



ライフサイクルが終了した IT 資産の破壊 vs. 消去

組織のドライブとデバイスに必要な
安全で検証を伴うデータサニタイズ

物理破壊についての 業界アナリストの見解

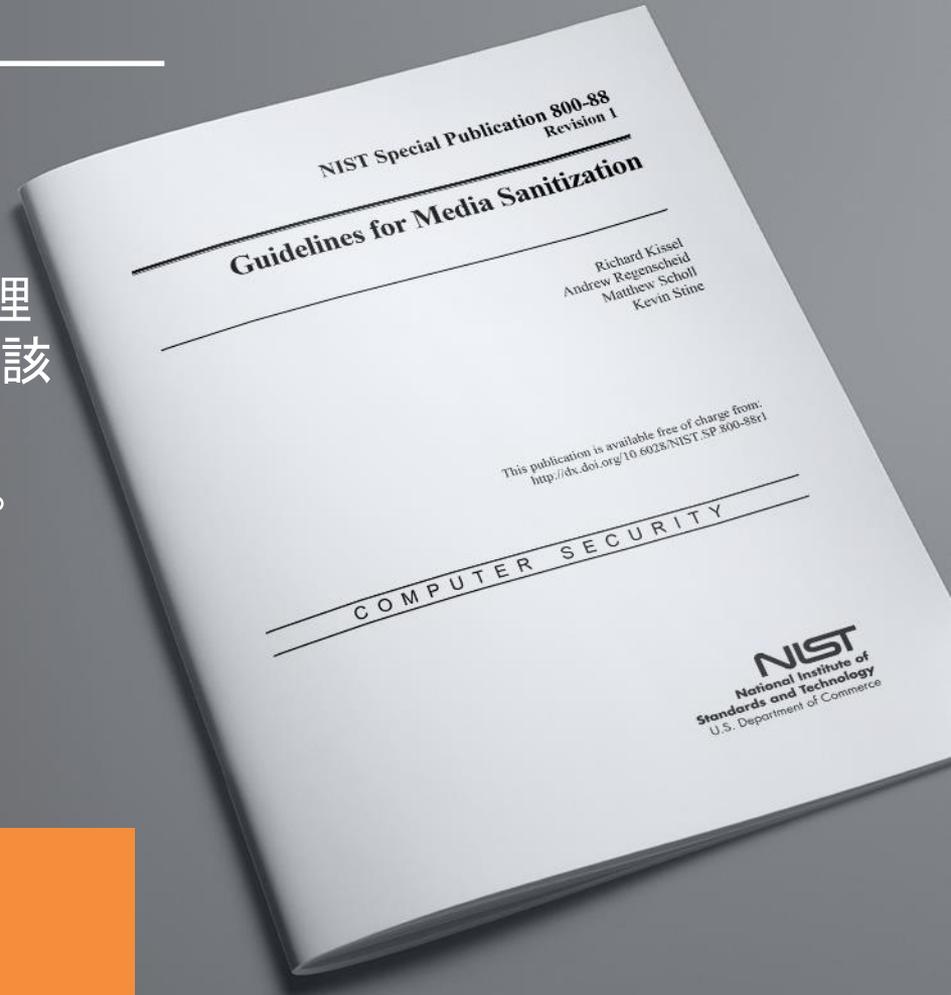
“ 一般的に、IT資産の中でデータを保持するデバイスを破壊すると、再利用可能な資産としての残存価値(RV)が減少し、環境に配慮するには新たにリサイクルのためのコストが発生します ”

ガートナー「データセキュリティのハイプ・サイクル」2019年6月

物理破壊についての 業界リーダーの見解

“ 環境への配慮、組織内での再利用、もしくは販売や寄付、コストや媒体の種類により物理破壊が難しいなど、除去(Purge)および該当する場合は消去(Clear)が、破壊(Destroy)よりも適切な場合があります。

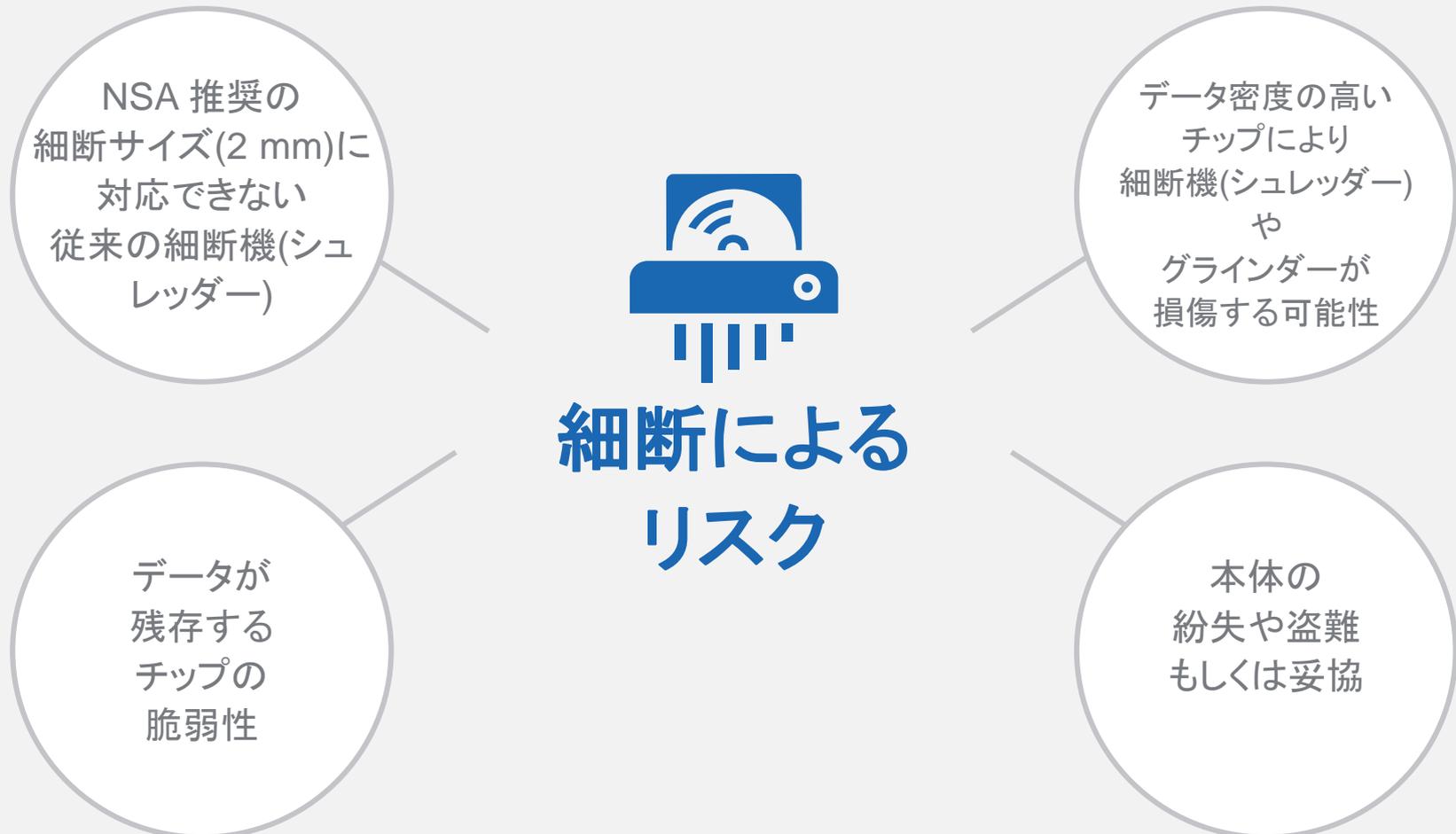
— NIST SP 800-88, Rev.1,
「情報のサニタイズと意思決定」



物理破壊: 課題 #1



物理破壊: 課題 #2



物理破壊: 課題 #3

物理破壊するとデバイスは使えません

| | |
|---------------|--|
| ビジネスコストの増加 | デバイス破壊に必要な年間平均コスト 170万ドル |
| テクノロジーのROI 低下 | 破壊されたデバイスの年間総価値 210万ドル |
| 不要な環境コスト | 電子機器廃棄物(e-waste)の全世界の年間価値 625億ドル |

世界経済フォーラム、電子機器の新しい循環についてのビジョン (2019年1月)

データ消去とは



HDD もしくはその他のデジタルストレージデバイス / 媒体に残存するすべての電子データの完全な破壊を目的としたソフトウェアベースのデータ上書き手法。

**Blancco のソフトウェアは、
1日あたり7万回以上の消去に使われています。**

Blancco のデータ消去が提供する 安全で永続的なデータサニタイズ

- ✓ サーバー、PC、モバイルデバイス、リムーバルメディア、取り外したドライブに対応
- ✓ ライフサイクル が終了した磁気(HDD)とフラッシュベース(SSD)のIT資産上のデータに対する不要なアクセス機会を排除
- ✓ ドライブまたはデバイス全体に対する100%安全な消去、隠しセクターに到達しフリーズロックを解除(該当する場合)
- ✓ すべての IT 資産のデータ消去に文書化と検証プロセスにより、異常を特定する検証プロセス

Blancco のデータ消去により 組織内外の法規制に準拠

Blancco データ消去ソリューション:

- ✓ ライフサイクルが終了したデバイスとデータのための組織内のデータ保護とセキュリティポリシー強化
- ✓ 地域、政府および国際的なデータ規制やガイドラインに対応 (GDPR、CCPA、HIPAA、PCI-DSS、NESAなど)
- ✓ 25種類以上の消去方式を実装 (英国政府準拠方式、米国国防総省準拠方式、NIST クリアとパーズなど)
- ✓ すべての消去済み IT 資産の改ざん防止の監査証跡を提供

Blancco ができること



プライバシー設計

データ漏えい防止を考慮しており、リスクに対してプロアクティブ対処



長期的に一貫したプロセス

アウトソース先のサービスプロバイダーやリサイクル事業者に関係なく(RFPの変更が必要になる)、組織は長期に渡って簡素化された一貫性のある監査対応が可能



プロセスの透明性

電子署名された消去レポートの自動配信により、スタッフと監査担当は、透明性が高く、簡素化された単で一貫性のあるプロセスを実行可能



ヒューマンエラーの削減

ユーザー権限、必須フィールド、自動化、および包括的なカスタマイズ性により、手作業による不正確な記録のリスクを軽減。自動化による精度向上。



作業コストの削減

LUN、サーバー、ドライブ、および仮想マシンのリモートサニタイズ機能により、移動時間と関連コストを節約。複数の IT 資産を同時に廃止することで、作業時間を短縮。



業務効率化

すぐに使えるプロフェッショナルなツールにより、組織内での利用とポリシー準拠を推進。データが不要になった際、業界のベストプラクティス、法規制、および認証要件に従い、エキスパートによるサニタイズをすぐ実行。



環境への配慮と利益

全性が保証されたデータサニタイズにより、IT 資産の再販を通してハードウェアコストを回収。可能な場合、IT 資産を物理的に破壊することなく、再利用を推進。



ERP 連携

Blancco Management Console に実装された REST API により、ERP / 資産管理などその他の既存のシステムと連携。

物理破壊が必要な場合

- ✓ IT 資産が破損して消去できない場合、ドライブごとの要件に従い破壊を実施
 - 資産を種類ごとに分ける
 - IT 資産の種類とデータの機密性に合わせて、細断サイズと消磁手法が十分であるか確認
- ✓ 新たなセキュリティレイヤーの追加: リスク軽減のため、サードパーティ事業者への依頼前に組織内で消去:
 - IT 資産の紛失や盗難によるデータ移行
 - 効果がなく適切ではない破壊手法
 - ドライブの断片からの先進的なデータ復元
- ✓ 必要に応じて、消去と破壊によるサニタイズの証明書を要求

データ消去の無償トライアルをご希望の方は
今すぐBlancco にお問い合わせください

www.blancco.com/demo/free-trial-request-enterprise/