3回上書きは過去のもの

『データ消去』の正しい知識

執筆　沼田 理

株式会社ゲットイット 技術顧問
ADEC（データ適正消去実行証明協議会）技術顧問

GET IT

沼田 理　*Numata Makoto*

オランダPHILIPS社などで技術開発に従事したのち、1986年より株式会社ワイ・イー・データにて、フロッピーディスクドライブ、ハードディスクドライブおよびテープドライブ等の磁気記憶装置の設計開発に携わる。2001年、日本のデータ復旧サービスのパイオニア、オントラック事業部に異動し、2006年より事業部長。2010年より日本データ復旧協会事務局長およびデータ復旧関連複数社において顧問。技術情報、web原稿の提供、IDF（デジタル・フォレンジック研究会）講師などを務める。2019年より、KLDiscovery Ontrack社ブランド・アンバサダー、ADEC（データ適正消去実行証明協議会）技術顧問。神奈川県情報流出事件以降は、新ガイドライン作成へ向けた行政からの技術諮問に応じるなど活動中。

執筆文献：「データ抹消に関する米国文書（規格）及びHDD、SSDの技術解説」「ADEC データ消去技術ガイドブック 第2版」他。

GET IT

1 『DoD：米国防総省規格は過去の遺物』

日本ではＨＤＤのデータ消去と言うと、米国国防総省が1973年に発表したDoD 5200.28-Mによる3回上書きによって「データの完全な消去」が実現できると信じている人が多く、この規格は2006年2月に国防総省自身によってすでに取り消されていることを知る人はほとんどいません。
同2006年9月にNIST（米国国立標準技術研究所）が発表したSP800-88の中では「2001年以降に製造された15GB 以上のATAディスクについては、上書き抹消を行う場合の上書き回数は1回で十分である」と宣言されており、このSP800-88の改定版として2014年12月発表されたNISTによるSP800-88Rev.1が、現在、世界的に最も重視されているデータ消去を含む情報セキュリティーの規格となっています。

GET IT

DoDからNISTへ！

神奈川県のＨＤＤ流出事件に端を発した、総務省の「自治体情報セキュリティ対策の見直し」に於いても、今年の５月２２日に、「自治体情報セキュリティ対策の見直しについて」の公表 https://www.soumu.go.jp/menu_news/s-news/01gyosei07_02000098.html で「自治体情報セキュリティ対策の見直しのポイント」https://www.soumu.go.jp/main_content/000688753.pdf を発表し、そのP-9では、今までの、漠然とした「全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない」から、「情報の機密性に応じた方法により、情報を復元困難な状態にする措置を徹底する必要がある」としてNIST SP800-88Rev.1準拠を今後の方向として明示し、今夏にも「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定を行なうことを公表しています。

NIST SP800-88Rev.1について

米国有名IT企業のデータ抹消に関する声明から代表的なものを紹介すると、

①. Seagate：返品時のメディア・サニタイズに関するプラクティス

(https://www.seagate.com/files/www-content/support-content/warranty/_shared/Files/TP689.2-1606US-Media-Sanitization-Practices_ja_JP.pdf)より抜粋。

Seagateでは、Seagateが修理したすべての製品が、米国政府の定めるドライブのサニタイズに関する仕様に確実に準拠するか、あるいはそれ以上の基準を満たすよう、米国家安全保障局（NSA）およびCenter for Magnetic Recording Research（CMRR）と連携してきました。米国国立標準技術研究所（NIST）は、ドライブのサニタイズに関して一定の基準を設定しています。2014年12月発行メディア・サニタイズに関するガイドライン特別発行文書800-88改訂版1に含まれる関連仕様では、磁気メディア向けに許容されるドライブのサニタイズは、メディアからデータをパージすることと定義されています。

②. マイクロソフト：物理記憶装置上のデータの削除

(https://www.microsoft.com/ja-jp/trust-center/privacy/data-management)より抜粋。

物理記憶装置上のデータの削除

保管用のディスク ドライブにハードウェア障害が発生した場合、Microsoft がそのディスク ドライブを交換または修理のために製造元に返却する前に、ディスク ドライブは確実にデータ消去されるか、破壊されます。ドライブ上のデータは完全に上書きされるので、そのデータを回復することはどのような手段でも不可能になります。

このようなデバイスが廃棄されるときは、米国のNIST 800-88 Guidelines for Media Sanitation に従ってデータ消去または破壊が行われます。

GET IT

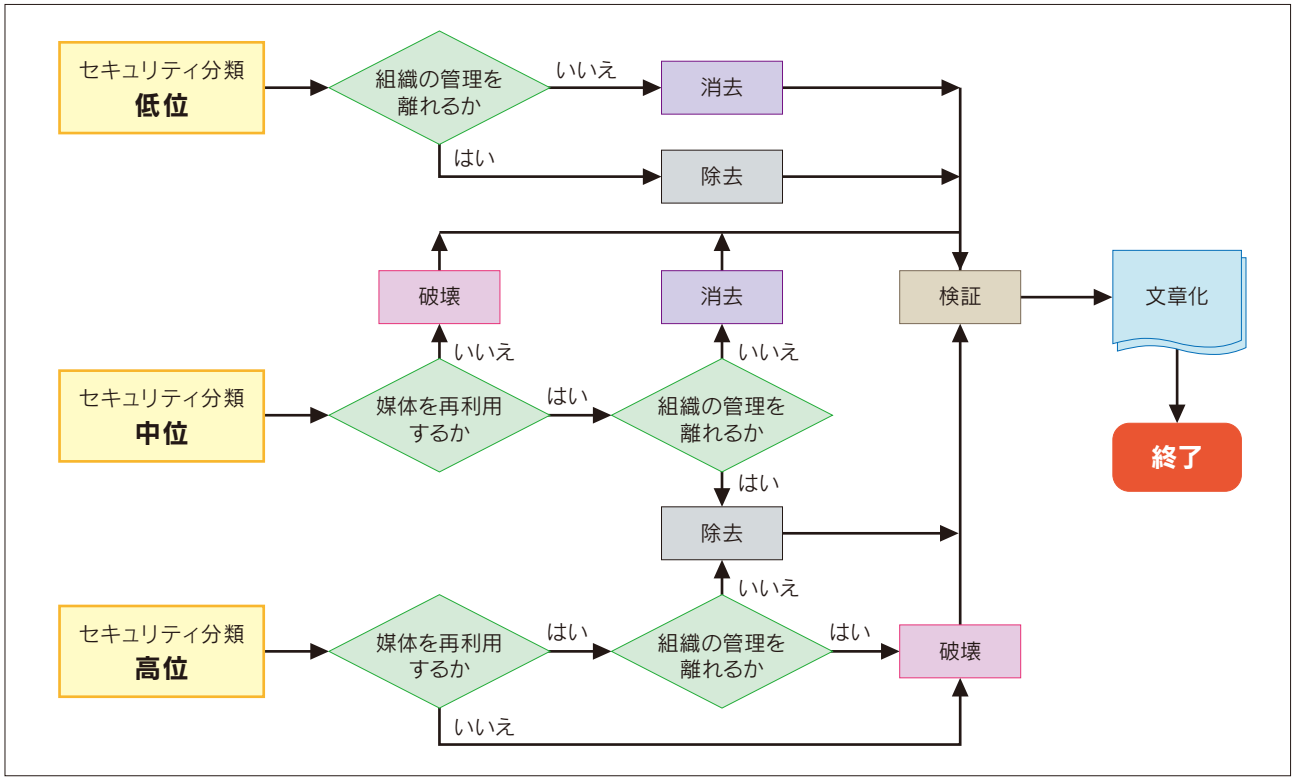
NIST SP800-88Rev.1では、情報をその機密の程度によって、

低度：情報が漏えいした場合の影響は限定的なレベル

中度：情報が漏えいした場合、重大な悪影響を及ぼすレベル

高度：情報が漏えいした場合、危機的・致命的な悪影響を及ぼすレベル

の3ランクに分け、データ消去後の取り扱われかた（再使用、廃棄等）の条件との組み合わせによって決定される情報漏えいのリスクに従って消去のレベルを決定し、そのレベルを満足することの出来る3ランクのデータ消去方法を具体的に解説しています。そして、「DoDによる3回上書き」や、よくデータ消去ソフトウェアの解説の中では最高度の消去手段として説明されている、「グートマン方式による35回上書き」を行った場合であっても、最低ランクの、クリア（消去：Clear）でしかなく、その上にパージ（除去：Purge）や、デストロイ（破壊：Destroy）と呼ばれるデータ消去レベルが要求されていることも認識する必要があります。



引用：NIST（米国国立標準技術研究所）「SP800-88 Rev.1 Guidelines for Media Sanitization（媒体のサニタイズに関するガイドライン）」、「Sanitization and Disposition Decision Flow（サニタイズと処分に関する意思決定の流れ）」 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

３段階の消去レベルについて（SATA接続のHDDの場合）

①. クリアClear（消去）　キーボードアタックに耐えること

（データ復旧ソフトなどでは復旧出来ない）

・OSが認識する範囲を消去。リカバリ領域等に使われるHPA、サービス部品として新しい大容量のHDDの容量をクリップして旧型のPCに対応させるためのDCO領域や不良セクタの代替セクタ処理を行った「再割り当て済みセクタ」のデータは消去の対象とならない。

・例：1回以上の上書き消去等

---

②. パージPurge（除去）　研究所レベルのアタックに耐えること

（高度な技術を持つ、データ復旧業者やデジタル・フォレンジック業者でも復旧出来ない）

・OSが認識する範囲に加えて、上記の全ての領域、再割り当て済みセクタも消去される。

・例：ANSIコマンドEnhanced SecureEraseの実行、暗号化消去、外部磁界による消磁等

---

③. デストロイDestroy（破壊）　媒体の再生（再組立等）に対して耐えられること

（HDDメーカなどでも読み出すことが全く出来ない）

・文字通り、完全にデータが抹消され、読み出すことは出来ない。

・例：物理破壊、粉砕、裁断、溶解等

GET IT

「物理破壊」や「外部磁界による消磁」はデストロイなのか？

昨年の12月に発生した、神奈川県のHDD流出問題を受けて総務省が、「物理的な破壊又は磁気的な破壊の方法により行う」と通知したことによって、HDDのデータ抹消手段として「物理破壊」の要求が多くなったようですが、現在日本で行われている物理破壊や、外部磁界による消磁は、NISTのデストロイに適合しているのでしょうか。ちなみに米国の規格で認められている物理破壊装置・機器の中に日本製の物は存在せず、外部磁気消去装置でも、1社1機種だけしか存在しないのです。

更に、物理破壊に関する米国の規定を探すと、それら機器の認定を行っているNSA/CSS（National Security Agency/ Central Security Service：アメリカ国家安全保障局）から、今年３月に発表された最新の文書が存在し、以下のように記載されています。

GET IT

Evaluated Products List for Hard Disk Destruction Devices より抜粋

・ハードディスクドライブ破壊装置を単独で使用した場合、磁気ストレージ機器に対するデータ抹消には相当しません。

・本書に記載されるハードディスクドライブの破壊装置は、磁気消磁装置と組み合わせて使用した場合にのみ磁気ハードディスクドライブのデータ抹消として認められます。単体での使用は、NSA / CSS 9-2 ストレージデバイスのデータ抹消マニュアルに記載された緊急事態においてのみ認められます。

・粉砕は、NSA / CSSの9-12ストレージデバイスのデータ抹消マニュアルの指示に従い、プラッタが2ミリメートル角以下のサイズを達成することが無ければ、データ抹消には相当しません。

Evaluated Products List for Magnetic Degaussers より抜粋

・すべてのハードディスクドライブ内のプラッタを変形させることによる物理的な破壊を伴う消磁を行うことを強く推奨します。ハードディスクドライブ破壊装置については、NSA / CSS評価製品リストを参照してください。

・このリストへの記載は、機器の継続的な性能を保証するものではありません。製造元に従って、またはNSA / CSS承認済みの磁場検証装置を使用して、機器を再テストする必要があります。

この理由は、

・上書き等により「消去されていないHDDのプラッタ（円盤）上のデータは読み出すことの出来る技術が存在する」

・外部磁気による消磁装置は、作業後の消去の確認が困難であり、更に「経時的な性能の劣化も激しいため、維持管理を正しく行なわなければ、性能の保証は出来ない」

の、2点に有るのです。いかがでしょうか？　デストロイとは言えないですよね。

　現実的には、日本で行われているレベルの物理破壊（穴あけ、折り曲げ等）後のHDDのデータ復旧をビジネスとして行うことの出来るデータ復旧業者やデジタル・フォレンジック業者の存在は、少なくとも私の記憶には無いことも事実です。

GET IT

2 『SSDとHDD』

PCに使われている外部記憶装置（コンピュータ等の機器に内蔵されているHDDやSSDであっても、コンピュータの歴史によって、正しい呼び方は“外部記憶装置”です。パソコンにUSB等で外部に接続される物を指すのではありません）の数量予測では、今年中にSSDがHDDを逆転すると見られているようですが、HDDとSSDでは全く動作原理が異なっているので、HDD用のデータ消去ソフトはSSDでは必ずしも十分な役に立つとは限りません。

SSDの動作に“上書き”はない

デジタル磁気記録（HDD）の基本動作（飽和磁気記録）

HDDに代表されるデジタル磁気記録は、“飽和磁気記録”の原理によって成立しています。飽和磁気記録とは、“磁性体は一定（飽和限界）以上の磁界が印加されると、着磁されている状態に係わらず、印加された磁界によって磁化される限界（飽和限界）の強さに着磁される”と言う現象ですから、HDDでは“どんなデータが書き込まれていても、消去動作は必要なく、目的のデータを書き込むことで、新しいデータに書き換えられる”ことになります。これが、HDDの使用しているデジタル磁気記録の特徴です。

そして、HDDの書き込み動作の最小単位は、通常はデータ容量512Byteの“セクタ”で、OSを介した場合はその“セクタ”の集合体である“クラスタ”で管理されています。

GET IT

フラッシュメモリ（SSD）の基本動作（ページ書き込みとブロック消去）

SSDに使われているNAND型フラッシュメモリは、簡単に言うと“半導体で出来たスイッチ”のようなもので、そのスイッチ自体に電圧が印加されていない（通電されていない）状態で放置されても、通電されているときにセットされた状態を記憶して、再度通電された時に、元の状態になっている（不揮発メモリ）性質を利用しています。このために、一度セットされてしまうと、一度リセット（消去）して元の状態に戻さないと、次の状態に変えることができません。つまり、データを上書きすることは出来ず、データを書き換えるためには、必ず消去（元に戻す）動作が必要なのです。

そして、書き込み動作は、製造元が決定した“ページ”と呼ばれる単位（データ容量2K、4K、8K byteが代表例）で行われ、OSはその“ページ”上に論理的な“セクタ”や“クラスタ”を作成して、HDDとの互換性を待たせています。また、消去動作は、書き込み単位の“ページ”ではなく、複数の（32、64、128、256ページが代表例）で構成されている“ブロック”単位で行われます。

このため、例えば、1ブロックに満たないデータ容量のファイルを更新しようとした場合、その元々記録されているブロックには、他のファイルも書き込まれているので消去することは出来ず、書き込み可能（消去済み状態で待機中）のページを探して、更新されたデータを書き込み、そこに元のセクタアドレスを与え、不要になった古いデータの書き込まれているページには、待機状態であったページのセクタアドレスを与えるような“アドレスの交換”のような作業・動作をすることが必要となるのです。

この結果として、「更新前の不要となったデータは上書き（消去）される事無く、別のセクタアドレスを割り当てられ、そのままの状態で、ブロックの消去が実行されるまで残存する」ことになります。

ここまでの説明で、HDD用の上書き消去用のソフトウェアではSSDを十分に消去することが出来ないことを「なんとなく理解できた」のではないでしょうか。

GET IT

まだまだ有るSSDの秘密動作（高速化技術）

このような（アドレスの書き換え）作業だけでは当然のことながら、不要になったデータを消去しないと、そのSSDの記憶容量一杯の有効なデータを保存しておくことが出来なくなってしまいますので、不要なデータは出来るだけ早く消去してしまうことが必要です。このために、SSDでは各社各様の色々な内部作業を通常のコンピュータとしての動作の陰（バックグラウンド）で実行させています。

ガベージ・コレクション：Garbage Collection（ハウスキーピングとも呼ばれる）

SSDの消去動作の基本単位であるブロックを効果的に使用するための技術で、データの断片化などによって、一つのブロック内に、必要なデータ（ページ）と不要となったガベージデータ（ページ）の混在が発生した場合に、必要データと不要データを、それぞれ別のブロックに集めることによって、消去可能なブロックを出来るだけ早く・多く確保し、SSDのアイドル時間にそのブロックの消去・初期化を行い、新規のデータの書込みが可能な状態に準備・待機させることで、書込み・書き換え動作速度の低下を予防する手段。

オーバ・プロビジョニング：Over Provisioning（データ・スプール領域）

SSDの内部の物理的な記憶容量をユーザ（OS）の使用できる公称容量とは別に、ガベージ・コレクションやアドレスの書き換え動作用として余分に用意することによって、記録容量が増加してコントローラによって行われる書き変え動作に使用可能な容量が減少して動作速度が低下してしまうことを予防する手段。後述の長寿命化を目的としたウェアレベリング用としても使用する。（サーバ用途で最大30%程度）

トリム：TRIM

SSDがHDDと異なる特性を持った記憶装置であることを、区別して取り扱うようになったWindows7以降のOSによるSSD専用のコマンドで、ファイルの削除・更新などで、不要なデータが書き込まれているセクタが発生した場合に、SSDのコントローラに対し、OSが不要なセクタアドレスを直接通知する機能。

GET IT

注：トリムが有効ではない（対応したOS・SSDではない）場合は、ガベージ・コレクションによるデータ（ページ）の分別作業は、全てのブロックの全てのページを対象として行われるが、トリムが有効な場合は、通知を受けた消去可能なセクタ（データ）の書き換えは不要と判定するので、ガベージ・コレクションが必要となる頻度を減少させることになり、動作速度の低下を予防することができる。

ウェアレベリング（長寿命化技術）

フラッシュメモリには書き換えにより劣化してしまうため、書き換え回数の限界（寿命）があるため、特定のブロックへの書き換えが集中することによる、局部的な劣化の発生でも全体の寿命を縮めてしまうことになるので、コントローラの特殊なアルゴリズムにより、書き換えが特定のページ・ブロックに集中しないように分散化させ、寿命を長く保つ手段。

SSDでは、これらの動作が複雑に組み合わされて動作しているため、HDD用のデータ消去ソフト（ユーザ使用領域に対して上書きを1回行なう＝クリア）では、SSDの内部の全てのページに対してデータを書き込むことが出来るとは断定することはできず、予想することの出来ない思わぬページ上にデータが残ってしまうことが有り、十分な消去結果を得ることは出来ません。

HDDとSSDはパソコン（OS）上の動作では互換性を持っているので、高速化を目的に交換すれば、何の問題もなく快適な高速動作環境を実現することが出来ますが、このように基本的な動作原理の異なる記憶媒体が、その内部のコントローラが管理する（ファームウェアによる）特殊な動作で補うことによって問題なく動作している様に見せている結果なのです。ですから、SSDを搭載しているパソコンの廃棄や譲渡をするためにデータの消去を行なう場合には、SSDの内部動作に正しく対応している「SSD専用のソフトウェア」を使用することが必要なのです。

GET IT

3 『データ消去サービスとは』

今まで使用していたＩＴ機器の定期的な保守点検等によって、外部記憶媒体であるHDDやSSD等を交換したり、又はサーバやPCのリース期限の満了によって返却・廃棄する場合に、その記憶媒体に書き込まれている情報の漏洩防止対策はどうしていますか。

昨年の神奈川県のＨＤＤ流出事件については、当事者である神奈川県が、「リース契約満了により返却したハードディスクの盗難及び再発防止策等について：https://www.pref.kanagawa.jp/docs/fz7/cnt/p0273317.html」上で、下記の様に説明し、対策を行なうことを発表しています。

原因

・盗難された原因は、富士通リースからデータ消去・廃棄作業を請け負ったブロードリンクの社員管理・作業管理体制や事故防止対策の不備により、ハードディスクが盗難可能な状態にあったことだが、県としてもデータ消去の履行確認が不十分であった。

再発防止策等

・重要情報が格納されている機器（サーバー等）をリース満了によりリース会社に返却する場合は、従前より情報漏洩防止のため、県内部の初期化作業でデータを全て消去した後、リース会社が「データ復旧が不可能とされている方法によりデータ消去作業を行うものとする」としている。
・今後は、情報漏洩防止を徹底するため、契約満了時には、県庁から搬出する前に職員が立ち会いのもと、データ記憶装置を物理破壊させるなど、契約の見直しを行う。

この事件の原因をどう考えることが正しいのでしょうか。勿論、実際の廃棄作業の責任を持つ、富士通リースとブロードリンクがISMS（ISO27001）の認証を取得していて、更にデータ消去証明書の提出を依頼されているにも関わらず、その作業を行なう前に、社員の内部犯行による盗難が防止できない体制であったことです。

GET IT

情報セキュリティ規格について

ISMS（ISO27001）

現在、多くの企業・団体がデータセキュリティーに関連する業務を委託する場合の条件として、ISMS（ISO27001）認証の取得を条件としているようですが（話題になった富士通リースもブロードリンク社も認証取得事業者）、その考え方は本当に正しいのでしょうか。

業者によっては、「当社は、情報セキュリティに対する品質が世界標準レベルである証明として、情報セキュリティの国際規格であるISO27001を取得しています」等と宣伝文句にしているのを見かけますが、そもそもISMSはマネージメントの基準であり、管理（マネージ）がどのように行われているかを審査・認定するものであるため、実際の作業現場に個別に存在するリスクに対する対策手法の規格ではないことを認識する必要があります。実際にそのISMSの対象となっている範囲はどこまでか、その対象範囲をよく見て、その作業内容に特有のリスクを探し出し、そのリスクをどのように軽減するか、その実際の手法を個別に細かく定めているのではありません。このように正しく理解すれば、ISMS認証の取得をもって、「情報セキュリティのレベルが世界の標準を満足している」とする様な表現が、宣伝文句に過ぎないことが理解できるはずです。

但し、取得していないよりは取得している方が安心できるという目安にはなることを否定するわけではありません。

プライバシーマーク（Pマーク）

JIS規格のJIS Q 15001（個人情報保護マネジメントシステム ― 要求事項）に適合した個人情報保護体制を運用可能な状態に構築していることを示していますが、その対象が、個人情報保護法によって規定されている範囲でしかないため、企業秘密や知的財産などは含まれません。ですから、一般的な機密情報に対しては、取得していないよりは取得している方が安心できる程度の目安でしかありません。

GET IT

ADECプロセス認証

ADEC（データ適正消去実行証明協議会）のプロセス認証は、基本的な考え方や判断の方法はISMSの審査方法に従っていますが、データ消去作業を行なう現場毎に限定して、現場毎に存在する個別のリスクを対象として、そのリスクに対応した対策が適切に取られているか否かを確認・審査を行なう制度です。

このように比較してみると、データ消去サービスを依頼する側にとって、最も適切なセキュリティ基準はADECのプロセス認証ということになるのではないでしょうか。

ここで原点に戻って、「情報」とはどのようなものか、「データ消去サービス」とは何かについて説明したいと思います。

GET IT

情報とは

現時点に於いて、最も適切な考え方と言えるのは、ヨーロッパのGDPR（General Data Protection Regulation：EU一般データ保護規則）の考え方だと思います。つまり、個人に関する情報（日本の個人情報保護法による個人情報だけではなく、個人的なプライバシーも含む）を例に挙げて説明すると、その個人に関する情報の持ち主は、その情報を集めて管理している法人・個人・組織・機関・団体などではなく、その個人本人であるとしています。そして、そのような情報の持ち主を指して「情報の主体」と表現しています。そして、その管理は本人が明示的に許している場合を除いて、その情報を集めて管理している団体等は、本人から情報を管理しても良いという預託を受けているに過ぎないとしていることです。

この考え方を拡大すれば、個人情報だけでなく、記憶媒体に書き込まれている全ての情報は、その媒体が正常に機能・動作するか否かに係わらず、読み出すことが出来た時点で、その情報は正当な所有者・管理者の明示的な許可なく取り扱うことは違反行為となるという事です。

データ消去サービスとは

「情報」の本質が理解できれば、「データ消去サービス」についての説明は全く不要であると考える、理解の早い方もいると思いますが、観点を変えて説明しますと、「データ消去サービスとは労務提供（サービス業・行為）です」。つまり、「情報の正規の所有者・管理者の依頼によって要求された業務（情報の消去）を、要求された通りに正しく提供する」ことです。

では、データ消去サービスを依頼する側、依頼される側の双方で最も大切なことは何でしょうか。それは、「双方がデータ消去に対する正しい・十分な知識を持つこと」です。

お客さまのご要望にゲットイットは正しくお応えいたします。ご不明な点がございましたら、お気軽にご連絡ください。

GET IT

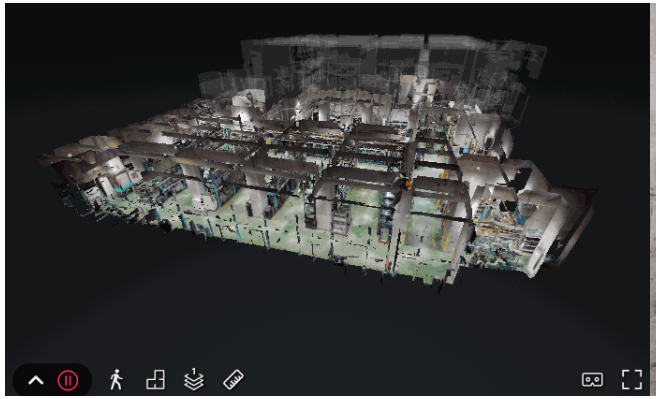
ZETTA

バーチャル見学　受付中

倉庫敷地面積2,000m²（都内最大規模）

ゲットイットの倉庫 ZETTA

「PanoWeave」を活用し、3D空間内を自由に移動して
バーチャルな施設見学を行うことが可能です。
見学をご希望される場合は、
メールにて弊社までご連絡ください。



法人企業さま向け見学受付
担当者　：力久（リキヒサ）
メール　：first@get-it.ne.jp
電話番号：03-5166-0900

本件に関するプレスお問い合わせ・報道関係者向け見学受付
担当者　：川澄（カワスミ）
メール　：pr@get-it.ne.jp
電話番号：03-5166-0900

GET IT

SUSTAINABLE DEVELOPMENT GOALS

＊ゲットイットは持続可能な開発目標（SDGs）を支援しています。

株式会社ゲットイット
〒104-0045
東京都中央区築地3-7-10
JS築地ビル4F
TEL 03-5166-0900
URL www.get-it.ne.jp