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

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

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
コンピュータセキュリティ部門
情報技術研究所

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

December 2014

米国商務省
Penny Pritzker、*長官*

米国国立標準技術研究所
Willie May、*NIST 標準技術局長兼商務次官*

発行機関

本文書は、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）によって、2002 年連邦情報セキュリティマネジメント法（Federal Information Security Management Act of 2002（FISMA））、合衆国法典（U.S. Code）第 44 編第 3541 条等、公法（P.L.）107-347 に基づく法的責任に従って策定された。NIST は、連邦情報システムの最小限の要求事項を含め、情報セキュリティ標準及びガイドラインを開発する責務があるが、これらの標準及びガイドラインは、国家安全保障システムについての政策的権限を有する適切な連邦機関の明示的な承認を得ることなしには、国家安全保障システムに適用されてはならない。このガイドラインは、行政管理予算局（OMB：Office of Management and Budget）による通達（Circular）A-130 8b(3)節 *機関情報システムの安全化*の要求事項に一致しており、通達 A-130 Appendix IV *主要節の分析*に記載された分析に沿っている。補足情報は、通達A-130 Appendix III *連邦政府の自動化された情報リソース*のセキュリティに記載されている。

本出版物における一切は、商務長官が法的権威に基づき連邦政府に対して義務及び拘束力を与えた標準及びガイドラインを否定するものではない。また、これらのガイドラインは、商務長官、行政管理予算局長、又は他の全ての連邦政府当局者の既存の権威に変更を加えたり、これらに取って代わったりするものと解釈すべきではない。本出版物は、非政府組織が自由意思で使用することもでき、米国における著作権の制約はないが、NIST に帰属する。

National Institute of Standards and Technology Special Publication 800-88 Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-88 Revision 1, 64 pages (December 2014)
CODEN: NSPUE2

本出版物は、以下から無料で利用可能である：
http://dx.doi.org/10.6028/NIST.SP.800-88r1

本文書中で特定される商業的組織、装置、又は資料は、実験手順又は概念を適切に説明するためのものである。このような特定は、NIST による推奨又は同意を意味するものではなく、これらの組織、資料、又は装置が、その目的のために利用可能な最善なものであることを意味しているわけでもない。

与えられた法的責任に従い、NIST によって現在作成中のその他の文書への参照が本文書にあるかもしれない。本文書におけるその情報は、概念及び方法論を含め、このような関連文書の完成前であっても連邦政府機関によって利用されるかもしれない。したがって、それぞれの文書が完成されるまで、現在の要求事項、ガイドライン、及び手順が、存在する限り、運用の効力を有する。計画及び移行目的に関して、連邦政府機関は、NIST によるこれらの新しい文書の開発に密接に従うことを希望するかもしれない。

組織は、パブリックコメント期間中の全てのドラフト文書をレビューし、NIST へフィードバックを提供するよう奨励する。上記以外の全ての NIST コンピュータセキュリティ部門の文書は、http://csrc.nist.gov/publications から入手可能である。

本出版物へのコメントは以下で受け付ける：

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive（Mail Stop 8930）Gaithersburg, MD 20899-8930
Email: 800-88r1comments@nist.gov

コンピュータシステムの技術に関する報告書

米国国立標準技術研究所（NIST：National Institute of Standards and Technology）情報技術研究所（ITL：Information Technology Laboratory）は、国家の計測及び標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済及び公共の福祉を促進している。ITL は、テスト、テスト技法、参照データ、概念実証及び技術的分析の開発を通じて、情報技術の開発と生産的利用の発展に努めている。ITL の責務は、連邦政府の情報システムにおいて、国家安全保障に関連する情報以外の情報に対する費用対効果の高いセキュリティとプライバシーを実現するための、管理面、運用面、技術面及び物理面での標準及びガイドラインを策定することを含んでいる。特別刊行物（Special Publication）800 シリーズは、情報システムセキュリティに関する ITL の調査、ガイドライン及び普及活動、ならびに産業界、政府機関及び学術機関との共同活動について報告する。

要旨

媒体のデータ抹消処理（訳注※他の文書によっては「サニタイズ」と書かれていることもある）とは、所定の労力では媒体上の対象データへのアクセスを不可能な状態にするためのプロセスのことである。本ガイドは、組織やシステム所有者が、情報の機密性の分類に基づいて、実用的なデータ抹消処理を決定する際に役立つ。

キーワード

媒体のデータ抹消処理； 機密性確保； データ抹消処理のためのツール及び方法； 媒体の種類；ストレージを備えたモバイル端末； 暗号化消去； 安全な消去

謝辞

本文書の初版の著者である Steven Skolochenko 氏と Xing Li 氏に感謝する。また、卓越した編集技術と本文書の徹底したレビューに対して Jim Foti 氏にも感謝するー彼の仕事により、本書は非常に素晴らしい文書となった。今回の改訂版にコメントを寄せてくれた個人や組織の方々に感謝の意を表する。皆様の貢献により、より正確で使いやすい文書になった。

エグゼクティブサマリ

現代のストレージ環境は急速に進化している。データは、そのライフタイムにおいて、複数の組織、システム、記憶媒体を経由する可能性がある。インターネットやデータストレージシステムが分散型クラウドベースのアーキテクチャに移行するにつれ、データ伝播の拡散性は高まるばかりである。その結果、今までよりも多くの人が効果的に媒体のデータ抹消処理を行う責任を負うことになるとともに、機微データが収集され、媒体上に保持される可能性は大きくなった。この責任は、機微データを発信する組織又はそれが最後に存在する組織だけに限定されるものではなく、途中で情報を一時的に保存又は処理する仲介者も含まれる。生成から廃棄までの間で情報を効率的かつ効果的に管理することは、当該データを扱ったすべての人の責任である。

洗練されたアクセス制御と暗号化を適用することで、攻撃者が機微情報に直接アクセスできる可能性を減らすことができる。その結果、機微情報を取得しようとする人は、例えばデータ抹消処理に関する十分な対応が行われないまま組織の外に捨てられた媒体上の残留データを回収するなど、代替のアクセス手段に労力を集中させようとする可能性がある。したがって、効果的なデータ抹消処理技術の適用と記憶媒体の追跡は、不正な開示から組織が機微データを効果的に保護することを保証するための重要な側面である。情報の保護が最優先である。その情報は、紙、光学媒体、電子媒体、又は磁気媒体に含まれている場合がある。

組織は、媒体が古くなったり使用できなくなったりした場合に、慈善寄付、組織内や組織外への譲渡、又は適用される法律及び規制に従ってリサイクルすることによって、媒体を廃棄することを選択することができる。法的及び倫理的義務により、個人識別情報（PII）などのデータを保護することがこれまで以上に重要になるため、たとえ組織内での譲渡であってもより一層の精査が必要である。媒体の最終目的地がどこであっても、組織の管理を離れた後、又は媒体に格納されたデータの機密区分では保護されなくなった後に、容易に再構築可能なデータの残留表記が媒体に格納されていないことを組織が保証することが重要である。

データ抹消処理とは、所定の労力では媒体上の対象データへのアクセスを不可能な状態にするためのプロセスのことである。本ガイドは、組織やシステム所有者が、情報の機密性の分類に基づいて、実用的なデータ抹消処理を決定する際に役立つ。これは、既知のすべてのタイプの媒体に具体的に対応するものではなく、また対応することもできないが、記載されているデータ抹消処理の決定プロセスは普遍的に適用することができる。

目次

1 はじめに

1.1 目的と範囲

情報の廃棄や媒体のデータ抹消処理に関する情報セキュリティ上の懸念は、媒体ではなく、記録された情報にある。媒体の廃棄やデータ抹消処理の問題は、媒体上に意図的に又は意図せずに置かれた情報によって引き起こされる。システムに使用される電子媒体には、システムの機密性のセキュリティ分類に見合った情報が含まれていると仮定すべきである。媒体を適切に取り扱わない場合、これらの媒体の放出は、情報の不正な開示の発生につながる可能性がある。連邦情報処理標準（FIPS）199[1] *連邦情報及び情報システムのセキュリティ分類標準*に基づく情報技術（IT）システムの分類は、システム情報及び媒体を理解し、管理する上での重要な第一歩である。

分類の結果に基づいて、システム所有者は、NIST 特別刊行物（SP）800-53 改訂 4 版[2] *連邦情報システム及び組織のセキュリティ及びプライバシーコントロール*を参照すべきであり、そこには“組織は、承認された機器、技術、及び手順を使用して、情報システムのデジタル媒体のデータ抹消処理を行う。組織は、媒体のデータ抹消処理や破砕措置を追跡し、文書化して検証するとともに、定期的にデータ抹消処理装置や手順をテストして、正しい性能を確かめる。組織は、情報システムのデジタル媒体が廃棄又は再利用のために組織外に放出される前に、それらをデータ抹消処理又は破壊することで、無認可の人が媒体に含まれる情報にアクセスして使用することを防ぐ”と規定されている。

本書は、関連するシステムの機密性のセキュリティ分類を考慮した上で、データ抹消処理及び廃棄の決定のための適切かつ適用可能な技術とコントロールを備えた媒体のデータ抹消処理プログラムを組織が実施する際の助けとなるものである。

本特別刊行物の目的は、媒体の廃棄や再利用を必要とする場合、又は組織の有効な管理から媒体が離れることになる場合の意思決定を支援することである。組織は、媒体及び情報の最終的なデータ抹消処理や廃棄についての効果的なリスクベースの意思決定を行うために、本ガイドと併せて現場のポリシー及び手順を策定し、使用すべきである。

本ガイドの情報は、現在の技術やアプリケーションの状況下において最も適している。また、システムのライフサイクルを通して行われる情報の廃棄、データ抹消処理、及び管理に関する決定のガイダンスも提供している。本ガイドで取り上げられていない形態の媒体が存在し、今もって本ガイドでカバーされない媒体が開発、展開されている。これらの場合、手順の節で概説されている本ガイドの趣旨が、FIPS 199 に従って評価されたシステムの機密性のセキュリティ分類に基づいて、すべての形態の媒体に適用される。

媒体のデータ抹消処理が行われる前に、システム所有者には、プライバシーに責任を持つ指定された職員（例：プライバシー責任者）、情報自由法（FOIA）責任者、及び地元の記録保持事務所に相談することを強く推奨する。この相談は、連邦記録法の記録保持規則及び要件を確実に遵守するためのものである。さらに、業務上のニーズに応じて過去の情報が把握され、維持されていることを確認するために、

---

[1] Federal Information Processing Standards (FIPS) Publication 199 *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, 13 pp. http://csrc.nist.gov/publications/PubsFIPS.html#199.

[2] NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (includes updates as of January 15, 2014), 460 pp. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

組織管理者にも相談すべきである。システム及びその環境の変化に応じて管理を調整しなければならない可能性があるため、この作業は継続的に行うべきである。

1.2 想定読者

情報の機密性を保護することは、連邦政府機関や企業からホームユーザまで、すべての人の関心事であるべきである。政府サービスの提供には相互接続と情報交換が重要であることを認識した上で、本ガイドは、データ抹消処理又は廃棄にどのプロセスを使用するかを決定する際の手助けとして使用することができる。

1.3 前提条件

本ガイドの前提は、組織が適切な情報カテゴリ、機密性のインパクトレベル、及び情報の所在を正しく特定できることである。理想的には、この活動はシステムのライフサイクルの最も早い段階で達成される [3]。この重要な初期段階は本書の範囲外であるが、この特定がなければ、組織はほぼ確実に機微情報が含まれた一部の媒体の管理を失うことになる。

本ガイドは、組織が情報を保存するために使用する可能性のあるすべての媒体を網羅しているわけではなく、また、本ガイドの有効期間中に開発される可能性のある将来の媒体を予測しようとするものでもない。ユーザは、媒体に含まれる情報のセキュリティ分類に基づいて、データ抹消処理や廃棄の決定を行うことが期待される。

1.4 他の NIST 文書との関係

FIPS や特別刊行物を含む以下の NIST 文書が、本書に直接関連している：

- FIPS 199 及び NIST SP800-60 改訂 1 版 [4] *情報及び情報システムの種類をセキュリティカテゴリにマッピングするためのガイド*は、システムの機密性に関するセキュリティ分類を確立するためのガイダンスを提供する。この分類は、組織がデータ抹消処理の決定を行う際に必要とすべき保証レベルに影響を与える。

- FIPS 200[5] *連邦情報及び情報システムにおける最低限のセキュリティ要件*は、組織が媒体のデータ抹消処理プログラムを持つことを要求するセキュリティ要件のベースになるものである。

---

[3] NIST SP800-64 Revision 2, *Security Considerations in the Systems Development Life Cycle*, October 2008, 67 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-64.

[4] NIST SP800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008, 2 vols. http://csrc.nist.gov/publications/PubsSPs.html#800-60.

[5] FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006, 17 pp. http://csrc.nist.gov/publications/PubsFIPS.html#200.

- FIPS 140-2[6] *暗号モジュールセキュリティ要件*は、米国政府が使用する暗号モジュールの標準を確立している。

- NIST SP800-53 改訂 4 版は、システム全体のセキュリティ分類に基づく連邦システムに対して、データ抹消処理を含む最低限の推奨セキュリティ管理を提供する。

- NIST SP800-53A 改訂 1 版[7] *連邦情報システム及び組織でのセキュリティ管理評価のためのガイド：効果的なセキュリティ評価計画の構築*は、システム全体のセキュリティ分類に基づく連邦システムに対して、データ抹消処理を含むセキュリティ管理を評価するためのガイダンスを提供する。

- NIST SP800-111[8] *エンドユーザ端末のための保管用暗号化技術ガイド*では、ストレージ暗号化技術の選択及び使用に関するガイダンスを提供する。

- NIST SP800-122[9] *個人識別情報（PII）の機密性保護ガイド*は、情報システムにおける個人識別情報の機密性を保護するためのガイダンスを提供する。

1.5 文書構成

ガイドは以下の節と付録に分かれている：

- 1 節（本節）では、文書の権限、目的と範囲、対象者、前提、他の文書との関係を説明し、その構成を概説する。

- 2 節では、データ抹消処理（sanitization：訳注※他の文書によっては「サニタイズ」と書かれていることもある）の必要性と基本的な情報の種類、データ抹消処理及び媒体の概要を紹介している。

- 3 節では、ライフサイクル全体のデータ管理に関連する役割と責任の概要を説明する。

- 4 節では、ユーザにデータ抹消処理の意思決定を支援するためのプロセスフローを提供する。

- 5 節では、いくつかの一般的なデータ抹消処理技術をまとめている。

- 付録 A は、様々な媒体を消去（Clear：訳注※他の文書によっては「クリア」と書かれていることもある）、除去（Purge：訳注※他の文書によっては「パージ」と書かれていることもある）、

---

[6] FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001 (includes change notices through December 3, 2002), 69 pp. http://csrc.nist.gov/publications/PubsFIPS.html#140-2.

[7] NIST SP800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010, 399 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-53A.

[8] NIST SP800-111, *Guide to Storage Encryption Technologies for End User Devices*, November 2007, 40 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-111.

[9] NIST SP800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010, 59 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-122.

又は破壊（Destroy）するための最低限の推奨データ抹消処理技術を規定する。本付録は、4 節で提供された決定フローチャートと一緒に使用する。

- 付録 B は、本ガイドで使用する用語を定義する。
- 付録 C は、媒体のデータ抹消処理を支援できるツール及び外部リソースをリスト化する。
- 付録 D は、暗号化消去を実装したストレージデバイスを選択する際の考慮事項を記載している。
- 付録 E は、ユーザがストレージデバイスベンダに要求すべきデバイス固有の特性を特定している。
- 付録 F は、本ガイドを作成する上で不可欠の情報源と文書の目録が含まれている。
- 付録 G は、組織のデータ抹消処理措置を文書化するためのデータ抹消処理証明書のサンプル様式を提供する。

2 背景

情報の廃棄やデータ抹消処理の決定は、情報システムのライフサイクルを通じて行われる。情報の廃棄及び媒体のデータ抹消処理に影響を与える重要な要因は、システムの開発開始時に決定される。初期のシステム要件には、ハードウェアとソフトウェアの仕様に加え、相互接続性、及びシステム所有者がシステムで使用する媒体の種類を特定するのに役立つデータフロー文書が含まれるべきである。ストレージデバイスの中には、データ抹消処理のための強化コマンドをサポートしているものがあり、これによりデータ抹消処理をより簡単に、より速く、より効果的にすることができる。新しい媒体の種類については、効果的なデータ抹消処理手順がまだ決定されていない可能性があるため、この決定はさらに根本的なものになるかもしれない。効果的なコマンド又はインタフェースベースのデータ抹消処理技術がなければ、媒体を破壊する選択肢しか残されていないかもしれない。その場合、その媒体を、別用途用のストレージデバイスとして受け取ることで利益を得ることができた可能性のある他の組織が再利用することができない。

システムで使用される情報の作成、保存、又は転送に使用される媒体にどのようなものがあるかについては、要件段階で決定すべきである。この分析により、ビジネスニーズと機密性に対するリスクのバランスをとりながら、システムが FIPS 200 に準拠するために考慮される媒体として正式なものとなる。

媒体のデータ抹消処理及び情報の廃棄に関する措置は、通常、システムのライフサイクルの廃棄段階に最も集中する。しかし、情報システムの寿命を通じて、データを含む多くの種類の媒体が、組織の効果が及ぶ管理の外に転送される。この措置は、メンテナンス要因、システムのアップグレード、又は構成の更新などの理由で行われることがある。

2.1 適切な媒体のデータ抹消処理及び情報の廃棄の必要性

媒体のデータ抹消処理は、機密性を保証するための重要な要素の一つである。*機密性*とは、“個人のプライバシーや専有情報を保護する手段を含む、情報へのアクセスと開示に対する認可された制限を保持すること”と定義されている [10]。さらに、“機密性の喪失とは、情報の不正な開示である”とされている [11]。

組織が保護責任を負う情報を適切に管理するためには、使用済み媒体を適切に保護しなければならない。不正な情報収集の豊富な情報源となるのは以下のいずれかであることがよくある：不適切に廃棄されたハードコピー媒体に対するゴミ箱あさり、不適切にデータ抹消処理された電子媒体の入手、又は情報の機密性に見合わない方法でデータ抹消処理された媒体のキーボードや実験室での再構築などによる。媒体は、以下の方法で組織の管理下に出入りする：紙の形でリサイクルボックスを介する、機器修理のためにベンダに送付する、及びハードウェアやソフトウェアの障害に応じて他のシステムに運用移管するなど。この潜在的な脆弱性は、情報がどこにあるのか、その情報が何であるのか、及びその情報をどのように保護するのかを正しく理解することで、緩和することができる。

[10] “Definitions,” Title 44 *U.S. Code*, Sec. 3542. 2006 ed. Supp. 5. Available: http://www.gpo.gov/; accessed 7/21/2014.

[11] FIPS 199, p.2.

2.2 媒体の種類

一般的に使われている媒体には、大きく分けて 2 つの種類がある：

- **ハードコピー**：ハードコピー媒体は、情報を物理的に表現したもので、紙のプリントアウトに関連していることが多い。しかし、プリンタやファクシミリのリボン、ドラム及びプラテンはいずれもハードコピー媒体の例である。紙のプリントアウトをする際に関連する消耗品は、最も管理されていないことが多い。効果的なデータ抹消処理を行わずに組織から捨てられた機微データを含むハードコピー素材は、“ゴミ箱あさりをする人”や好奇心の強すぎる従業員に大きな脆弱性を晒し、望ましくない情報開示の危険性がある。

- **電子媒体（すなわち、“ソフトコピー”）**：電子媒体とは、ビット及びバイトを含むデバイスであり、ハードドライブ、RAM（ランダムアクセスメモリ）、ROM（リードオンリーメモリ）、ディスク、フラッシュメモリ、メモリデバイス、電話機、モバイルコンピューティングデバイス、ネットワークデバイス、事務機器、及び付録 A に記載されているその他の多くの種類のデバイスである。

将来的には、組織は、本ガイドで特に取り上げられていない種類の媒体を使用することがある。本書に記載されているプロセスは、使用中の媒体の種類に関係なく、媒体のデータ抹消処理の意思決定のガイドとなるべきである。すべての種類の媒体に対して本ガイドを効果的に使用するためには、組織及び個人は、媒体そのものではなく、媒体に記録された可能性のある情報に焦点を当てるべきである。

2.3 データ記憶媒体の動向

磁気媒体のデータ抹消処理に関する歴史的な取り組みは、ベンダやモデル間で比較的類似した方法で実装された一つの共通タイプの記憶媒体が広く使用されてきたことの恩恵を受けていた。磁気媒体の記憶容量は比較的一定の割合で増加しており、ベンダはより大きな容量を達成するために必要に応じて技術を変更してきた。この技術が超常磁性限界、又は既存の媒体や記録のやり方で磁気状態を変化させる限界に近づくにつれ、ストレージベンダがより大容量のデバイスを生産するためには、さらなる新しいアプローチや技術が必要になってきている。

フラッシュメモリベースのストレージデバイス、又はソリッドステートドライブ（SSD）などの代替技術も、コスト低下、高性能化及び耐衝撃性のために普及してきている。SSD はすでにストレージ技術の常識を変え始めており、少なくともデータ抹消処理の観点から見ると、この変化は革命的なものである（進化的なものとは対照的に）。消磁（磁気媒体のデータ抹消処理を行うための基本的な方法）は、フラッシュメモリベースのデバイスではほとんどの場合にもはや適用できない。磁気媒体の進化的変化もまた、データ抹消処理に影響を与える可能性がある。従来の磁気媒体とは劇的に異なる新しいストレージ技術、さらには磁気ストレージのバリエーションに対してさえも、明らかにデータ抹消処理の研究が必要であり、有効性を確保するためにデータ抹消処理手順の再調査が必要である。

ストレージデバイスがデータ保存に使用される媒体の種類を明確に示さない場合があるため、革命的な変化も進化的な変化もデータ抹消処理の決定をより困難にしている。媒体の種類を正確に判断し、関連するデータ抹消処理手順を適用することは、ユーザの責任となる。

2.4 データ抹消処理の動向

*磁気媒体*を含むストレージデバイスでは、ゼロバイナリのような固定パターンを持つ一回上書きパスをすれば、たとえ最先端の実験室レベルの技術をデータの復元を試みるために適用したとしても、通常はデータの回復を妨げる。上書き手順の実行にあたってネイティブの読み書きインタフェースのみに依存する場合の主な欠点の 1 つは、その時にアクティブな論理ブロックアドレッシング（LBA）アドレスにマッピングされていない領域（不良領域や現在割り当てられていない領域など）がアドレス指定されないことである。専用のデータ抹消処理コマンドは、これらの領域への対応をより効果的にサポートする。このようなコマンドを使用するには以下のようなトレードオフが発生する。なぜなら、媒体のすべての領域をより徹底的に取り扱うべきであるが、これらのコマンドを使用するには、そのコマンドが期待通りに実装されているというベンダからの信頼と保証も必要になるためである。

磁気媒体上の上書き技術に慣れてしまったユーザや、媒体の種類が進化しても（フラッシュメモリベースのデバイスなどに）これらの技術を適用し続けてきたユーザは、データが意図せずに開示されるリスクを高めている可能性がある。ホストインタフェース（ATA（Advanced Technology Attachment）や SCSI（Small Computer System Interface）など）は、様々なタイプの媒体が基本的に持つ同じ（又は非常に似ている）アクセスデバイスではあるが、データ抹消処理技術が当該媒体に十分に適合していることが非常に重要である。

媒体の種類によっては、破砕技術を適用することが将来的により難しくなったり、不可能になったりする可能性がある。磁気媒体の進化に伴い、（磁気媒体向けの）消磁などの従来技術は複雑化している。なぜなら、磁気記録技術の新たなバリエーションの中には、保磁力（磁力）をより高くした媒体も出てきているためである。その結果、既存の消磁装置では、このような媒体を効果的に消磁するのに十分な力が得られない場合がある。

破砕技術を電子記憶媒体（例えば、フラッシュメモリ）に適用することも困難になってきている。それは、一般的に適用されている粉砕技術に必要な粒子径が、フラッシュメモリの記憶密度の増加に比例して小さくなるからである。フラッシュメモリチップでは、構成材料の硬さのために粉砕機に損害を与える場合があるといった課題がすでに顕在化しており、この問題は、粉砕機がチップをさらに小さく粉砕しようとするにつれてさらに深刻になる。

2.6 節で述べる暗号化消去（Cryptographic Erase：CE）は、媒体に保存されているデータが暗号化されている状況下で使用できる新しいデータ抹消処理技術である。CE では、データを暗号化するために使用された暗号化鍵にデータ抹消処理を行うことで媒体のデータ抹消処理が行われる一方、暗号化されたデータ自体を含む媒体上の記憶領域に対してデータ抹消処理を行うわけではない。CE 技術は、通常は、非常に迅速に媒体のデータ抹消処理を行うことができ、部分的データ抹消処理（記憶媒体の一部分に対してデータ抹消処理を行う技術）をサポートする可能性がある。部分的データ抹消処理は、選択的データ抹消処理と呼ばれることもあり、クラウドコンピューティング及びモバイルデバイスへの応用が期待される。しかし、今日の CE の運用上の使用には、いくつかの課題がある。場合によっては、CE が効果的に媒体のデータ抹消処理を行ったことを検証することが困難な場合がある。この課題及び可能なアプローチについては、4.7.3 節に記載する。検証ができない場合は、組織は検証可能な代替のデータ抹消処理方法を使用するか、検証可能なデータ抹消処理技術と CE を併用すべきである。

データ抹消処理技術の適用にあたって注目されるデバイス固有の特性のリストは、付録 E に記載される。これらの特性を利用して、媒体のユーザはベンダに尋ねるべき種類の質問を導くことができるが、理想的には、ベンダがこの情報を容易に利用できるようにすることで、情報に基づいたリスクベースのデータ抹消処理の決定を促進するために、ユーザが簡単に当該情報を検索できるようになる。例えば、媒体の保磁力を知ることで、利用可能な消磁装置が媒体を効果的に消磁できるかどうかをユーザが判断することを支援できる。

2.5 データ抹消処理の種類

データ抹消処理については、データが意図せずに流出しないようにすることが主な目的である。データはシステムに接続された媒体に保存される。本ガイダンスでは、媒体のデータ抹消処理コンポーネント、すなわち特定の媒体タイプに保存されているデータの表現に容易に適用されるデータ抹消処理に焦点を当てている。その他にも、画面に機微データが焼き付けられている可能性のあるモニタなど、システムの一部として潜在的な懸念事項が存在する。記憶媒体以外のシステム領域（モニタ画面など）に保存されている機微データは、本文書では扱わない。

媒体が別目的で再利用されたり、耐用年数を迎えたりすると、組織は媒体上の情報に対してシステムライフサイクルのデータ抹消処理の決定を実行する。例えば、未開封の DVD に収録されている大量生産された商用ソフトウェアプログラムには、機密データが含まれている可能性は低いと考えられる。そのため、何らのデータ抹消処理技術を適用せずに、単に媒体を廃棄すると決定してもよい。反対に、PII を処理したシステムのハードドライブについては、廃棄する前にデータ抹消処理を行う必要があると組織が判断する可能性のほうが相当高い。

データ抹消処理をせずに廃棄することは、情報開示が組織のミッションに影響を与えず、組織の資産に損害を与えることなく、且つ誰にも金銭的な損失や危害を与えることはない場合にのみ検討すべきである。

情報のセキュリティ分類は、内部環境要因に併せて、媒体との扱い方の決定を導くべきである。鍵となるのは、最初に情報の機密性の観点で考え、その後に媒体の種類に応じた配慮を行うことである。

組織の中には、分類されたシステムのどれにも属さない情報が存在している。このような情報は、メモや白書、プレゼンテーションなど、社内コミュニケーション用のハードコピーであることが多い。時には、当該情報が機微情報とみなされることがある。例えば、社内の懲戒通知書、財務・給与交渉、又は戦略会議の議事録などが挙げられる。組織は、これらの媒体に内部運用機密レベルのラベルを貼り、本書に記載されているデータ抹消処理方法と関連付けるべきである。

データ抹消処理とは、媒体上の対象データ（データ抹消処理技術の対象となるデータ）へのアクセスを、所定レベルの回復労力では不可能にするためのプロセスである。データを復元しようとするときに適用される労力のレベルは、広範囲にわたる可能性がある。例えば、当事者は、媒体の特性に関する専門的なツール、スキル、又は知識を使用しない単純なキーボード攻撃を試みるかもしれない。全く反対に、当事者は広範な能力を持ち、最先端の実験室レベルの技術を応用できるかもしれない。

消去、除去、及び破壊は、媒体のデータ抹消処理を行うために取ることができる措置である。データ抹消処理の分類は以下のように定義される：

- **消去（Clear）**は、すべてのユーザアドレス指定可能なストレージ領域のデータに対してデータ抹消処理を行うための論理的な技術を適用し、単純な非侵襲のデータ回復技術から保護する。通常は、新しい値で書き換えたり、メニューオプションを使用してデバイスを工場出荷時の状態にリセットしたりする（書き換えがサポートされていない場合）など、ストレージデバイスへの標準的な読み書きコマンドを介して実行される。

- **除去（Purge）**は、物理的又は論理的な技術を適用して、最先端の研究室レベルの技術を使用しても対象データの回復を不可能にする。

- **破壊（Destroy）**は、最新の研究室レベルの技術を使用しても対象データの回復を不可能にし、且つその後のデータの保存に当該媒体が使用できないようにする。

データ抹消処理技術のより詳細な概要は、5 節に記載されている。特定のタイプの媒体／デバイスに対するデータ抹消処理要件は、付録 A に記載されている。

本ガイドのユーザには、情報を分類し、それが記録されている媒体の性質を評価し、機密性へのリスクを評価し、且つ媒体に対する将来の計画を決定することを勧める。その後、組織は、適切なデータ抹消処理方法を選択することができる。選択された方法は、コストや環境への影響などについて評価されるべきであり、そして機密性へのリスクを最も緩和し、且つプロセスに課せられた他の制約を最も満足させるような決定がなされるべきである。

2.6 暗号及び暗号化消去の利用

多くのストレージ製造メーカが、暗号化機能とアクセス制御機能を統合したストレージデバイス（自己暗号化ドライブ（SED）とも呼ばれる）を販売している。SED は、暗号化されていないデータが不用意にデバイスに保持される可能性を大幅に低減する常時暗号化が行われる点に特徴がある。エンドユーザは、指定された領域のすべてのデータが暗号化されていることを保証するための暗号化機能をオフにすることはできない。SED の重要な付加的な利点は、コントローラと記憶媒体を緊密に結合することで、暗号化鍵が保存されている場所をデバイスが直接アドレスできることであり、その一方、ソフトウェアを介して抽象化されたユーザアクセスインターフェースだけに依存するソリューションでは、これらの領域に直接アドレスできない可能性がある。

SED は、通常、ブート前アプリケーションや関連データの保存に特化した領域など、特定の明確に識別された領域を潜在的に除いた、ユーザアドレス可能な領域のすべてを暗号化する。

暗号化消去（CE）は、対象データの暗号化鍵に対してデータ抹消処理を行うことを可能にした対象データの暗号化を利用する。これにより、媒体上には暗号文だけが残り、読み出しアクセスを防ぐことで効果的にデータ抹消処理を行うことができる。

対象データの暗号化に使った暗号化鍵がないと、データは回復不可能である。その時、暗号化鍵なしにこの情報を復号するのに必要な労力のレベルは、暗号化鍵の強度、又はデータを暗号化するために使用される暗号アルゴリズム及び暗号利用モードの強度のいずれか小さい方である。

強力な暗号を使用する場合、対象データのデータ抹消処理は、当該対象データの暗号化に使用された暗号化鍵のデータ抹消処理に置き換えられる。したがって、CE を使用することで、他のデータ抹消処理技術よりもはるかに速いスピードで確実にデータ抹消処理を行うことができる。暗号化自体が、本ガイドライン文書で特定された制約下において、データ抹消処理を実現する役割を果たす。連邦政府機関は、SED が上述された条件を満たしていることを保証するために、FIPS 140 認証暗号モジュール[12]を使用しなければならない。

通常、CE は 1 秒の何分の 1 かの時間で実行することができる。これは、ストレージデバイスが大きくなるにつれて他のデータ抹消処理方法ではより多くの時間がかかるようになる場合に、特に重要である。また、CE は他のデータ抹消処理方法の補足又は追加としても使用することができる。

[12] NIST は、認証された暗号モジュールのリスト（http://csrc.nist.gov/groups/STM/cmvp/validation.html）及び暗号アルゴリズムのリスト（http://csrc.nist.gov/groups/STM/cavp/validation.html）を管理している。

2.6.1 媒体の除去に CE を使用しない場合

- 以前に機微データがデバイスに保存されたことがあり、その後に当該デバイスのデータ抹消処理が最初に行われないまま暗号化が有効になった場合は、CE を使用して媒体を除去してはならない。

- 暗号化を始める前に、データ抹消処理が行われないまま機微データがデバイス上に保存されたかどうかが不明な場合は、CE を使用してはならない。

2.6.2 CE の使用を検討する場合

- 媒体に保存する前に、CE の対象となるすべてのデータ（データ及び仮想化されたコピーを含む）が暗号化されている場合は CE の使用を検討する。

- 暗号化鍵（対象データの暗号化鍵や関連するラッピング鍵など）が保存されている媒体上の場所がわかり、当該鍵が保存されている媒体上の実際の場所に対処することが保証され、適切な媒体固有のデータ抹消処理技術を使用してそれらの領域のデータ抹消処理が実行できる場合に、CE の使用を検討する。

- 対象データの暗号化に使用された暗号化鍵のすべてのコピーについてデータ抹消処理が行われたことを確認できる場合は、CE の使用を検討する。

- 対象データの暗号化鍵自体が 1 つ以上のラッピング鍵で暗号化されており、且つ対応するラッピング鍵のデータ抹消処理が実行できると確信している場合は、CE の使用を検討する。

- CE の操作を行うためにデバイスが提供するコマンドを明確に識別して使用できる能力がユーザにあると確信した場合は、CE の使用を検討する。

2.6.3 その他の CE に関する考慮事項

暗号化鍵がストレージデバイスの外に存在する場合（典型的にはバックアップや第三者預託のため）、将来、暗号化された媒体に保存されたデータを回復するためにその鍵が使用される可能性がある。

CE は、対象データの暗号化に使用された暗号化鍵が適切に保護されているという確信が組織にある場合にのみ、データ抹消処理方法として使用されるべきである。このような保証は、ソフトウェアベースの完全ディスク暗号化ソリューションで使用されるような、ソフトウェア暗号モジュールでは得られにくい場合がある。なぜなら、これらの製品は通常、暗号化鍵をファイルシステム又はソフトウェアにアクセス可能な媒体上の他の場所に保存するためである。ソフトウェア暗号化モジュールと CE を併用することが適切かつ有利な状況もあるかもしれない。例えば、紛失したモバイルデバイスの迅速なリモートワイプの実行などである。しかし、組織が暗号化鍵の保護とデータ抹消処理プロセスによる当該鍵のすべてのコピーの破壊の両方に確信を持っていない限り、CE は別の適切なデータ抹消処理方法と組み合わせて使用すべきである。

CE を使用したデータ抹消処理は、鍵がデバイス外においてどのようにどこで保管され管理されているかについて、高いレベルの信頼性を組織が持っていない限り、鍵がバックアップ又は第三者預託されたデバイスに対して信頼すべきではない。そのようなデータや資格情報、鍵のバックアップ又は第三者預託されたコピーなどは、別に定めるデバイスのデータ抹消処理ポリシーの対象とすべきである。その

ポリシーでは、バックアップ又は第三者預託されたコピーが実際に保存されているデバイスの範囲内でそのバックアップやコピーを取り扱うべきである。

適用可能な考慮事項のリストと、ベンダが実装したメカニズムを報告する方法のサンプルは、付録 E に記載されている。CE を実装しようとするユーザは、ここで特定された考慮事項が対処され、FIPS 140 認証暗号モジュールのみを使用しているといった合理的な保証（付録 E に記載されているベンダの報告書など）をベンダに求めるべきである。

2.7 データ抹消処理及び廃棄の決定に影響を与える要因

データ抹消処理の決定を行う際には、いくつかの要因を、システムの機密性のセキュリティ分類と併せて、考慮すべきである。データ抹消処理プロセスの費用対効果のトレードオフは、最終的な決定に先立って理解されるべきである。例えば、ディスケットのような安価な媒体を消磁することは、費用対効果が高くない場合がある。消去又は除去が推奨されるソリューションであっても、（訓練や追跡、検証などを考慮すると）媒体を破壊する方がそれ以外の選択肢のいずれかを使用するよりも費用対効果がより高い場合がある。組織は、媒体を破壊するほうが合理的であり、既存リスクの評価によっても示される場合には、適用されるデータ抹消処理のレベルを高める能力を保持する。

組織は、以下のような環境要因を考慮すべきである（ただし、これらに限定されない）：

- 組織がデータ抹消処理を必要とする記憶媒体の種類（書換不可の光学媒体、磁気媒体など）及びサイズ（メガバイト、ギガバイト、テラバイトなど）はどうか？
- 媒体上に保存されているデータに対する機密性要件は何か？
- 媒体は管理された領域で処理されるのか？
- データ抹消処理プロセスは組織内で行うべきか、外注すべきか？
- 媒体の種類別にデータ抹消処理される媒体の予想量どの程度か？[13]
- データ抹消処理装置やツールの利用可否はどうか？
- データ抹消処理装置／ツールを使用する職員の訓練レベルはどの程度か？
- データ抹消処理にはどのくらいの時間がかかるか？
- ツール、訓練、検証、及び媒体の供給ストリームへの再投入を考慮した場合のデータ抹消処理コストはどの程度か？

2.8 データ抹消処理の範囲

ほとんどのデータ抹消処理操作では、操作の対象は、ユーザが媒体上に保存したすべてのデータである。しかし、場合によっては、媒体の一部分についてデータ抹消処理をしたいという要望や必要性があ

[13] NIST SP800-36, *Guide to Selecting Information Technology Security Products,* October 2003, 67 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-36.

るかもしれない。部分的データ抹消処理は、媒体の一部に保存された機微データが別の領域（再配置された不良ブロックなど）には配置されていないことを確認するのが困難な場合があるため、多少のリスクを伴う。さらに、データ抹消処理のためにストレージデバイスのベンダが提供する専用インタフェースは、通常デバイスレベルで動作し、媒体の一部分に適用することができない。その結果、部分的データ抹消処理は、ユーザが利用可能な典型的な読み書きコマンドに依存するのが普通であり、それらは、関心のある媒体領域に直接アドレスするために存在している可能性があるインタフェースの抽出機能を迂回することができないかもしれない。

暗号化機能を統合したことを特徴とするストレージデバイスの中には、いくつかの形態の部分的データ抹消処理をサポートする独自メカニズムを CE が提供するものもある。これらのデバイスの中には、データの一部を異なる暗号化鍵で暗号化する機能をサポートしているものもある（例えば、異なる暗号化鍵で異なるパーティションを暗号化する）。インタフェースが暗号化鍵の一部分のみのデータ抹消処理をサポートしている場合、CE による部分的データ抹消処理が可能である。媒体に適用される他のデータ抹消処理技術と同様に、保証レベルは、ベンダの実装及び確実にデータ抹消処理できる領域にのみデータが保存されていたことを保証するレベルの両方に依存する。データはこれらの領域の外に保存されることがある。なぜなら、ユーザ又はシステム上のソフトウェアが媒体上の指定された領域の外にデータを移動させたため、又はユーザが完全には理解していない方法でストレージデバイスが媒体にデータを保存したためである。

部分的データ抹消処理ですべての機微データを効果的に対処することを確実に保証することは困難であるため、可能な限り、デバイス全体のデータ抹消処理を行うほうが部分的データ抹消処理よりも望ましい。組織は、このアプローチの潜在的なリスクを理解し、本節で前述した要因とビジネスミッションや特定のユースケースとのバランスをとりながら、この手法について適切に判断すべきである。例えば、データセンタ内のドライブには、複数の顧客からの顧客データが保存されているかもしれない。ある顧客がサービスを終了し、別の顧客が同じ媒体上にデータを保存し始める場合、組織は、同じストレージデバイスに保存されている他の顧客のデータを媒体の他の領域に保持するために、部分的データ抹消処理を適用することを選択するかもしれない。その理由は、ドライブが組織の物理的な所有物であり続けること、顧客によるアクセスがインタフェースコマンドに制限されていること、及び組織が当該媒体の特定部分に対して利用可能な部分的データ抹消処理メカニズムを信頼していることである。部分的データ抹消処理の代替方法では全くデータ抹消処理が行われない場合には、部分的データ抹消処理は検討すべき利点を提供する。

3 役割と責任

3.1 プログラムマネージャ／機関長官

“最終的に、組織の成功に対する責任はその組織の上級管理職にある[14]。”効果的な情報セキュリティガバナンス構造を確立することにより、彼らは、組織のミッションをサポートするために、組織のコンピュータセキュリティプログラムとその全体的なプログラムの目標、目的、及び優先順位を確立する。最終的に、組織の長は、適切なリソースがプログラムに適用されていることを確認し、プログラムの成功を確実にする責任がある。上級管理者は、情報の種類と場所を正しく識別し、適切に情報のデータ抹消処理を行うリソースが配分されていることを確認するためのリソースが割り当てられていることを保証する責任がある。

本節の残りの部分におけるその他の責任は説明のためのものであり、その意図は、組織が媒体のデータ抹消処理を行うための様々な責任を考え抜き、それらの責任を適切に割り当てることを確実にすることである。

3.2 最高情報責任者（CIO）

CIO[15]は、情報セキュリティポリシーを公布する責任がある。このポリシーの構成要素に、情報の廃棄と媒体のデータ抹消処理がある。情報管理者である CIO は、組織又は現場でのデータ抹消処理要件が本文書のガイドラインに従うことを保証する責任がある。

3.3 情報システム所有者

情報システム所有者[16]は、保守契約や契約上の合意が適切に行われ、情報の開示が組織に与える影響に見合う水準でシステム媒体及び情報の機密性を保護するのに十分であることを確認すべきである。

3.4 情報の所有者／管理者

情報所有者は、必要に応じて、サービス提供者がオンサイトの媒体メンテナンスの適切な監督を行っていることを確認すべきである。また、情報所有者は、自らの管理下にある情報の機微性を十分に理解し、情報の利用者がその機密性及び媒体のデータ抹消処理のための基本的な要件を認識していることを確認する責任がある。

---

[14] NIST SP800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems,* February 2006, 16. http://csrc.nist.gov/publications/PubsSPs.html#800-18.

[15] 1996 年情報技術管理改革法（“Clinger-Cohen Act”; P.L. 104-106 (Division E) 10 Feb. 1996）に基づき、組織が正式な CIO 職を指定していない場合、FISMA は関連する責任を同格の組織職員によって取り扱われることを要求する。

[16] 情報システム所有者の役割は、特定の組織や情報システムのシステム開発ライフサイクルの段階に依存して、様々な方法で解釈することができる。組織によっては、情報システム所有者を“プログラム管理者”や“ビジネス所有者／資産所有者／ミッション所有者”と呼ぶこともある。

3.5 上級機関情報セキュリティ責任者（SAISO）

SAISO は、情報の廃棄及び媒体のデータ抹消処理に関する情報セキュリティポリシー要求事項が実装され、組織全体でタイムリーかつ適切な方法で実行されることを確認する責任がある。また、SAISO は、データ抹消処理手順を理解し、適切に実施するために、技術的な基盤／人材へのアクセスも必要とする。

3.6 システムセキュリティ管理者／責任者

この取り組みにおいてシステム管理担当者を支援するのは、日々のセキュリティ実施／管理業務を担当するシステムセキュリティ管理者／責任者の責任であることが多い。この担当者は、普通、コンピュータセキュリティプログラム管理室の所属ではないが、特定のシステムのセキュリティ施策を調整する責任がある。この役割は、コンピュータシステムセキュリティ責任者又は情報システムセキュリティ責任者と呼ばれることもある。

3.7 資産管理責任者

資産管理責任者は、組織内で再配布されたり、外部団体に寄贈されたり、破壊されたりしたデータ抹消処理済みの媒体やデバイスが適切に処分されていることを確認する責任がある。

3.8 記録管理責任者

記録管理責任者には、システムやデータの所有者又は管理者に満たされなければならない保存要件を助言する責任があり、媒体のデータ抹消処理によって保存すべき記録が破壊されないようにする。

3.9 プライバシー保護責任者

プライバシー保護責任者は、プライバシー情報及びそれが記録された媒体の廃棄をめぐるプライバシー問題に関する助言を行う責任がある。

3.10ユーザ

ユーザは、自らに与えられた業務を遂行し情報の適切な取り扱いを確保するために、自らが使用する情報の機密性を知り、理解する責任がある。

4 情報のデータ抹消処理と廃棄の意思決定

組織は、異なるレベルの機密性を持つストレージデバイスを維持することがあり、デバイスに保存されるデータの種類を理解することが重要である。なぜなら、データの機密性を維持するための効率性と有効性のバランスを最適化する技術を適用するためである。データの機密性レベルは、FIPS 199 に記載されている手順を使用して特定すべきである。SP800-60 改訂 1 版に記載されている情報タイプとセキュリティ分類の対応付けに関する追加情報が利用可能である。

ほとんどのデバイスが何らかの形で消去をサポートしているが、すべてのデバイスが信頼性の高い除去メカニズムを持っているわけではない。中程度の機密性のあるデータについて、媒体の所有者は、時間、知識及びデータ復元のスキルを持った人がいくつかのデータを復元できるかもしれないということを認識した上で、媒体に消去技術を適用するリスクを受け入れる選択をすることができる。

環境への懸念、(組織内での、又は媒体の販売や寄付による）媒体の再利用要望、媒体や媒体デバイスのコスト、又はある種の媒体を物理的に破壊することの難しさを考慮する場合、除去（及び場合によっては消去）の方が破壊よりも適切であるかもしれない。

リスク判断には、媒体から復元可能な情報が開示された場合の潜在的な結果、情報復元にかかるコストとその有効性、及びデータ抹消処理にかかるコストとその有効性を含めるべきである。さらに、データの機微性を保持する期間も考慮すべきである。これらの値は、環境によって異なる場合がある。

媒体に含まれる情報の機密性のセキュリティ分類に見合ったデータ抹消処理の決定を行うことを支援するために、組織は、本節での説明と図 4-1 を使用することができる。決定プロセスは、媒体の種類ではなく、情報の機密性に基づく。組織が個々のケースに応じて最適なデータ抹消処理方法を決定したら、媒体の種類がデータ抹消処理の目標を達成するために使用される技術に影響を与える。

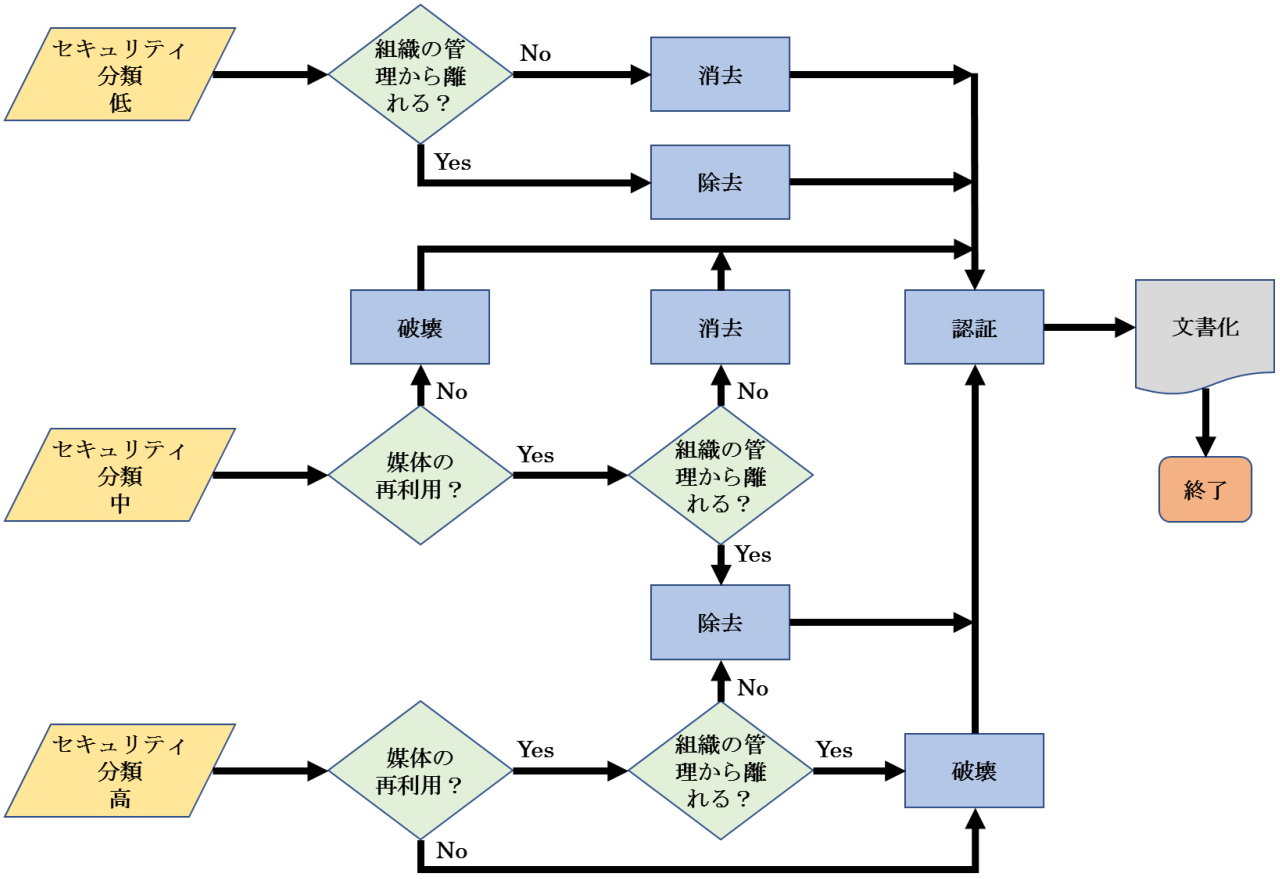

図 4-1：データ抹消処理及び廃棄の決定フロー

4.1 システムのライフサイクルにおける情報の決定

媒体のデータ抹消処理の必要性と実施方法は、システムのライフサイクル中の廃棄フェーズに到達する前に特定され、開発されるべきである。システム開発の開始時に、初期のシステムセキュリティ計画が策定されると[17]、媒体のデータ抹消処理の管理方法が作成・文書化され、展開される。データ抹消処理を行う能力に影響を与える重要な決定の一つは、システム内で使用する予定の媒体の種類を選択することである。これはほぼビジネス上の決定ではあるが、システム所有者は、この決定がシステムのライフサイクルの残りの期間を通してデータ抹消処理に必要なリソースの種類に影響を与えることを早期に理解しなければならない。

組織は、機微データを含む可能性のある記憶媒体を特定するための支援を製品ベンダに依頼することができる。この情報は、一般的には“ボラティリティに関する声明文（statement of volatility）”の中で文書化されている。その声明文は、データ抹消処理の容易さ又は困難さに基づいて、どの機器を購入するかの決定をサポートするために使用してもよい。ボラティリティに関する声明文は有用であるが、ベンダ間で声明文を比較する際には注意すべきである。なぜなら、ベンダによってボラティリティの詳細が異なる場合があるためである。

組織は、データ抹消処理のための媒体の特定に注意を払うべきである。使用される多くの製品は複数の形態の媒体を含み、それぞれが異なるデータ抹消処理方法を必要とする可能性がある。例えば、デス

[17] NIST SP800-18 Revision 1, p.19.

クトップコンピュータはハードドライブ、マザーボード、RAM 及び ROM を含み、モバイルデバイスは不揮発性リムーバブルメモリだけでなくオンボードの揮発性メモリを含んでいる。

暗号化消去など、迅速に適用できる技法の利用可能性の向上は、データ抹消処理技術と技法を組み合わせることで、組織が不注意な開示をするリスクを低減する機会を提供する。例えば、組織は、そのようなリスクや暴露を減らすために、データ抹消処理施設で“正式に”データ抹消処理を行うために媒体を送るにあたって、当該媒体を取り外す前にユーザのデスクトップで暗号化消去を適用することを選択できる。

4.2 セキュリティ分類の決定

システムのライフサイクルの初期段階では、システムの機密性に対するセキュリティ分類を含めて、FIPS 199、NIST SP800-60 改訂 1 版、又は CNSSI 1253[18]に記載されているガイダンスを使用してシステムを分類する。このセキュリティ分類は、少なくとも 3 年ごと（又はシステム内で重大な変更が発生した場合）の見直しによりシステムの寿命を通じて再検証され、機密区分に必要な変更を行うことができる。セキュリティ分類が完了した後、システムの所有者は、システムの情報を適切に保護していることを保証するデータ抹消処理プロセスを設計することができる。

多くの情報は、特定のシステムに関連付けられているのではなく、通常は紙に書かれた内部のビジネスコミュニケーションに関連付けられている。組織は、これらの媒体に内部運用機密レベルのラベルを貼り、本書に記載されているデータ抹消処理方法と関連付けるべきである。

4.3 媒体の再利用

データ抹消処理の重要な決定は、媒体の再利用又はリサイクルを計画しているかどうかである。媒体のいくつかの形態は、組織のリソースを節約するために再利用されることが多い。

損傷又はその他の理由で組織の内外を問わず媒体の再利用を想定していない場合、最もシンプルで費用対効果が最も高い管理方法は破壊することかもしれない。

4.4 媒体の管理

組織のデータ抹消処理の決定に影響を与える要因は、誰が媒体を管理し、アクセスできるかである。この側面は、媒体が組織の管理から離れるときに考慮しなければならない。媒体の管理は、当該媒体がリース契約から返却された場合、又は組織外で再利用するために寄付又は再販された場合に、譲渡されることがある。媒体の管理例としては、以下のようなものがある：

[18] Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, March 27, 2014. https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

組織の管理下にある場合：

- 保守のために引き渡される媒体については、組織と保守提供者との間に契約上の合意があり、且つその合意で情報の機密性保護を具体的に提供している場合、組織の管理下にあると見なされる。

- 組織の監督下で組織のサイトにて保守事業者が行っている保守も、組織の管理下にあると見なされる。

組織の管理下にない場合（外部による管理）：

- 保証、払い戻し又はその他の理由で交換される媒体であって、特定の媒体が組織に返却されない場合は、組織の管理下にはないと見なされる。

4.5 データ保護レベル

組織内であっても、様々なデータ保護ポリシーが確立されている場合がある。例えば、会社には技術部と営業部があるかもしれない。営業担当者はソースコードや回路図などの詳細な独自技術データにアクセスする必要がなく、エンジニアは自社の顧客の PII にアクセスする必要がない。両方とも同じ機密区分内にいるかもしれないが、文脈上は異なっており、必要な管理に関する内部規則及び外部規則は異なっている。このように、データ保護レベルは組織管理と補完する考慮事項である。データ抹消処理が必要かどうかを特定する際には、組織管理とデータ保護レベルの両方を考慮すべきである。

4.6 データ抹消処理及び廃棄の判断

組織がシステムの機密性の評価を完了し、情報のデータ抹消処理の必要性を判断し、データ抹消処理の適切な時間枠を決定し、使用する媒体の種類と媒体の廃棄を決定すると、適切で必要なレベルのデータ抹消処理について、効果的なリスクベースの決定を行うことができる。繰り返しになるが、環境要因や媒体の種類によって、データ抹消処理のレベルが変化する可能性がある。例えば、紙のコピーを除去しても一般的には意味がないので、それらを破棄することが許容可能な代替案になる。

データ抹消処理の意思決定が完了したら、組織はその決定を記録し、これらの決定をサポートするためのプロセス及び適切なリソースが配置されていることを確認すべきである。このプロセスは、媒体のデータ抹消処理プロセスの中で最も困難な部分であることが多い。なぜなら、データ抹消処理だけでなく検証という措置も含まれるからであり、それらには意思決定と行動の把握、リソースの特定、及び主要な関係者との重要なインタフェースの保持などがある。

4.7 検証方法

選択された情報のデータ抹消処理及び廃棄のプロセスを検証することは、機密性を維持するための必要不可欠なステップである。2 種類の検証を検討すべきである。一つ目は、データ抹消処理が適用されるたびに検証する（適用可能な場合において。ほとんどの破壊技術は、データ抹消処理された媒体の各部分についての実用的な検証をサポートしていないため）。二つ目は、代表的なサンプリング検証であり、媒体のうち選択された一部分に適用される。可能であれば、サンプリングは、もともとのデータ抹

消処理作業の担当部門ではなかった人員によって実施されるべきである。低リスク許容の場合で完全な検証の後にサンプリングを行う場合には、元の検証で使用したものとは異なる検証ツールを使用すべきである。

4.7.1 設備の検証

データ抹消処理プロセスの検証だけが組織に求められる保証ではない。組織がデータ抹消処理ツール（消磁装置や専用ワークステーションなど）を使用している場合は、機器の校正、機器のテスト、及び定期的なメンテナンスも必要になる。

4.7.2 人材能力の検証

もう一つの重要な要素は、データ抹消処理を実施する人員に対する潜在的な訓練ニーズ及び現在の専門性である。組織は、設備オペレータがデータ抹消処理機能を実行する能力があることを確認すべきである。

4.7.3 データ抹消処理結果の検証

データ抹消処理検証の目的は、対象データのデータ抹消処理が効果的に行われたことを確認することである。デバイスインタフェース（ATA 又は SCSI ストレージデバイス、ソリッド・ステート・ドライブ（SSD）など）がサポートされている場合、（実験室以外の）効果的なデータ抹消処理の最高レベルの保証は、通常、アクセス可能なすべての領域を完全に読み取って、データ抹消処理された期待値がすべてのアドレス可能な場所にあることを検証することによって達成される。時間と外的要因が許すならば、完全な検証を行うべきである。この検証方法は、通常、データ抹消処理後に、ネイティブインターフェイスを介してデータを読み書き可能な運用状態にデバイスがある場合にのみ適用される。

組織が代表サンプリングを選択する場合には、電子媒体のデータ抹消処理検証に適用される 3 つの主な目標がある：

1. 解析ツールを適用するたびに、媒体上の疑似ランダムな位置を選択する。これにより、機微データが残っている状況において、媒体の一部分のみをデータ抹消処理するだけのデータ抹消処理ツールでは検証に成功する可能性は低くなる。

2. アドレス指定可能な空間（ユーザアドレス指定可能エリアと予約エリア）全体の領域を選択する。例えば、概念的に媒体を同じ大きさのサブセクションに分割する。媒体が十分にカバーされるように、十分な数のサブセクションを選択する。実際のサブセクションの数は、デバイス及びアドレッシング方式によって異なる。LBA アドレッシングを利用するストレージデバイスのサブセクションの推奨される最少数は 1,000 である。各サブセクション内から少なくとも 2 つの重ならない擬似ランダムな位置を選択する。例えば、1,000 個の概念的なサブセクションが選択された場合には、媒体アドレス空間の 1,000 個のサブセクションの 1 番目から少なくとも 2 個の擬似ランダムな位置が読み込まれて検証され、次に 2 番目のサブセクションから少なくとも 2 個の擬似ランダムな位置が読み込まれて検証され、以下同様に繰り返す。

a. 加えて、既に特定された場所に加えて、ストレージデバイス上の最初と最後のアドレス可能な場所を含める。

3. 各々の連続したサンプル位置（最初と最後のアドレス指定可能な位置のものを除く）は、サブセクションの少なくとも 5%をカバーし、サブセクション内の他のサンプルと重ならないようにすべきである。重複しない 2 つのサンプルが与えられたとき、すべてのサブセクションで 2 つのサンプルを採取した後、結果として得られる検証は媒体の少なくとも 10%をカバーすべきである。

暗号化消去は、書き換えやブロック消去などの手順とは異なる検証上の考慮事項がある。なぜなら、暗号化消去後の物理媒体の内容は既知ではない可能性があるためで、結果として所定の値と比較することができないからである。暗号化消去を活用する場合、検証には複数のオプションがあり、それぞれが媒体の一部分のクイックレビューを使用する。それぞれが、媒体全体からサンプリングされる疑似ランダムな場所の選択を含む。

最初のオプションは、暗号化消去の前に疑似ランダムな場所を読み込み、暗号化消去の後に再度読み込んで結果を比較する。これが最も効果的な検証手法である可能性が高い。別のオプションは、媒体全体で文字列を検索したり、既知の場所にあるファイル、例えば特定の領域に保存されている可能性の高いオペレーティングシステムファイルなどを探したりすることである。

各サンプルの場所やサイズの大きさは、データ抹消処理アプリケーションをホストするマシンの記憶媒体に対象データを転送する際のリスクを考慮すべきである。その結果、暗号化消去技術の検証でカバーされる媒体の割合は比較的小さい（少なくとも、非暗号化によるデータ抹消処理技術の検証における上記ガイダンスの 10%よりは小さい）かもしれないが、それでもアドレス可能な領域の広い範囲に適用されるべきである。

しかし、これらの技術は常に利用できるとは限らない。なぜなら、データ抹消処理を行う人が、ドライブに保存されたデータにアクセスして読み取るために必要な認証トークンを持っていない可能性があるためである。組織が、CE が記憶媒体のデータ抹消処理を効果的に行ったことを検証できない場合、CE と組み合わせて又は CE の代わりに、検証可能な代替のデータ抹消処理方法を採用すべきである。

データ抹消処理プロセスの一部として、データ抹消処理操作後に各媒体のピースに対して実行される検証に加えて、別の検証ツールを使用した二次検証のために、媒体製品の一部分がランダムに選択されるべきである。二次検証ツールは別の開発者によるものであるべきである。二次検証については、完全検証を行うべきである。データ抹消処理された媒体の少なくとも 20%（データ抹消処理された媒体製品数）を検証すべきである。二次検証では、一次動作が期待通りに動作していることを保証する。

4.8 文書化

データ抹消処理後、データ抹消処理された電子媒体の各部分について、媒体廃棄証明書を作成すべきである。媒体廃棄証明書は、実施された措置を記録した紙又は電子記録である。例えば、最近のほとんどのハードドライブは、モデルやシリアル番号などの値を示すラベルにバーコードが含まれている。データ抹消処理を行う人は、追跡アプリケーションに詳細を入力し、媒体がデータ抹消処理されたときにそれぞれのバーコードをスキャンするだけでよいことがある。システムによっては媒体への物理的なアクセスが非常に困難な場合もあるため、自動文書化が重要になる場合がある。

媒体廃棄証明書を作成するかどうか、及びどの程度のデータを記録するかについての決定は、媒体上のデータの機密性レベルに依存する。機密性が非常に低いデータを含む多数のデバイスについては、組織は証明書を作成しないことを選択できる。

証明書を完全に作成する場合には、少なくとも以下の詳細について証明書に記録すべきである：

- 製造者
- モデル
- シリアル番号
- 組織的に割り当てられた媒体番号又は資産番号（該当する場合）
- 媒体タイプ（磁気媒体、フラッシュメモリ、ハイブリッドなど）
- 媒体ソース（すなわち、媒体の提供先であるユーザ又はコンピュータ）
- データ抹消処理前の機密区分（オプション）
- データ抹消処理の説明（すなわち、消去、除去、破壊）
- 利用する方法（消磁、上書き、ブロック消去、暗号化消去など）
- 利用するツール（バージョンを含む）
- 検証方法（完全検証、クイックサンプリングなど）
- データ抹消処理後の機密区分（オプション）
- データ抹消処理後の宛先（既知の場合）
- データ抹消処理と検証の両方に対して：
    - 氏名
    - 役職／肩書き
    - 日付
    - 場所
    - 電話番号又はその他の連絡先情報
    - 署名

任意で、組織は、以下のことを記録することを選択してもよい（既知の場合）。

- データのバックアップ（すなわち、データがバックアップされたかどうか、及びバックアップされた場合はどこにあるか）

証明書のサンプルは付録 G に記載されている。

記憶デバイスの検証が成功し、データ抹消処理によって記憶デバイスの機密性レベルが低下した場合、以前の機密性レベルを示すデバイス上のマーキングはすべて削除されるべきである。更新された機密性レベルを示す新しいマーキングを適用すべきである。ただし、当該デバイスが組織を離れる予定であって、機微データの再導入を防ぐために当該デバイスが組織を離れるまでアクセスが注意深く管理された場所に保管されている場合は除く。

媒体廃棄証明書の価値は、媒体のライフサイクルにおける組織の記憶媒体の取り扱いに依存する。媒体が環境に導入された時、媒体が最後に使用された場所から離れた時、及びデータ抹消処理先に到達した時の記録が維持されていれば、組織は、企業全体で媒体のデータ抹消処理がどの程度うまく適用されているかを最も効果的に特定することができる。データ抹消処理先以外の場所で追跡が途絶した場合、データ抹消処理の記録は、特定の媒体のデータ抹消処理を行ったことを示すだけで、組織が運用環境に導入されたすべての媒体のデータ抹消処理を効果的に行うかどうかということではない。

5 データ抹消処理方法のまとめ

いくつかの異なる方法が、媒体のデータ抹消処理のために使用することができる。本節では、最も一般的な 4 つの方法を紹介する。本ガイドのユーザは、廃棄する情報を分類し、その情報が記録されている媒体の特性を評価し、機密性のリスクを評価し、当該媒体の将来の計画を決定すべきである。そして、表 5-1 の情報を用いて、適切なデータ抹消処理方法を決定する。選択された方法は、コスト、環境への影響などを評価すべきであり、不正な情報開示のリスクを最も軽減するように決定すべきである。

表 5-1：データ抹消処理方法

方法	説明
消去 （Clear）	媒体のデータ抹消処理を行う一つの方法は、ソフトウェア製品又はハードウェア製品を使用して媒体上のユーザアドレス指定可能な記憶領域を非機微データで上書きすることであり、その時にデバイスの標準的な読み書きコマンドを使用する。このプロセスは、ファイルの論理的な保存場所（例えば、ファイル割り当てテーブル）を上書きすることだけでなく、すべてのユーザアドレス指定可能な場所を上書きすることも含むべきである。上書きプロセスのセキュリティ目標は、対象データを非機微データに置き換えることである。上書きは、破損している媒体や書き換え不可能な媒体には使用できず、また機微データが保持されている可能性のあるデバイスのすべての領域に対応できない場合がある。さらに、媒体の種類やサイズが、上書きが適切なデータ抹消処理方法であるかどうかに影響を与える可能性がある。例えば、フラッシュメモリベースのストレージデバイスには、予備セルが含まれており、ウェアレベリングを実行する場合がある。この場合、このアプローチを使用して以前のすべてのデータのデータ抹消処理を行うことはユーザにとって不可能である。なぜなら、当該デバイスは、ネイティブの読み書きインタフェースを使用して機微データが保存されているすべての領域に直接アドレスすることをサポートしていない可能性があるためである。 消去操作は、専用のストレージデバイス以外の媒体の場合には、文脈的に異なる場合がある。例えば、デバイス（基本的な携帯電話やオフィス機器の一部など）では、当該デバイスを工場出荷時状態に戻す機能（通常、ファイルポインタを削除するだけ）を提供するだけで、不揮発性ストレージの内容に対して書き換えたり、媒体固有の技術を適用したりする機能を直接サポートしない。書き換えがサポートされていない場合、デバイス及び関連する媒体を消去するには、メーカリセットや書き換えを含まない手順が唯一の選択肢となる場合がある。これらであっても、ユーザが利用できるデバイスインタフェースが消去したデータの復元を容易にしない限り、消去の定義を満たす。
除去 （Purge）	除去の方法（媒体によって異なり、本文書全体でさらに記載されている考慮事項を適用しなければならない）には、上書き、ブロック消去、及び暗号化消去（Cryptographic Erase）などが含まれる。これらは、専用の標準化されたデバイスのデータ抹消処理コマンドを使用して、一般的な読み書きコマンドに内在する抽出機能を迂回するように媒体固有の技術を適用する。 破砕技術もまた、適切な媒体タイプに効果的に適用された場合、デバイスを除去された状態にする。例えば、焼却、裁断、分解、消磁、及び粉砕など。これらすべてのアプローチに共通する利点は、最先端の研究室レベルの技術を使用してもデータを回復することが不可能であることを保証することである。しかし、曲げたり、切断したり、緊急時

	処置（ストレージデバイスに穴を開けるために銃器を使用するなど）を使用したりすることは、媒体に損傷を与えるだけの可能性があり、媒体の一部は損傷を受けずに残っているため、高度な研究室レベルの技術を使用してアクセスが可能である場合もある。 消磁（Degaussing）は、消磁の強度が媒体の保磁力に合わせて注意深く調整されている場合、レガシーの磁気デバイスを除去された状態にする。保磁力は、ラベルに記載されている情報のみからでは判断が難しい場合がある。したがって、保磁力の詳細については、デバイスメーカに問い合わせられたい。フラッシュメモリベースのストレージデバイスや非磁性の不揮発性ストレージデバイスも含む磁気ストレージデバイスに対しては、消磁だけに頼るべきではない。消磁は、多くの種類のデバイスを使用不能にする（そのような場合、消磁は破砕技術でもある）。
破壊 （Destroy）	媒体の破壊には、様々な種類や技術、手順がある。技術によっては、デバイスインタフェースを介して対象データを復元することを不可能にし、その後のデータの保存に使用できなくなることがある。しかし、最新の研究室レベルの技術を用いても対象データを復元することが不可能でない限り、当該デバイスは破壊されたとは見なされない。 ● *分解（Disintegrate）*、*粉砕（Pulverize）*、*溶融（Melt）*、*及び焼却（Incinerate）*：これらのデータ抹消処理方法は、媒体を完全に破壊するように設計されている。通常は、これらは外部委託された金属破砕施設又は認可を受けた焼却施設で実施され、それらの施設ではこれらの措置を効果的かつ安心安全に実施するための特定の能力を有している。 ● *裁断（Shred）*：紙のシュレッダは、外側の容器を物理的に取り除いた媒体について、ディスケットのような柔軟な媒体であれば破壊するために使用することができる。ごみの細断サイズは、データの機密性に比例して、データが再構築できないことが合理的に保証されるほど十分に小さくするべきである。データの再構成をさらに困難にするために、裁断された媒体に同種の非機微材料（例えば、裁断された紙や裁断された柔軟な媒体）を混合することができる。 破砕技術の適用は、以下の場合の唯一の選択肢となる可能性がある。媒体が破損していて消去や除去など他の技術が当該媒体に効果的に適用できない場合、又は消去方法や除去方法での検証が失敗した場合（既知又は未知の理由による）。

付録 A ー 最低限のデータ抹消処理についての推奨事項

決定が、ひとたび 4 節に記載されたような要因に基づき、関連する組織的環境要因を適用して行われた後に、本付録の表を使用して、特定の媒体の推奨されたデータ抹消処理を決定することができる。その推奨は、当該媒体からの情報の不正開示による被害の影響を軽減するために、FIPS 199 のシステムの機密性のセキュリティ分類を反映させるべきである。

ここでは本付録の表の使用が推奨されるが、消去、除去、及び破壊の意図を満たす他の方法も存在する。本表に記載されていない方法が、組織で検証され満足のいくものであることが確認される限り、適切なものであるかもしれない。本表には、利用可能な媒体のすべての種類が記載されているわけではない。本ガイドに含まれていない媒体の場合、組織は、当該媒体の消去、除去、又は破壊の意図を満たすプロセスを特定し、使用することが強く求められる。

組織や機関が信頼してテストしたデータ抹消処理技術や方法、ツールを持っている場合、その情報を、連邦政府セキュリティ実践（FASP）のウェブサイト [19]などの公開フォーラムを通じて共有することが強く奨励されている。FASP の取り組みは、重要インフラ保護（CIP）及びセキュリティのベストプラクティスを特定、評価及び普及させるための連邦最高情報責任者（CIO）評議会の連邦ベストセキュリティプラクティス（BSP）の試験的な取り組みが成功したことを受けて開始された。

各種類のデバイスに適切な初期設定を行うことは、データ抹消処理作業が可能な限り効果的に行われることを保証するのに役立つ。以下にいくつかの特定の項目を挙げているが、ユーザは、本リストの他の項目の推奨設定に関する追加情報についても、メーカの推奨事項及び DISA セキュリティ技術実装ガイド（STIG）[20]のようなガイドを確認することが推奨される。

モバイルデバイスが不揮発性リムーバブルメモリを有する場合、表 A-3 で特定されるデータ抹消処理プロセスによって対処されたかどうかにかかわらず、追加情報を含んでいる可能性がある。メーカや通信プロバイダに連絡して、当該リムーバブルメモリに保存されているデータの種類を確認し、そのリムーバブルメモリに対して追加のデータ抹消処理が必要かどうかを特定する。このようなリムーバブルメモリ及び関連するデータ回復機能に関する更なる詳細は、NIST SP800-101 改訂 1 版 [21]に記載されている。モバイルデバイスに含まれるデータの機微度や影響度のレベルに応じた適切なデータ抹消処理が当該モバイルデバイスに十分に組み込まれていない場合は、（情報を保護するために）当該デバイスを破壊するのではなく、データ抹消処理サービスを提供している企業に連絡して、そのサービスがニーズに合っているかどうかを確認することを検討されたい。

多くの内部ストレージデバイス（SD カードなどのリムーバブル媒体とは異なる）やインストールされた媒体を組み込んだストレージサブシステムは、専用のデータ抹消処理コマンドをサポートしている。これらのコマンドの利用可能性は、当該デバイスへのフリーズロックコマンドが発行される方法やタイミングなどのシステム（すなわち、BIOS/UEFI-Basic Input-Output System/Unified Extensible Firmware Interface）の特性によって影響を受ける場合がある。これらのコマンドを利用しやすくしてデータ抹消処理を実行できる専用のコンピュータや機器（例えば、システムの電源を入れた後にドライブの安全な接続を容易にする外付けドライブベイを持った PC やワークステーション）を使用することで、この問題の対処に役立つようになる。フリーズロックやコマンドの利用可能性に対するその他の制限を回避するための動作や方法はコンピュータによって異なるため、特定のモデルの動作の詳細につい

[19] http://csrc.nist.gov/groups/SMA/fasp/

[20] http://iase.disa.mil/stigs/

[21] NIST SP800-101 Revision 1, *Guidelines on Mobile Device Forensics*, May 2014, 87 pp. http://dx.doi.org/10.6028/NIST.SP.800-101r1.

てはコンピュータメーカに問い合わせられたい。この問題に対処するための代替アプローチが存在するが、コンピュータのハードウェア、ソフトウェア及びファームウェアによって異なる。また、カリフォルニア大学サンディエゴ校（UCSD）の磁気記録研究センタ（CMRR）では、この問題の回避策に関するツールや文書も開発している（詳細は付録 C を参照）。

データ抹消処理手順の中には、オプションの方法が追加されているものもある。オプションコンポーネントを適用するかどうかの選択は、データの機密性のレベル、及びデータ抹消処理手順の非オプション部分の正しい実装の保証に依存する。例えば、組織は、PII の場合であれば、利用可能なオプションコンポーネントがある適用された方法では当該オプションコンポーネントを実行すべきであると決定するかもしれない。また、オプションの方法を含め、いくつかの手順は合計でもわずか数分で実行できるため、時間的な要因に基づいて選択することもできる。その場合、組織は、データがより高い機密性カテゴリに属していなくても、オプションコンポーネントを含めることを決定する可能性がある。

表 A-1：ハードコピーストレージのデータ抹消処理

ハードコピーストレージ	
紙及びマイクロフォーム	
消去：	該当なし、破壊を参照されたい。
除去：	該当なし、破壊を参照されたい。
破壊：	サイズが 1 mm x 5 mm（0.04 インチ x 0.2 インチ）以下の小片を生成するクロスカットシュレッダを使用して紙を破壊する、又は 3/32 インチ（2.4 mm）のセキュリティスクリーンを備えた分解装置を使用して紙材料を粉砕／分解する。 マイクロフォーム（マイクロフィルム、マイクロフィッシュ、又はその他の縮小されたイメージ写真ネガ）を焼却して破壊する。
注意：	素材を燃やした場合、白い灰になるまで燃やさなければならない。

表 A-2：ネットワークデバイスのデータ抹消処理

ネットワークデバイス	
ルータ及びスイッチ（家庭用、ホームオフィス用、企業用）	
消去：	メーカのフルリセットを実行して、ルータやスイッチを工場出荷時のデフォルト設定にリセットする。
除去：	破壊を参照されたい。ほとんどのルータやスイッチは、データ内容を消去する（除去はしない）機能しか提供していない。ルータやスイッチが除去機能を提供している場合があるが、これらの機能はデバイスのハードウェア及びファームウェアに固有のものであり、注意して適用すべきである。デバイスメーカに問い合わせて、データ回復が不可能であり、且つ当該デバイスがファイルポインタを削除するだけではないことを保証するために、媒体依存の技術（書き換えやブロック消去など）を適用する除去機能を当該デバイスが持っているかどうかを確認する。

破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	消去と（該当する場合）除去の両方について、適切なデータ抹消処理手順に関する追加情報をメーカに問い合わせる。 ネットワークデバイスにはリムーバブルストレージが含まれている場合がある。リムーバブル媒体は、媒体固有の技術を使用して取り外し、データ抹消処理を実施しなければならない。

表 A-3：モバイルデバイスのデータ抹消処理

モバイルデバイス （デバイスにリムーバブルストレージがある場合、－最初に暗号化をチェックし、暗号化されている場合は暗号化を解除した後－、データ抹消処理の前にリムーバブルストレージを取り外す）	
Apple iPhone 及び iPad（現世代及び将来の iPhone と iPad）	
消去：	完全データ抹消処理オプションを選択（通常は「設定」>「一般」>「リセット」>「すべてのコンテンツと設定の消去」メニューにある）（暗号化消去がサポートされているので、データ抹消処理操作は数分で済むはずである。これは、暗号化がオンで、すべてのデータが暗号化されていることを前提とする。）リモートワイプを介して実行されるデータ抹消処理は消去操作として扱われるべきであり、データ抹消処理の結果を検証することはできない。
除去：	完全データ抹消処理オプションを選択（通常は「設定」>「一般」>「リセット」>「すべてのコンテンツと設定の消去」メニューにある）（暗号化消去がサポートされているので、データ抹消処理操作は数分で済むはずである。これは、暗号化がオンで、すべてのデータが暗号化されていることを前提とする。）
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	消去／除去操作の後、デバイスの複数の領域（ブラウザ履歴、ファイル、写真など）に手動で移動して、デバイス上に個人情報が保持されていないことを確認する。デバイスのデータ抹消処理を行う前に、データが安全な場所にバックアップされていることを確認する。 現在の iPhone はハードウェア暗号化を装備しており、デフォルトでオンになっている。

ブラックベリー（データ抹消処理前にデバイス上のデータをバックアップする）	
消去：	BB OS 7.x/6.x - 「オプション」>「セキュリティオプション」>「セキュリティワイプ」を選択し、データ抹消処理を行うデータの種類のサブカテゴリをすべて選択していることを確認する。その後、テキストフィールドに“blackberry”と入力した後、“Wipe”（BB OS 6.x では“Wipe Data”）をクリックする。BB OS 10.x では、（続ける前に媒体カードを復号する）「設定」＞「セキュリティとプライバシー」＞「セキュリティワイプ」を選択する。テキストフィールドに“blackberry”と入力した後、“Delete Data”をクリックする。データ抹消処理作業は、媒体のサイズによっては数時間かかることもある。リモー

	トワイプを介して実行されるデータ抹消処理は消去操作として扱われるべきであり、データ抹消処理の結果を確認することはできない。
除去：	BB OS 7.x/6.x - 「オプション」>「セキュリティオプション」>「セキュリティワイプ」を選択し、データ抹消処理を行うデータの種類のサブカテゴリをすべて選択していることを確認する。その後、テキストフィールドに“blackberry”と入力した後、“Wipe”（BB OS 6.x では“Wipe Data”）をクリックする。BB OS 10.x では、「設定」>「セキュリティとプライバシー」>「セキュリティワイプ」を選択する。テキストフィールドに“blackberry”と入力した後、“Delete Data”をクリックする。データ抹消処理作業は、媒体のサイズによっては数時間かかることもある。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	消去／除去操作の後、デバイスの複数の領域（ブラウザ履歴、ファイル、写真など）に手動で移動して、デバイス上に個人情報が保持されていないことを確認する。集中管理（BES）により、デバイスの暗号化が可能になる。 適切なデータ抹消処理手順の追加情報や、デバイスのバージョンや OS のバージョンによる実装の違いについての詳細は、メーカに問い合わせる。米国国防情報システム局（DISA）のセキュリティ技術実装ガイド（STIG）（http://iase.disa.mil/stigs/）などのガイドを使用して適切な初期設定を行うことで、データ保護とデータ抹消処理の保証のレベルが可能な限り強固なものであることを確認するのに役立つ。デバイスにリムーバブル記憶媒体が含まれている場合は、媒体依存の適切な手順を使用して当該媒体のデータ抹消処理を行うことを確認する。

Google Android OS を実行しているデバイス（暗号化を開始する前に電源に接続する）	
消去：	デバイスの設定メニューから工場出荷時リセットを実行する。例えば、Android 4.4.2 を実行している Samsung Galaxy S5 では、「設定」を選択し、「ユーザとバックアップ」で「バックアップとリセット」を選択し、「工場出荷時データリセット」を選択する。Android のその他のバージョンや携帯電話端末については、取扱説明書を参照する。リモートワイプを介して実行されるデータ抹消処理は消去操作として扱われるべきであり、データ抹消処理の結果を確認することはできない。
除去：	Android 端末の機能は、デバイスメーカやサービス提供者によって決定される。このように、工場出荷時データリセットオプションによって提供される保証のレベルは、特定のデバイスのアーキテクチャ及び実装の詳細に依存する場合がある。工場出荷時データリセットを使用して媒体を除去しようとするデバイスでは、eMMC Secure Erase 又は Secure Trim コマンド、もしくはその他の同等の方法（デバイスの記憶媒体によって異なる）を使用すべきである。 Android のバージョンによっては暗号化をサポートしており、暗号化消去をサポートしている場合がある。デバイスメーカ（又は、該当する場合はサービス提供者）に問い合わせて、データ回復が不可能であり、且つ当該デバイスがファイルポインタを削除するだけではないことを保証するために、媒体依存のデータ抹消処理技術又は暗号化消去を適用する除去機能を当該デバイスが持っているかどうかを確認する。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。

注意：	DISA STIG（http://iase.disa.mil/stigs/）などのガイドを使用して適切な初期設定を行うことで、データ保護とデータ抹消処理の保証のレベルが可能な限り強固なものであることを確認するのに役立つ。消去操作又は（該当する場合）除去操作の後、デバイスの複数の領域（ブラウザ履歴、ファイル、写真など）に手動で移動して、デバイス上に個人情報が保持されていないことを確認する。疑問がある場合は、デバイスのマニュアルを確認するか、技術サポートに連絡する。 消去と除去の両方について、適切なデータ抹消処理手順に関する追加情報をメーカに問い合わせる。

Windows Phone OS 7.1/8/8.x（暗号化のために集中管理が必要な場合がある）	
消去：	ライブタイル又はアプリリストから設定オプション（小さな歯車のマーク）を選択する。“設定”ページで、ページの一番下までスクロールして“About”ボタンを選択する。Aboutページには、下部に「電話リセット」ボタンがある。このボタンをクリックして次に進む。警告メッセージが表示されたら、「はい」を選択する。処理が完了すると、すべての個人的なコンテンツが消去されることに注意されたい。リモートワイプを介して実行されるデータ抹消処理は消去操作として扱われるべきであり、データ抹消処理の結果を確認することはできない。
除去：	Windows Phoneデバイスの機能は、デバイスメーカやサービス提供者によって決定される。このように、工場出荷時データリセットオプションによって提供される保証のレベルは、特定のデバイスのアーキテクチャ及び実装の詳細に依存する場合がある。工場出荷時データリセットを使用して媒体を除去しようとするデバイスでは、eMMC Secure Erase又はSecure Trimコマンド、もしくはその他の同等の方法（デバイスの記憶媒体によって異なる）を使用すべきである。 環境によっては、Windows Phoneデバイスは暗号化をサポートしており、暗号化消去をサポートしている場合がある。デバイスメーカ（又は、該当する場合はサービス提供者）に問い合わせて、データ回復が不可能であり、且つ当該デバイスがファイルポインタを削除するだけではないことを保証するために、媒体依存のデータ抹消処理技術又は暗号化消去を適用する除去機能を当該デバイスが持っているかどうかを確認する。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	消去／除去操作の後、デバイスの複数の領域（ブラウザ履歴、ファイル、写真など）に手動で移動して、デバイス上に個人情報が保持されていないことを確認する。デバイスのデータ抹消処理を行う前に、データを安全な場所にバックアップすることを確認する。 適切なデータ抹消処理手順、及びデバイスのバージョンやOSのバージョンによる実装の違いについての詳細は、メーカに問い合わせる。DISA STIG（http://iase.disa.mil/stigs/）などのガイドを使用して適切な初期設定を行うことで、データ保護とデータ抹消処理の保証のレベルが可能な限り強固なものであることを確認するのに役立つ。

その他の全てのモバイルデバイス。これには、携帯電話、スマートフォン、PDA、タブレット、及び前記のモバイルカテゴリでカバーされないその他のデバイスが含まれる。	
消去：	全ての情報を手動で削除してから、メーカのフルリセットを実行して、モバイルデバイスを工場出荷時状態にリセットする。リモートワイプを介して実行されるデータ抹消処理は消去操作として扱われるべきであり、データ抹消処理の結果を確認することはできない。
除去：	破壊を参照されたい。多くのモバイルデバイスでは、データ内容を消去する（除去はしない）機能しか提供していない。モバイルデバイスが除去機能を提供している場合があるが、これらの機能はデバイスのハードウェア及びソフトウェアに固有のものであり、注意して適用すべきである。デバイスメーカに問い合わせて、データ回復が不可能であり、且つ当該デバイスがファイルポインタを削除するだけではないことを保証するために、媒体依存の技術（書き換えやブロック消去など）又は暗号化消去を適用する除去機能を当該デバイスが持っているかどうかを確認する。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	消去操作又は（該当する場合）除去操作の後、デバイスの複数の領域（ブラウザ履歴、ファイル、写真など）に手動で移動して、デバイス上に個人情報が保持されていないことを確認する。 消去と（該当する場合）除去の両方について、適切なデータ抹消処理手順についてメーカに問い合わせる。

表 A-4：機器のデータ抹消処理

機器	
オフィス機器。これには、コピー、プリンタ、ファクス、複合機を含める。	
消去：	メーカのフルリセットを実行して、オフィス機器を工場出荷時のデフォルト設定にリセットする。
除去：	破壊を参照されたい。ほとんどのオフィス機器は、データ内容を消去する（除去はしない）機能しか提供していない。オフィス機器が除去機能を提供している場合があるが、これらの機能はデバイスのハードウェア及びファームウェアに固有のものであり、注意して適用すべきである。デバイスメーカに問い合わせて、データ回復が不可能であり、且つ当該デバイスがファイルポインタを削除するだけではないことを保証するために、媒体依存の技術（書き換えやブロック消去など）又は暗号化消去を適用する除去機能を当該デバイスが持っているかどうかを確認する。オフィス機器はリムーバブル記憶媒体を有していてもよく、その場合には、媒体依存のデータ抹消処理技術がその関連するストレージデバイスに適用されてもよい。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	消去と（該当する場合）除去の両方について、デバイスの複数の領域（保存されたファクス番号、ネットワーク構成情報など）に手動で移動して、デバイス上に個人情報が保持されていないことを確認する。

	消去と（該当する場合）除去の両方について、インク、トナー及び関連消耗品（ドラム、定着器など）が、適用される法律、環境、及び健康への考慮に従って、取り外され、破壊又は廃棄されるべきである。これらの消耗品の中には、機械が印刷したデータの痕跡を保持するものがあるため、データ暴露のリスクをもたらす可能性があり、それに応じて取り扱うべきである。デバイスが機能している場合、関連するリスクを減らすための１つの方法は、白紙ページを印刷し、次に黒一色のページを印刷し、さらに別の白紙ページを印刷することである。また、専用の色成分（シアン、マゼンタ、イエローのトナーや関連消耗品など）を有するデバイスでは、白紙ページの間に各色の１ページ分の印刷を行うべきである。印刷されたシートは、オフィス機器の機密保持（データ抹消処理前）に従って処理されるべきである。これらの手順は、一回限り使用のロール状のインク／トナーなどの消耗品には適用されないことに注意されたい。なぜなら、それらは通常再利用されることなく、したがって装置に追加のページを送ることによって対処されることはないためである。しかしながら、依然としてそれらは取り外して破壊する必要がある。さらに、オフィス機器の消耗品も健康リスクをもたらす可能性があり、印刷部品やトナーへの暴露を最小限に抑えるためには、適切な手順を用いて取り扱うべきである。 消去と（該当する場合）除去の両方について、適切なデータ抹消処理手順に関する追加情報をメーカに問い合わせる。

表 A-5：磁気媒体のデータ抹消処理

磁気媒体	
フロッピー	
消去：	組織で承認されたソフトウェアを使用して媒体を上書きし、上書きされたデータに対して検証を行う。消去パターンは、すべて 0 の列などの固定データ値を持つ少なくとも 1 回書き込みパスであるべきである。複数の書き込みパスやより複雑な値もオプションとして使用することができる。
除去：	組織的に承認され、媒体用に最低限の格付けをされた消磁装置で消磁する。
破壊：	フロッピーディスクやディスケットを、認可された焼却炉で焼却する又は裁断する。

磁気ディスク（フレキシブル又は固定）	
消去：	組織で承認されたソフトウェアを使用して媒体を上書きし、上書きされたデータに対して検証を行う。消去パターンは、すべて 0 の列などの固定データ値を持つ少なくとも 1 回書き込みパスであるべきである。複数の書き込みパスやより複雑な値もオプションとして使用することができる。
除去：	組織的に承認され、媒体用に最低限の格付けをされた消磁装置で消磁する。
破壊：	ディスクやディスケットを、認可された焼却炉で焼却する又は裁断する。
注意：	磁気ディスクを消磁すると、通常、そのディスクは永久に使用できなくなる。

リール及びカセット形式の磁気テープ	
消去：	テープ上のすべてのデータについて、組織的に承認されたパターンを用いて、最初にデータを記録したシステムと同様の特性を持つシステムを使用して、再記録（上書き）する。例えば、以前に録画した VHS フォーマットの機微なビデオ信号を、同等の VHS フォーマットのレコーダで上書きする。磁気テープのすべての部分は、既知の非機微の信号で一度だけ上書きされるべきである。再記録（上書き）による磁気テープの消去は、そのプロセスがテープ駆動機構を長時間占有するため、ほとんどのアプリケーションでは実用的ではないかもしれない。
除去：	磁気テープを、組織的に承認され、媒体用に最低限の格付けをされた消磁装置で消磁する。
破壊：	テープを、認可された焼却炉で焼却する又は裁断する。
注意：	破砕前にリール又はカセットからテープを取り外すなどの破砕の準備段階は不要である。ただし、破砕施設の要件やリサイクル対策に応じるために、部品（テープやリール、カセット）の分別が必要な場合がある。

ATA ハードディスクドライブ。*これには、PATA、SATA、eSATA などが含まれる。*	
消去：	組織的に承認され、検証された上書き技術／方法／ツールを使用して媒体を上書きする。消去パターンは、すべて 0 の列などの固定データ値を持つ少なくとも 1 回書き込みパスであるべきである。複数の書き込みパスやより複雑な値もオプションとして使用することができる。
除去：	4 つのオプションが利用可能である： 1. ATA Sanitize Device 機能セットコマンド（サポートされている場合）の一つを使用してデータ抹消処理を実行する。以下のオプションのいずれか又は両方を使用できる： a. 上書き EXT コマンド。媒体表面に固定パターンの 1 回書き込みパスを適用する。固定パターンの例としては、すべて 0 の列や擬似乱数パターンなどがある。媒体を除去するには、1 回書き込みパスで十分である。 *オプション*: 1 回書き込みパスの代わりに、擬似乱数パターンの合計 3 回の書き込みパスを使用し、そのうち 2 回目の書き込みパスが指定されたパターンの反転バージョンとなるように、反転オプションを利用する。 b. デバイスが暗号化をサポートしており、本書に記載されている技術仕様が満たされている場合の暗号化消去コマンド（CRYPTO SCRAMBLE EXT としても知られる） *オプション*: 暗号化消去がデバイスに正常に適用された後、上書きコマンド（サポートされている場合）を使用して、媒体に 0 の列又は擬似乱数パターンのパスを 1 回書き込む。上書きコマンドがサポートされていない場合、代替として、暗号化消去の後に Secure Erase 又は消去手順を適用することができる。 2. ATA セキュリティ機能セットの SECURE ERASE UNIT コマンドを強化消去モードで使用する（サポートされている場合）。ATA Sanitize Device 機能セットコマン

	ドは、その ATA デバイスでサポートされている場合、ATA セキュリティ機能セットの SECURITY ERASE UNIT コマンドよりも優先される。 3. 暗号化消去は、Trusted Computing Group（TCG）の Opal Security Subsystem Class（SSC）又は Enterprise SSC インタフェースを介して、必要に応じてコマンドを発行してすべての MEK を変更させることにより行う（本書に記載されている要件が満たされている場合）。詳細については、TCG 及びデバイスメーカに問い合わせる。 *オプション*: 暗号化消去がデバイスに正常に適用された後、上書きコマンド（サポートされている場合）を使用して、媒体に 0 の列又は擬似乱数パターンのパスを 1 回書き込む。上書きコマンドがサポートされていない場合、代替として、暗号化消去の後に Secure Erase 又は消去手順を適用することができる。 4. 組織的に承認された自動消磁装置で消磁するか、又はハードディスクドライブを分解し、組織的に承認された消磁スキャナで中に入っている円盤記録媒体を除去する。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	消磁以外の消去技術及び除去技術の各々について検証を行わなければならない。消磁によって提供される保証は、効果的な消磁装置を選択し、適切に適用し、その結果を定期的に抜き取り検査して、期待通りに動作していることを確認することに依存する。ATA データ抹消処理で反転オプションを使用した 3 パスの上書き手順を利用した場合、検証プロセスは単に（3 パス目で再度書き込まれたであろう）元のパターンを検索することである。 ストレージデバイスは構成機能をサポートしている場合があり、ATA 規格で定義されている媒体の一部へのアクセス能力を人為的に制限する。例えば、ホスト保護領域（HPA）、デバイス構成オーバーレイ（DCO）、アクセス可能な最大アドレスなどがある。専用のデータ抹消処理コマンドがこれらの領域に対応している場合であっても、それらの存在をそのままにしておくと、データ抹消処理手順の有効性を確実に検証する能力に影響を与える可能性がある。記憶媒体のアドレス指定可能な領域全体へのアクセス能力を制限する構成オプションはすべて、データ抹消処理技術を適用する前にリセットすべきである。OEM 提供の復元イメージなどの回復データがこの方法で保存されている可能性があるため、再インストール媒体も利用可能である場合を除いて、データ抹消処理がシステムの回復能力に影響を与える可能性がある。 暗号化消去を適用する場合、暗号処理が正常に完了したことを保証するための検証を、暗号化消去の後に適用される消去技術や除去技術などの追加のデータ抹消処理技術（該当する場合）の前に実施しなければならない。また、4.7 節に記載されているようなクイックサンプリング検証は、暗号化消去に続いて追加の技術を適用した後に実行されるべきである。 暗号化のすべての実装が、除去メカニズムとしての暗号化消去の信頼性の観点で必ずしも適しているわけではない。暗号化消去を使用するかどうかの判断は、本ガイダンス及び付録 D で事前に特定された属性の検証に依存する。 ATA セキュリティ機能セット SECURITY ERASE UNIT コマンドの実装にはばらつきがあることを考慮すると、初めにメーカに問い合わせてストレージデバイスのモデル固有の

	実装が組織のニーズに合っていることを確認することなしに、このコマンドを使用することは推奨されない。 本ガイダンスは旧式の磁気媒体のみに適用されるので、データ抹消処理の前に媒体の種類を確認することが重要である。HAMR 媒体やハイブリッドドライブなどの新しく出てきた種類の媒体は、ラベルでは容易に識別できない場合があることに注意されたい。ストレージデバイスでの媒体の種類の詳細については、メーカに問い合わせられたい。 ストレージデバイス内の媒体を消磁すると、通常、そのデバイスは使用できなくなる。

SCSI ハードディスクドライブ。*これには、パラレル SCSI、シリアルアタッチド SCSI（SAS）、ファイバーチャネル、USB アタッチドストレージ（UAS）及び SCSI Express を含む。本節では、部分的データ抹消処理は対象外である。*	
消去：	組織的に承認され、検証された上書き技術／方法／ツールを使用して媒体を上書きする。消去手順は、すべて 0 の列などの固定データ値を持つ少なくとも 1 回パスの書き込みで構成されるべきである。複数パスやより複雑な値もオプションとして使用することができる。
除去：	4 つのオプションが利用可能である： 1. SCSI SANITIZE コマンド（サポートされている場合）を適用する。以下のオプションのいずれか又は両方を使用できる： a. OVERWRITE サービス措置。媒体表面に固定パターンの 1 回書き込みパスを適用する。固定パターンの例としては、すべて 0 の列や擬似乱数パターンなどがある。媒体を除去するには、1 回書き込みパスで十分である。 *オプション*: 1 回書き込みパスの代わりに、擬似乱数パターンの合計 3 回の書き込みパスを使用し、そのうち 2 回目の書き込みパスが指定されたパターンの反転バージョンとなるように、反転オプションを利用する。 b. デバイスが暗号化をサポートしている場合の CRYPTOGRAPHIC ERASE サービス措置 *オプション*: 暗号化消去がデバイスに正常に適用された後、上書きコマンド（サポートされている場合）を使用して、媒体に 0 の列又は擬似乱数パターンのパスを 1 回書き込む。上書きコマンドがサポートされていない場合、代替として、消去手順を適用することができる。 2. 暗号化消去は、TCG の Opal SSC 又は Enterprise SSC インタフェースを介して、必要に応じてコマンドを発行してすべての MEK を変更させることにより行う。詳細については、TCG 及び TCG Opal 又は Enterprise ストレージデバイスを出荷しているベンダに問い合わせる。 *オプション*: 暗号化消去がデバイスに正常に適用された後、上書きコマンド（サポートされている場合）を使用して、媒体に 0 の列又は擬似乱数パターンのパスを 1 回書き込む。上書きコマンドがサポートされていない場合、代替として、消去手順を適用することができる。

	3. 組織的に承認された自動消磁装置で消磁するか、又はハードディスクドライブを分解し、組織的に承認された消磁スキャナで中に入っている円盤記録媒体を除去する。消磁装置／消磁スキャナは、媒体に対して十分な格付けがされているべきである。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	検証方法の小節に記載されているように、消磁以外の消去技術及び除去技術の各々について検証を行わなければならない。消磁によって提供される保証は、効果的な消磁装置を選択し、適切に適用し、その結果を定期的に抜き取り検査して、期待通りに動作していることを確認することに依存する。 SCSI データ抹消処理で反転オプション（補完オプションとも呼ばれる）を使用した 3 パスの上書き手順を利用した場合、検証プロセスは単に（3 パス目で再度書き込まれたであろう）元のパターンを検索することである。データを除去するには 1 パスの上書きで十分であることが広く受け入れられているが、データパターンを反転させる機能を組み込んだ専用コマンドを使用することで、デバイスメーカ間での磁気記録機能の実装のばらつきに関連する残留リスクを軽減する効率的かつ効果的なアプローチが可能になる。 ストレージデバイスは構成機能をサポートしている場合があり、ATA 規格で定義されている媒体の一部へのアクセス能力を人為的に制限する。例えば、SCSI モードパラメータブロック記述子の NUMBER OF LOGICAL BLOCKS フィールド（SCSI MODE SENSE コマンド及び MODE SELECT コマンドでアクセス可能）がある。専用のデータ抹消処理コマンドがこれらの領域に対応している場合であっても、それらの存在をそのままにしておくと、データ抹消処理手順の有効性を確実に検証する能力に影響を与える可能性がある。記憶媒体のアドレス指定可能な領域全体へのアクセス能力を制限する構成オプションはすべて、データ抹消処理技術を適用する前にリセットすべきである。 暗号化消去を適用する場合、暗号処理が正常に完了したことを保証するための検証を、暗号化消去の後に適用される消去技術や除去技術などの追加のデータ抹消処理技術（該当する場合）の前に実施しなければならない。また、検証方法の小節に記載されているようなクイックサンプリング検証は、暗号化消去に続いて追加の技術を適用した後に実行されるべきである。 暗号化のすべての実装が、除去メカニズムとしての暗号化消去の信頼性の観点で必ずしも適しているわけではない。暗号化消去を使用するかどうかの判断は、本ガイダンス及び付録 D で事前に特定された属性の検証に依存する。 本ガイダンスは旧式の磁気媒体のみに適用されるので、データ抹消処理の前に媒体の種類を確認することが重要である。HAMR 媒体やハイブリッドドライブなどの新しく出てきた種類の媒体は、ラベルでは容易に識別できない場合があることに注意されたい。ストレージデバイスでの媒体の種類の詳細については、メーカに問い合わせられたい。 ストレージデバイス内の媒体を消磁すると、通常、そのデバイスは使用できなくなる。

表 A-6：周辺接続型ストレージのデータ抹消処理

周辺接続型ストレージ	
外付けローカル接続ハードドライブ。*これには、USB、Firewire などが含まれる（eSATA を ATA ハードドライブとして扱う）*	
消去：	組織的に承認され、テストされた上書き技術／方法／ツールを使用して媒体を上書きする。消去パターンは、すべて 0 の列などの固定データ値を持つ少なくとも 1 回パスであるべきである。複数パスやより複雑な値も代替として使用することができる。
除去：	外付けローカル接続ハードドライブの実装はモデルやベンダによって大きく異なるため、デバイスに特定のコマンドを発行しても、望ましいデータ抹消処理の結果が合理的かつ一貫して保証することができない可能性がある。 外付けドライブベイに ATA 又は SCSI ハードドライブが搭載されている場合、コマンドをデバイスにネイティブに配信できるならば、関連する媒体固有のガイダンスに基づいて当該デバイスのデータ抹消処理を行うことができる。しかし、ドライブは、筐体から取り出されたときには、データ抹消処理できないようにしたベンダ固有の方法で構成されている可能性がある。さらに、データ抹消処理技術が適用されている場合、筐体に再インストールした時に、ハードドライブが期待通りに動作しない可能性がある。 デバイスメーカに問い合わせて、データ回復が不可能であり、且つ当該デバイスがファイルポインタを削除するだけではないことを保証するために、媒体依存の技術（書き換え、ブロック消去、暗号化消去など）を適用する除去機能を当該デバイスが持っているかどうかを確認する。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	検証方法の小節に記載されているように、消去技術及び除去技術の各々について検証を行わなければならない。 外付けローカル接続ハードドライブ（特にセキュリティ機能や暗号化機能を備えたもの）の中には、そのドライブを筐体から取り外しても、対処できない可能性のある隠れたストレージ領域を備えている場合もある。デバイスベンダは、セキュリティサブシステムと相互交信するために、独自のコマンドを利用することがある。媒体上に予約された領域があるかどうか、及び（存在する場合は）それらを取り外し又はデータ抹消処理を行うために利用可能なツールがあるかどうかを判断するためにメーカに問い合わせるようにする。

表 A-7：光媒体のデータ抹消処理

光媒体	
CD、DVD、BD	
消去／ 除去：	該当なし

破壊：	推奨順に破壊する： 1. 市販の光ディスク粉砕装置を用いて CD 媒体の情報含有層を取り除く。これは CD にのみ適用され、DVD や BD 媒体には適用されないことに注意されたい。 2. 認可された施設を使用して光ディスク媒体を焼却（灰になるまで）する。 3. 光ディスク媒体シュレッダ又は分解装置を使用して、公称エッジ寸法 0.5mm、表面積 0.25mm² 以下の小片に粉砕する。

表 A-8：フラッシュメモリベースのストレージデバイスのデータ抹消処理

フラッシュメモリベースのストレージデバイス	
ATA ソリッドステートドライブ（SSD）。*これには PATA、SATA、eSATA などが含まれる。*	
消去：	1. 組織的に承認され、テストされた上書き技術／方法／ツールを使用して媒体を上書きする。消去手順は、すべて 0 の列などの固定データ値を持つ少なくとも 1 回パスの書き込みで構成されるべきである。複数パスやより複雑な値も代替として使用することができる。 注意：フラッシュベースの媒体上での上書きは、当該媒体の有効寿命を大幅に短縮する可能性があり、且つマッピングされていない物理媒体のデータ抹消処理が行えない（つまり、古いデータが当該媒体上に残っている）可能性があることに留意することが重要である。 2. ATA セキュリティ機能セットの SECURE ERASE UNIT コマンドを使用する（サポートされている場合）。
除去：	3 つのオプションが利用可能である： 1. ATA データ抹消処理コマンドを適用する（サポートされている場合）。以下のオプションのいずれか又は両方を使用できる： a. ブロック消去コマンド *オプション*: ブロック消去コマンドがデバイスに正常に適用された後、記憶媒体のユーザアドレス指定可能な領域全体に 1 の列を書き込み、その後、2 回目のブロック消去を実行する。 b. デバイスが暗号化をサポートしている場合の暗号化消去コマンド（暗号スクランブルによるデータ抹消処理としても知られる） *オプション*: 暗号化消去がデバイスに正常に適用された後、ブロック消去コマンド（サポートされている場合）を使用して、当該媒体をブロック消去する。ブロック消去コマンドがサポートされていない場合、代替として、Secure Erase 又は消去手順を適用することができる。 2. 暗号化消去は、TCG の Opal SSC 又は Enterprise SSC インタフェースを介して、必要に応じてコマンドを発行してすべての MEK を変更させることにより行う。詳細については、TCG 及び TCG Opal 又は Enterprise ストレージデバイスを出荷しているベンダに問い合わせる。

	オプション: 暗号化消去がデバイスに正常に適用された後、ブロック消去コマンド（サポートされている場合）を使用して、当該媒体をブロック消去する。ブロック消去コマンドがサポートされていない場合、代替として、Secure Erase 又は消去手順を適用することができる。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	検証方法の小節に記載されているように、消去技術及び除去技術の各々について検証を行わなければならない。 暗号化消去を適用する場合、暗号処理が正常に完了したことを保証するための検証を、暗号化消去の後に適用される消去技術や除去技術などの追加のデータ抹消処理技術（該当する場合）の前に実施しなければならない。また、検証方法の小節に記載されているようなクイックサンプリング検証は、暗号化消去に続いて追加の技術を適用した後に実行されるべきである。 ストレージデバイスは構成機能をサポートしている場合があり、ATA 規格で定義されている媒体の一部へのアクセス能力を人為的に制限する。例えば、ホスト保護領域（HPA）、デバイス構成オーバーレイ（DCO）、アクセス可能な最大アドレスなどがある。専用のデータ抹消処理コマンドがこれらの領域に対応している場合であっても、それらの存在をそのままにしておくと、データ抹消処理手順の有効性を確実に検証する能力に影響を与える可能性がある。記憶媒体のアドレス指定可能な領域全体へのアクセス能力を制限する構成オプションはすべて、データ抹消処理技術を適用する前にリセットすべきである。OEM 提供の復元イメージなどの回復データがこの方法で保存されている可能性があるため、再インストール媒体も利用可能である場合を除いて、データ抹消処理がシステムの回復能力に影響を与える可能性がある。 暗号化のすべての実装が、除去メカニズムとしての暗号化消去の信頼性の観点で必ずしも適しているわけではない。暗号化消去を使用するかどうかの判断は、本ガイダンス及び付録 D で事前に特定された属性の検証に依存する。 Enhanced Secure Erase 機能の実装にはばらつきがあることを考慮すると、初めにメーカに問い合わせてストレージデバイスのモデル固有の実装が組織のニーズに合っていることを確認することなしに、このコマンドを使用することは推奨されない。 ATA Secure Erase は磁気媒体に対しては除去メカニズムであったが、フラッシュメモリに対しては消去メカニズムに過ぎない。なぜなら、実装にばらつきがあり、且つ使用外に回されたスペアセルなどの領域に機微データが残る可能性があるためである。 フラッシュメモリベースのストレージデバイスや不揮発性フラッシュメモリ記憶媒体を含むハイブリッドデバイスでは、データ抹消処理技術として消磁だけに頼ってはならない。フラッシュメモリコンポーネントが媒体依存の技術を使用してデータ抹消処理されるならば、不揮発性フラッシュメモリ媒体が存在する場合に消磁が使用されてもよい。

SCSI ソリッドステートドライブ（SSDs）。*これには、パラレル SCSI、シリアルアタッチド SCSI（SAS）、ファイバーチャネル、USB アタッチドストレージ（UAS）及び SCSI Express を含む。*	
消去：	組織的に承認され、テストされた上書き技術／方法／ツールを使用して媒体を上書きする。消去手順は、すべて 0 の列などの固定データ値を持つ少なくとも 1 回パスの書き込みで構成されるべきである。複数パスやより複雑な値も代替として使用することができる。 注意：フラッシュベースの媒体上での上書きは、当該媒体の有効寿命を大幅に短縮する可能性があり、且つマッピングされていない物理媒体のデータ抹消処理が行えない（つまり、古いデータが当該媒体上に残っている）可能性があることに留意することが重要である。
除去：	2 つのオプションが利用可能である： 1. SCSI SANITIZE コマンド（サポートされている場合）を適用する。以下のオプションのいずれか又は両方を使用できる： a. BLOCK ERASE サービス措置 b. デバイスが暗号化をサポートしている場合の CRYPTOGRAPHIC ERASE サービス措置 *オプション*: 暗号化消去がデバイスに正常に適用された後、ブロック消去コマンド（サポートされている場合）を使用して、当該媒体をブロック消去する。ブロック消去コマンドがサポートされていない場合、代替として、消去手順を適用することができる。 2. 暗号化消去は、TCG の Opal SSC 又は Enterprise SSC インタフェースを介して、必要に応じてコマンドを発行してすべての MEK を変更させることにより行う。詳細については、TCG 及び TCG Opal 又は Enterprise ストレージデバイスを出荷しているベンダに問い合わせる。 *オプション*: 暗号化消去がデバイスに正常に適用された後、ブロック消去コマンド（サポートされている場合）を使用して、当該媒体をブロック消去する。ブロック消去コマンドがサポートされていない場合、代替として、消去手順が許容できる。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	検証方法の小節に記載されているように、消去技術及び除去技術の各々について検証を行わなければならない。 ストレージデバイスは構成機能をサポートしている場合があり、ATA 規格で定義されている媒体の一部へのアクセス能力を人為的に制限する。例えば、SCSI モード選択がある。専用のデータ抹消処理コマンドがこれらの領域に対応している場合であっても、それらの存在をそのままにしておくと、データ抹消処理手順の有効性を確実に検証する能力に影響を与える可能性がある。記憶媒体のアドレス指定可能な領域全体へのアクセス能力を制限する構成オプションはすべて、データ抹消処理技術を適用する前にリセットすべきである。 暗号化消去を適用する場合、暗号処理が正常に完了したことを保証するための検証を、暗号化消去の後に適用される消去技術や除去技術などの追加のデータ抹消処理技術（該当する場合）の前に実施しなければならない。また、検証方法の小節に記載されているような

	クイックサンプリング検証は、暗号化消去に続いて追加の技術を適用した後に実行されるべきである。 暗号化のすべての実装が、除去メカニズムとしての暗号化消去の信頼性の観点で必ずしも適しているわけではない。暗号化消去を使用するかどうかの判断は、本ガイダンス及び付録 D で事前に特定された属性の検証に依存する。 フラッシュメモリベースのストレージデバイスでは、データ抹消処理技術として消磁を行ってはならない。

NVM Express SSD	
消去：	組織的に承認され、テストされた上書き技術／方法／ツールを使用して媒体を上書きする。消去手順は、すべて 0 の列などの固定データ値を持つ少なくとも 1 回パスの書き込みで構成されるべきである。複数パスやより複雑な値も代替として使用することができる。
除去：	2 つのオプションが利用可能である： 1. VM Express Format コマンド（サポートされている場合）を適用する。以下のオプションのいずれか又は両方を使用できる： a. User Data Erase コマンド b. デバイスが暗号化をサポートしている場合の Cryptographic Erase コマンド *オプション*: 暗号化消去がデバイスに正常に適用された後、User Data Erase コマンド（サポートされている場合）を使用して、当該媒体を消去する。User Data Erase コマンドがサポートされていない場合、代替として、消去手順を適用することができる。 2. 暗号化消去は、TCG の Opal SSC 又は Enterprise SSC インタフェースを介して、必要に応じてコマンドを発行してすべての MEK を変更させることにより行う。詳細については、TCG 及び TCG Opal 又は Enterprise ストレージデバイスを出荷しているベンダに問い合わせる。 *オプション*: 暗号化消去がデバイスに正常に適用された後、User Data Erase コマンド（サポートされている場合）を使用して、当該媒体を消去する。User Data Erase コマンドがサポートされていない場合、代替として、消去手順が許容できる。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	消去技術及び除去技術の各々について検証を行わなければならない。 暗号化消去を適用する場合、暗号処理が正常に完了したことを保証するための検証を、暗号化消去の後に適用される消去技術や除去技術などの追加のデータ抹消処理技術（該当する場合）の前に実施しなければならない。また、検証方法の小節に記載されているようなクイックサンプリング検証は、暗号化消去に続いて追加の技術を適用した後に実行されるべきである。

	暗号化のすべての実装が、除去メカニズムとしての暗号化消去の信頼性の観点で必ずしも適しているわけではない。暗号化消去を使用するかどうかの判断は、本ガイダンス及び付録 D で事前に特定された属性の検証に依存する。 フラッシュメモリベースのストレージデバイスでは、データ抹消処理技術として消磁を行ってはならない。

USB リムーバブル媒体。*これは、ペンドライブ、サムドライブ、フラッシュメモリドライブ、メモリスティックなどが含まれる。*	
消去：	組織的に承認され、テストされた上書き技術／方法／ツールを使用して媒体を上書きする。消去パターンは、消去パターンは少なくとも 2 回パスであるべきであり、1 回目パスにパターンを、2 回目パスにその補数を含むようにする。追加のパスを使用することもできる。
除去：	ほとんどの USB リムーバブル媒体はデータ抹消処理コマンドをサポートしていないか、サポートされている場合でも、これらのデバイス間で標準化された方法でインタフェースがサポートされているわけではない。データ抹消処理機能及びコマンドの利用可能性と機能性の詳細については、メーカに問い合わせられたい。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	除去が望ましいケースのほとんどは、USB リムーバブル媒体を破壊すべきである。

メモリカード。これには、SD、SDHC、MMC、コンパクトフラッシュメモリ、マイクロドライブ、メモリスティックなどが含まれる。	
消去：	組織的に承認され、テストされた上書き技術／方法／ツールを使用して媒体を上書きする。消去パターンは、消去パターンは少なくとも 2 回パスであるべきであり、1 回目パスにパターンを、2 回目パスにその補数を含むようにする。追加のパスを使用することもできる。
除去：	該当なし
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	なし

ボードやデバイスに組み込まれたフラッシュメモリ。*これには、マザーボード、及びネットワークアダプタや不揮発性フラッシュメモリを含むその他のアダプタなどの周辺カードが含まれる。*	
消去：	デバイスがサポートしている場合は、状態を工場出荷時設定にリセットする。
除去：	該当なし。フラッシュメモリを容易に特定して基板から取り外すことができる場合には、当該フラッシュメモリを搭載していた基板の廃棄とは別に、当該フラッシュメモリを破壊してもよい。そうでなければ、基盤全体を破壊すべきである。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。

注意：	組み込みフラッシュメモリは、従来、媒体のデータ抹消処理ガイドラインでは特に取り上げられていなかったが、システムの複雑化及びフラッシュメモリの同時使用が増えるに伴い、機微データが存在する可能性も相補的に高まっている。例えば、最新のマザーボードに統合されたリモート管理機能では、IP アドレス、ホスト名、ユーザ名とパスワード、証明書、又は機微と考えられるその他のデータの保存が必要になる場合がある。その結果、消去について、デバイスの状態を完全にリセットするために複数のインタフェースとの相互通信が必要になる場合がある。この概念を例に当てはめると、リモート管理インタフェースだけでなく、BIOS／UEFI インタフェースも含まれることになる。 他の種類の媒体と同様に、データ抹消処理技術の選択は環境固有の考慮事項に基づく。組み込みフラッシュメモリの消去も除去もしないという選択もあるが、潜在的なリスクを認識して受け入れ、環境の変化に応じてリスクを再評価し続けることが重要である。

表 A-9：RAM ベース及び ROM ベースのストレージデバイスのデータ抹消処理

RAM ベース及び ROM ベースのストレージデバイス	
ダイナミックランダムアクセスメモリ（DRAM）	
消去／除去：	DRAM を含むデバイスの電源を切り、電源から取り外し、バッテリーを取り外す（バッテリー式の場合）。別の方法としては、デバイスから DRAM を取り外す。
破壊：	細断、分解又は粉砕を行う。
注意：	いずれの場合も、DRAM は少なくとも 5 分間は電源が入っていない状態にしなければならない。

電子オルタブル PROM（EAPROM）	
消去／除去：	メーカのデータシートに従ってチップ全体に除去を行う。
破壊：	細断、分解又は粉砕を行う。
注意：	なし

電子的消去可能 PROM（EEPROM）	
消去／除去：	組織的に承認され、検証された上書き技術／方法／ツールを使用して媒体を上書きする。
破壊：	デバイスを細断、分解、粉砕、又は認可された焼却炉で焼却する。
注意：	なし

付録 B ー 用語集

ATA	磁気媒体インタフェース仕様。別名“IDE（Integrated Drive Electronics）”
BD	ブルーレイディスク（Blu-ray Disc）は、CD や DVD と同じ形状とサイズであるが、より高密度であり、データ記録を多層化するためのオプションを提供する
Bend 曲げ	記憶媒体を物理的に別の形状に変形させる機械的プロセスを使用することであり、最先端の実験室レベルの技術を用いても媒体の読み取りを困難又は不可能にする
Clear 消去	すべてのユーザアドレス指定可能なストレージ領域のデータ抹消処理を行うための論理的技術を適用することによるデータ抹消処理方法のことであり、ユーザが利用可能な同じインタフェースを使用しての単純な非侵襲的データ回復技術から保護する。通常は、ストレージデバイスへの標準的な読み書きコマンドを使用して行われ、例えば、新しい値で書き換えたり、メニューオプションを使用して当該デバイスを工場出荷時状態にリセットしたりする（書き換えがサポートされていない時）
CD	コンパクトディスク（Compact Disc）は、光学的な手段でデータを読み取る媒体の一種である
CD-RW	CD-RW（Compact Disc Read/Write）は、除去や複数回書き換えることができる CD である
CD-R	CD-R（Compact Disc Recordable）は、一度だけ書き込み可能で、何度でも読み出せる CD である。別名 WORM
CE	「暗号化消去」を参照
CMRR	カリフォルニア大学サンディエゴ校にある磁気記録研究センタ（Center for Magnetic Recording Research）は、磁気ストレージの最先端の研究を進め、大学院生及びポスドク専門家を育成している（CMRR ホームページ：http://cmrr.ucsd.edu/）
Cut 裁断	電子記憶媒体の表面に破損を生じさせるためにツール又は物理的な技術を使用することであり、当該媒体を 2 つ以上の小片に分割し、最先端の実験室レベルの技術を使用してもデータを回復することが困難又は不可能にする可能性がある
Cryptographic Erase 暗号化消去	暗号化された対象データの媒体暗号化鍵（MEK：Media Encryption Key）（又は鍵暗号化鍵（KEK：Key Encryption Key））に対するデータ抹消処理方法のことであり、復号された対象データに回復することを不可能にする
Data データ	“理解可能な情報”を導き出す情報の断片
Degauss 消磁	逆磁界をかけて磁束を仮想的にゼロにすること。現行のハードディスク（IDE、EIDE、ATA、SCSI、Jaz を含むが、これらに限定されない）を消磁すると、これらのドライブは永久に使用できなくなる。なぜなら、当該ドライブにはハードドライブ上のトラック位置情報を保存しているためである。別名“脱磁”
Destroy 破壊	最先端の研究室レベルの技術を用いても対象データの回復を不可能にするデータ抹消処理方法であり、結果として、その後もデータ保存用の媒体として使用できなくなる
Digital デジタル	データを表現するためにコンピュータ技術で一般的に使用される符号化方式

Disintegration 分解	媒体のデータ抹消処理を行うための物理的な破砕方法。構成部品に分離する措置
Disposal 廃棄	廃棄とは、媒体に機微データが含まれていないと判断した後の放出結果のことである。これは、当該媒体に機微データがまったく含まれていなかったか、又はデータ抹消処理技術が適用されて当該媒体に機微データが含まれなくなった場合に行われる
DVD	デジタルビデオディスク（Digital Video Disc）は、CD と同じ形状とサイズであるが、より高い密度を持っており、データ記録を両面や二重層にするためのオプションを提供する
DVD-RW	DVD フォーラムが提供する、映画及びデータ両用の書き換え可能な（再録可能な）DVD
DVD+RW	DVD+RW アライアンスが提供する、映画及びデータ両用の書き換え可能な（再録可能な）DVD
DVD+R	DVD+RW アライアンスが提供する、DVD+RW の一回記録（読み切り）バージョン
DVD-R	DVD フォーラムが保証した、映画及びデータ両用の一回記録（読み切り）型 DVD
Electronic Media 電子媒体	電気的なプロセスを経てデータが記録された媒体を指す総称
Erasure 消去	磁気的に保存された情報を通常の方法では復元できない状態にすることを意図したプロセス
FIPS	連邦情報処理基準（Federal Information Processing Standard）
Format フォーマット	データ用に事前確立されたレイアウト
Hard Disk ハードディスク	ドライブユニット内に恒久的に固定された硬質磁気ディスクであり、データを保存するために使用される。また、１つ以上の磁気ディスクを含むリムーバブルカートリッジであってもよい
Incineration 焼却	媒体のデータ抹消処理を行うための物理的な破砕方法。完全に灰になるまで燃やす措置
Information 情報	データの意味のある解釈又は表現
Magnetic Media 磁気媒体	磁気記憶媒体のみを使用して永続的な保存を行うストレージデバイスのクラスであり、熱の助け（すなわち、熱アシスト磁気記録（HAMR：Heat Assisted Magnetic Recording））、又はフラッシュメモリベースの媒体のような他の永続的な記憶媒体の追加的な使用を必要としない
Media 媒体	媒体（medium）の複数形
Media Sanitization 媒体のデータ抹消処理	媒体に書き込まれたデータを、通常の手段だけでなく特別な手段によっても回復できない状態であるようにするために取られた措置を指す一般的な用語

Medium 媒体	データが記録されている又は記録されている可能性のある材料。紙、パンチングカード、磁気テープ、磁気ディスク、ソリッドステートデバイス、光ディスクなど
Melting 熔解	媒体のデータ抹消処理を行うための物理的な破砕方法。一般に熱を使って固体状態から液体状態に変化させること
Optical Disk 光ディスク	光レーザ装置を用いて読み取るプラスチック製ディスク
Overwrite 上書き	媒体に保存されているデータの物理的な場所の上にデータを書き込むこと
Physical Destruction 物理的破砕	媒体のデータ抹消処理方法
Pulverization 粉砕	媒体のデータ抹消処理を行うための物理的な破砕方法。粉末又は粉塵に粉砕する措置
Purge 除去	最先端の研究室レベルの技術を用いても対象データの回復を不可能にするための物理的又は論理的な技術を適用するデータ抹消処理方法
Read 読み出し	情報システムにおける基本的処理であり、記憶媒体から要求元への情報の流れだけが起きる
Read-Only Memory 読み取り専用メモリ	ROM とは、予め記録された記憶媒体のことで、読み取ることしかできず、書き込むことはできない
Record 記録	磁気テープ、磁気ディスク、光ディスクなどの媒体にデータを書き込むこと
Remanence 残留磁気	記憶媒体に残っている残余情報
ROM	「読み取り専用メモリ」を参照
Sanitize データ抹消処理	所定の努力レベルでは媒体上の対象データへのアクセスを不可能にするプロセス。消去、除去及び破壊は、媒体のデータ抹消処理を行うことができる措置である
SANITIZE コマンド	ATA 標準及び SCSI 標準のコマンドであり、ファームウェアベースのプロセスを利用してデータ抹消処理を実行する。デバイスが*データ抹消処理*コマンドをサポートしている場合、当該デバイスは以下の 3 つのオプションのうち少なくとも 1 つをサポートしなければならない：*上書き*、*ブロック消去*（通常、フラッシュメモリベースの媒体の場合）、又は*暗号スクランブル*（暗号化消去）。これらのコマンドは、通常、ネイティブの読み書きインタフェースを使って書き換えようとするよりもかなり高速に実行される。ATA 標準では、データ抹消処理は、ユーザデータ領域、現在割り当てられていないユーザデータ領域（“以前に割り当てられた領域、及びアクセスできなくなった物理セクタ”を含む）、及びユーザデータキャッシュに対処しなければならないことを明確に示している。結果として得られる媒体の内容は、使用されたコマンドに基づいて異なる。*上書き*コマンドは、ユーザが媒体に適用されるデータパターンを指定することを可能にし、そのパターン（又は、選択された場合はその逆のパターン）

	が当該媒体に書き込まれるようにする（実際の媒体の内容は符号化のために変化する可能性があるが）。*ブロック消去*コマンドの結果はベンダ固有であるが、0 の列又は 1 の列になる可能性が高い。*暗号スクランブル*コマンドの結果はベンダ固有であるが、暗号化されたスクランブルデータになる可能性が高い（ただし、ベンダが定義した値に設定された暗号化されていない領域を除く）
SCSI	磁気媒体のインタフェース仕様。Small Computer System Interface の略
Secure Erase Command 安全な消去コマンド	ATA 標準の*上書き*コマンド（“Security Erase Unit”）のことで、ファームウェアベースのプロセスを利用して媒体を上書きする。このコマンドは、通常、ネイティブの読み書きインタフェースを使って書き換えようとするよりもかなり高速に実行される。“通常消去”と“強化消去”の 2 つまでのオプションがある。その標準で定義されている通常消去は、LBA 0 から READ NATIVE MAX 又は READ NATIVE MAX EXT の大きい方までのコンテンツ内のデータのみをアドレス指定するようになっており、0 の列又は 1 の列でその内容を置き換える。*強化消去*コマンドでは、“・・・以前に書き込まれたすべてのユーザデータは、再割り当てにより使用されなくなったセクタを含めて、上書きされなければならない”と規定されており、データ抹消処理後の媒体の内容はベンダ固有のものとなっている。*強化消去*によって行われる実際の措置はベンダやモデルによって異なり、効果のレベルが異なる様々な措置が含まれる可能性がある。*安全な消去*コマンドは SCSI 標準では定義されていないため、SCSI インタフェースを持つ媒体には適用されない
Shred 裁断	媒体のデータ抹消処理方法。小さな粒子に切断又は引き裂く措置
SSD	ソリッドステートドライブ（Solid State Drive）は、ソリッドステートメモリを使用して永続的にデータを保存するストレージデバイスである
Storage ストレージ	データの復元可能な保持。電子的、静電的、又は電気的なハードウェア又は他の要素（媒体）であり、それにデータが入力されたり、それからデータが読み出されたりする
Target Data 対象データ	所与のプロセスの対象となる情報であり、通常は、記憶媒体の一部分上にほとんど又はすべての情報を含む
Validate 認証	媒体のデータ抹消処理プロセスのフローチャート内のステップであり、情報が読み出せないことを保証するための媒体テストを行うことを含む
Verification 検証	情報が読み出せないことを保証するための媒体テストプロセス
WORM	一度だけ書き込み可能で、何度でも読み出せる。「CD-R」も参照
Write 書き込み	情報システムにおける基本的処理であり、行為者から記憶媒体への情報の流れだけが起きる

付録 C ー ツール及びリソース

多くの政府機関、米軍及び学術機関が、一定の保証レベルをもった検証を行うために、データ抹消処理ツール、技術及び手順を徹底的に研究してきた。NIST は、いかなるツールセットの評価を行わず、特定の媒体に含まれる情報を消去、除去又は破壊する能力を検証しない。

組織は、自ら評価できる製品を探すことが推奨される。当該組織は、信頼できるサービス又は他の連邦組織によるツールや製品の評価を使用することができ、選択したデータ抹消処理ツールを使用する際はその有効性を継続的に監視し検証すべきである。

組織が信頼してテストした製品を持っている場合は、連邦政府コンピュータセキュリティ管理者フォーラム [22]などの公開フォーラムでその情報を共有することが強く推奨される。

C.1 NSA 媒体破砕ガイダンス

本ガイドでは、また、国家安全保障局（NSA）公開ウェブサイト [23]の媒体破砕ガイダンスの場所に掲載されている NSA のデバイスを検討することを推奨する。NSA は、“これらのリストに掲載されている製品は、機微情報又は機密情報を含む媒体のデータ抹消処理、破壊又は廃棄のための特定の NSA 性能要件を満たしている。リストに記載されていることが、NSA 又は米国政府による保証を意味するものではない。”としている。NSA のウェブサイトに掲載されている評価済製品のリストは、以下をカバーする：

- クロスカットペーパーシュレッダ
- 光媒体
- 消磁装置
- 記憶装置
- 粉砕機

C.2 オープンソースのツール

標準インタフェースに基づいたデータ抹消処理コマンドを活用することをサポートする様々な利用可能なオープンソースのツールがある。他のデータ抹消処理ツールと同様に、必要な機能が提供されていることを確認するために、独立した検証を行うべきである。しかし、オープンソースのツールが利用できることで、組織はそのコマンドがどのように機能するかを理解し、ドライブ上でデータ抹消処理コマンドのテストを行うことができるほか、ホームユーザが自分個人の媒体のデータ抹消処理に適用できるようにサポートする。

[22] http://csrc.nist.gov/groups/SMA/forum/

[23] http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

例えば、オープンソースプロジェクトの一つである **hdparm** は、SourceForge[24].で公開されている。

C.3 電子リサイクル（e-Cycling）に関する EPA 情報

データ抹消処理後の使用済み電子機器の寄贈を希望する、又は残余素材の廃棄ガイダンスを探している組織や個人は、環境保護庁（EPA）の電子リサイクル及び電子廃棄物に関する情報ウェブサイト（http://www.epa.gov/e-Cycling/）を参照すべきである。このサイトでは、データ抹消処理、廃棄及び寄贈に関するアドバイス、規制及び標準文書を提供している。また、他のデータ抹消処理ツールのリソースへの外部リンクも提供している。

C.4 媒体のデータ抹消処理及び破砕の外部委託

組織が媒体のデータ抹消処理や破砕を外部委託できるのは、事業管理者及びセキュリティ管理者が、利用可能なリソースを最適化しながら機密性を維持するうえで、それらが最も合理的な選択肢であると判断した場合である。この選択肢を実施する場合、本ガイドでは、組織が媒体のデータ抹消処理に携わる他の当事者と契約を締結する際に、“相当な注意”を払うことを推奨する。この場合の相当な注意とは、16 CFR 682 の概説に従って受け入れることであり、それには“相当な注意には、廃棄会社の業務や本規則（本ガイド）への準拠に関する独立した監査を点検すること、複数の参考文献又はその他の信頼できる情報源から廃棄会社に関する情報を入手すること、廃棄会社が認定業界団体又は類似の第三者によって認証されていることを要求すること、廃棄会社の情報セキュリティポリシー又は手順を点検し評価すること、又は潜在的な廃棄会社の能力及び完全性を判断するためのその他の適切な措置を講じること、などが含まれる [25]”と記載されている。

C.5 トラステッドコンピューティンググループのストレージ仕様

TCG のストレージ仕様（Opal SSC インタフェース仕様又は Enterprise SSC インタフェース仕様）に関する情報は、TCG のウェブサイトに掲載されている：

http://www.trustedcomputinggroup.org/

C.6 ATA 標準及び SCSI 標準

ATA 標準及び SCSI 標準に関する情報は、以下のサイトで入手できる：

http://www.t13.org/

http://www.t10.org/

---

[24] http://hdparm.sourceforge.net/

[25] “Disposal of Consumer Report Information and Records Section,” Title 16 *Code of Federal Regulations*, Pt. 682.3 (b) (3).

注：ATA 標準及び SCSI 標準は、以下の団体によって発行されている：

a) 米国標準規格としての INCITS 及び ANSI（http://www.incits.org 及び http://www.ansi.org を参照）

b) 国際標準としての ISO/IEC（http://www.iso.org 及び http://www.iec.ch を参照）

C.7 NVM Express 仕様

NVM Express に関する情報は、以下のサイトで入手できる：

http://www.nvmexpress.org/

付録 D ー 暗号化消去デバイスガイドライン

特定のデバイスで暗号化消去を使用するかどうかの判断は、組織のデータ抹消処理要件に依存する。また、実装が将来のデータ回復に対して十分な保証を提供しているかどうかの判断は、エンドユーザの能力にも依存する。保証レベルは、表 D-1 に記載されている要因に大きく依存する。

表 D-1：暗号化消去の考慮事項

領域	考慮事項	関連資料
鍵生成	乱数源エントロピーのレベル、及びランダムデータに適用されるホワイトニング処理の品質。これは暗号化鍵に適用され、CE 操作の影響を受けるラッピング鍵にも適用される可能性がある	SP800-90[26] SP800-90A SP800-90B SP800-90C SP800-133
媒体暗号化	対象データの保護のために使用される暗号アルゴリズム／モードのセキュリティ強度及び実装の妥当性	FIPS 140-2[27] FIPS 197 SP800-38A（ECB を含まない） SP 800-38E
鍵レベル及び鍵ラッピング	データ抹消処理される鍵は、媒体暗号化鍵（MEK）ではなく、代わりに MEK や別の鍵をラップ（つまり、暗号化）するために使用する鍵かもしれない。この場合、使用するラッピング技術のセキュリティ強度と保証レベルは、CE 操作の強度レベルに見合ったものであるべきである	FIPS 197 SP800-38A SP800-38F SP800-131A

媒体のデータ抹消処理のために暗号化消去に依存する前に、ユーザは、以下に挙げるこれらの領域に対処するために、ストレージデバイスによって実装されたメカニズムを確認すべきである：

1. **メーカ／モデル／バージョン／媒体の種類**：ステートメントが適用される製品とバージョン、及びデバイスが使用する媒体の種類（つまり、磁気媒体、SSD、ハイブリッド、その他）。

   多くのデバイスでは、対象データを複数の異なる媒体（回転円形記憶媒体に加えて、DRAM（Dynamic Random Access Memory）キャッシュなど）に保存する。保管場所及びそれぞれがどのようにデータ抹消処理されるかを特定することが重要である。

[26] 認証された決定論的乱数ビット生成器（DRBG）の一覧は以下から入手できる：http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgval.html.

[27] FIPS 140-2 適合性試験は、暗号モジュール認証プログラム（CMVP：http://csrc.nist.gov/groups/STM/cmvp/）及び暗号アルゴリズム認証プログラム（CAVP：http://csrc.nist.gov/groups/STM/cavp/）の枠組みの中で実行される。

2. **鍵生成**：SP800-90[28]に記載されているうちのいずれかのような決定論的乱数ビット生成器（DRBG）が使用されたかどうか、及びそれが検証されたかどうかを識別する。

3. **媒体暗号化**：アルゴリズム、鍵の強度、暗号利用モード、及び適用可能な認証を確認する。

4. **鍵レベル及び鍵ラッピング**：MEK（別の値でラッピングされているか、ラッピングされていないかのいずれか）が直接データ抹消処理されるのか、又は MEK をラッピングする鍵（鍵暗号化鍵、又は KEK）がデータ抹消処理されるのかを特定する。ラッピング技術の記載は、KEK（MEK ではなく）がデータ抹消処理される場合にのみ適用される。ラッピングの詳細が提供される場合は、使用されるアルゴリズム、強度、及び（該当する場合は）暗号利用モードを含むべきである。

5. **アドレスされたデータ領域**：どの領域が暗号化されているか、及びどの領域が暗号化されていないかを記述する。暗号化されていない領域については、どのようにデータ抹消処理が行われるのかを記述する。

6. **鍵のライフサイクル管理**：デバイス上の鍵は、デバイスのライフサイクルを通じて複数のラッピング処理（ラッピング、アンラッピング、及び再ラッピング）が行われるかもしれない。データ抹消処理される鍵がどのように、暗号化消去処理の直接的な部分ではないラッピング処理の間に、処理されるかを特定する。例えば、ユーザが常に暗号化されている SED を受け取り、単に認証インタフェースをオンにしただけの場合がある。ユーザの認証資格情報でラップされていた場合、以前の MEK のインスタンスがどのようにデータ抹消処理されたかを特定する。

7. **鍵のデータ抹消処理技術**：データ抹消処理される鍵に対する媒体依存のデータ抹消処理方法を記述する。例として、媒体が磁気である場合には 1 回以上の反転上書きパス、SSD の場合にはブロック消去、他の種類の媒体の場合には他の媒体固有の技術などがある。

8. **鍵預託又はバックアップ**：デバイスが鍵預託又はバックアップをサポートしているかどうかを確認する。預託された鍵のレベル以下の任意の鍵が、そのデバイスから預託されたり、そのデバイスに注入されたりしたことがあるかどうかの検知を当該デバイスがサポートしているかどうかを確認する。MEK が直接データ抹消処理されており、KEK のみが預託可能な場合は、その事実を明確に特定する。

9. **エラー状態の処理**：デバイスが、暗号化消去処理が完全に完了するのを妨げるエラー状態をどのように処理するかを特定する。例えば、鍵が保存されていた場所のデータ抹消処理ができない場合、暗号化消去処理はユーザに成功か失敗かのどちらを報告するのか？

10. **インタフェースの明確さ**：どのインタフェースコマンドがステートメントに記載されている機能をサポートしているかを特定する。デバイスが複数の MEK の使用をサポートしている場合、利用可能なインタフェースコマンド、及びすべての MEK を確実に変更するのに必要な追加のコマンド又は措置を利用して、すべての MEK が変更されるのかどうかを確認する。特定の条件下では、すべての MEK が消去されなければならないわけではないこと（例えば、対象データの部分的データ抹消処理）に注意されたい。

[28] NIST SP800-90A (as amended), *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January 2012, 136 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-90A.

D.1 暗号化消去機能の記載例

以下の記載は、ストレージデバイスのベンダが、ベンダのウェブサイトや広く利用可能な製品資料など、デバイスの潜在的な利用者がアクセス可能な場所に配置すべきである。占有の性質に関する情報は、公表されている製品情報では利用できない場合がある。

1. **メーカ／モデル／バージョン／媒体の種類**：Acme ハードドライブモデル abc12345 バージョン 1+。媒体の種類は旧式の磁気媒体である。

2. **鍵生成**：SP800-90 で規定されている DRBG を使用する［認証番号］。

3. **媒体暗号化**：媒体は、SP800-38A に記載されている Cipher Block Chaining（CBC）モードの AES-256 による媒体暗号化で暗号化される。本デバイスは、FIPS 140 認証を受けている［認証番号］。

4. **鍵レベル及び鍵ラッピング**：媒体の暗号化鍵は、暗号化消去時に直接データ抹消処理される。

5. **アドレスされたデータ領域**：デバイスは、LBA アドレス指定可能な領域に保存されるすべてのデータを暗号化する。ただし、プリブート認証領域、変数領域及びデバイスログ領域を除く。デバイスのログデータは、暗号化消去後にもデバイスに保持される。

6. **鍵のライフサイクル管理**：MEK がラップされた状態、ラップされていない状態及び再ラップされた状態の間を移動する際に、以前のインスタンスは、3 回の反転上書きパスを使用してデータ抹消処理される。

7. **鍵のデータ抹消処理技術**：パスの間に反転するパターンで 3 回パスを行う。

8. **鍵預託又は注入**：デバイスは、データ抹消処理のレベル以下での鍵の預託又は注入をサポートしていない。

9. **エラー状態の処理**：記憶デバイスは、鍵が保存されている場所に不具合が発生した場合、その場所の書き換えを試み、暗号化消去処理の操作を継続して、その他の点で操作が成功したならばユーザに成功と報告する。

10. **インタフェースの明確さ**：デバイスは、ATA インタフェースを有して ATA Sanitize Device 機能セットの CRYPTO SCRAMBLE EXT コマンド、及び内容を暗号的に消去することで当該デバイスのデータ抹消処理を実行する機能を持つ TCG Opal インタフェースをサポートする。これらのコマンドの両方とも、本ステートメントで記載した機能を適用する。

付録 E ー 注目されるデバイス固有の特性

ストレージベンダは、同じ標準化されたコマンドセットを利用した様々な種類のデバイスや媒体を実装する。コマンドセットの例としては、ATA、SCSI、NVM Express などがある。例えば、ATA デバイス用の強化された Security Erase コマンドは、ベンダの違いによって実装が異なると思われる。ベンダによっては、暗号化消去、ブロック消去（フラッシュメモリデバイス用）、又はその他の技術などを実行する“内部”実装を持っている場合がある。そのデータ抹消処理措置がどのように行われているのかをユーザが確実に知ることは、困難又は不可能であるかもしれない。

ユーザによる情報に基づいた意思決定をサポートするために、ベンダは、特定のデバイスにサポートされている専用のデータ抹消処理コマンドがどのように実装されているかについての情報を提供することを選択してもよい。ベンダから報告された場合、この情報も、適切なデータ抹消処理機能及びアプローチの利用可能性に基づいてどのストレージデバイスを購入すべきかについて、調達機関が情報に基づいた決定を行う際にも役立つ。このベンダから報告される情報では、以下の事項を取り扱うべきである：

- 媒体の種類（すなわち、旧式の磁気媒体、HAMR（熱補助型磁気記録）、シングル磁気記録媒体、SLC／MLC／TLC フラッシュメモリ、ハイブリッドなど）
    - デバイスに磁気媒体が含まれている場合には、磁気媒体の保磁力（媒体を消磁しようとするかどうかについての情報に基づいた判断をサポートするため）
- どのデータ抹消処理コマンドがサポートされているか（サポートされている場合）
- サポートされている各々のデータ抹消処理コマンドに対して：
    - データ抹消処理コマンドで対処されない領域のリスト
    - コマンドが正常に完了するまでに必要な推定時間
    - 該当する場合は、検証試験の結果

付録 F ー 主要な参考文献

SP800-88 改訂 1 版に関連する更なる有用な情報源である。

- *All About Degaussers and Erasure of Magnetic Media,* Athana International [Web page], http://www.athana.com/ddequip/allaboutdegaussers.htm [accessed 7/18/14].

- J. Anastasi, *The New Forensics: Investigating Corporate Fraud and the Theft of Intellectual Property.* Hoboken, N.J.: John Wiley and Sons, 2003.

- J. Daughton, *Magnetoresistive Random Access Memory (MRAM)*, (February 4, 2000), 13pp. http://www.nve.com/Downloads/mram.pdf [accessed 7/21/14].

- H.A. Davis, National Security Agency. NSA/CSS POLICY MANUAL 9-12. (NSA/CSS STORAGE DEVICE DECLASSIFICATION MANUAL) http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf N.p.: n.p., 2006.

- *Degaussing Described.* Weircliffe International Ltd, 9th English edition, 2006. Archived copy available at: https://web.archive.org/web/20070129044258/http://www.weircliffe.co.uk/pdf/Weircliffe_Degaussing.pdf [accessed 7/18/14]..

- Y. Deng, "What is the future of disk drives, death or rebirth?" *ACM Computing Surveys*, 43(3), Article no. 23, (April 2011). http://dx.doi.org/10.1145/1922649.1922660.

- S.L. Garfinkel, and A. Shelat, "Remembrance of Data Passed: A Study of Disk Sanitization Practices," *IEEE Security & Privacy* 1(1), 17-27, (Jan.-Feb. 2003). http://dx.doi.org/10.1109/MSECP.2003.1176992.

- G. Gibson, and M. Polte, *Directions for Shingled-Write and Two- Dimensional Magnetic Recording System Architectures: Synergies with Solid-State Disks*, CMU-PDL-09-104, Carnegie Mellon University Parallel Data Laboratory, Pittsburgh, Pennsylvania, May 2009, 2pp. http://repository.cmu.edu/cgi/viewcontent.cgi?article=1004&context=pdl [accessed 7/21/14].

- *A Guide to Understanding Data Remanence in Automated Information Systems*, National Computer Security Center, NCSC-TG-025, Version 2. https://www.marcorsyscom.usmc.mil/Sites/PMIA%20Documents/Resources/national/NCSC-TG-025%20Data%20Remanence.html [accessed 7/21/14].

- P. Gutmann, "Data Remanence in Semiconductor Devices," *Proceedings of the 10th USENIX Security Symposium*, Washington, D.C. (August 13-17, 2001), 16pp. http://static.usenix.org/publications/library/proceedings/sec01/full_papers/gutmann/gutmann.pdf [accessed 7/21/14].

- P. Gutmann, , "Secure Deletion of Data from Magnetic and Solid-State Memory," *Proceedings of the Sixth USENIX Security Symposium*, San Jose, California, (July 22-25, 1996) 77-90. http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html [accessed 7/21/14].

- G.F. Hughes, T. Coughlin, T., and D.M. Commins, "Disposal of Disk and Tape Data by Secure Sanitization," *IEEE Security & Privacy* 7(4), 29-34 (July-Aug. 2009). http://dx.doi.org/10.1109/MSP.2009.89.

- InterNational Committee for Information Technology Standards. *Information technology – AT Attachment 8 - ATA/ATAPI Command Set - 2 (ATA8-ACS-2)*, INCITS 482-2012, American National Standards Institute, New York, May 30, 2012.

- InterNational Committee for Information Technology Standards., *Information technology - SCSI Primary Commands - 4 (SPC-4)*, INCITS 513, May 17, 2014. http://www.t10.org/cgi-bin/ac.pl?t=f&f=spc4r37.pdf [accessed 7/18/14].

- J. Hasson, "V.A. Toughens Security after PC Disposal Blunders," *Federal Computer Week,* August 26, 2002. http://fcw.com/Articles/2002/08/26/VA-toughens-security-after-PC-disposal-blunders.aspx [accessed 7/21/14].

- C. King, and T. Vidas, "Empirical analysis of solid state disk data retention when used with contemporary operating systems," *Digital Investigation* 8 (2011), S111-S117. http://dx.doi.org/10.1016/j.diin.2011.05.013.

- *Microsoft EFI FAT32 File System Specification*, Microsoft Corporation, December 6, 2000. http://msdn.microsoft.com/en-us/library/windows/hardware/gg463080.aspx [accessed 7/21/14].

- B.J. Phillips, C.D. Schmidt, and D.R. Kelly, "Recovering data from USB flash memory sticks that have been damaged or electronically erased," *e-Forensics '08: Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, Adelaide, Australia (January 21-23, 2008), article no. 19. http://dx.doi.org/10.4108/e-forensics.2008.2771.

- A. Suresh, G. Gibson, and G. Ganger. *Shingled Magnetic Recording for Big Data Applications*, CMU-PDL-12-105, Carnegie Mellon University, Parallel Data Lab, Pittsburgh, Pennsylvania, May 2012, 29 pp. http://www.pdl.cmu.edu/PDLFTP/FS/CMU-PDL-12-105.pdf [accessed 7/18/14].

- U.S. Army. *Information Assurance,* Army Regulation (AR) 25–2, October 24, 2007 (with Rapid Action Release on March 23, 2009). http://armypubs.army.mil/epubs/pdf/r25_2.pdf [accessed 7/18/14].

- U.S. Department of Defense, "Clearing and Sanitization Data Storage," Table C8.T1 in *National Industrial Security Program: Operating Manual*, DoD 5220.22-M-Sup-1, Washington, D.C. (February 1, 2005), pp.82-83. http://www.dtic.mil/whs/directives/corres/pdf/522022MSup1.pdf Page 81[accessed 7/21/14].

- *Understand Degaussing*, Peripheral Manufacturing Inc. [Web page], http://www.periphman.com/understand_degaussing.shtml [accessed 7/21/14].

- M. Wei, L.M. Grupp, F.E. Spada, and S. Swanson, "Reliably Erasing Data From Flash- Based Solid State Drives," *9th USENIX Conference on File and Storage Technologies (FAST '11)*, San Jose, California (February 15-17, 2011), 13pp. http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf [accessed 7/21/14].

- B. Xu, J. Yang, H. Yuan, J. Zhang, Q. Zhang, and T.C. Chong, "Thermal Effects in Heat Assisted Bit Patterned Media Recording," *IEEE Transactions on Magnetics* 45(5) 2292-2295 (May 2009). http://dx.doi.org/10.1109/TMAG.2009.2016466.

付録 G ― シンプルな「データ抹消処理証明書」フォーム

本証明書は、収集すべき情報の種類及び証明書のフォーマットを示すための簡易例である。組織は、代替として、データ抹消処理の詳細を電子的に記録することを選択することもできる。これには、ネイティブアプリケーションを使用する方法と、自動データ転送ユーティリティ（データベース又は電子メールアドレスにデータを送信するボタンが付いた PDF フォームなど）が付いた本フォームのようなものを使用する方法がある。将来的に記録を参照する必要が生じた場合には、電子記録が最も早く検索できる機能を提供し、当該記録が確実に保持される可能性が高くなる。

データ抹消処理証明書		
データ抹消処理実施者		
氏名：	役職：	
組織名：	所在地：	電話番号：
媒体情報		
製造者：	モデル番号：	
シリアル番号：		
媒体資産番号：		
媒体タイプ：	媒体ソース（*すなわち、ユーザ名又はPC資産番号*）：	
機密区分：	データバックアップ：☐あり ☐なし ☐不明	
バックアップ所在地：		
データ抹消処理詳細		
処理方法のタイプ：☐消去 ☐除去 ☐損傷 ☐破壊		
使用した方法：☐消磁 ☐上書き ☐ブロック消去 ☐暗号化消去 ☐その他：		
方法の詳細：		
利用ツール（*バージョンを含む*）：		
検証方法：☐完全 ☐クリックサンプリング ☐その他：		
データ抹消処理後の機密区分：		
注意：		
媒体の行先		
☐組織内での再利用 ☐組織外での再利用 ☐リサイクル工場 ☐製造会社 ☐その他（*詳細の個所*に明記）		
詳細：		
署名		
私は、この明細書に記載された情報が、私の知る限りにおいて正確であることを保証します。		
署名：		日付：
認証		
氏名：	役職：	
組織名：	所在地：	電話番号：
署名：		日付：