべき手段を用いて、**全ての媒体に対して個別のデータ抹消作業を行う**ことが必要となります。

注：Purge（除去）レベルでは、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。

クラウドやデータセンターの物理・論理構造

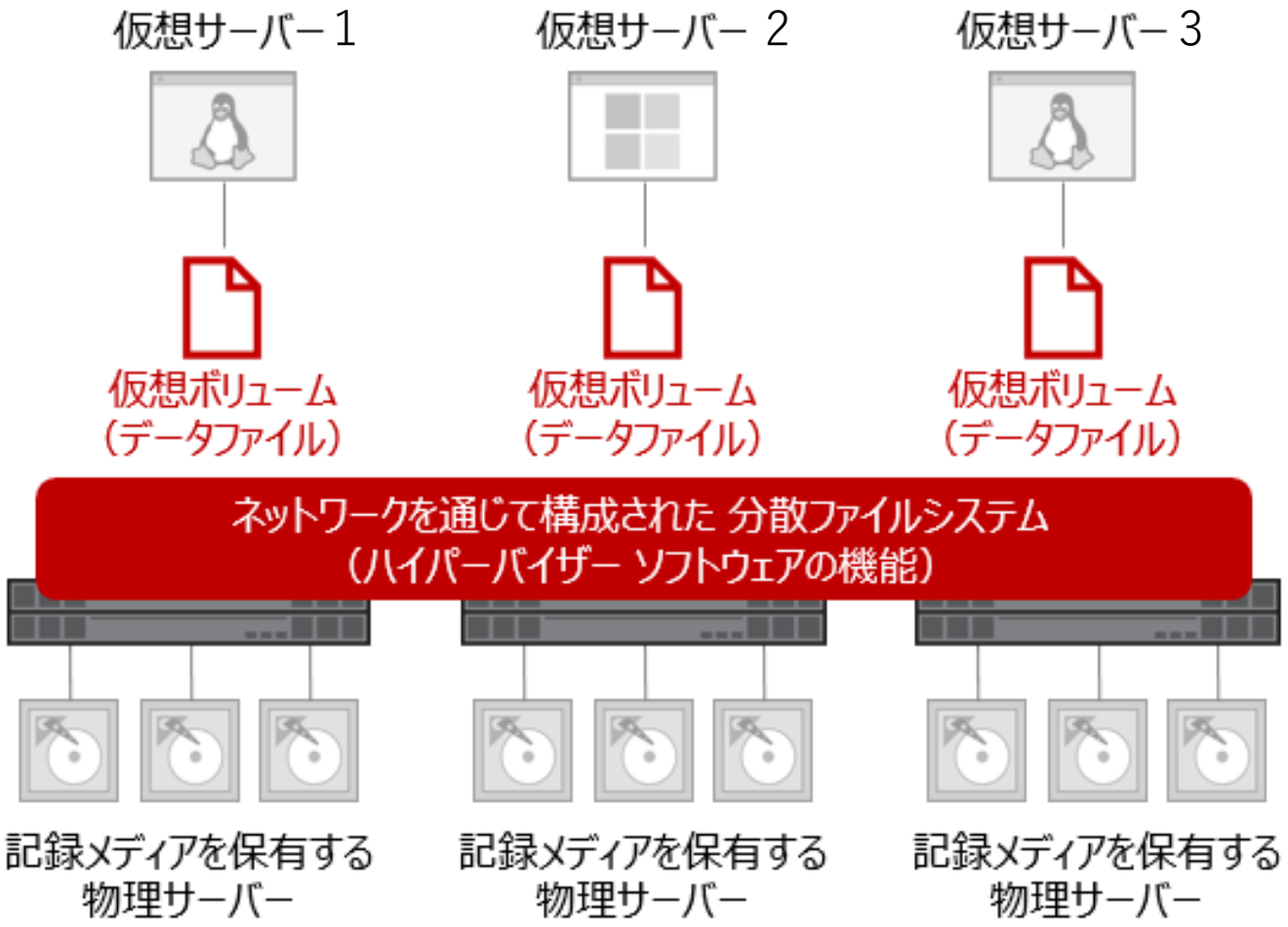


画像提供：NetApp様

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）
- 仮想環境では、データが格納される記録メディアもハイパーバイザーにより仮想的なゲストとして扱われ、これを仮想ボリュームと呼びます。
- **仮想ボリュームの構成は**、ハイパーバイザーの種類によりますが、一般的な概念としては、**ハイパーバイザーが認識するネットワーク上の分散ファイルシステムの上に構成された「データファイル」**です。

クラウドやデータセンターのデータ抹消
仮想ボリュームの場合

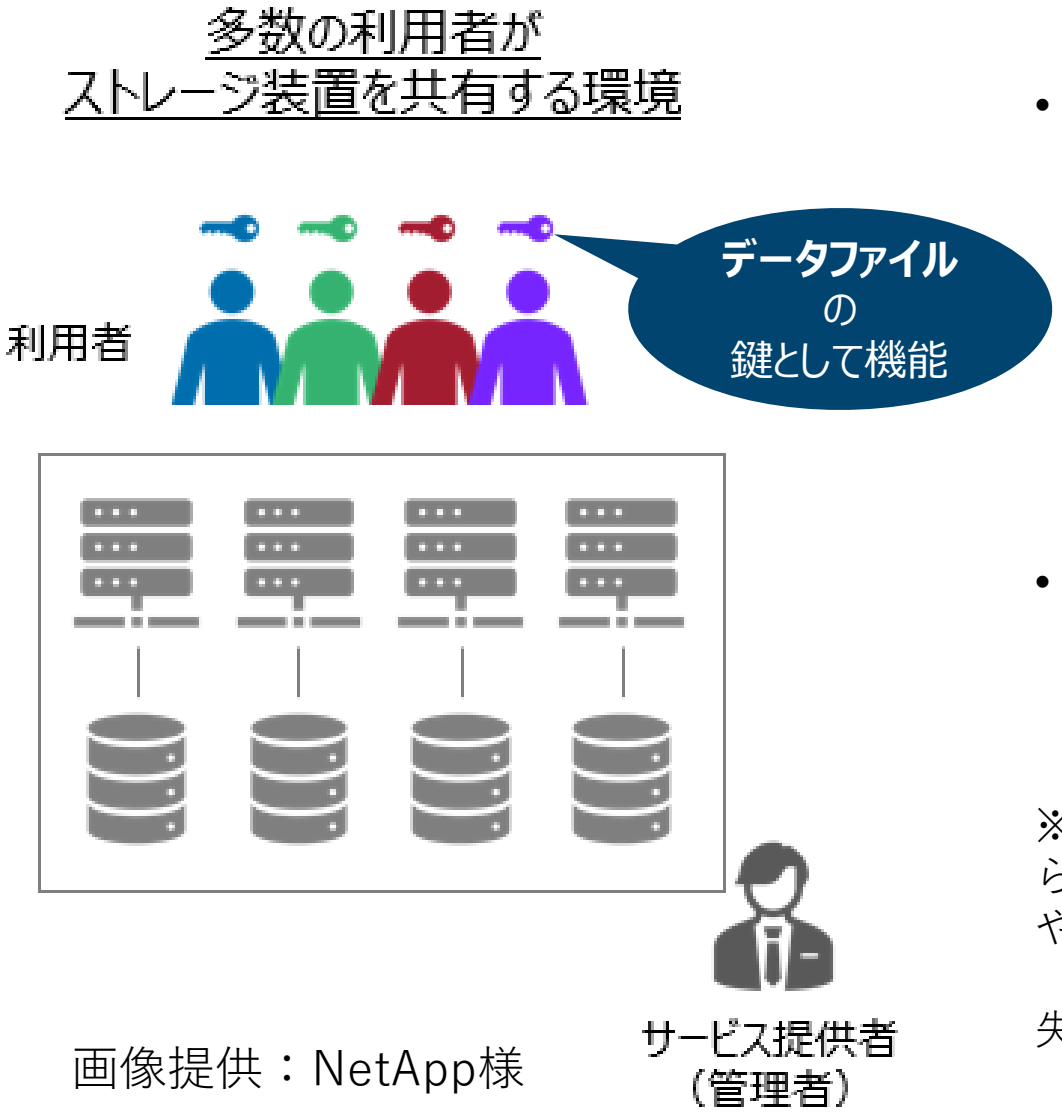


画像提供：NetApp様

例：仮想サーバ1が不要になり、**Purge（除去）レベル**のデータ抹消を実行する場合でも、全ての物理サーバの記録媒体に分散記録されているため、全てのRAIDグループを構成している、**全ての記録媒体を取り外し**、然るべき手段を用いて、**全ての媒体に対して個別のデータ抹消作業を行うこと**が必要となります。

注：Purge（除去）レベルでは、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。

クラウドやデータセンターのデータ抹消（解決策）



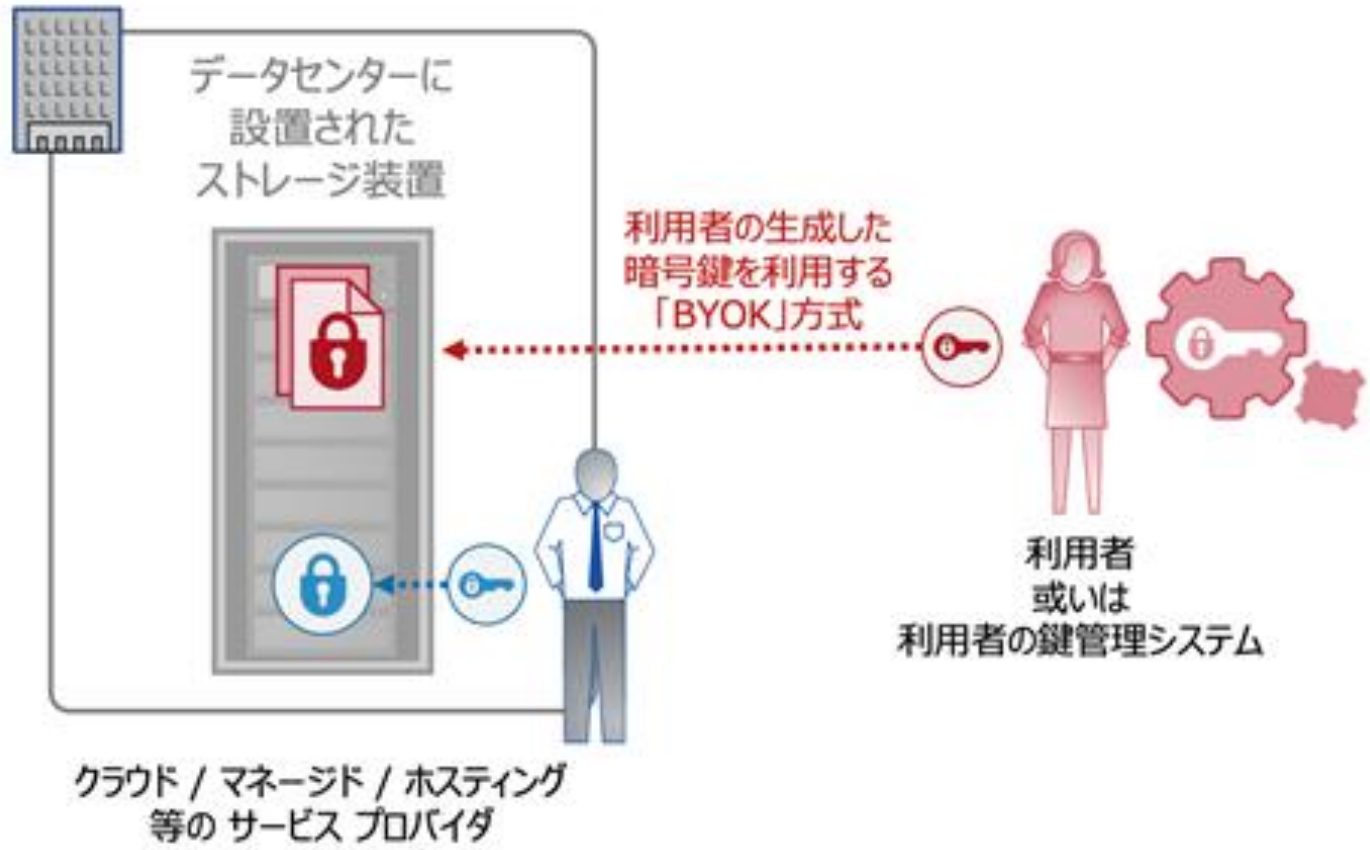
画像提供：NetApp様

「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。

クラウドやデータセンターの鍵管理方式



暗号鍵をサービスプロバイダー事業者が生成・管理するケースと、利用者が自身で暗号鍵を生成・管理するケース（BYOK：Bring Your Own Key）がある。
サービスの利用者責任等を含めて考慮すると、利用者は自身のデータに関する安全性を守るためにも自身が生成・管理する暗号鍵を利用することが望ましい。

暗号・暗号鍵管理について（参考資料）

クラウドサービス提供に於ける情報セキュリティ対策ガイドライン（第３版）

2021年9月30日総務省発行より抜粋

ガイドラインの対象：ISMAP管理基準及び政府統一基準は、政府情報システムに求められる情報セキュリティ対策について記載、ISMAP管理基準は、対策の実施主体をSaaS/PaaS/IaaS等のクラウドサービス事業者として記載している。本ガイドラインは、地方公共団体及び民間事業者を含むあらゆる主体が利用するクラウドサービスに求められる情報セキュリティ対策を記載しており、その提供主体としては中小規模も含むSaaS/PaaS/IaaS 等の全てのクラウドサービス事業者を想定している

Ⅱ．１０．１．暗号と認証

【目的】

情報資産の機密性及び完全性を保護するために、暗号を適切かつ有効に利用する。

Ⅱ．１０．１．１．【基本】 方針

情報を保護するための暗号利用に関する方針を、策定し、実施すること。

【ベストプラクティス】

i. 暗号技術は、電子政府推奨暗号リスト（CRYPTREC暗号リスト）に記載されている暗号技術を採用する。

ii. 暗号に関わる組織の方針を実施する際は、各国の規制、国境を越える暗号化された情報の流れに関する規制及び国内の制約を考慮すること。

Ⅱ．１０．１．２．【基本】 情報提供

事業者は、利用者に、事業者が処理する情報を保護するために、暗号を利用する環境に関する情報を提供すること。また、事業者は、利用者自らの暗号による保護を適用することを支援するために、事業者が提供する能力についても利用者に情報を提供すること。

暗号・暗号鍵管理について（参考資料）

クラウドサービス提供に於ける情報セキュリティ対策ガイドライン（第３版）
2021年9月30日総務省発行より抜粋

Ⅱ．１０．１．３．【基本】 暗号鍵の作成と管理

組織が定めた方針に従って、システム内で使用する暗号鍵を生成・配布・保管・アクセス・廃棄すること。

【ベストプラクティス】

i. 事業者は、利用者の独自の暗号による保護を支援する機能について、利用者に情報を提供する。

ii. 最適な慣行に従って、暗号アルゴリズム、鍵の長さ及び使用法を選定する。

iii. 全ての暗号鍵は、改変及び紛失から保護する。

iv. 秘密鍵及びプライベート鍵は、認可されていない利用及び開示から保護する。

v. 鍵の生成、保管及び保存のために用いられる装置は、物理的に保護する。

vi. 不適切な使用を起こりにくくするために、鍵の活性化及び非活性化の期日を定め、これによって、鍵管理の方針で定めた期間内でだけ鍵を使用できるようにする。

vii. 秘密鍵及びプライベート鍵はセキュリティを保って管理することに加え、公開鍵の真正性についても考慮する。

viii. 公開鍵を発行する認証局は、要求された信頼度を提供するために適切な対応策及び手順を備えている、認知された組織であること。

ix. 暗号サービスの外部供給者（例えば、認証局）とのサービスレベルに関する合意又は契約の内容では、賠償責任、サービスの信頼性及びサービス提供のための応答時間に関する事項を扱うこと。

暗号鍵の管理は組織の方針に従う。ユーザに限定はしていない

暗号・暗号鍵管理について（参考資料）

クラウドサービス提供に於ける情報セキュリティ対策ガイドライン（第３版）

2021年9月30日総務省発行より抜粋

Ⅳ. PaaS/IaaS 編

Ⅳ．４．３．装置の対策

Ⅳ．４．３．６．【基本】 装置のセキュリティを保った処分又は再利用

記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを全て消去していること、若しくはセキュリティを保って上書きしていることを検証すること。事業者は、装置のセキュリティを保った処分又は再利用を行うための取決めについて、利用者と合意していること。

【ベストプラクティス】

i. 秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊するか、その情報を消去若しくは上書きする。

ii. 消去又は上書きには、標準的な消去又は初期化の機能を利用するより、消磁や暗号化消去等の手法で元の情報を復元不可能な状態にするための技術を利用する。

ご清聴ありがとうございました。
ご質問をお受けいたします。

　ADEC（データ適正消去実行証明協議会）では「消去技術認証基準委員会」内部に、「クラウドデータ消去認証分科会」を設置し、「暗号化消去技術」に関するガイドブック（分冊）を作成中であり、今回の資料の作成につきましても参加者の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