使用済パソコンのデータ消去。
かんたん、確実、安心な
新しいしくみ。

「よからぬ人」の手にわたってしまって
情報漏えいする危険を防ぐために。
～総務省の新ルール準拠～

TOPIER

一般社団法人 東北情報機器再生推進機構

このスライドでご紹介すること

- **TOPIERのご紹介**
- **「K県使用済パソコン記憶装置流出事件」がきっかけ**
- **総務省の新ルールをわかりやすく解説**
- **では、実際にどうすればいいのか？**
  （行政も民間も同じこと）
- **無償サービスとアンケートにご協力ください**

TOPIERのご紹介

一般社団法人 東北情報機器再生推進機構（略称：トピア）

【活動の趣旨】

パソコンやスマートフォンなど使用済情報機器は増加の一途をたどっていますが、法律等に基づいた適正な排出処理がなされているのは、ごく一部にすぎません。

特にパソコンは、事業所や家庭に相当台数が眠ったままで、そのおおきな理由は、個人情報、企業情報などのデータ漏えいへの懸念です。

当機構は、パソコン等情報機器の 3R（リユース＝再利用、リサイクル＝再資源化、リデュース＝廃棄防止）を図ることを目的として、2022年1月に設立されました。

一般社団法人 東北情報機器再生推進機構（略称：トピア）

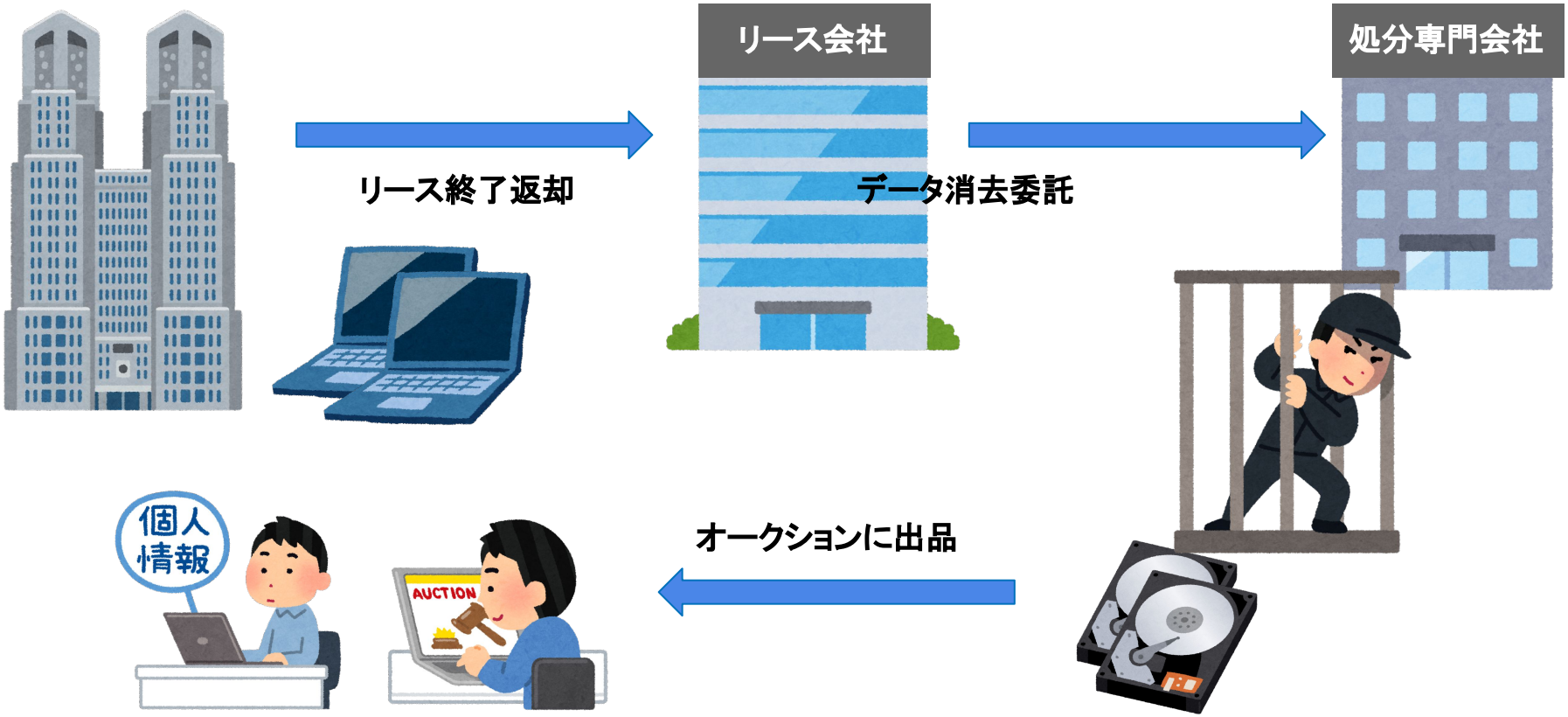
【活動の内容】

- 使用済パソコンのデータ消去と回収処理（個人・法人向け）
- 使用済パソコンの分解資源化と障がい者就労支援
- 使用中パソコンの復活高速化整備サービスの提供と普及啓発
- 使用済パソコン地産地消3Rのためのマッチングサービスの研究
- 使用済パソコンのデータ消去のシステム研究

2019年の事件が
きっかけでした

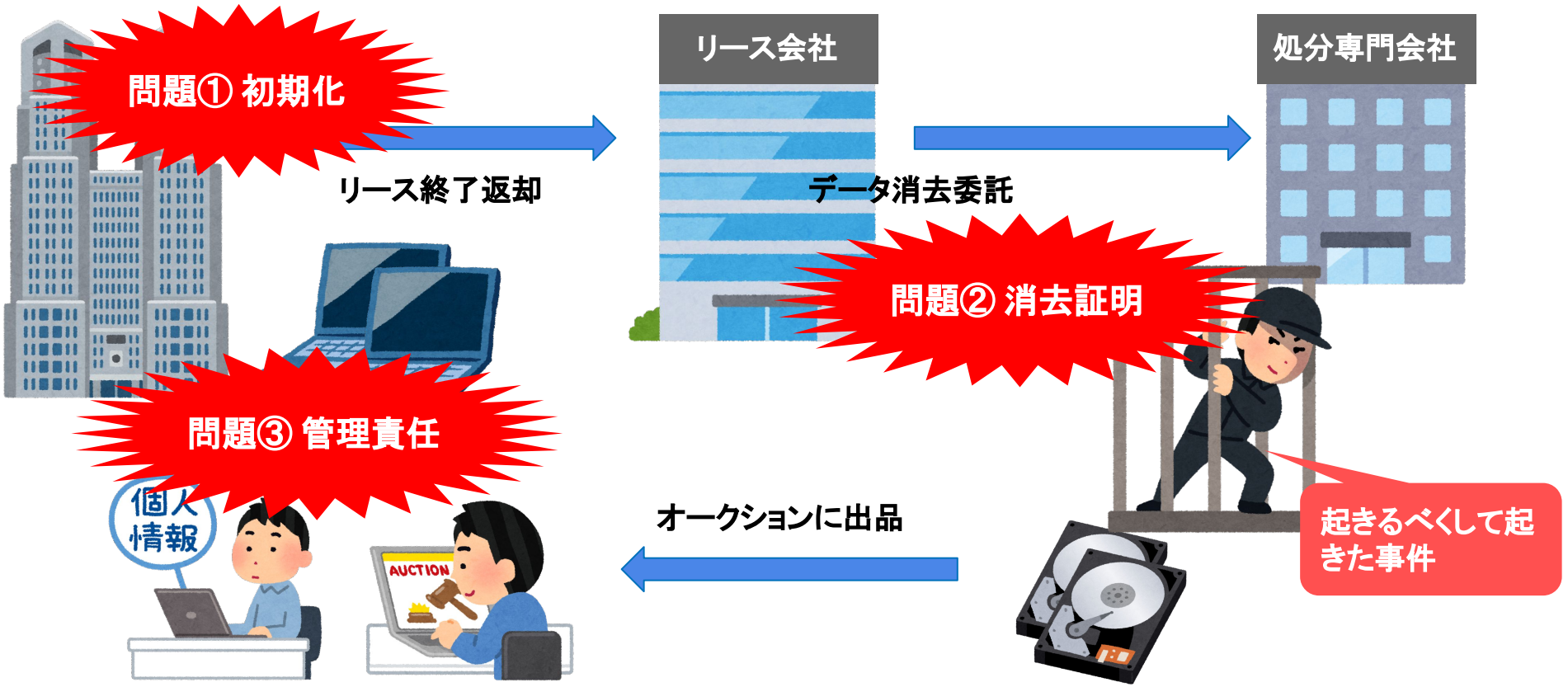
K県庁ハードディスク流出事件

K県庁ハードディスク流出事件



K県庁では、パソコンのリース契約満了の際に、ハードディスクを「初期化」した上で、機器をリース会社に返却。リース会社は、処分専門業者に、ハードディスクのデータ消去を委託しました。
ところが、作業を担当した従業員がハードディスクを持ち出して、オークションサイトに出品。
落札者が「データ復元ソフト」を使ってみたところ、情報が復元されてしまいました。

K県庁ハードディスク流出事件



問題①　ハードディスクの「初期化」だけでは、データ復元が可能。
問題②　実際には作業がなされていなかったのに、処分専門会社はリース会社に「データ消去証明書」を提出。
問題③　個人情報等の取り扱いについて、K県庁の管理責任は免れない。

再発防止に
総務省が動いた

総務省のガイドライン

情報資産の廃棄のガイドライン

総務省「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」（平成13年策定、令和4年3月改定）に、情報資産の廃棄等時の取扱いについて、詳細な説明が加えられました。

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（令和４年３月版）

平成13年　3月30日　策　定
令和　4年　3月25日　改　定

総　務　省

分類	機器の廃棄等の方法	確実な履行を担保する方法
（1）マイナンバー利用事務系の領域において住民情報を保存する記憶媒体 ※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ	当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが適当である。 なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述（3）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。
（2）機密性２以上に該当する情報を保存する記憶媒体（上記（1）に該当するものを除く。）	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。 具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	庁舎内において後述（3）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
（3）機密性１に該当する情報を保存する記憶媒体	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。 具体的には、（2）に記述した方法①～⑤のほか、OS等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。 OS及び記憶装置の初期化（フォーマット等）による方法は、HDDの記憶演算子にはデータの記憶が残った状態となるため、適当ではない	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。
※上記（1）は、オンプレミスの場合を想定したもの（ハウジングやプライベートクラウドを含む）		

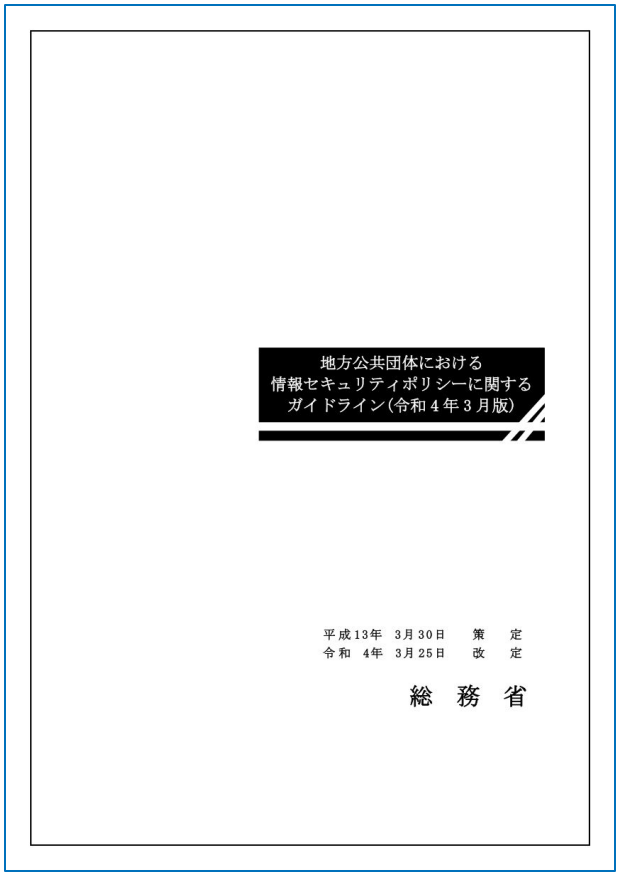
図表 24　情報の機密性に応じた機器の廃棄等の方法

※本プレゼンテーションのダウンロード用PDFには、該当箇所を当機構でわかりやすく要約したページも含んであります。

https://www.soumu.go.jp/main_content/000805453.pdf（PDF、全262ページ）

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

総務省「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」（平成　13年策定、令和4年3月改定）に、情報資産の廃棄等時の取扱いについて、詳細な説明が加えられました。



主な改定内容

1. **業務委託・外部サービス利用時の情報資産の取扱い**
2. 情報セキュリティ対策の動向を踏まえた記載の充実
3. 多様な働き方を前提とした情報セキュリティ対策
4. マイナンバー利用事務系から外部接続先へのデータのアップロード

https://www.soumu.go.jp/main_content/000805453.pdf（PDF）

情報セキュリティ対策基準の例文と解説①

第2章　情報セキュリティ対策基準

2. 情報資産の分類と管理

（2）情報資産の管理

⑩情報資産の廃棄等

（ア）情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、　その情報の機密性に応じ、情報を復元できないように処置しなければならない。

（イ）情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

（ウ）情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

情報セキュリティ対策基準の例文と解説②

第2章　情報セキュリティ対策基準

4.物理的セキュリティ

4.1. サーバ等の管理

（7）機器の廃棄等

情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、　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。

【解説】

情報システム機器が不要になった場合やリース返却等を行う場合には、機器内部の記憶装置からの情報漏えいのリスクを軽減する観点から、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。この場合、一般的に入手可能な復元ツールの利用によっても復元が困難な状態とすることが重要であり、　OS 及び記憶装置の初期化（フォーマット等）による　方法は、ハードディスク　等の記憶演算子にはデータの記憶が残った状態となるため、適当でないことに留意が必要である。また、原則として、以下の表に記載されている方法により、記録されている情報の機密性に応じて、情報システム機器の廃棄等を行わなければならない。

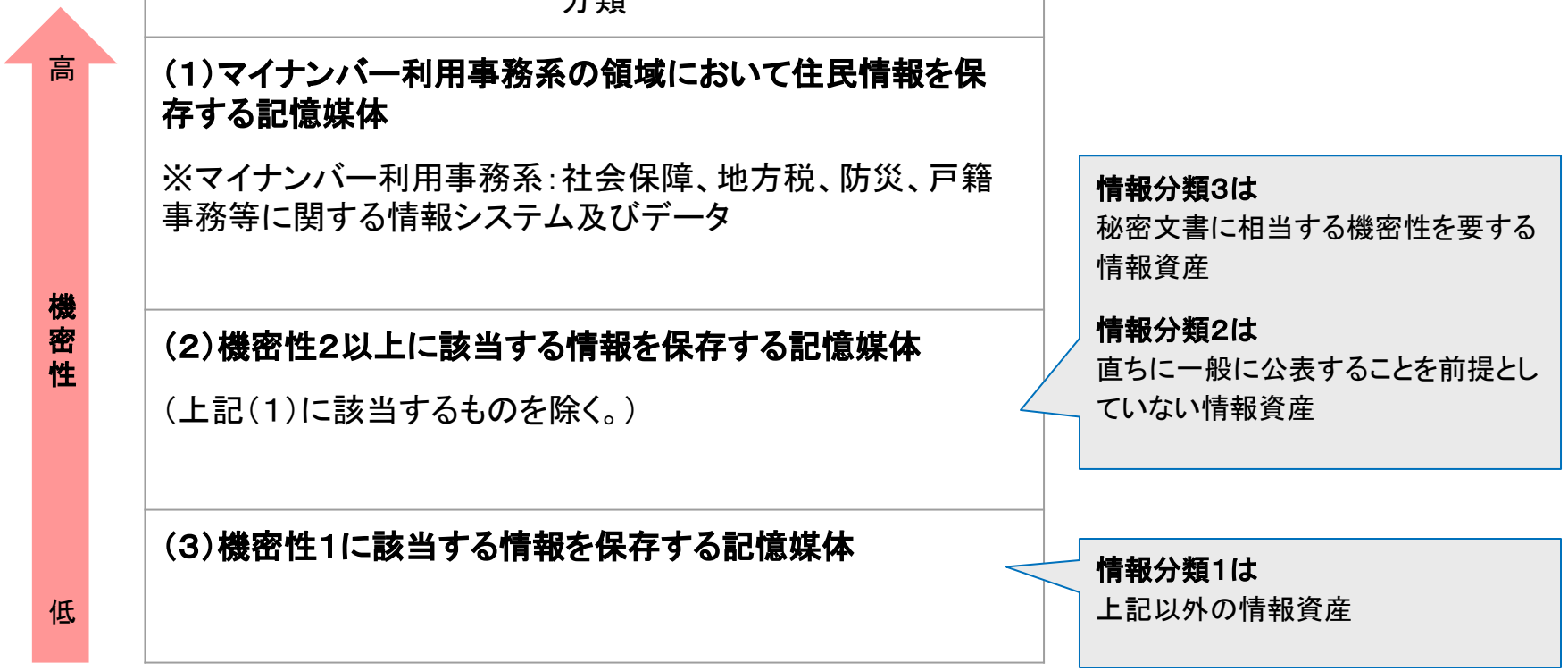
情報の機密性に応じた機器の廃棄等の方法①

情報資産の機密性に応じて、廃棄の方法と履行担保の方法が解説されています。次ページで分類を解説。

分類	機器の廃棄等の方法	確実な履行を担保する方法
(1)マイナンバー利用事務系の領域において住民情報を保存する記憶媒体 ※マイナンバー利用事務系:社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ	当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが適当である。なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述(3)で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。
(2)機密性2以上に該当する情報を保存する記憶媒体 (上記(1)に該当するものを除く。)	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③ OS 等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	庁舎内において後述(3)で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
(3)機密性1に該当する情報を保存する記憶媒体	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。具体的には、(2)に記述した方法①～⑤のほか、OS 等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。 OS 及び記憶装置の初期化(フォーマット等)による方法は、HDD の記憶演算子にはデータの記憶が残った状態となるため、適当ではない	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。

情報の機密性に応じた機器の廃棄等の方法②

情報資産の機密性を3つに分類しています。マイナンバー住民情報を含むものを最上位におき、非公表前提の情報、その他と続いています。



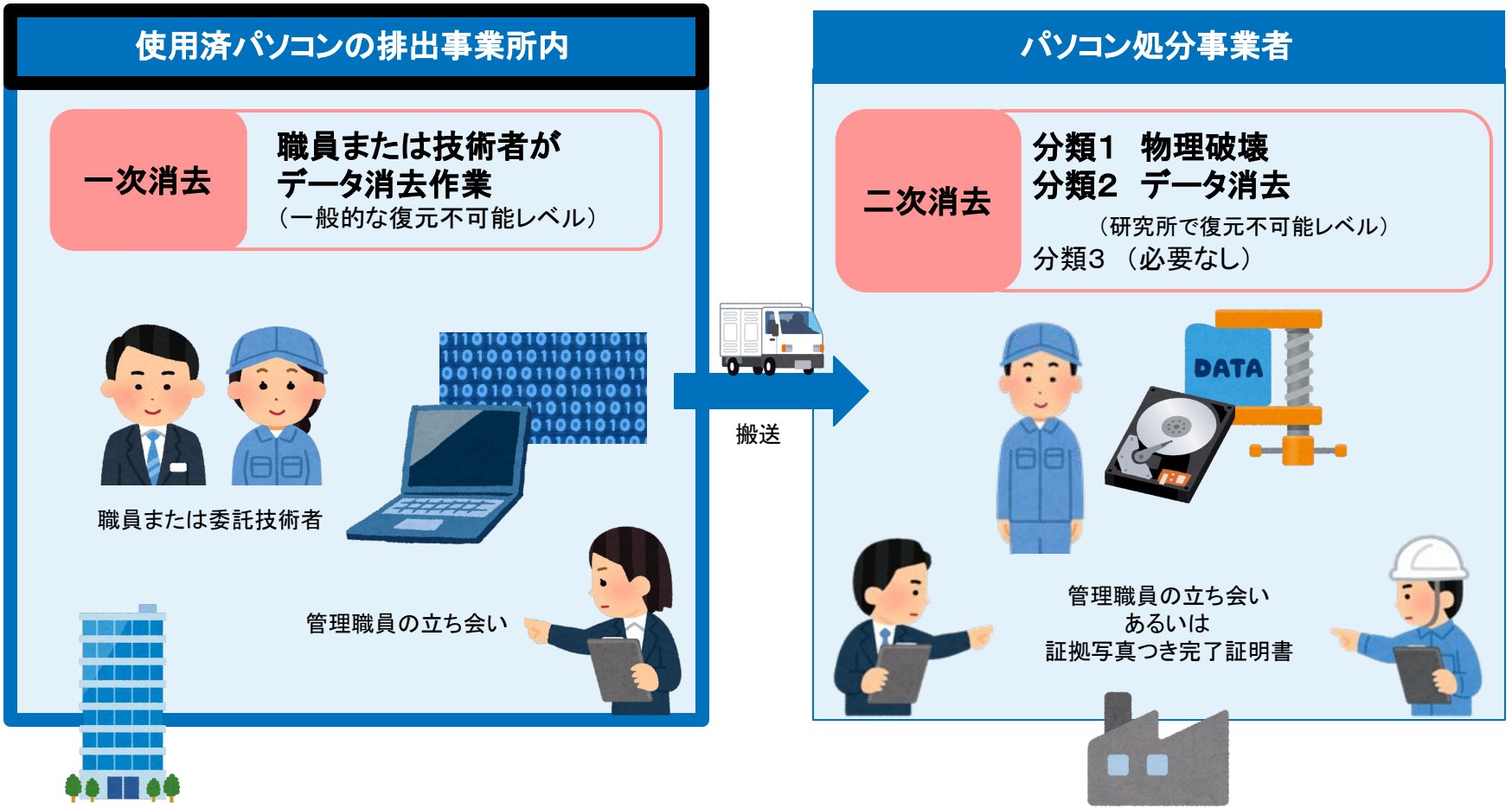
情報の機密性に応じた機器の廃棄等の方法①

3分類に応じた、廃棄の方法と履行担保の方法が説明されています。次ページに解説図。

分類	機器の廃棄等の方法	確実な履行を担保する方法
(1)マイナンバー利用事務系の領域において住民情報を保存する記憶媒体 ※マイナンバー利用事務系:社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ	当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが適当である。なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述(3)で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。
(2)機密性2以上に該当する情報を保存する記憶媒体 (上記(1)に該当するものを除く。)	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③ OS 等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	庁舎内において後述(3)で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
(3)機密性1に該当する情報を保存する記憶媒体	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。具体的には、(2)に記述した方法①～⑤のほか、OS 等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。 OS 及び記憶装置の初期化(フォーマット等)による方法は、HDD の記憶演算子にはデータの記憶が残った状態となるため、適当ではない	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。

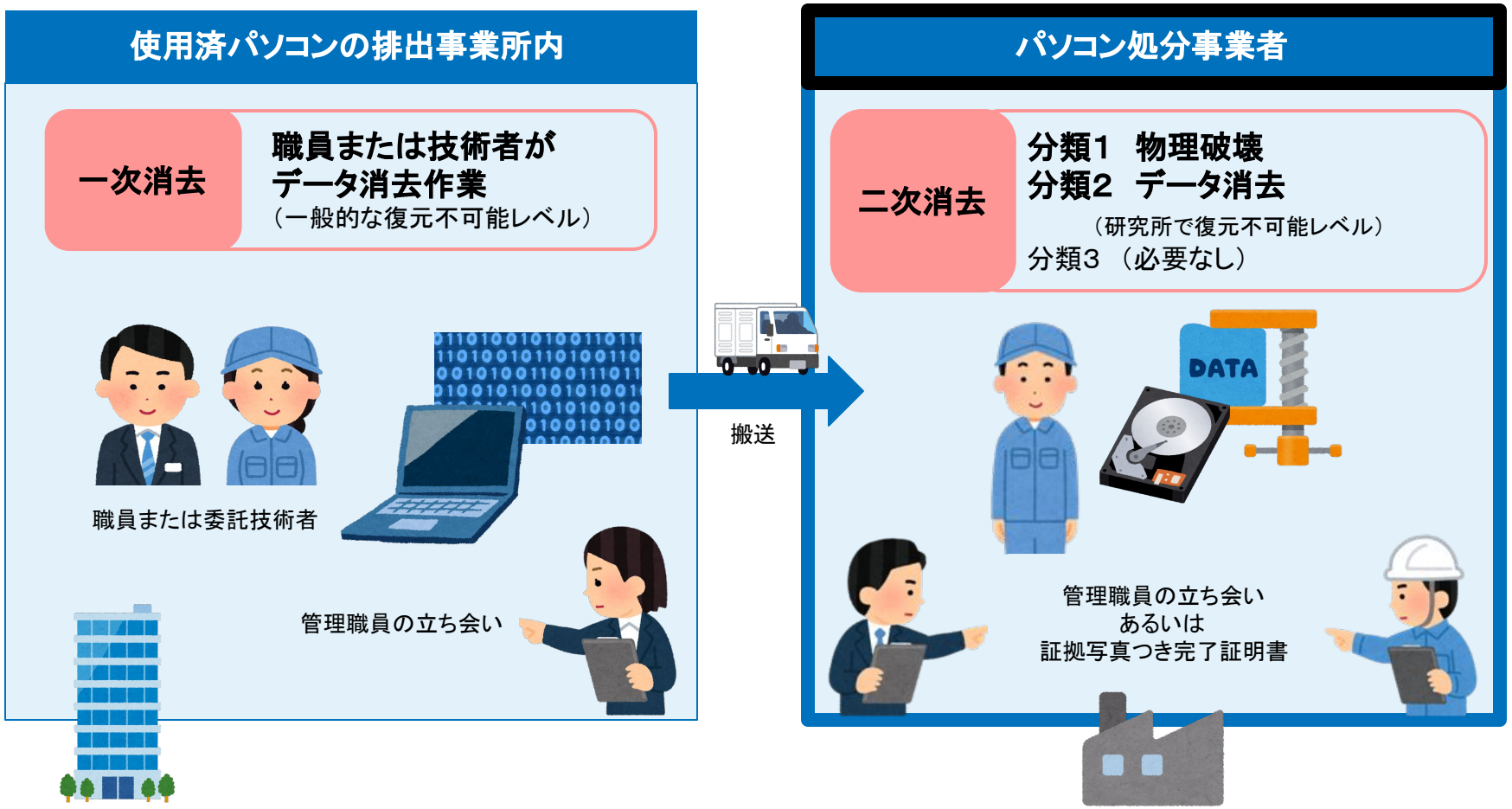
リスクを避けるために→事業所内一次消去と委託先二次消去①

まず、排出事業所の庁舎内で、職員あるいは契約技術事業者が、データ消去作業を行います。その品質レベルは、一般的に入手可能なソフトでは復元ができないレベルと指定されています。これは、情報機密分類1～3に共通です。



リスクを避けるために→事業所内一次消去と委託先二次消去②

次に、記憶装置（パソコン本体含む）を処分事業者の工場に搬送します。情報分類1（マイナンバー関連）は、物理的破壊（穴あけなど）を実行。分類2は、再度のデータ消去作業（研究所等の攻撃からも耐えられるレベル）を実行。分類3は指定はありません。



まとめ

一次データ消去

- いずれの機密分類でも、庁舎内でのデータ消去作業が必須です。
- 職員（または社員）が行う場合は、専用ソフトの調達が必要となります。
- パソコンによっては、ソフトが動作しない場合など例外も生じますから、代替手段の検討も必要です。
- 専門技術業者に依頼することは可能です。

二次データ消去

- 重要機密情報である情報分類1と2には、さらに強固な情報抹消作業が求められています。
- 物理破壊を行う場合でも、データ抹消を強固なものとするために、さらに精密なソフト消去を推奨します。

消去履歴

- 一次二次を通じて、消去履歴（消去証明書等）を残すことは必須です。
- 万一の場合に備え、機体および記憶装置の製造番号も含めて記録し、改ざんが不可能なエビデンス（証拠）を残すことが重要です。

地方自治体以外の企業などの対応

- 総務省ルールの適用範囲外ですが、公益性や事業のセキュリティリスクの重大性に応じた対策をご検討ください。

TOPIERが新しく構築したしくみ

それなら
こういう新方式で

現地で消去、確実な証明のしくみを開発（宮城県補助金活用）①

事業所内で、データ消去の作業を、簡便におこなえる、自動消去システムを開発しました。貸与されたUSB専用機器をパソコンに差し込んで、説明書に従って操作すれば、自動的にデータ消去が実行されます。高度な消去レベルにも対応しています。また、専門技術者が再確認するので安心です。

使用済パソコンの排出事業所内

・貸与されたUSB専用機器をPCに指して操作すれば、自動的にデータ消去。

・消去済PCを起動すると、消去確認が表示。

・大量やサーバーは、複数台消去専用装置（独自開発）で一気に処理。

TOPIER

・データ消去済PCと専用機器内の記録で、消去記録確認し、証明書発行システムに自動登録。

・PC機体番号等を自動取り込みするので、確実な証明が可能。

・物理破壊の場合でも改ざんの難しい証明方法を用意。

現地で消去、確実な証明のしくみを開発（宮城県補助金活用）②

データ消去の処理結果は、データ消去登録証明書発行システム（独自構築）に登録され、第三者機関としての消去証明書を発行します。記録が保存されていますから、万一の際にも再検証等にも耐えます。一連の構築には、宮城県「みやぎ産業廃棄物3R等推進事業費補助金」を活用しました。

使用済パソコンの排出事業所内

2022年2月

データ消去証明書

一般社団法人東北情報機器再生推進機構は、本機構が認定したデータ消去ソフトウェアおよび消去事業者により実施された消去結果を下記の通り証明します。

メーカー	DELL
モデル名	Vostro 3681
シリアル番号	GWH12351323
ストレージ1	CT500MX500SSD1 (500GB) 1821EAA111 アルゴリズム: [DoD short] 結果: [OK]
消去事業者	作業者1
確認日時	2021-07-31 00:30:29

from Miyagi

以上のとおりデータ消去が実施されたことを証明します。

・後日、データ抹消証明書を提出します。

・処理のデータはシステムを通じて随時確認することができます。

データ消去登録
証明書発行システム

TOPIER

パソコン	ストレージ	アップロード情報	操作
メーカー DELL モデル名 Vostro 3681 シリアル番号 GWH12351323	モデル名 CT500MX500SSD1 シリアル番号 1821EAA111 アルゴリズム DoD short	利用者 作業者1 IPアドレス 172.38.187.95 日時 2021-07-31 00:30:29	消去証
メーカー QEMU モデル名 Standard PC (i440FX + PIIX, 1996) シリアル番号 Not Specified	モデル名 QEMU HARDDISK シリアル番号 QM00002 アルゴリズム DoD Short	利用者 作業者1 IPアドレス 192.168.0.195 日時 2021-08-31 13:50:45	消去証
メーカー QEMU	モデル名 QEMU HARDDISK	利用者 作業者1	消去証

・データ消去登録証明書発行システムは当機構が厳重に保守し、第三者機関としての後日のデータ抹消証明にも対応可能です。

しくみの無償提供とアンケートご協力のお願い

使用済パソコンのデータ消去をお手伝いして、資源の有効活用に資するため、簡便かつ安心に活用できるデータ消去システムが完成しつつあります。※宮城県「みやぎ産業廃棄物3R等推進事業費補助金」活用事業（令和3-4年度）

しくみを無償でご利用いただいて、安全にパソコンを処分していただくとともに、さらなる改良のために、使い勝手等のアンケートにご協力をお願いいたします。

①2台以下の場合

- USB専用機器を無償で貸与します。
- 説明書にしたがって操作し、パソコンのデータ消去をおこなってください。
- 当機構でデータ消去が確実に行われたことを確認し、証明書を発行します。
- その後、機器は適切な処分をおこないます。

②3台以上の場合

- 所定の日時に事業所を技術者が訪問し、事業所内でのデータ消去作業（一次消去）をおこないます。複数台対応データ消去機も使用します。
- 使用済パソコンをお預かりし、工場でのデータ消去作業（二次消去もしくは破壊）を行います。
- 当機構でデータ消去が確実に行われたことを確認し、証明書を発行します。
- その後、機器は適切な処分をおこないます。

おきがるに
ご相談ください

TOPIER

一般社団法人 東北情報機器再生推進機構

お問い合わせ・ご相談は

TEL **022-395-4912**

受付 10:00～17:00（株式会社あるく、土日祝休）

FAX 022-774-1491　メール info@topier.jp

担当／倖田（こうだ）

ウェブサイト https://topier.jp