Blancco 導入による組織の NIST SP 800-88 準拠

NIST SP 800-88 とは？

NIST(米国国立標準技術研究所)の SP 800シリーズは「NIST のサイバーセキュリティ活動によるガイドライン、推奨事項、技術仕様、年次レポート」の提供を目的としています。これらは米国の連邦政府機関のニーズに応えるために設計されていますが、さまざまな業界においてリファレンスとなっています。 NIST SP 800-88 は、2002年の連邦情報セキュリティマネジメント法 (FISMA) による法定責任に従い、記憶媒体のサニタイズに関する情報セキュリティの基準とガイドラインの概要を示すために作成されました。この文書の遵守は、米国連邦政府によって義務付けられていますが、非政府系組織でも自主的に採用されています。

Blancco は、さまざまな業界において組織の NIST SP 800-88 準拠を支援しています。NIST 文書の特定の領域における適用例と、Blancco による対処方法については、以下の表をご覧ください。

NIST の文書について	BLANCCO がどのように役立つか
消去(Clear)、除去(Purge)、および破壊(Destroy)は、媒体をサニタイズするための具体的な施策です。サニタイズのカテゴリは次のように定義されています。 **消去(Clear)**は、単純かつ非侵襲的なデータ復元技術から保護するために、ユーザーが指定技術を適用することです。通常、新しい値による書き換えや、工場出荷状態へのリセット(書き換えがサポートされていない場合)を選ぶなど、ストレージデバイスに対する標準的な読み取り/書き込みコマンドにより適用されます。 **除去(Purge)**は、最先端のラボ技術により対象となるデータ復元を不可能にする物理的もしくは論理的な技術を適用することです。 **破壊(Destroy)**は、最先端のラボ技術により対象となるデータ復元を不可能にし、媒体をデータ保存に利用できないようにすることです。 このガイドをもとにユーザーは、情報のカテゴライズ、情報が記録されている媒体の性質や機密保持リスクを評価し、将来の計画を決定しなければなりません。次に、組織は適切な種類のサニタイズ種別を選択します。どのサニタイズを選択するかは、コスト、環境への配慮などの観点から検討されるべきであり、機密性に対するリスクを最も軽減しつつ、プロセスに課せられた条件や制約に適切に応えられることが求められます。	Blancco は、ソフトウエアベースのデータ消去ソリューションにより、データサニタイズ手法として NIST が定める 消去(Clear)と除去(Purge)の両方に対応しています。 Blancco Drive Eraser は、SAN 環境、サーバー、PC に接続された SSD (NVMe 接続を含む) と HDD の除去(Purge)レベルのサニタイズに対応しています。 さらに、Blancco LUN Eraser は、論理ユニット(LU)ドライブのデータサニタイズにおいて、NIST の消去(Clear)要件を満たしています。 Blancco のすべての消去は実施後に検証が行われ、監査証跡として活用できる改ざん防止機能が付いた消去レポートを生成します。 さらに、Blanccoのソフトウエアベースの消去は業務効率化、コスト削減、データサニタイズ プロセスの管理性向上に貢献します。
(暗号消去への言及): 部分的なサニタイズだと、すべての機密データを指定できないため、デバイス全体のサニタイズが重要になります。	Blancco Drive Eraser は、リマップセクタや隠し領域を含むドライブすべての領域を対象として消去を実施します。HDDと SSD ドライブの両方において、Blancco Drive Eraser はウェアレベリングを扱うオーバープロビジョニングに対応しています。そして、改ざん防止の消去レポートによりサニタイズが適切に実施されたことを証明します。

続き….

NIST の文書について	BLANCCO がどのように役立つか
環境への配慮、媒体の再利用(組織内または媒体の売却や譲渡)、媒体またはデバイスのコストを考慮する場合、物理的な破壊が出来ないことがあるため、除去(Purge)もしくは消去(Clear)が、破壊(Destroy)よりも適切な場合があります。	Blancco のデータ消去ソリューションは、ライフサイクルが終了したさまざまなデバイスにおいて、データを復元できないよう消去し、デバイスの安全な再利用、再割り当て、さらに、中古市場への売却ができるようになります。これは環境に配慮した施策であり、同時に、コスト削減にも貢献します。これらは、すでに確立されたベストプラクティスとなっており、現在、世界中で数億の IT 資産が安全にリユースされています。

選択したサニタイズおよび廃棄プロセスの検証は、機密性を維持するための重要な工程です。検証には2種類の検証を考慮する必要があります。 1つはサニタイズを実施する度に行う検証です。
 	
もう一つは、サニタイズに続いて、電子媒体を適切に処分したことを証明することです。
 	
サニタイズを完了する際の証明書には、少なくとも次の詳細情報を記録しておく必要があります:
• 製造メーカー
• モデル
• シリアルナンバー
• 組織ごとに割り当てられた媒体もしくは資産番号(該当する場合)
• 媒体種別 (例: 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 (例: 媒体のユーザーもしくは利用していた機器)
• サニタイズ前の機密性の分類(オプション)
• サニタイズの説明(例: 消去、除去、破壊)
• 利用した手法 (例: 消磁、 上書き、ブロック消去、暗号消去)
• 利用したツール (バージョンを含む)
• 検証手法 (例: 全体、 クイックサンプリングなど)
• サニタイズ後の機密性の分類(オプション)
• サニタイズ後の宛先(既知の場合)
• サニタイズと検証の担当者:
  ○ 氏名
  ○ 担当
  ○ 日時
  ○ 場所
  ○ 電話もしくは連絡先情報
  ○ 署名
	Blancco のソフトウエアによるデータ消去が実行されるごとに、監査に対応できる改ざん防止機能が付いた消去レポートが発行され、消去と検証が適切に実施されたことを証明します。この消去レポートにはカスタムフィールドを追加することができ、NIST の要件に準拠できる安全な電子署名と共に、実際に使用された IT 資産と消去方式についての詳細情報を記録することができます。
	
	消去レポートは、オンプレミスもしくは、AWS がホストするクラウドサービスとして利用可能な Blancco Management Console に保存·管理され、必要な時にいつでも参照できます。

続き….

NIST の文書について	BLANCCO がどのように役立つか
USB リムーバブルメディア - 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 **消去(Clear):** 組織内で承認/テストされた上書き/手法/ツールを使用して媒体を上書きします。 消去(Clear)パターンは、最初のパスにパターン、2番目のパスにその補数を含めるために、少なくとも2つのパスが必要です。さらに追加のパスが利用可能です。	NIST 800-88 の要件およびその他のデータ消去の規制要件に対応するために、Blancco Removable Media Eraser は、SD カード、サムドライブ、フラッシュメモリドライブなど、さまざまな種類のリムーバブル媒体を復元できないよう安全に消去するよう設計されています。消去レポートは、消去の検証実施時に発行されます。
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、暗号化されていた場合、暗号化を解除。次に、サニタイズの前にリムーバブル ストレージを取り外し) NIST の文書では、Apple、Android、Windows、BlackBerry など主要なモバイル デバイスのデータサニタイズ手法について説明しています。モバイル デバイスは工場出荷時設定へのリセット、上書き、または消去(Clear)/除去(Purge)の要件を満たす暗号消去のいずれかでサニタイズする必要があります。また、これらのデバイスが再利用、リサイクル、再販しない場合、物理的に破壊することがありますが、可能であれば、消去と検証を実施する必要があります。	Blancco Mobile Diagnostics & Erasure は、iOS、Android、Windows Phone、そして BlackBerry OSを安全に消去することができ、NIST 800-88 で定められた要件に対応できます。 **BMDE にできること:** • NIST のデータ消去方式、暗号消去、検証可能な工場出荷時リセット、およびそのほかのモバイル向け消去方式が選択可能 • 上書き処理が適切に実施され、すべてのセクタに書き込まれたことを検証 • 改ざん防止の監査証跡によるデータ消去レポートの生成 • 自動化された複数端末の同時消去 さらに、Blancco Mobile Diagnostics & Erasure は、モバイル デバイス内にある SD カードやその他のストレージ 媒体を消去する機能を提供しています。
コピー、プリンター、FAX機器 **消去(Clear):** メーカーが提供するリセット機能により、オフィス機器を工場出荷時のデフォルト設定に戻します。 **除去(Purge):** 破壊(Destroy)を参照してください。多くのオフィス機器はデータコンテンツを消去する(除去(Purge)ではない)機能のみを提供しています。オフィス機器が除去(Purge)機能を提供することがありますが、これらはデバイスのハードウエアとファームウエア固有のものであり、注意して利用する必要があります。そのため、デバイスの製造元に対して、単にファイルポインターを取り除くのではなく、データを復元不可能にできる手法(書き換えやブロック消去など)、もしくは、暗号消去をデバイスが備えているかを確認してください。オフィス機器にはリムーバブル ストレージ 媒体を利用していることがあり、その場合、該当する媒体に最適なサニタイズ手法を適用します。 **破壊(Destroy):** 細断、分解、粉砕、または、認可された焼却炉でデバイスを焼却します。	Blancco Drive Eraser は、NIST Purge がデータ消去方式として選択されている場合、プリンター/FAX/コピー機にある HDD を除去(Purge)レベルで安全に消去します。消去レポートは消去の検証時に生成されます。 Blancco Removable Media Eraser は、SD カードやプリンター、FAX などのデータストレージを含む、さまざまな種類のリムーバブル メディアを安全に消去するように設計されています。消去レポートは消去の検証時に生成されます。

続き….

blancco

NIST の文書について	BLANCCO がどのように役立つか
ATA ハードディスクドライブ - PATA、SATA、eSATAなど **消去(Clear):** 組織が承認および検証した上書きテクノロジー/手法/ツールにより媒体を上書きします。 消去(Clear)パターンは、すべてゼロなどの固定値を持つ少なくとも1回の書き込みパスが必要です。複数の書き込みパス、または、より複雑な値の書き込みを選択できます。 このサニタイズには、4つの選択肢があります。ATA サニタイズ デバイス機能セットコマンド(3回の上書き消去)、SECURE ERASE UNIT コマンド、TCG(Trusted Computing Group)が策定した暗号消去 Opal Security Subsystem Class(SSC)や Enterprise SSC、そして消磁です。	Blanco Drive Eraser ソフトウエアは、PC、サーバーなどから取り外したドライブと内蔵 HDD を消去でき、PATA、SATA、eSATA など、あらゆるドライブ種別において NIST 要件を満たす自動化されたサニタイズ プロセスをサポートします。 **Blancco Drive Eraser の主要なベネフィット:** • 複数の HDD を同時にデー消去 • BIOS フリーズロックの解除を含むハードドライブの消去プロセスを自動化 • ローカルおよびリモートでの展開 • RAID ディスマントルとパススルー • 内部のデータ消去プロセスにおける誤検知を特定 • 監査と法規制対応のための電子署名された消去レポートの生成 • 地域および世界各国のデータ保護規制やガイドラインに対応 Blancco Drive Eraser は、プロセスの検証/認証によって裏付けされ た消去方式 NIST Purge および NIST Clear に対応しています。
SCSI ソリッド ステートドライブ (SSSD) — パラレル SCSI、シリアル接続 SCSI(SAS)、Fibre Channel、USB 接続ストレージ(UAS)、および SCSI Express など NIST の文書では、3つのサニタイズ手法が提案されています。1つは消去(Clear)です。ユーザーは、組織が承認/検証した上書きテクノロジー/手法/ツールにより媒体を上書きします。 消去(Clear)プロシージャは、すべてゼロなどの固定値を持つ少なくとも1回の書き込みパスである必要があります。また、複数の書き込みパス、または、より複雑な値の書き込みを選択できます。 2つ目は、SCSI サニタイズ、ブロック消去、または暗号消去コマンドを使用した除去(Purge)です。3つ目は物理的な破壊です。 NVM Express SSD についても同じ選択肢が提示されており、除去(Purge)を実施するための NVM 固有のコマンドに変更されています。 さらに、消去(Clear)や除去(Purge)の各手法に対して検証を行う必要があります。暗号消去が適用される場合、暗号化のオペレーションが正常に完了したことを確認するために、暗号消去後にする消去(Clear)や除去(Purge)などの追加のサニタイズ手法(該当する場合)を実施する前に検証を行う必要があります。除去(Purge)のメカニズムとして、すべてを暗号化の実装に依存するのが適切であるとは限りません。暗号消去を採用するかどうかの決定は、このガイダンスで以前に特定された属性の検証に依存します。また、消磁はフラッシュ メモリベースのストレージデバイスのサニタイズ手法としては採用できません。	Blanco Drive Eraser ソフトウエアは、PC やサーバー内蔵、もしくは取り外した SSD の消去に対応しており、独自の消去方式は特許を取得しています。 **Blancco 独自の特許を取得した SSD 消去のベネフィット:** • ファームウエアレベルの消去: ブロック消去や暗号消去など SSD のサニタイズに必要な内部の消去コマンドを活用 • 複数の乱数による上書き、フリーズロックの解除、包括的な検証を含む • サポートされた SSD セキュリティプロトコルの活用 • プロセス自動化により、すべての工程を適切な順序で最後まで実施 • SSD コントローラーによる圧縮や重複排除の適用を回避 • ドライブすべての論理容量に対してランダムなデータストリームを適用 • 単純な繰り返しのビットパターンではなく、ランダムかつ非圧縮のデータを利用 • ダブルパスの上書きによりデータを SSD の論理容量全体に(圧縮ではなく)書き込み • さまざまなインターフェースに対応(SATA、SAS、eMMC、NVMeなど) • 安全な消去に必要な SSD 内部のセキュリティ機能へのアクセス • ドライブの運用上の妥当性を保証 • 消去プロセスの異常を検出 • 電子署名された改ざん防止の監査証跡

続き….

組織がデータサニタイズポリシーを定め、あらゆる IT 資産に対してベストプラクティスを適用する際は、上記の推奨事項を順守し、業界、顧客、従業員のデータの保護に必要なリスクを慎重に検討してください。 IDSC(International Data Sanitization Consortium) が提供する「IT 資産のデータ消去ポリシーと手順」テンプレートをダウンロードして、すぐに始めることができます。

Why Blancco?

Blancco は20年以上にわたり、世界各国のデータ保護規制やガイドラインへの準拠をサポートするソリューションを提供しています。市場で最も多くの認定を取得したデータ消去ソフトウエア企業として、北大西洋条約機構(NATO) やコモンクライテリアなど15以上のグローバルな認証/承認/推奨を受けて、データ消去ソリューションにより、これら規制要件への厳格な対応が求められる業界のニーズをサポートしています。

NIST SP 800-88 Rev 1 の詳細をご確認ください。NIST クイックスタートガイドを今すぐダウンロード。