NIST Special Publication 800-88

媒体のサニタイズに関するガイドライン

米国国立標準技術研究所による勧告

Richard Kissel
Matthew Scholl
Steven Skolochenko
Xing Li

コンピュータセキュリティ

米国国立標準技術研究所
情報技術ラボラトリ
コンピュータセキュリティ部門
Gaithersburg, MD 20899-8930

2006 年 9 月

米国商務省　長官
Carlos M. Gutierrez

米国国立標準技術研究所　所長
William Jeffrey

この文書は下記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
NRI SECURE TECHNOLOGIES

コンピュータシステム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、以下、NIST と称す。）の情報技術ラボラトリ（ITL：Information Technology Laboratory）は、国家の測定およ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、米国の経済と公共福祉に貢献している。情報技術ラボラトリは、テストの実施、テスト技法の開発、参照データの作成、実装によるコンセプト実証、技術的分析を通じて、情報技術の開発と生産的利用の発展に努めている。I 情報技術ラボラトリの責務は、連邦政府の情報システムにおいて、費用対効果の高いセキュリティを施し、国家安全保障にかかわらない情報のプライバシを確保するための、技術的、物理的、管理的および運用のための標準とガイドラインを策定することにある。NIST Special Publication 800 シリーズでは、情報システムセキュリティにおける情報技術ラボラトリの調査、ガイドライン、普及活動ならびに産業界、政府機関および教育機関との共同活動について報告する。

米国国立標準技術研究所、Special Publication 800-88
米国国立標準技術研究所、Special Publication 800-88、41 ページ（2006 年 3 月）

合衆国政府印刷局
WASHINGTON: 2004

謝辞

本書執筆陣である Richard Kissel、Matthew Scholl、Steven Skolochenko および Xing Li は、本書草稿をレビューしてくれた同僚とコメントを寄せてくれたすべての方々に感謝の意を表したい。特に、内部レビュープロセスを支援してくれた Rick Ayers、Murugiah Souppaya、Mark Wilson、Tanya Brewer および Elizabeth Lennon に感謝する。また、William Gill、Dr. Chun Tse および Dr. Simson Garfinkel にも、それぞれが行った調査、技術支援および寄稿に感謝する。さらに、最終レビューでの鋭い洞察と支援を提供してくれた FDA の Kevin Stine にも感謝する。

本研究は、国土安全保障省（DHS：Department of Homeland Security）の後援を受けており、本研究における DHS の支援と指導に深く感謝する。

正誤表

Special Publication 800-88 には、以下の変更が加えられた。

日付	バージョン	変更内容	ページ番号
09-11-06	10-06	「暗号化は、一般に認められたサニタイズの手段ではない。コンピュータの性能向上によって暗号文の解読に要する時間が短縮されるため、暗号化されたデータの復元を不可能にすることが保証できなくなった」を削除。	7
9-11-06	10-06	「表面積が 5 ミリメートル」を「光ディスク用のメディアシュレッダ（粉砕装置）を使って、1 辺の基準寸法が 5 ミリメートル（mm）で表面積が 25 平方ミリメートル（mm^2）の小片に分解する。」に変更。	21
9-11-06	10-06	「表面積が 5 ミリメートル」を「光ディスク用のメディアシュレッダ（粉砕装置）を使って、1 辺の基準寸法が 5 ミリメートル（mm）で表面積が 25 平方ミリメートル（mm^2）の小片に分解する。」に変更。	22

目次

目次 vi
図 viii
表 viii
要旨 ix
1 はじめに 1
1.1 作成機関 1
1.2 目的と範囲 1
1.3 対象とする読者 2
1.4 前提条件 2
1.5 ほかの NIST 文書との関係 3
1.6 構成 3
2 背景 5
2.1 適切な媒体のサニタイズと情報の処分に対するニーズ 5
2.2 媒体の種類 5
2.3 データ記憶媒体の傾向 6
2.4 サニタイズの種類 7
2.5 サニタイズと処分に関する意志決定に影響するそのほかの要素 9
3 役割および責務 10
3.1 プログラム管理者／各省庁の長官 10
3.2 主席情報官（CIO：CHIEF INFORMATION OFFICER） 10
3.3 情報システムオーナー 10
3.4 情報オーナー 10
3.5 政府機関上級情報セキュリティ担当官
（SAISO：SENIOR AGENCY INFORMATION SECURITY OFFICER） 10
3.6 システムセキュリティ管理者／担当官 11
3.7 財産管理担当官 11
3.8 記録管理担当官 11
3.9 プライバシ担当官 11
3.10 ユーザ 11
4 情報のサニタイズと処分に関する意志決定 12
4.1 システムライフサイクルにおける情報に関する意志決定 13
4.2 サニタイズに対するニーズの識別 13
4.3 セキュリティ分類の決定 13
4.4 媒体の再利用 14
4.5 媒体管理 14
4.6 サニタイズと廃棄に関する意志決定 14
4.7 方法の検証 15

4.8　文書化.....15
5　サニタイズ技法の要約.....16
付録 A　データを含む媒体のサニタイズに関する最小限の推奨事項.....17
付録 B　用語集.....25
付録 C　ツールと資料.....29
付録 D　ホームユーザおよび在宅勤務者向けの考慮事項.....31
付録 E　資料.....33
付録 F　サニタイズの有効性を確認する書式の例.....35

図

図 4-1. サニタイズと処分に関する意志決定の流れ 12

表

表 2-1. サニタイズの種類.....7

表 5-1. サニタイズの方法.....16

表 A-1. 媒体サニタイズに関する意志決定のマトリックス 17

要旨

情報システムは、各種の媒体を使って情報を捕捉し、処理し、保存する。これらの情報は、保存することを意図された記憶媒体だけでなく、情報の作成、処理、または送信に使われる機器にも格納される。これらの情報が不正に開示されるリスクを軽減しその機密性を確保するためには、これらの媒体を特別な方法で処分する必要がある。情報技術(IT)システムによって作成、処理、および保存される情報を、その発生から処分までの存続期間全体を通して効率的かつ効果的に管理することは、情報システムオーナーとデータの管理者にとって主要な関心事である。

ますます高度な暗号化が行われるようになってきたため、組織の機密情報にアクセスしようとする攻撃者は、そのような情報をシステムの外部に求めざるを得なくなった。そうした攻撃方法の 1 つは、媒体から削除されたはずのデータの復元である。このような残存データによって、許可されていない個人がデータを再現し、機密情報にアクセスできるようになる可能性がある。サニタイズを行うと、削除されたデータを簡単に復元できなくなるため、このような攻撃を阻止できる。

記憶媒体を譲渡したり、古くなって使われなくなったり、情報システムで使用できなくなったりまたは不要になったりした場合は、削除後に残存する磁気、光学、電気、またはそのほかの表現形式によるデータを簡単に復元できないようにすることが重要である。サニタイズとは、データを簡単に取り出したり再現したりできないという合理的な保証を得るために記憶媒体からデータを削除する一般的なプロセスを指す。

このガイドは、組織やシステムオーナーが情報の機密性のレベルに基づいてサニタイズに関する実際的な意志決定を行えるように支援するものである。既知のすべての種類の媒体を具体的に取り扱うものではなく、またそれは不可能であるけれども、記載されているサニタイズの意志決定プロセスは、広く一般に適用できる。また、合衆国法典第 40 編において、余剰設備が「教育の分野で有用」であり、「連邦政府の設備は重要な国家資産である」ことをシステムオーナーや管理者に忠告している。余剰設備や媒体は、法律の許す範囲内で、できるだけ学校や非営利組織が利用できるようにすべきである。

1　はじめに

1.1　作成機関

米国国立標準技術研究所（NIST: National Institute of Standards and Technology、以下 NIST と称する）は、2002 年施行の連邦情報セキュリティマネジメント法（FISMA: Federal Information Security Management Act、以下 FISMA と称す）、公法 107-347 に基づくその法的責任を推進するために、この文書を作成した。

NIST は、すべての連邦政府機関の運営および資産に適切な情報セキュリティをもたらすために、最低限の要求事項を含んだ標準およびガイドラインを作成する責務があるが、このような標準およびガイドラインは国家安全保障にかかわるシステムには適用されない。このガイドラインは、行政管理予算局（OMB; Office of Management and Budget）Circular A-130、第 8b(3)項、『政府機関の情報システムの保護（Securing Agency Information Systems）』の要求事項に一致しており、これは A-130 の付録 IV「重要部門の分析」で分析されているとおりである。補足情報は、A-130、付録 III に記載されている。

本文書における一切は、商務長官が法的権威に基づき連邦政府に対して義務および拘束力を与えた標準および指針を否定するものではない。また、これらの指針は、商務長官、行政管理予算局長、または他のすべ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るものと解釈してはならない。

1.2　目的と範囲

情報の廃棄と媒体のサニタイズに関する情報セキュリティ上の懸念は、媒体にではなく、記録されている情報にある。媒体の廃棄とサニタイズの問題は、媒体に意図的にまたは意図せずに格納された情報に左右される。こんにちのオペレーティングシステムが備える高度な機能からすれば、システム上で使われる電子媒体には、システムの機密性の分類に応じた情報が含まれているとみなすべきである。これらの媒体を適切に取り扱わないと、手放したときに情報の不正な開示が発生する可能性がある。連邦情報処理基準（FIPS：Federal Information Processing Standards、以下 FIPS と称す）199『*連邦政府の情報および情報システムに対するセキュリティ分類規格（Standards for Security Categorization of Federal Information and Information Systems）*』に基づいて情報技術（IT）システムを分類することは、システムの情報と媒体を理解し、管理するための重要な第一歩である。

分類結果に基づいて、システムオーナーは NIST SP800-53『*連邦政府情報システムにおける推奨セキュリティ管理策（Recommended Security Controls for Federal Information Systems）*』を参照すべきである。当該文書では、次のように規定されている。「組織は、承認された装置、技法および手順を使用して、情報システムのディジタル記憶媒体をサニタイズする。組織は、記憶媒体のサニタイズと破壊の活動を追跡、文書化、および検証し、サニタイズ装置／手順を定期的にテストして正常に動作することを保証する。組織は、情報システムのディジタル記憶媒体を廃棄または組織外での再利用のために持ち出す前に、サニタイズまたは破壊し、許可されてない個人が記憶媒体に含まれた情報にアクセスして利用することを防止する。」

この文書では、各組織が、関連するシステムの機密性の分類を考慮しながら、サニタイズと廃棄に関する意志決定を行うための適切かつ適用可能な技法と管理策を使って、媒体サニタイズプログラムを実現するのを支援する。

この文書の目的は、媒体の廃棄や再利用が必要な場合や、媒体が組織の実効的な管理を離れる場合の意志決定を支援することである。各組織は、媒体と情報の最終的なサニタイズまたは処分、あるいはその両方に関して実効性のあるリスクベースの意志決定を行うために、ローカルのポリシーと手続きを策定して、このガイドとともに、使用すべきである。

このガイドの情報は、最新の技術とアプリケーションが使われている状況に適用するのが最適である。また、システムライフサイクルの全体を通して行われる情報廃棄に関するサニタイズ、および管理策に関する意志決定のためのガイダンスも提供する。このガイドで取り上げていない形式の媒体が存在するほか、このガイドの対象になっていない媒体もこれから開発および配備される。そのような場合も、手順に関するセクションに示したこのガイドの意図は、FIPS 199『*連邦政府の情報および情報システムに対するセキュリティ分類規格（Standards for Security Categorization of Federal Information and Information Systems）*』によるシステムの機密性の分類結果に基づいて、すべての媒体形式に適用される。

媒体をサニタイズする前に、システムオーナーは、プライバシの責任者に任命された担当官（プライバシ担当官など）、情報公開法（FOIA：Freedom of Information Act）の責任者、およびローカルの記録保持担当部署と協議することが強く推奨される。この協議の目的は、連邦記録法（Federal Records Act）の記録保持に関する規制や要件を確実に遵守するためである。また、業務上必要な場合に過去の情報を確実に捕捉し、維持するため、組織の管理職層とも協議すべきである。システムやシステム環境の変化に応じて管理策を調整しなければならない可能性があるため、この協議は継続的に行うべきである。

1.3 対象とする読者

情報の機密性の保護は、連邦政府機関、企業からホームユーザに至るまで、あらゆる人々の関心事である。政府サービスの提供には、相互接続と情報交換が不可欠であるという認識に立てば、このガイドは、サニタイズや廃棄にどのようなプロセスを使用するかを決定するための参考資料として使用できる。

1.4 前提条件

このガイドは、各組織が適切な情報の分類、機密性の影響レベル、および情報の場所を正しく識別できることを前提としている。この活動は、システムライフサイクルの最も早い段階で行われるのが理想である。この重要な初期段階は、この文書の対象外であるが、このような識別を行わない組織は、機密情報を含む媒体を（ほぼ確実に）管理できなくなる。

このガイドでは、組織が情報を保存するために使用できるすべての媒体を取り上げるつもりも、このガイドの有効期間内に開発される可能性がある将来の媒体を予測するつもりもない。読者には、媒体に含まれている情報のセキュリティ分類に基づいて、サニタイズと廃棄に関する意志決定を行うことが期待される。

1.5 ほかの NIST 文書との関係

FIPS 199『連邦政府の情報および情報システムに対するセキュリティ分類規格（Standards for Security Categorization of Federal Information and Information Systems）』および NIST SP 800-60『情報および情報システムのタイプとセキュリティ分類のマッピングガイド（Guide for Mapping Types of Information and Information Systems to Security Categories）』には、システムの機密性の分類を確立するためのガイダンスが示されている。この分類は、組織がサニタイズの意志決定を行う際に要求すべき保証のレベルに影響する。

FIPS 200『*連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項（Minimum Security Requirements for Federal Information and Information Systems）*』には、各組織に媒体サニタイズプログラムを用意することを求めるセキュリティ要件の基礎が設定されている。

NIST SP 800-53『*連邦政府情報システムにおける推奨セキュリティ管理策（Recommended Security Controls for Federal Information Systems）*』には、連邦政府システムの全体的なセキュリティ分類に基づく最低限の推奨セキュリティ管理策（サニタイズを含む）が示されている。

NIST SP 800-53A『連邦政府情報システムのためのセキュリティ管理策アセスメントガイド（*Guide for Assessing the Security Controls in Federal Information Systems*）』には、連邦政府システムの全体的なセキュリティ分類に基づくセキュリティ管理策（サニタイズを含む）の評価に関するガイダンスが示されている。

1.6 構成

このガイドは、以下の 5 つのセクションと 6 つの付録に分かれている。

- **セクション 1**（このセクション）では、この文書の作成機関、目的と範囲、対象読者、および前提条件について説明し、文書の構成を示す。
- **セクション 2** では、サニタイズに対するニーズの概要と、情報、サニタイズ、および媒体の基本的な種類の概要を示す。
- **セクション 3** では、サニタイズの意志決定を左右する手順と原則に関する一般的な情報を提供する。
- **セクション 4** では、サニタイズの意志決定を支援するプロセスの流れを示す。
- **セクション 5** では、いくつかの一般的なサニタイズ技法の要約を示す。
- **付録 A** では、媒体のマトリックスを使って、各種の媒体を消去、除去、または破壊するために推奨される、最低限のサニタイズ技法を示す。この付録は、セクション 5 に示す意志決定フローチャートとともに使用すること。
- **付録 B** では、このガイドで使用している用語の解説を示す。
- **付録 C** では、媒体のサニタイズを支援するツールと参考になる外部情報源の一覧を示す。

- **付録 D** では、組織のリソースにアクセスできないホームユーザや在宅勤務者向けの情報のサニタイズに関する考慮事項を示す。
- **付録 E** では、このガイドの執筆に不可欠だった情報源や文書の一覧を示す。
- **付録 F** では、組織のサニタイズ活動を文書化するための書式の例を示す。

2 背景

情報の廃棄とサニタイズに関する意志決定は、システムライフサイクルの全体を通して行われる。情報の廃棄や媒体のサニタイズに影響を与える重要な要素は、システム開発の開始時に決定される。初期のシステム要件には、ハードウェアやソフトウェアの仕様だけでなく、システムオーナーがそのシステムで使用される媒体の種類を特定するのに役立つ相互接続やデータフローの文書も含めるべきである。要件段階では、システムで使用される情報を作成、捕捉、または転送するために、ほかにどのような種類の媒体が使われるかを明らかにすべきである。この分析で業務ニーズと機密性へのリスクのバランスを取ることにより、システムがFIPS 200『*連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項（Minimum Security Requirements for Federal Information and Information Systems）*』に準拠するために検討する媒体の形式が明確になる。

媒体のサニタイズと情報の廃棄の活動は、通常、システムライフサイクルの廃棄段階で最も精力的に行われる。しかし、データを含んだ多くの種類の媒体は、情報システムの存続期間全体を通して、組織が積極的に管理する環境の外へ移動される。このようなことは、保守上の理由やシステムのアップグレードのために行われたり、構成の更新中に行われたりする。

2.1 適切な媒体のサニタイズと情報の処分に対するニーズ

媒体のサニタイズは、機密性を保証するための主要な要素の 1 つである。機密性とは、「しかるべき承認を受けて、情報へのアクセスと開示に対して制限を設けることであり、これには個人のプライバシと機密情報の保護手段が含まれる」（合衆国法典第 44 編第 3542 条）。

「機密性の損失とは、情報の不当な開示である」（FIPS 199『連邦政府の情報および情報システムに対するセキュリティ分類規格（Standards for Security Categorization of Federal Information and Information Systems）』）。

各組織が保護する責任を負う情報に対して適切な管理策を用意するためには、使用する媒体を適切に保護する必要がある。不正な情報収集の豊富なソースになることが多いのは、不適切に廃棄されたハードコピー媒体をごみ箱あさりによって探す方法、不適切にサニタイズされた電子媒体を入手する方法、または格納されている情報の機密性にふさわしくない方法でサニタイズされた媒体からキーボードや実験室を使って再現する方法（訳注:「キーボード」は、ソフトウェアなどによって論理的に再現すること。「実験室」は、信号復元装置など物理的手段を使って再現すること）である。媒体は、紙形式でリサイクルの分別箱に捨てられたり、機器の修理のためにベンダーに送られたり、緊急事態への対応としてほかのシステムにホットスワップされたりすることにより、組織の管理下に入ったり管理下から出たりする。このような潜在的な脆弱性は、情報の場所、情報の種類、および情報の保護方法を適切に理解することによって軽減できる。

2.2 媒体の種類

一般的に使用される媒体には、主に次の 2 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ある。紙の印字出力、プリンタ、ファックスのリボン、ドラム、プラテンなどは、すべてハードコピー媒体の例である。この種類の媒体は、管理されていないことが最も多い。リサイクルの分別箱やゴミ箱に捨てられた情報は、ゴミ箱あさりや好奇心の強すぎる従業員に対して重大な脆弱性となる。

- 電子(ソフトコピー)。電子媒体は、ハードディスクドライブ、ランダムアクセスメモリ(RAM)、読み取り専用メモリ(ROM)、ディスク、メモリデバイス、電話、携帯コンピュータデバイス、ネットワーク機器、および付録 A に示したそのほかの多くの種類の機器に格納されたデータである。

将来、各組織はこのガイドで具体的に取り上げていない種類の媒体を使用することになる。この文書で説明するプロセスは、使用する媒体の種類に関係なく、媒体のサニタイズに関する意志決定の指針となるはずである。このガイドをすべての種類の媒体について効果的に使用するために、各組織および各個人は媒体に記録されている情報に重点を置くべきである。

2.3 データ記憶媒体の傾向

コンピュータ技術は、急速に変化する。ユーザは、より高性能でコンパクトな機器を求める。この要求を満たすために、新しい技術によって処理速度と格納容量は常に増加する一方で、機器のサイズは縮小している。これらの技術に対しては、新しい消去や除去の技法が必要になる可能性がある。

技術の高度化により、磁気ディスクタイプの記憶媒体に関する従来のベストプラクティスが様変わりする状況が生まれた。基本的には、記憶媒体のトラック密度の変化やそれに伴う変化によって、媒体の消去と除去が同一になる状況が生まれた。つまり、2001 年以降に製造された ATA ディスクドライブ(15 GB 超)では、キーボード攻撃と実験環境室のどちらから媒体を保護するにも、媒体を一回上書きすることによる消去で十分である。

今後登場するデータ格納技術を次にいくつか示す。

- ホログラフィック記憶装置。光のパターンを保持する感光性結晶を光が通過することにより、ホログラフィ(3 次元)像上にデータが保存される。数千倍の記憶容量を持ち、機械的な動作を必要としない。一度に 1 ビットのデータの読み取りまたは書き込みを行う現在の 2 次元記憶装置とは異なり、1 つの読み取りまたは書き込みコマンドで大量のデータの読み取りまたは書き込みが可能である。研究者によれば、100 万ビットのデータを含むページ(データブロック)を数千個格納したホログラフィックデータ記憶システムを、角砂糖 1 個の大きさに収容できるとされている。10 ギガバイト(GB)のデータが 1 立方センチメートルに収まることになる。ホログラフィックシステムには可動部分がなく、そのページには並列にアクセスできるため、ホログラフィックシステムのデータスループットは毎秒 1 ギガビットに達すると予想されている。

- 分子メモリ。バクテリオロドプシンと呼ばれるタンパク質を使ってデータを保存する。このタンパク質は、レーザーによって bR(0 の状態)から Q(1 の状態)に

変化させることができるため、理想的な AND データ記憶ゲート（フリップフロップ）になる。分子メモリは安価に製造でき、動作可能な温度の範囲が半導体メモリより広い。分子はマイクロ秒単位で状態を変化させるが、読み取りまたは書き込み操作のステップ全体の実行には 10 ミリ秒程度かかる。これは遅いようにも思えるが、この装置はホログラフィック記憶装置と同じようにデータページを並列に取得するため、10 Mbps のスループット速度を実現できる。

2.4 サニタイズの種類

組織内での媒体の管理方法を決定する秘訣は、最初に情報を考慮し、次に媒体の種類を考慮することである。情報のセキュリティ分類は、内部の環境要因とともに、媒体の扱い方に関する意志決定を左右する。繰り返しになるが、秘訣は最初に情報の機密性の観点から考え、次に媒体の種類に応じて考えることである。

各組織には、分類されたどのシステムにも関連付けられない情報が存在する。これらの情報は、メモ、ホワイトペーパー、プレゼンテーションなどのハードコピーを使った内部的なコミュニケーションであることが多い。これらの情報が機密に関わると考えられる場合もある。例として、内部懲戒文書、金銭や給与に関する交渉、戦略会議の議事録などが考えられる。各組織は、内部で運用している分類に従ってこれらの媒体にラベルを付け、この文書で説明するサニタイズの種類を関連付けるべきである。

媒体ごとに、さまざまなサニタイズの種類がある。ここでは、媒体のサニタイズを、廃棄、消去、除去、破壊の 4 つに分類する。廃棄は、特別な処分方法をとらずに媒体をそのまま捨てることである。情報が開示されても、組織の使命に対する影響がなく、組織の資産に損害が発生せず、財務上の損失が発生せず、個人に害が及ばない場合は、媒体をそのまま廃棄できる。廃棄に言及するのは、必ずしもすべての媒体にサニタイズが必要ではないこと、および機密でない情報を含む媒体の処理方法としては廃棄も依然として有効であることを各組織に保証するためである。廃棄は厳密にはサニタイズの一種ではないため、この項以外で言及したり取り上げたりすることはしない。

このガイドの読者には、情報を分類し、情報が記録されている媒体の性質を判断し、機密性へのリスクを判定し、その媒体に関する将来の計画を決定した上で、適切なサニタイズの種類を決めることが推奨される。選択した種類については、コスト、環境への影響などについて評価するとともに、機密性へのリスクを最も軽減し、プロセスに課せられるそのほかの制約を最大限に満たす意志決定を行うべきである。

表 2-1. サニタイズの種類

種類	説明
廃棄	廃棄は、サニタイズに関する特別な配慮を行わずに媒体を捨てる行為である。これは、機密でない情報を含む古紙をリサイクルすることによって行われることが多いが、ほかの媒体を含む場合もある。
消去	情報の消去は、強力なキーボード攻撃から情報の機密性を保護する、媒体サニタイズの一種である。項目を単に削除するだけでは消去として十分ではない。消去では、データ、ディスク、またはファイルの復旧ユーティリティによって情報を取り出すことができないようにする必要が

種類	説明
	ある。また、標準入力装置やデータ収集ツールから実行されるキーストロークによる復元の試みに対する抵抗力を持つ必要がある。たとえば、上書きは媒体の消去方法として容認できる。 媒体上の格納領域を非機密データで上書きするソフトウェアまたはハードウェアの製品が存在する。このプロセスには、ファイルの論理的な格納場所（ファイルアロケーションテーブルなど）の上書きだけでなく、アドレス指定可能なすべての場所の上書きが含まれる場合もある。上書きプロセスのセキュリティ上の目標は、記録されているデータをランダムなデータに置き換えることである。上書きは、破損した媒体や書き込みが不可能な媒体には使用できない。上書きが適切なサニタイズ方法かどうかは、媒体の種類やサイズに左右される場合もある（SP 800-36 を参照）。 研究の結果、こんにちの媒体のほとんどは 1 回上書きするだけで効果的に消去できることがわかっている。 各種媒体の消去に関する具体的な推奨事項については、付録 A を参照されたい。
除去	情報の除去は、実験環境室から情報の機密性を保護する、媒体サニタイズプロセスの一種である。一部の媒体では、媒体を消去するだけでは除去として十分ではない。しかし、2001 年以降に製造された ATA ディスクドライブ（15 GB 超）では、「消去」と「除去」の意味は同一である。 実験環境室には、標準外のシステムを使って通常の運用環境の外で媒体を対象にデータ復元の試みを行うリソースおよび知識を使用した脅威が伴う。この種類の攻撃には、信号処理装置と特別に訓練された人材が使用される。 ファームウェアの Secure Erase（完全消去）コマンドの実行（ATA ドライブのみ）や消磁などが、除去の方法として容認できる。ハードディスクドライブの部品を消磁すると、通常、装置を管理しているファームウェアが破壊されるため、ドライブも破壊される。 消磁とは、記録された磁区を破壊するために、磁気媒体を強力な磁場にさらすことである。消磁器は、磁気媒体のサニタイズに使われる磁場を生成する装置である。消磁器は、除去できる磁気媒体の種類（低エネルギーまたは高エネルギー）に基づいてランク付けされている。消磁器は、強力な永久磁石または電磁石コイルを使って動作する。消磁は、破損した媒体の除去、格納容量がきわめて大きい媒体の除去、フロッピーディスクの高速除去などに有効な方法である。消磁は、光学媒体（CD や DVD）などの非磁気媒体の除去には効果がない（SP 800-36『Guide to Selecting Information Security Products』を参照）。 各種媒体の除去に関する具体的な推奨事項については、付録 A を参照されたい。各組織にとって媒体の除去が適当なサニタイズ方法でない場合は、媒体を破壊することが推奨される。
破壊	媒体の破壊は、究極のサニタイズ方法である。媒体を破壊すると、本来の目的でその媒体を再利用することができなくなる。物理的な破壊は、分解、焼却、粉砕、細断、溶解など、さまざまな方法を使って行われる。 情報のセキュリティ分類が高位であるために、または環境要因のために破壊が決定された場合、残存媒体は実験環境室に耐えられるものであるべきである。 ▪ *分解、焼却、粉砕、および溶解。*これらのサニタイズ方法は、媒体を完全に破壊することを目的としている。これらは、通常、これらの活動を効果的かつ安全確実に行う特別な能力を持つ委託先の金属破壊／焼却施設で実行される。 ▪ *細断。*フロッピーディスクなどの柔軟性のある媒体は、その外部容器から取り外したあと、シュレッダを使って破壊できる。細断されたくずのサイズは、データの機密性レベルに応じて、情報を再現できないという十分な保証が得られる程度まで小さくなっているべきである。 コンパクトディスク（CD、CD-RW、CD-R、CD-ROM）、光ディスク（DVD）、光磁気（MO）ディスクを含む大容量の光記憶媒体は、粉砕、クロスカット細断、または焼却によって破壊する必要がある。 媒体の破壊は、訓練済みの許可された職員が行うべきである。媒体の破壊を行う前に、安全性、危険物、および特別な廃棄方法へのニーズを特定し、それらに対応すべきである。

2.5 サニタイズと処分に関する意志決定に影響するそのほかの要素

サニタイズに関する意志決定を行うときは、システムの機密性の分類とともに、いくつかの要素を考慮すべきである。最終的な決定の前に、媒体サニタイズプロセスのコストとメリットを理解すべきである。たとえば、フロッピーディスクなどの安価な媒体を消磁するのは、費用対効果が高くない可能性がある。消去または除去が推奨される方法ではあるが、媒体を破壊するほうが（訓練、追跡、検証などを考慮すると）ほかのいずれかの方法よりも費用対効果が高い場合もある。各組織は、妥当であり、かつ既存のリスクのアセスメントによって示唆される場合は、適用するサニタイズのレベルをいつでもあげることができる。

各組織は、以下の環境要因を考慮すべきである。ただし、この一覧は網羅的なものではない。

- 組織ではどのような種類（書き換え不可能な光ディスク、磁気ディスクなど）とサイズ（メガバイト、ギガバイト、テラバイトなど）の記憶媒体をサニタイズする必要があるか
- 媒体に格納されているデータの機密性はどの程度か
- 媒体は、管理された区域で処理されるか
- サニタイズプロセスを組織内部と委託先のどちらで行うべきか
- サニタイズする媒体の種類ごとの想定容量はどの程度か[1]
- サニタイズ用の機器やツールの準備状況はどうか
- サニタイズの機器／ツールに関する要員の訓練レベルはどうか
- サニタイズにどのくらいの時間がかかるか
- ツール、訓練、有効性の確認、および媒体を供給の流れに戻すことを考慮した場合、どの種類のサニタイズのコストが高くなるか

[1] SP 800-36『*Guide to Selecting Information Security Products*』

3 役割および責務

3.1 プログラム管理者／各省庁の長官

「組織を成功させる責任は、最終的には組織の上級管理職にある。」[2]上級管理職は、組織の任務を支えるために、実効性のある情報セキュリティのガバナンス構造を確立し、組織のコンピュータセキュリティ計画とその計画全体の目標、目的、および優先順位を確立する。最終的には、組織の長は、計画に十分なリソースを適用し、計画を成功させる責任を負う。上級管理職層は、情報の種類と場所を正しく識別し、情報を適切にサニタイズするためのリソースを確実に割り当てる責任を負う。

3.2 最高情報責任者(CIO:Chief Information Officer)

CIO[3]は、情報セキュリティポリシーを公布する責任を負う。情報の廃棄と媒体のサニタイズは、このポリシーの構成要素の 1 つである。CIO は、情報の管理者として、組織または特定部署のサニタイズの要件が本文書のガイドラインに確実に従うようにする責任を負う。

3.3 情報システムオーナー

情報システムオーナー[4]は、保守や契約が整備されており、かつ情報の開示が組織に与える影響に応じてシステムの媒体と情報の機密性を保護するのに十分なものであることを保証すべきである。

3.4 情報オーナー

情報オーナーは、サービスプロバイダによる現場での媒体の保守が(必要な場合に)適切に監督されていることを保証すべきである。情報オーナーは、情報の利用者が情報の機密性と媒体のサニタイズの基本的な要件を確実に認識させる責任も負う。

3.5 上級情報セキュリティ責任者(SAISO:Senior Agency Information Security Officer)

SAISO は、情報の処分と媒体のサニタイズに関する情報セキュリティポリシーの要件が組織全体に導入され、タイムリーかつ適切な方法で実施されていることを保証する責任を負う。

---

[2]NIST SP 800-18『*連邦情報システムのためのセキュリティ計画作成ガイド(Guide for Developing Security Plans for Federal Information Systems)*』、16 ページ。

[3]Information Technology Management Reform Act(情報技術マネジメント改革法、別名 Clinger-Cohen 法)。政府機関において正式な CIO の役職を指名していない場合、FISMA では、その責任を政府機関の同等の責任者に担わせることを求めている。

[4]情報システムオーナーの役割は、対象政府機関および情報システムのシステム開発ライフサイクルにおける段階に応じて、さまざまに解釈することができる。機関によっては、情報システムオーナーをプログラムマネージャと呼んだり、業務オーナー、資産オーナー、ミッションオーナーと呼んだりすることがある。

3.6 システムセキュリティ管理者／責任者

日常的なセキュリティ導入／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*は、この取り組みにおいてシステム管理担当者を支援することが多い。この人物は、通常はコンピュータセキュリティプログラムの管理担当部署に属さないが、特定システムのセキュリティ活動を調整する責任を負う。この役割は、コンピュータシステムセキュリティ責任者また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 資産管理担当者

資産管理担当者は、サニタイズされた媒体や機器が組織内に再配布されたり、外部の主体に寄付されたり、破壊されたりした場合に、それらの状況が適切に把握されていることを保証する責任を負う。

3.8 記録管理担当者

記録管理担当者は、保護すべき記録が媒体のサニタイズによって破壊されないように、順守すべき記録の保存要件を、システムオーナーおよび／またはデータオーナー、または管理者に対して、知らせる責任を負う。

3.9 プライバシ担当者

プライバシ担当官は、プライバシ情報(および、その情報が記録されている媒体)の廃棄にまつわるプライバシの問題に関して助言を提供する責任を負う。

3.10 ユーザ

ユーザは、割り当てられた仕事を遂行する際に使用している情報の機密性を認識し、理解するとともに、情報の適切な取り扱いを保証する責任を負う。

4　情報のサニタイズと処分に関する意志決定

このセクションの説明と図 4-1 は、各組織が媒体に含まれる情報の機密性のセキュリティ分類に応じたサニタイズに関する意志決定を行うにあたっての手助けとなる。この意志決定プロセスは、媒体の種類ではなく、情報の機密性に基づいている。各組織が個々の状況に最も適したサニタイズの種類を決定すれば、サニタイズの目標を達成するために使われる技法が媒体の種類に応じて決まる。

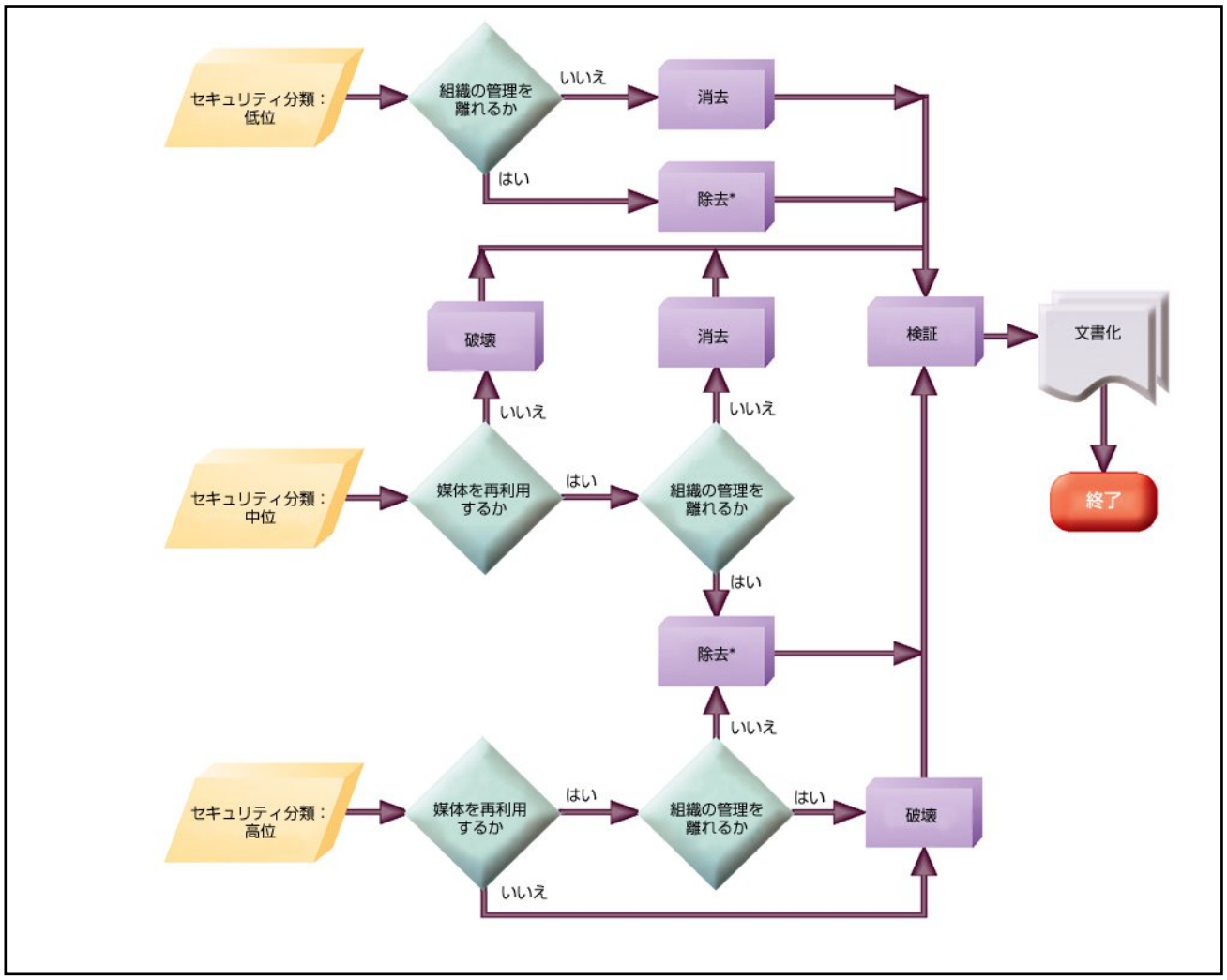


図 4-1. サニタイズと処分に関する意志決定の流れ

* 一部の媒体では、媒体を消去するだけでは除去として十分ではない。しかし、2001 年以降に製造された ATA ディスクドライブ（15 GB 超）では、「消去」と「除去」の意味は同一である。研究の結果、こんにちの媒体のほとんどは、現在利用できるサニタイズ技術を使って 1 回上書きするだけで効果的に消去および除去できることがわかっている。

4.1 システムライフサイクルにおける情報に関する意志決定

システムライフサイクルにおけるシステムの廃棄段階に達する前に、媒体サニタイズに対するニーズを識別し、その実施方法を策定すべきである。システム開発の開始にあたって最初のシステムセキュリティ計画を作成するときは（NIST SP 800-18『*連邦情報システムのためのセキュリティ計画作成ガイド（Guide for Developing Security Plans for Federal Information Systems）*』を参照）、媒体サニタイズの管理策を策定し、文書化し、配備する。サニタイズを実施する能力に影響を与える重要な意志決定の 1 つは、システムで使用する媒体の種類の選択である。これは主に業務上の意志決定であるが、システムオーナーはこの意志決定がシステムライフサイクル全体を通してサニタイズに必要なリソースの種類に影響を与えることを前もって理解する必要がある。

各組織は、サニタイズする媒体を慎重に識別すべきである。使用されている製品の多くは、複数の媒体形式を含んでおり、それぞれに異なるサニタイズ方法が必要である可能性がある。たとえば、PC には、ハードディスクドライブ、RAM および ROM が含まれている可能性がある。携帯機器には、揮発性メモリが組み込まれ、加入者識別モジュール（SIM：Subscriber Identity Module）の形で取り外し可能な不揮発性メモリが付いている。

4.2 サニタイズに対するニーズの識別

サニタイズに関する意志決定の第一段階の 1 つは、媒体のサニタイズが必要かどうか、および、いつ必要かを判断することである。

システムに保持されている情報を表現したものを含む媒体は、システムライフサイクルのあらゆる時点で生成される。これらの媒体は、データの単純な印字出力、画面出力のキャプチャ、ユーザの活動に関してキャッシュされたメモリなど、異なる形式を取る可能性がある。各組織は、情報に対する適切な統制を維持するため、どの媒体がいつデータを捕捉しているかを知る必要がある。これを知ることにより、各組織は媒体を廃棄するために適切なサニタイズをいつ実施する必要があるかを特定できる。これらの適切な廃棄に関する意志決定は、システムの定常的な活動の中においては、職場にシュレッダを設置し、電子機器のライフサイクルの最後に当該機器の破壊を行うという単純な場合もある。

4.3 セキュリティ分類の決定

システムライフサイクルの初期段階では、FIPS 199 と NIST SP 800-60 に記載されているガイダンス（システムの機密性に関するセキュリティ分類を含む）を使ってシステムを分類する。このセキュリティ分類は、システムの存続期間全体を通して見直しと有効性の再確認が行われ、必要に応じて機密性の分類が変更される場合もある。セキュリティ分類が完了すると、システムオーナーはシステムの情報の適切な保護を保証するサニタイズプロセスを設計できる。

多くの情報は、特定のシステムに関連付けられておらず、通常は書面によって行われる内部の業務上のコミュニケーションに関連付けられている。各組織は、内部で運用している分類に従ってこれらの媒体にラベルを付け、この文書で説明するサニタイズの種類を関連付けるべきである。

4.4 媒体の再利用

サニタイズに関する重要な意志決定の 1 つは、媒体が再利用またはリサイクルすることを意図するかである。一部の媒体形式では、多くの場合組織のリソースを節約するために再利用される。

破損やそのほかの理由で媒体を組織の内部または外部で再利用することが予定されていない場合、最も簡単で費用対効果の高い管理方法は破壊である可能性がある。

4.5 媒体管理

組織のサニタイズに関する意志決定を左右する要素の 1 つは、媒体の管理と媒体へのアクセスをだれが行うかである。この側面は、媒体が組織の管理を離れるときに考慮する必要がある。媒体がリース契約によって返却されるときや、組織の外部で再利用するために寄付または転売されるとき、媒体の管理責任が移転されることがある。媒体管理の例を次に示す。

組織の管理下にある場合:

- 組織と保守業者の間で、情報の機密性に関する契約が整備されている場合は、保守のために引き渡された媒体は依然として組織の管理下にあるとみなされる。
- 組織の施設内で組織の監督のもとで保守業者が保守を行う場合も、組織の管理下にあるとみなされる。

組織の管理下にない場合:

- 保証、払い戻し、またはそのほかの目的で交換され、組織に返却されない媒体は、組織の管理下にないとみなされる。

4.6 サニタイズと廃棄に関する意志決定

組織は、システムの機密性の評価を完了し、情報のサニタイズに対するニーズを明らかにし、使用する媒体と媒体処分の種類を決定したら、適切かつ必要なレベルのサニタイズに関して実効性のあるリスクベースの意志決定を行うことができる。この場合も、環境要因と媒体の種類によってサニタイズのレベルが変わる可能性がある。たとえば、紙コピーの「除去」は通常意味をなさないため、「破壊」が妥当な代替策となる。

サニタイズに関する意志決定が完了したら、決定事項を文書化し、それらの決定事項を支えるためのプロセスと適切なリソースが準備されていることを確認すべきである。このプロセスは、サニタイズの実施だけでなく、その正当化(決定事項と活動の文書化、リソースの特定、および重要な担当者と十分な合意)も含むため、媒体サニタイズプロセスの最も難しい部分になることが多い。

4.7 方法の検証

情報のサニタイズと廃棄に関して選択したプロセスを検証することは、機密性を保つうえで不可欠の手順である。適切な保護が維持されていることを組織に対して保証するために、媒体の代表的なサンプルについて、適切なサニタイズが行われているかどうかをテストすべきである。プロセスの検証は、プロセスのどの部分にも利害関係を持たない職員が実施すべきである。

4.7.1 機器の検証

組織が求める保証は、サニタイズプロセスの検証だけに限らない。組織がサニタイズのツール（消磁器など）を使用している場合は、機器の補正、機器の検査、および定期的な保守も必要である。

4.7.2 要員の力量の検証

もう 1 つの重要な要素は、サニタイズを行う要員の潜在的な訓練の必要性と、現時点で備わっている専門能力を確認することである。各組織は、機器のオペレータがサニタイズの機能を実行する能力を持っていることを確認すべきである。

4.8 文書化

組織がサニタイズの記録を保持し、どの媒体がいつどのようにサニタイズされ、最終的にどのように廃棄されたかを文書化することは重要である。組織が情報を管理できなくなったことが疑われる場合の多くは、媒体サニタイズの記録が適切に管理されてないことが原因である。

各組織は、資産管理担当者を媒体サニタイズプロセスの文書化に参加させることによって、機器と在庫管理の適切な責任追跡性を確立すべきである。

各組織は、低いセキュリティ分類の情報を含む媒体について、合理的な文書化活動を行うべきである。資産管理者は、一般にこれらを消耗品または壊れやすいものとして考えている。

各組織がサニタイズ活動の文書化に使用する書式の例を付録 F に示す。

5　サニタイズ技法の要約

媒体をサニタイズするには、いくつかの方法がある。このセクションでは、最も一般的な方法を 3 つ示す。このガイドの利用者は、破棄する情報を分類し、その情報が記録されている媒体の性質を見極め、その機密性に対するリスクを見積もり、その媒体に関する将来の計画を決定したうえで、表 5-1 を参考にして適切なサニタイズ方法を決めるべきである。選択した方法については、そのコストや環境に対する影響などを評価するとともに、情報が許可なしに開示されるリスクを最大限軽減する意志決定を行うべきである。

表 5-1. サニタイズの方法

方法	説明
消去	媒体をサニタイズする方法の 1 つは、媒体上の格納領域を非機密データで上書きするためのソフトウェア製品またはハードウェア製品を使用することである。このプロセスには、ファイルの論理的な格納場所（ファイルアロケーションテーブルなど）の上書きだけでなく、アドレス指定可能なすべての場所の上書きが含まれる場合もある。上書きプロセスのセキュリティ上の目標は、記録されているデータをランダムなデータに置き換えることである。上書きは、破損した媒体や書き換えが不可能な媒体には使用できない。上書きが適切なサニタイズ方法かどうかは、媒体の種類やサイズに左右される場合もある（SP 800-36 を参照）。
除去	消磁とファームウェアの Secure Erase コマンドの実行（ATA ドライブのみ）は、除去の方法として容認できる。 消磁とは、記録された磁区を破壊するために、磁気媒体を強力な磁場にさらすことである。消磁器は、磁気媒体のサニタイズに使われる磁場を生成する装置である。消磁器は、除去できる磁気媒体の種類（低エネルギーまたは高エネルギー）に基づいてランク付けされている。消磁器は、強力な永久磁石または電磁石コイルを使って動作する。消磁は、破損した媒体や動作不能になった媒体の除去、格納容量がきわめて大きい媒体の除去、フロッピーディスクの高速除去などに有効な方法である（SP 800-36 を参照）。
破壊	媒体の破壊には、多くの異なる種類、技法および手順がある。情報のセキュリティ分類が高位であるために破壊が決定された場合、破壊後の媒体は実験環境室に耐えられなければならない。 ▪ *分解、粉砕、溶解、および焼却。*これらのサニタイズ方法は、媒体を完全に破壊することを目的としている。これらは、通常、これらの活動を効果的かつ安全確実に行う特別な能力を持つ委託先の金属破壊施設や認可された焼却施設で実行される。 ▪ *細断。*フロッピーディスクなどの柔軟性のある媒体は、その外部容器から取り外したあと、シュレッダを使って破壊できる。細断されたくずのサイズは、データの機密性に応じて、そのデータを再現できないという十分な保証が得られる程度まで小さくなっているべきである。 コンパクトディスク（CD、CD-RW、CD-R、CD-ROM）、光ディスク（DVD）、MO ディスクを含む大容量の光記憶媒体は、粉砕、クロスカット細断、または焼却によって破壊する必要がある。素材を粉砕または細断する場合は、すべての残留物を 1 辺の基準寸法が 5 ミリメートル（mm）で表面積が 25 平方ミリメートル（mm2）になるまで分解する必要がある。

付録A　データを含む媒体のサニタイズに関する最小限の推奨事項

意志決定を行い（セクション 4 を参照）、組織の関連する環境要因を当てはめれば、表 A-1 を使って、該当する媒体に関して推奨されるサニタイズを決定できる。この推奨事項は、媒体に含まれる情報が許可なしに開示された場合の被害の影響を軽減するために、連邦情報処理基準（FIPS）199 によるシステムの機密性の分類を反映すべきである。

ここでは表 A-1 の使用を推奨するが、消去、除去（今でも適切な場合がある）、および破壊の目的を満足する方法はほかにもあり、この表に示されていない方法でも、組織が調査して満足のいくものであることがわかれば、適切である可能性がある。この表は、利用可能なすべての種類の媒体を示しているわけではない。使用している媒体がこの表に含まれていない場合、各組織はそれらの媒体を消去、除去または破壊するという目的を満たすプロセスを特定し、使用することが強く推奨される。

組織または政府機関が信頼し、その有効性を確認したサニタイズの技術、方法およびツールがある場合は、それらの情報を Federal Agency Security Practices（FASP）の Web サイトなどの公開フォーラムの場で共有することを強く奨励する。FASP の取り組みは、連邦最高情報協議会(Federal Chief Information Officer Council)のセキュリティに関するベストプラクティス(Best Security Practices)の試験的取り組みが成功したことを受けて、開始された。この取り組みは、重要インフラ保護（CIP：critical infrastructure protection）とセキュリティに関するベストプラクティスを特定、評価し、普及させるためのものである。FASP はhttp://csrc.nist.gov/fasp/にある。

表 A-1. 媒体サニタイズに関する意志決定のマトリックス

媒体の種類	消去	除去	物理的破壊
ハードコピー記憶			
紙およびマイクロフォーム	物理的破壊を参照。	物理的破壊を参照。	▪ 大きさ 1×5 ミリメートルの小片を作り出すクロスカットシュレッダ（NSA のシュレッダ EPL に掲載されている装置を参照）を使って紙を破壊するか、3／32 インチのセキュリティスクリーンを装備した粉砕装置（NSA の粉砕機 EPL を参照）を使って紙素材を粉砕／分解する。 ▪ 焼却によってマイクロフォーム（マイクロフィルム、マイクロフィッシュ、またはそのほかの縮小画像ネガ）を破壊する。素材を焼却する場合は、残留物が白い灰になるまで行う必要がある。
携帯機器			
携帯電話	すべての情報（通話履歴や電話番号など）を手動で削除し、メーカーが用意した完全リセット機能を実行して工場出荷時の設定に戻す。 ** 適切なサニタイズ手順については、メーカーに問い合わせること。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。 ▪ 認可された焼却施設で携帯電話を燃やすことによって焼却する。

媒体の種類	消去	除去	物理的破壊
PDA（Personal Digital Assistant：Palm や PocketPC など）	すべての情報を手動で削除し、メーカーが用意したハードリセット機能を実行して工場出荷時の状態に戻す。 ** 適切なサニタイズ手順については、メーカーに問い合わせること。	消去と同じ。	▪ 認可された焼却施設で PDA を燃やすことによって PDA を焼却する。 ▪ 細断する。 ▪ 粉砕する。
ネットワーク装置			
ルータ（家庭、ホームオフィス、企業）	メーカーが用意した完全リセット機能を実行し、工場出荷時の設定に戻す。 ** 適切なサニタイズ手順については、メーカーに問い合わせること。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。 ▪ 焼却する。ルータの焼却は、認可された焼却施設でルータを燃やすことによって行う。
機器			
コピー機	メーカーが用意した完全リセット機能を実行し、工場出荷時の設定に戻す。 ** 適切なサニタイズ手順については、メーカーに問い合わせること。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。 ▪ 焼却する。コピー機の焼却は、認可された焼却施設でコピー機を燃やすことによって行う。
ファックス装置	メーカーが用意した完全リセット機能を実行し、工場出荷時の設定に戻す。 ** 適切なサニタイズ手順については、メーカーに問い合わせること。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。 ▪ 焼却する。ファックス装置の焼却は、認可された焼却施設でファックス装置を燃やすことによって行う。
磁気ディスク			
フロッピーディスク	政府機関の承認を受けたソフトウェアを使って媒体を上書きし、上書きしたデータの有効性を確認する。	NSA／CSS の承認を受けた消磁器で消磁する。	▪ 認可された焼却施設でフロッピーディスクを燃やすことによってフロッピーディスクを焼却する。 ▪ 細断する。

媒体の種類	消去	除去	物理的破壊
ATA ハードディスクドライブ	政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。	1. Secure Erase を使って除去する。Secure Erase ソフトウェアは、カリフォルニア大学サンディエゴ校（UCSD：University of California, San Diego）の CMRR のサイトからダウンロードできる。 2. NSA／CSS の承認を受けた自動消磁器でハードディスクドライブの除去を行うか、ハードディスクドライブを分解し、内部のプラッタを NSA／CSS の承認を受けた消磁棒を使って消磁することにより、ハードディスクドライブの除去を行う。** 3. 政府機関の承認を受け、その有効性が確認されている除去技術／ツールを使って媒体の除去を行う。 ** 現世代のハードディスクドライブは、消磁すると永久に使用できなくなる。	▪ 分解する。 ▪ 細断する。 ▪ 粉砕する。 ▪ 焼却する。ハードディスクドライブの焼却は、認可された焼却施設でハードディスクドライブを燃やすことによって行う。
ハードディスクドライブ付きの USB リムーバブルメディア（Pen Drive、Thumb Drive、フラッシュドライブ、メモリースティック）	政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。	1. Secure Erase を使って除去を行う。Secure Erase ソフトウェアは、UCSD の CMRR サイトからダウンロードできる。 2. NSA／CSS の承認を受けた自動消磁器でハードディスクドライブの除去を行うか、ハードディスクドライブを分解し、内部のプラッタを NSA／CSS の承認を受けた消磁棒を使って消磁することにより、ハードディスクドライブの除去を行う。** 3. 政府機関の承認を受け、その有効性が確認されている除去技術／ツールを使って媒体の除去を行う。 ** 現世代のハードディスクドライブは、消磁すると永久に使用できなくなる。	▪ 分解する。 ▪ 細断する。 ▪ 粉砕する。 ▪ 焼却する。ハードディスクドライブの焼却は、認可された焼却施設でハードディスクドライブを燃やすことによって行う。
Zip ディスク	政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。	NSA／CSS の承認を受けた消磁器を使って消磁する。 ** 現世代の Zip ディスクは、消磁すると永久に使用できなくなる。	▪ 認可された焼却施設で Zip ディスクを燃やすことによって Zip ディスクを焼却する。 ▪ 細断する。

媒体の種類	消去	除去	物理的破壊
SCSIドライブ	政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。	NSA／CSS の承認を受けた自動消磁器でハードディスクドライブの除去を行うか、ハードディスクドライブを分解し、内部のプラッタを NSA／CSS の承認を受けた消磁棒を使って消磁することにより、ハードディスクドライブの除去を行う。 *** 現世代のハードディスクドライブは、消磁すると永久に使用できなくなる。	▪ 分解する。 ▪ 細断する。 ▪ 粉砕する。 ▪ 焼却する。ハードディスクドライブの焼却は、認可された焼却施設でハードディスクドライブを燃やすことによって行う。
磁気テープ			
リール型およびカセット型の磁気テープ	再記録（上書き）または消磁によって磁気テープの消去を行う。再記録（上書き）によって磁気テープの消去を行う方法は、そのプロセスによってテープ装置が長時間占有されるため、ほとんどの応用事例では現実的でない。 上書きによる消去：上書きは、元のデータを記録したシステムと同じようなシステムで実行すべきである。たとえば、以前に記録された機密情報を含む VHS 方式のビデオ信号は、同等の VHS レコーダで上書きする。磁気テープのすべての部分を、既知の機密でない信号を使って一回だけ上書きすべきである。	NSA／CSS の承認を受けた消磁器を使って消磁する。 消磁による除去：以前の既知の信号が再生できなくなる程度に信号を除去できる消磁器で、磁気テープの除去を行う。消磁による除去は、磁気テープに対して NSA／CSS の承認を受けた消磁器を使用することにより、より簡単に実行できる。	▪ 認可された焼却施設で磁気テープを燃やすことによって焼却する。 ▪ 細断する。 破壊の前にテープをリールやカセットから取り外すなどの準備手順は不要である。ただし、構成要素（テープとリールまたはカセット）の分離は、破壊施設の要件に適合させるため、あるいは、リサイクル対策としてそうする必要がある場合もある。
光ディスク			
CD	物理的破壊を参照。	物理的破壊を参照。	以下の推奨事項に従って破壊する。 ▪ 市販の光ディスク研削装置を使って CD 媒体の情報記録層を取り除く。 ▪ 認可された施設を使って光ディスク媒体を焼却する（灰にする）。 ▪ 光ディスク用のメディアシュレッダ（粉砕装置）を使って、1 辺の基準寸法が 5 ミリメートル（mm）で表面積が 25 平方ミリメートル（mm^2）の小片に分解する。** ** これは、現在の容認可能な小片の大きさである。今後入手するディスクメディアシュレッダは、CD の表面積を 25 mm^2まで分解できるものであるべきである。

媒体の種類	消去	除去	物理的破壊
DVD	物理的破壊を参照。	物理的破壊を参照。	以下の推奨事項に従って破壊する。 ▪ 市販の光ディスク研削装置を使って DVD 媒体の情報記録層を取り除く。 ▪ 認可された施設を使って光ディスク媒体を焼却する（灰にする）。 ▪ 光ディスク用のメディアシュレッダ（粉砕装置）を使って、1 辺の基準寸法が 5 ミリメートル（mm）で表面積が 25 平方ミリメートル（mm^2）の小片に分解する。** ** これは、現在の容認可能な小片の大きさである。今後入手するディスクメディアシュレッダは、DVD の表面積を 25 mm^2まで分解できるものにすべきである。
メモリ			
CompactFlash ドライブ、SD	政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。	物理的破壊を参照。	以下の推奨事項に従って媒体を破壊する。 ▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。 ▪ 認可された焼却施設で燃やすことによって焼却する。
ダイナミックランダムアクセスメモリ（DRAM：Dynamic Random Access Memory）	電源を切り、（バックアップバッテリがある場合は）バッテリを取り除くことによって DRAM の除去を行う。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。
電気的可変 PROM（EAPROM：Electronically Alterable PROM）	メーカーのデータシートに基づいてチップ全体の除去を行う。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。
電気的消去可能 PROM（EEPROM：Electronically Erasable PROM）	政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。 以前の用途や機密性を示すラベルやマークをすべて取り除く。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。 ▪ 認可された焼却施設で燃やすことによって焼却する。

媒体の種類	消去	除去	破壊
消去可能プログラマブル ROM（EPROM：Erasable Programmable ROM）	以下の推奨事項に従って媒体の消去を行う。 1. メーカーの推奨事項に従って紫外線による除去を実行することで、機能している EPROM の消去を行う。ただし、その所要時間の要件を 3 倍に増やす。 2. 政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。 ▪ 認可された焼却施設で燃やすことによって焼却する。
フィールドプログラマブルゲートアレイ（FPGA：Field Programmable Gate Array）デバイス（不揮発性）	政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。
フィールドプログラマブルゲートアレイ（FPGA：Field Programmable Gate Array）デバイス（揮発性）	電源を切り、（バックアップバッテリがある場合は）バッテリを取り除くことによって、機能している FPGA の消去を行う。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。
フラッシュカード	政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。
フラッシュ EPROM（FEPROM：Flash EPROM）	メーカーのデータシートに基づいてチップ全体の除去を行う。	以下の推奨事項に従って媒体の除去を行う。 1. 政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。 2. メーカーのデータシートに基づいてチップ全体の除去を行う。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。 ▪ 認可された焼却施設で燃やすことによって焼却する。
磁気バブルメモリ	政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。	次のようにして磁気バブルを崩壊させることにより、除去する。 1. 消磁：NSA／CSS の承認を受けた消磁器で消磁する。ただし、実際のバブルアレイに全界磁（最低 1500 ガウス）が確実に適用されるように注意する必要がある。消磁を行う前に、回路カード、バブルメモリ装置、またはその両方からすべての遮へ	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。 現実的な場合は、破壊装置の性能が最大限に発揮されるように、コアメモリ装置から外箱と電子回路基板を取り除くべきである。

媒体の種類	消去	除去	破壊
		い材を取り除く必要がある。 2. バイアス磁界の増加：バイアス磁界制御機能が組み込まれている磁気バブルメモリは、磁気バブルを崩壊させるのに十分なレベルまでバイアス電圧をあげることで、除去が行える可能性がある。この手順を試行する前に、バブルメモリのメーカーから具体的な技術ガイダンスを入手することを推奨する。	
磁気コアメモリ	以下の推奨事項に従って媒体の消去を行う。 1. 政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。 2. NSA／CSS の承認を受けた消磁器で消磁する。	上書きまたは消磁によってコアメモリ装置の除去を行う。 政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。 NSA／CSS の承認を受けた消磁器で消磁する。以前の用途や機密性を示すラベルやマークをすべて取り除く。注：筐体の遮へいや離間距離による磁界の減衰は、磁界を抹消する性能に影響を与えるため、考慮すべき要素である。消磁を行う前に、鋼鉄の遮へい材（筐体、ケース、取り付け金具など）をすべて取り除くべきである。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。 現実的な場合は、性能が最大限に発揮されるように、コアメモリ装置から外箱と電子回路基板を取り除くべきである。
不揮発性 RAM（NOVRAM：Non Volatile RAM）	1. 政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。 2. 個々の上書きがメモリ内に存在する期間は、元のデータが存在していた期間より長くなければならない。 3. バッテリ電源を含むすべての電源を取り外す。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。
PC カードまたは PCMCIA（Personal Computer Memory Card International Association）カード	物理的破壊を参照。	物理的破壊を参照。	認可された焼却施設での焼却によって破壊するか、（NSA で評価済みの）粉砕装置を使ってカード内部の回路基板と構成要素を基準寸法 2 ミリメートルの小片に分解する。
プログラマブル ROM（PROM：Programmable ROM）	物理的破壊を参照。	物理的破壊を参照。	認可された焼却施設で焼却によって破壊する。
RAM	電源を切り、（バックアップバッテリがある場合は）バッテリを	消去と同じ。	▪ 細断する。

媒体の種類	消去	除去	破壊
	取り除くことによって、機能している DRAM の除去を行う。		▪ 分解する。 ▪ 粉砕する。
ROM	物理的破壊を参照。	物理的破壊を参照。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。
ハードディスクドライブなしの USB リムーバブルメディア（Pen Drive、Thumb Drive、フラッシュドライブ、メモリースティック）	政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。	消去と同じ。	▪ 細断する。 ▪ 分解する。 ▪ 粉砕する。
スマートカード	物理的破壊を参照。	物理的破壊を参照。	▪ クレジットカードの形状をしたスマートカード装置およびデータストレージトークンは、金切りばさみ、はさみ、またはストリップカットシュレッダ（切り取り幅 2mm）を使って、スマートカードに内蔵されているメモリチップを切断または破砕する。トークン（SIM チップ、USB ドライブ、およびそのほかの物理的に強固なプラスチック筐体）のなかに実装されたスマートカードは、細断できないため、認可された焼却施設で焼却するか、2mm 大の小片に粉砕することによって破壊する。
磁気カード			
磁気カード	政府機関の承認を受け、その有効性が確認されている上書き技術／方法／ツールを使って媒体を上書きする。	NSA／CSS の承認を受けた消磁器で消磁する。	▪ 細断する。 ▪ 焼却する。磁気カードの焼却は、認可された焼却施設で磁気カードを燃やすことによって行うこと。

付録B 用語集

用語	定義
消去（Clear）	ソフトウェア製品またはハードウェア製品を使って、媒体上の格納領域を非機密データで上書きすること。このプロセスには、ファイルの論理的な格納場所（ファイルアロケーションテーブルなど）の上書きだけでなく、アドレス指定可能なすべての場所の上書きが含まれる場合もある。消去と除去の収束に関する解説を参照のこと。
CD	Compact Disc（コンパクトディスク）。光学的な方法でデータが記録される媒体の一種。
CD-RW	Compact Disc ReWritable（書き換え可能コンパクトディスク）。複数回の除去と書き換えが行える CD。
CD-R	Compact Disc Recordable（追記型コンパクトディスク）。書き込みは一回限りだが、読み取りは何回でも可能な CD。WORM とも呼ばれる。
CMRR	Center for Magnetic Recording Research（磁気記録研究センター）。CMRR は、磁気記憶の最先端技術を促進し、大学院生や博士課程を修了した専門家の教育を行っている。このセンターは、カリフォルニア大学サンディエゴ校にある。
データ（Data）	「理解可能な情報」の抽出元となる情報の断片。
消磁（Degauss）	逆磁場を印加することによって磁場を実質的にゼロまで低減すること。脱磁ともいう。現世代のハードディスクドライブ（IDE、EIDE、ATA、SCSI、Jaz を含むが、これらに限定されない）では、データセクタのあいだにある専用領域にトラックの位置情報が保存されているため、これらのドライブを消磁すると、ドライブを永久に使用できなくなる。
破壊（Destruction）	媒体が本来の目的で再利用できないこと、および情報の復元が事実上不可能または容認できないほどコストがかかることを保証するために行われる措置の結果。
ディジタル（Digital）	一般にコンピュータ技術において、データをバイナリビット（1 と 0）で表すために広く使われている 2 進数の符号体系。
分解（Disintegration）	媒体をサニタイズするための物理的な破壊方法の 1 つで、構成要素の部品に分割する行為。
廃棄（Disposal）	廃棄は、サニタイズに関する特別な配慮を行わずに媒体を捨てる行為である。これは、機密でない情報を含む古紙をリサイクルすることによって行われることが多いが、ほかの媒体を含む場合もある。
DVD	Digital Video Disc（ディジタルビデオディスク）。DVD は、CD と同じ形状と大きさを持つディスクだが、記録密度が高く、両面や 2 層に記録することもできる。
DVD-RW	DVD Forum が規格化した映画とデータの両方に対応する書き換え（再記録）可能な DVD ディスク。
DVD+RW	DVD+RW Alliance が規格化した映画とデータの両方に対応する書き換え（再記録）可能な DVD ディスク。
DVD+R	DVD+RW Alliance が規格化した DVD+RW 光ディスクの追記型（読み取り専用）バージョン。
DVD-R	DVD Forum によって承認された映画とデータの両方に対応する追記型（読み取り専用）DVD ディスク。
電子媒体（Electronic Media）	電気的なプロセスによってデータを記録する媒体を指す一般用語。
抹消（Erasure）	磁気的に保存された情報を通常の手段で取得できないようにするためのプロセス。
FIPS	Federal Information Processing Standard（連邦情報処理基準）。
フォーマット（Format）	あらかじめ規定されたデータの配置方法。

用語	定義
ハードディスク（Hard Disk）	ドライブユニットのなかに恒久的に固定され、データを格納するために使われる堅い磁気ディスク。
焼却（Incineration）	媒体をサニタイズするための物理的な破壊方法の 1 つで、灰になるまで完全に燃やす行為。
情報（Information）	データの有意の解釈または表現。
媒体（Media）	媒体（Medium）の複数形。
媒体のサニタイズ（Media Sanitization）	媒体上に書き込まれたデータを通常の手段と特別な手段のどちらでも復元できないようにするために行われる措置を指す一般用語。
媒体（Medium）	紙、パンチカード、磁気テープ、磁気ディスク、半導体素子、光ディスクなど、データが記録されている（記録できる）素材。
溶解（Melting）	媒体をサニタイズするための物理的な破壊方法の 1 つで、一般に加熱によって固体を液体状態に変化させること。
光ディスク（Optical Disks）	光レーザー装置を使って「書き込み（符号化）」と「読み取り」を行うプラスチック製のディスク。このディスクは、反射率の高い金属を含んでおり、半導体レーザーなどの細い光線源で照射したときに反射の効果が低くなる領域を含むことにより、ビットを使ったデータ表現を行う。
上書き（Overwrite）	磁気媒体に保存されたデータの上に別のデータのパターンを書き込むこと。NSA の研究によれば、ほとんどのドライブは 1 回の上書きで十分にサニタイズできる。消去と除去の収束に関する解説を参照のこと。
物理的破壊（Physical Destruction）	CD などの光媒体に適したサニタイズ方法の 1 つ。
粉砕（Pulverization）	媒体をサニタイズするための物理的な破壊方法の 1 つで、粉末やちりになるまで砕く行為。
除去（Purge）	サニタイズされたデータを実験環境室の手法によって復元できないようにすること。消去と除去の収束に関する解説を参照のこと。
読み取り（Read）	情報システムにおける基本的な処理。この結果として、対象から主体への情報の流れだけが発生する。
記録（Record）	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。
復旧手順（Recovery Procedures）、復旧可能（recoverable）	システム障害の発生後に情報システムのデータファイルや計算機能を復元するのに必要な行為。
残存データ（Remanence）	消去後の記憶媒体に残った残存情報。
残留物（Residue）	情報処理操作は完了したが、消磁や上書きがまだ行われていない記憶媒体に残っているデータ。
ROM	Read Only Memory（読み取り専用メモリ）。一般に、製造過程でその内容が記録される市販のディスクや半導体素子。
サニタイズ（Sanitize）	媒体から情報を削除して、データの復元を不可能にするプロセス。機密扱いのラベル、マーク、活動ログをすべて取り除くことが含まれる。

用語	定義
Secure Erase	ファームウェアベースのプロセスを使ってハードディスクドライブを上書きする技術。ANSI ATA ディスクおよび SCSI ディスクのインタフェース仕様で定義されているドライブコマンドであり、ドライブのハードウェア内部で実行される。5220 ブロック抹消処理のおよそ 1／8 の時間で完了する。CMRR の要請で、部分的に ATA の仕様に加えられた。2001 年以降に製造された ATA ディスクドライブ（15 GB 超）は、Secure Erase コマンドを備えており、CMRR の Secure Erase 確認テストに合格している。SCSI ドライブにも標準化された内部的な Secure Erase コマンドが存在するが、実装は任意であり、CMRR がテストした SCSI ドライブには現在のところ実装されていない。SCSI ドライブが全世界のハードディスクドライブに占める割合はごく一部であるため、このコマンドはユーザの要望があれば実装される予定である。
細断（Shred）	媒体をサニタイズする方法の 1 つで、小片に寸断する行為。
記憶（Storage）	データを取得可能な形で保存すること。データの入力と取得が可能な電子的、静電気的、または電気的なハードウェアまたはそのほかの要素（媒体）。
WORM	Write-Once Read Many（追記型記憶）。
書き込み（Write）	情報システムにおける基本的な操作。この結果として、主体から対象への情報の流れだけが発生する。

（本ページは意図的に白紙のままとする）

付録C ツールと資料

多くの政府機関、米国軍事機関、および教育機関は、サニタイズ用のツール、技法および手順について、一定レベルの保証が得られるかどうかを確認するため、広範囲の研究を行ってきた。米国国立標準技術研究所（NIST）は、どのツールセットについても、特定の媒体に含まれる情報を消去、除去、または破壊する能力を確認するための評価を行っていない。

各組織は、自組織で評価できる製品を求めることが奨励される。各組織は、信頼できるサービスや、ほかの連邦政府機関によるツールや製品の評価を利用することができる。また、選択したサニタイズツールを使用しながら、その有効性を継続的に監視し、確認することが期待される。

組織が信頼し、その有効性を確認した製品がある場合は、それらの情報を Federal Agency Security Practices（FASP）の Web サイトなどの公開フォーラムの場で共有することを強く奨励する。FASP の取り組みは、連邦最高情報協議会(Federal Chief Information Officer Council)のセキュリティに関するベストプラクティス(Best Security Practices)の試験的取り組みが成功したことを受けて、開始された。この取り組みは、重要インフラ保護（CIP：critical infrastructure protection）とセキュリティに関するベストプラクティスを特定、評価し、普及させるためのものである。FASP はhttp://csrc.nist.gov/fasp/にある。

このガイドでは、利用者が、NSA の公開 Web サイトに掲載されている NSA 装置を検討することも推奨する。NSA によれば、「これらのリストに掲載された製品は、NSA の個別性能要件を満たしているが、リストへの掲載は NSA や米国政府による推奨を意味するものではない。」

NSA/CSS-EPL-02-01-M - NSA/CSS Evaluated Products List (EPL) for High Security Crosscut Paper Shredders, Annex A to NSA/CSS 02-01, version M, dated: April 2005

NSA/CSS-EPL-02-02-F - NSA Evaluated High-Security Disintegrators, Annex A to NSA/CSS 02-02, version F, dated: April 2005

NSA/CSS EPL 04-02-B - Optical Media Destruction Devices, Annex A to NSA/CSS 04-02, version B, Date: 30 September 2005

NSA/CSS-EPL-9-12A-B - Degausser Approved Products List - Annex A to NSA/CSS Manual 130-2, version B, dated: May 2005”

NSA の装置リストに加えて、国防保全局（DSS：Defense Security Service）は、ベンダーが主張するサニタイズ機能に関して評価した製品のリストである APL（Assessed Product List）を公開している。DSS APL によれば、「APL は、どの企業の製品も推奨するものでもなく、また機密に関わる環境で各製品を使用することに対する承認や運用認可を意味するものでもない。APL の目的は、セキュリティ担当者に製品の機能情報を提供することである。これにより、セ

キュリティ担当者はそれぞれのセキュリティ要件を満たすために製品の適用の可否を判断できる。」[5]

この一覧は、http://www.dss.mil/infoas/assessed_products_list.docにある。

ハードディスクドライブ装置やファームウェアの除去コマンドにアクセスして利用できる装置では、それが組織にとって最適な方法である可能性がある。ファームウェアの除去コマンドを使用することにより、デバイスの再利用が可能になり、データ保護に関する強力な保証を得ることができる。ATA ハードディスクドライブのファームウェアによる Secure Erase の詳細については、http://cmrr.ucsd.edu/hughes/subpgset.htmを参照されたい。

使用済みの電子機器を寄付したいと考えている組織や個人、またはサニタイズ後の残存物の廃棄に関するガイダンスを探している組織や個人は、環境保護局（EPA：Environmental Protection Agencies）の電子リサイクルと電子廃棄物に関する情報を提供する Web 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、サニタイズ、廃棄、寄付に関する助言、規制、および標準規格刊行物を提供している。また、ほかのサニタイズツールの情報源への外部リンクも提供している。

業務やセキュリティを担当する管理職層が、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ためには外部委託が最も妥当な方法であると判断した場合、各組織は媒体のサニタイズと破壊を外部に委託できる。この方法を実施する場合は、各組織が媒体のサニタイズに従事する第三者と契約を結ぶ際に「適正な評価」を行うこと（「デューディリジェンス」の実施）を推奨する。この場合の適正な評価は、その概要を示した 16 CFR 682 で次のように認識されている。「適正な評価には、候補となる廃棄業者の力量や健全性を判断するために、廃棄業者の経営と本規則（ガイド）の遵守に関する独立した監査を確認すること、複数の照会先または信頼できるそのほかの情報源から廃棄業者に関する情報を入手すること、廃棄業者が公認の同業者団体または同様の第三者による認定を得ることを求めること、廃棄業者の情報セキュリティに関するポリシーまたは手続きを確認および評価すること、またはそのほかの適切な措置を取ることが含まれる。」[6]

[5] http://www.dss.mil/infoas/assessed_products_list.doc

[6] 連邦取引委員会 16 CFR Part 682『*Disposal of Consumer Report Information and Records*』、Section 682.3（b）（3）。

付録D ホームユーザおよび在宅勤務者向けの考慮事項

媒体をサニタイズする必要があるホームユーザや在宅勤務者にとって、組織のために開発された媒体サニタイズの方法は、現実的でなかったり、安全でなかったりする可能性がある。在宅勤務者は、どのようなサニタイズを試みる場合でも、あらかじめ組織のポリシーを確認すべきである。ホームユーザや在宅勤務者が従うことのできるガイドラインを次にいくつか示す。

- 在宅勤務者の場合は、まず組織のサニタイズに関するポリシーと指示にしたがっているかどうかを確認すること。組織のポリシーと手続きは、これらの指示よりも優先される。
- 支給されたマニュアルを確認すること。システムの情報サニタイズに関するガイドラインが支給されている場合は、それらの指示に従うこと。マニュアルのサニタイズに関するガイドラインは、これらの指示よりも優先される。
- 不安や不明点がある場合、または情報がサニタイズされたことを適切に保証しながら安全な方法でサニタイズを実施することができない場合は、組織または社外の販売業者を通じて、システムを専門家に預けること。
- 媒体をいつでも廃棄できる状態にしておくこと。*データを参照する必要が生じた場合に備えて、すべての情報のバックアップコピーを作成し、安全な場所に保管すること。*
- システムを廃棄できる状態になったら、廃棄に関するすべての指示に確実に従うこと。多くの媒体には有害物質が含まれている。

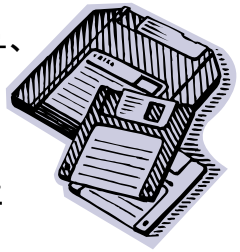
判断事項：対象媒体をサニタイズする必要があるかどうか。対象は、電話帳に代表電話番号が保存されているだけの携帯電話か、それとも税金の書類、銀行口座の情報、投資の記録などが入っている家庭用 PC か。

準備：すべての電源が接続されていないこと、プラグが抜かれていること、あるいは取り外されていることを確認する。

条件：携帯電話、PDA、そのほかの形態のモバイルコンピューティング機器の場合。

措置：すべての情報を手動で削除する。次に、マニュアルを参照して工場出荷時設定へのハードリセットの方法を調べる。機器からリムーバブル記憶媒体がすべて取り外されていることを確認する。

条件：大容量のリムーバブル記憶媒体の場合。たとえば、コンパクトディスク（CD、CD-RW、CD-R、CD-ROM）、光ディスク（DVD）、コンパクトフラッシュ、メモリースティック、SD カード、USB ドライブ、MO ディスクなど（ただし、これらに限定されない）。



措置：これらの媒体は、細断、物理的な破壊、または媒体を読み取り機器に物理的に再挿入できないようにすることによって、破壊すべきである。

条件：PC の場合。

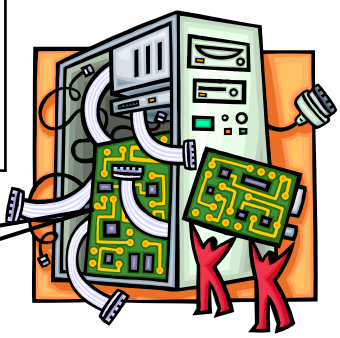
措置：次の 2 つの方法を使ってサニタイズを実施できる。

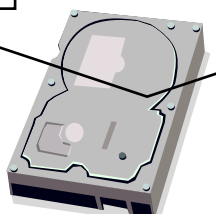
1. ソフトウェアを使ってサニタイズを実施する。PC のメーカーに推奨ツールを照会し、業界やコンピュータの雑誌におけるサニタイズツールの評価を確認する。これらの参考情報は、印刷資料であれば地域の図書館で見つけられる。またインターネットでも探せる。インターネットで「Sanitize Tools」（サニタイズツール）や「Disk Drive Sanitization」（ディスクドライブのサニタイズ）を検索すると、サニタイズ用ツールの研究に関する情報源がいくつも得られる。利用者は、NIST Federal Agency Security Practices（FASP）の Web サイト（http://csrc.nist.gov/fasp/）で、一部の連邦政府機関がサニタイズに使用しているツールや手順を参照することもできる。

2. キーボード攻撃による情報の復元を防止するため、ディスクドライブに物理的な損傷を加える。これを行うには、すべての電源を確実に切断する。コンピュータのハードディスクドライブの場所を特定する。場所の特定は、支給されたマニュアルや配線図を使って行う。PC からハードディスクドライブを取り外す。

   鋼鉄の遮へい材や取り付け金具を取り外し、ハードディスクドライブユニットへの電気的な接続部分を切断する。

次に、適切な施設で安全器具を装着した者が（ハンマーで叩くなどの方法で）ハードディスクドライブに物理的な力を加える。これにより、ハードディスクドライブは変形、折り曲げ、押しつぶし、またはそのほかの方法で破壊され、機能しているコンピュータに再挿入できなくなる。ディスクの表面に衝撃／損傷を与えるには、ハードディスクドライブユニットの上に直接十分な力を加えるべきである。また、コンピュータとのインタフェースとなるコネクタも、押しつぶし、折り曲げ、またはそのほかの方法により、相当な修理を行わない限りハードディスクドライブを再接続できないほどに破壊する必要がある。[7]





[7] 国防総省メモ、2001 年 7 月 8 日、件名「Destruction of DoD Computer Hard Drives Prior to Disposal」

付録E 資料

- All About Degausser and Erasure of Magnetic Media. Athana International. 20 June 2005
- Anastasi, Joe. The New Forensics: Investigating Corporate Fraud and the Theft of Intellectual Property . N.p.: John Wiley and Sons, 2003. 1-288.
- Army Regulation 25–2. U.S Army. ELECTRONIC PUBLISHING SYSTEM, 17 Nov 2003.
- D.Millar, “Clean Out Old Computers Before Selling/Donating,” June 1997;
- Davis, Harvey A. National Security Agency. NSA/CSS POLICY MANUAL 9-12. N.p.: n.p., 2000.
- "Degaussing Described." Weircliffe International Ltd in the interests of magnetic media users and others who are affected by the phenomena of Ferro-magnetism (2005).
- Dictionary definition of **EPROM**
  The American Heritage® Dictionary of the English Language, Fourth Edition Copyright © 2004, 2000 by Houghton Mifflin Company. Published by Houghton Mifflin Company.
- "Future of Computing (Optical & Biological Possibilities)." Future of Computing. 04 June 1997. Dept. of Engineering, Imperial College London. 10 Nov. 2005
- Garfinkel, Simson L., and Abhi Shelat. "Remembrance of Data Passed: A Study of Disk Sanitization Practices." IEEE Security & Privacy 1st ser. 1 (2003). 09 June 2005
- Gutmann, Peter, ed. Secure Deletion of Data from Magnetic and Solid-State Memory. San Jose: Sixth USENIX Security Symposium Proceedings, 1996.
- Gutmann, Peter, ed. Data Remanence in Semiconductor Devices. Washington, D.C: 10th USENIX SECURITY SYMPOSIUM, 2001.
- J.Hasson, “V.A. Toughens Security after PC Disposal Blunders,” *Federal Computer Week*, 26 Aug. 2002;
- LeaseForum. "Understanding Data Storage, Data Liability and Current Data Removal Methodologies." Addressing Data at Asset Retirement. N.p.: n.p. 2002. 1-8.
- Magnetoresistive Random Access Memory (MRAM). Comp. James Daughton. 4 Feb. 2000. NVE. 17 June 2005
- Microsoft, “Microsoft Extensible Firmware Initiative FAT32 File System Specification,” 6 Dec. 2000;
- National Computer Security Center, “A Guide to Understanding Data Remanence in Automated Information Systems,”

- Understand Degaussing. Peripheral Manufacturing Inc. 18 June 2005.
- US Department of Defense, “Cleaning and Sanitization Matrix,” DOS 5220.22-M, Washington, D.C., 1995.

付録F サニタイズの有効性を確認する書式の例

組織名:_____

物件の説明: _____

メーカー／モデル: _____

製造番号／資産番号:_____
_____
_____

情報のバックアップを行ったか: ☐ はい
☐ いいえ

(「はい」の場合)バックアップの場所: _____

物件の処分: ☐ 消去
☐ 除去
☐ 破壊

実施日: _____
実施担当者: _____
電話番号: _____
確認担当者: _____
電話番号: _____

使用されたサニタイズ方法: _____

媒体の最終的な処分方法: ☐ 廃棄
☐ 内部で再利用
☐ 外部で再利用
☐ メーカーへ返却
☐ そのほか: _____