2021年度 第3回ASIFスキルアップセミナー

ストレージの物理障害対応と車載機器へのデジタルフォレンジックの活用例

AOS DATA

AOSデータ株式会社

2021年11月29日

アジェンダ

1. 会社紹介
   （システムデータ事業部 事業部長 清本光彦）

2. HDDやmicroSDの物理障害における復旧事例
   （データ復旧事業部 技術グループ マネージャー 小菅大樹）

3. 車載機器へのデジタルフォレンジックの活用例
   （リーガルデータ事業部 営業部 マネージャー 清利樹）

4. 質疑応答

1. 会社紹介

システムデータ事業部
事業部長
清本　光彦

AOSグループ会社概要

AOSテクノロジーズ株式会社

代表取締役社長　佐々木 隆仁
設　立　：1995年3月
資本金　：4億8,000万円
従業員数　：100名
（グループ全体）

東京都港区虎ノ門5-13-1
虎ノ門40MTビル4F
TEL：03-6809-2530
FAX：03-5733-7011

● **グループ概要**

AOSデータ株式会社、リーガルテック株式会社、データテック株式会社、JAPANMADE事務局、AOS Legal Technologies Inc.（米国）、AOS Legal Technologies SARL（スイス）、AOS KOREA Co.（韓国）の７社で構成されています。

AOSデータ株式会社

代表取締役社長　春山　洋
設　立　：2015年4月
資本金　：3億5,250万円
従業員数　：83名

東京都港区虎ノ門5-1-5
メトロシティ神谷町4F
TEL：03-6809-2578
FAX：03-5733-7011

● **主な製品・サービス**

データバックアップ「AOSBOX」、データ復旧「ファイナルデータ」、データ移行「ファイナルパソコン引越し」、データ抹消「ターミネータ」、データ復旧サービス「data119」、データ消去サービス、リーガルサービス、リーガルテックツール販売、eDiscoveryサービス

リーガルテック株式会社

代表取締役社長　佐々木 隆仁
設　立　：2012年6月
資本金　：5,100万円
従業員数　：13名

東京都港区虎ノ門5-13-1
虎ノ門40MTビル4F
TEL：03-6809-2530
FAX：03-5733-7011

● **主な製品・サービス**

LegalSearch.jp（法律検索）、Keiyaku.Ai（次世代契約プラットフォーム）、Tokkyo.Ai（特許検索）

『データアセットマネジメント』

私達は、データのライフサイクルに基づき、お客様の資産である
データの管理から活用まで幅広くトータルソリューションを提供いたします。

カテゴリ	サービス
移行	データ移行ソフト「ファイナルパソコン引越し」
セキュリティ	ランサムウェア対策ソフト「ファイナルランサムディフェンダー」
	個人情報保護対策ソフト「プライバシーディフェンダー」
バックアップ	クラウドバックアップサービス「AOSBOX」
調査	フォレンジック調査/eディスカバリー
復旧	データ復旧ソフト「ファイナルデータ」
	データ復旧サービスセンター/データ復旧安心サービスパック
消去	データ消去ソフト「ターミネータ」
	データ消去サービス
AI	アノテーション、OCR、メディア

弊社の代表的な製品とサービス

AOS DATA

データ復旧サービスセンター

国内最大級の復旧サービスセンターは、NECパーソナルコンピュータ様等と正規業務提携し、ハードディスクの復旧技術は業界最先端。

データ復旧ソフト：ファイナルデータ

官公庁にも導入され、犯罪捜査の証拠復旧でのプロ用から初心者向けまで、幅広い方々にご利用いただいております。

BCN AWARD 2020 システムメンテナンスソフト部門 最優秀賞

11年連続 No.1

デジタルフォレンジック調査

官公庁捜査機関へフォレンジック・ツール、サービスを提供。優秀なフォレンジック技術者が在籍し、レビューセンターは最大80名が稼働可能。

画像解析フォレンジック

識別困難な状態から証拠となる画像、動画データを抽出。監視カメラ、スマホなどの画像データから犯罪捜査、不正調査の証拠となる画像を解析。

クラウドバックアップサービス：AOSBOX

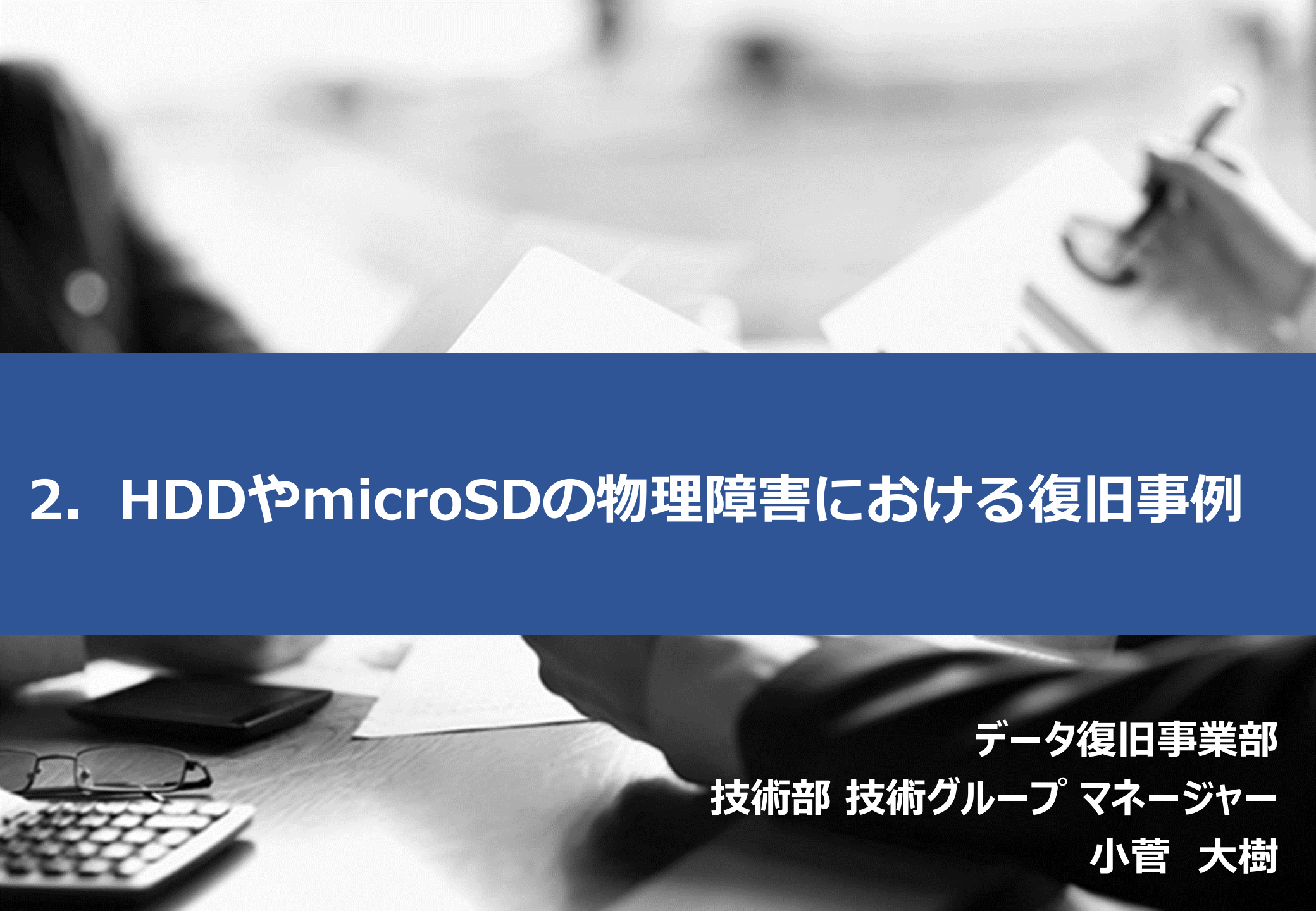
個人ユーザー90万人、法人ユーザー4,500社の導入実績。アイティクラウド社が運営する「Itreview」にて8期連続3部門でアワードを受賞

ITreview LEADER 2021 WINTER

データ移行ソフト：ファイナルパソコン引越し

国内累計出荷数1,100万本を突破。「第35回 Vector プロレジ大賞 データ引越部門賞」を受賞するなど、多くのユーザーに選ばれた実績。

第35回 Vector プロレジ大賞 データ引越 部門賞



2. HDDやmicroSDの物理障害における復旧事例

データ復旧事業部
技術部 技術グループ マネージャー
小菅　大樹

1. 弊社復旧サービスのご紹介
2. データ復旧サービスについて
3. ドライブレコーダーの復旧実績
4. HDDの復旧方法と障害種類
5. microSDの復旧方法と障害種類

小菅　大樹

Kosuga　Daiki

データ復旧事業部　技術グループ　マネージャー

2007年　リコーテクノシステムズ（株）に入社
　　現：リコージャパン（株）
2010年　大手データ復旧会社に入社
2014年　AOSリーガルテック（株）に入社
　　現：AOSデータ（株）
　　■データ復旧 物理部門の立ち上げ
　　■スクラッチ復旧技術の開発に従事
　　■Flash mediaの復旧開発に従事

所属：
・NPO　データ復旧技術研究会　会員

・専門分野はHDDの物理障害復旧
・HDDの復旧を累計1万台以上行ってます。

AOSデータ　株式会社
データ復旧事業部のご紹介

サービスの特徴

サービス

■**安心の定額制**
症状により軽度、中度、重度の3ランクの定額設定をしており、かつ初期調査も無料につき安心してお申込みいただけます

■**迅速な対応**
初期調査は媒体到着後、平均１-２日以内にお見積もりを提示、その後のデータ復旧作業は平均２-４日でお客様にお届けいたします

■**多彩なオプションサービス**
・お客様の現場に技術者を派遣して、現地で復旧する「オンサイトサービス」
・訴訟対応、内部監査などの証拠取得を支援する「フォレンジックサービス」

技術

■**全てのデバイスを復旧**
サーバーからパソコン、スマホ、メモリカードに至るまで、全てのデバイスの論理障害や物理障害の復旧が可能です

■**メーカー様などと提携**
PCメーカー、周辺機器メーカー、HDDメーカー、キャリア様の公認データ復旧会社として、正式に業務委託契約を締結しております

■**安心の作業環境**
ISO27001(情報セキュリティマネジメントシステム)に準拠したラボにて、作業は全て完結します

提携パートナー様

NEC
lenovo
dynabook
EPSON
SONY
VAIO
acer
mouse computer
I-O DATA
BUFFALO
Synology
WD Western Digital
JVC KENWOOD
OLYMPUS
SAMSUNG
FUJI xerox
au
Y!mobile
NTT東日本
Rakuten Mobile
YAMADA
ヨドバシカメラ
ビックカメラ
Joshin
nojima
立ちどまらない保険。 MS&AD あいおいニッセイ同和損保
損保ジャパン日本興亜

販売パートナー様とのビジネスモデル例

	業務内容	メリット	ご契約先例
①紹介型	コールセンターにお問合せのお客様をご紹介いただくだけで、その後は弊社がお客様にヒアリングし、データの復旧から納品と代金の回収まで行います。	コールセンターの生産性向上とお客様から受注し納品した場合、その金額（売上額）に基づき、紹介料をお支払い致します。	メーカー様 キャリア様 修理会社様
②再販型	貴社のお客様（法人様）に弊社のデータ復旧サービスをご販売いただく方法です。 障害媒体の送付や復旧データの報告は、弊社－お客様間で対応可能です。	弊社のデータ復旧サービスを仕切り価格でご提供します。 貴社の売上拡大とCSに貢献します。	Sier様 ITベンダー様
③委託型	貴社のデータ復旧サービスの全てまたは一部を弊社に委託いただく方法です。	貴社のサービスメニュー拡大と業売上拡大及びCSに貢献します。 また同業者様には、弊社データ復旧ソフト「ファイナルデータ」を特別価格でご提供致します。	メーカー様 修理会社様 データ復旧業者様
④安心パック（金額補償型）	データ復旧時の費用をお客様に月単位または年単位でお支払いただく事により、無料でデータ復旧サービスを提供する方法です。	全ての媒体に対し、ご提案が可能です。 貴社の端末補償や延長補償サービスメニューに追加する事が可能です。 商品の付加価値化や差別化に貢献します。	メーカー様 キャリア様 修理会社様 量販店様

■データ復旧サービスとはどんなサービスか？

→障害が発生したPCなどの筐体からデータを救出するサービス。

Point

・PC修理サービスとは異なる。

■データ復旧サービスとフォレンジックサービスとの違いは？

→復旧されたデータに対し法的証拠能力を有するか

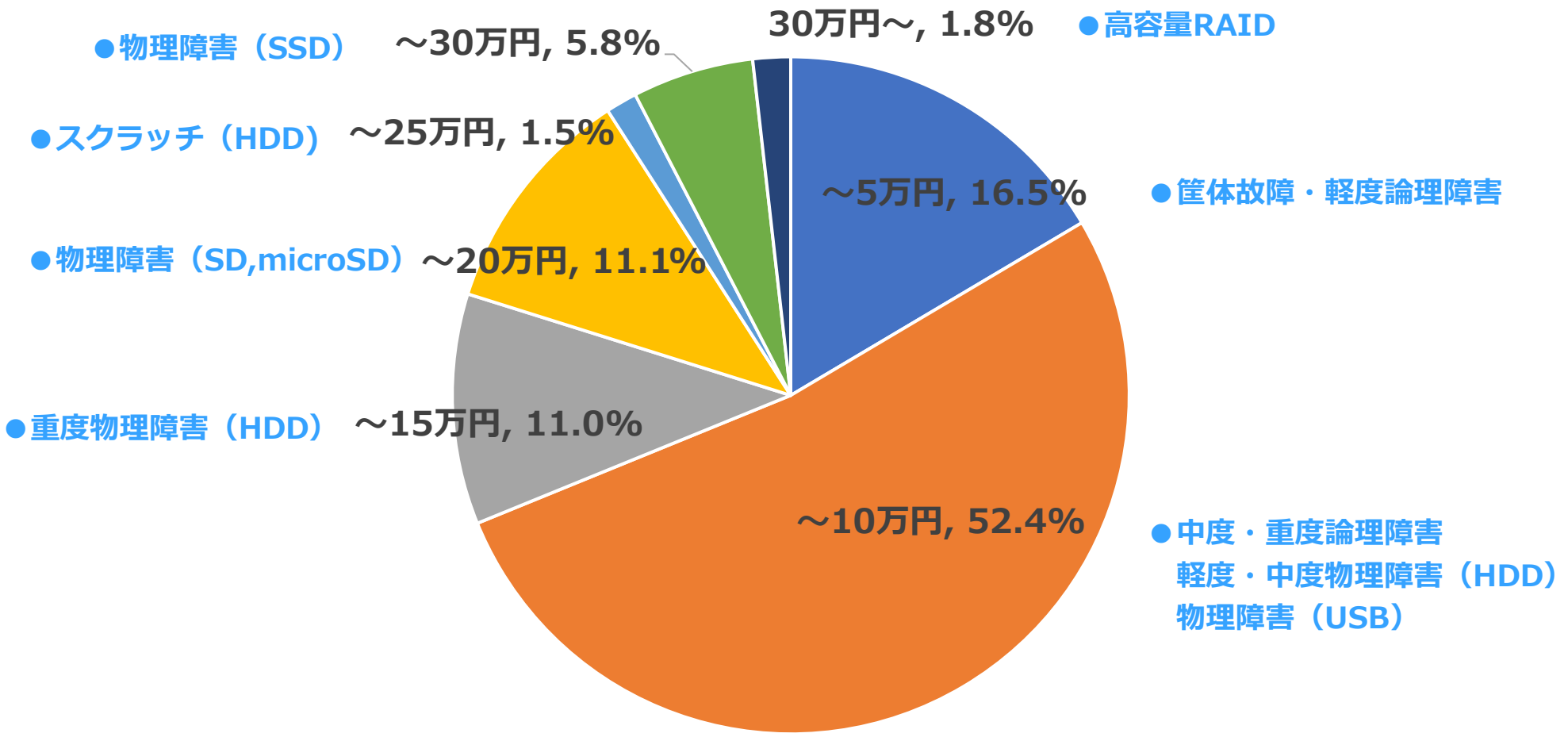
Point

・フォレンジックの場合、データが出なかったというのも重要な情報である。

■データ復旧の費用

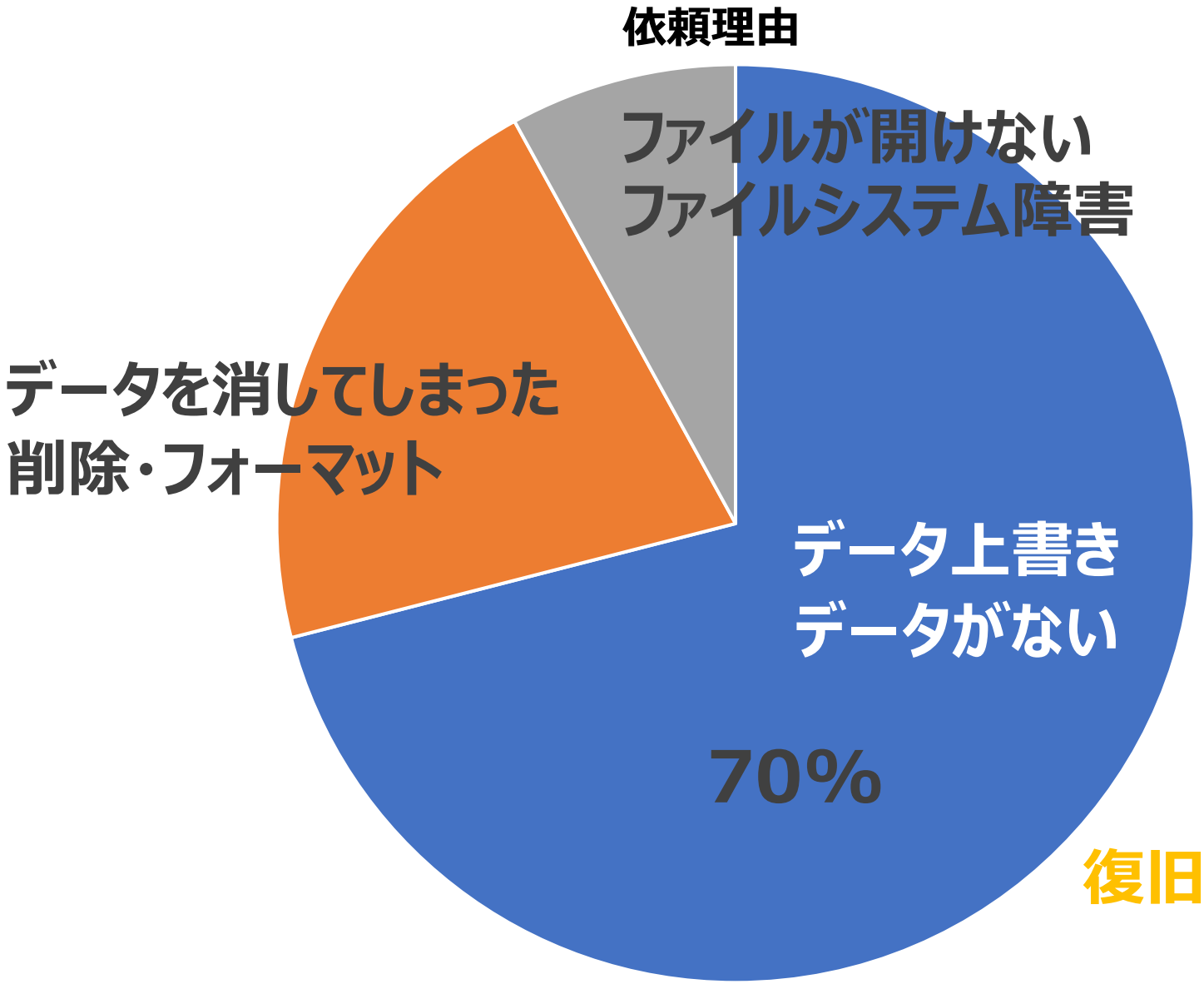
2020年10月-2021年9月
AOSデータのお客様への提供価格
※復旧保険を除く

顧客への案内金額構成比



業者や障害状況によって価格が大きく異なるため、一概には言えないが、
弊社の場合7万～10万の価格帯が多い

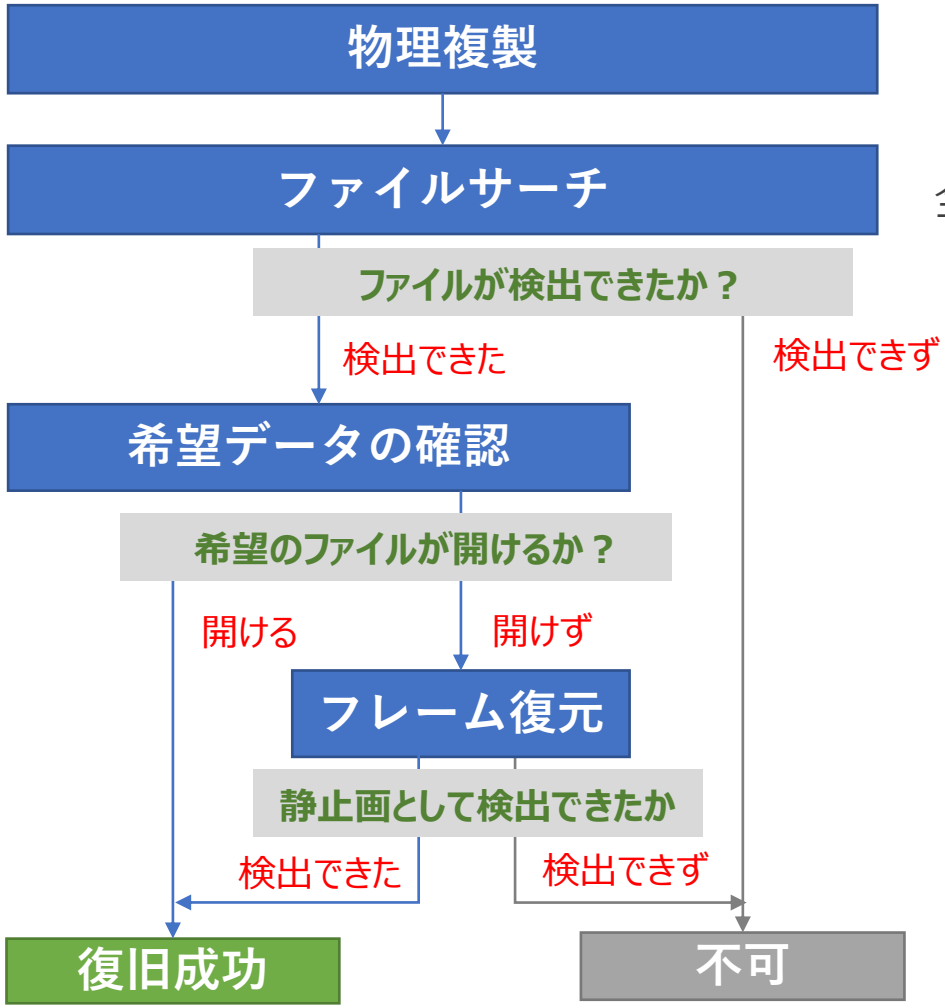
ドライブレコーダーについて



復旧率は約４５％

集計期間：2020/10-2021/9

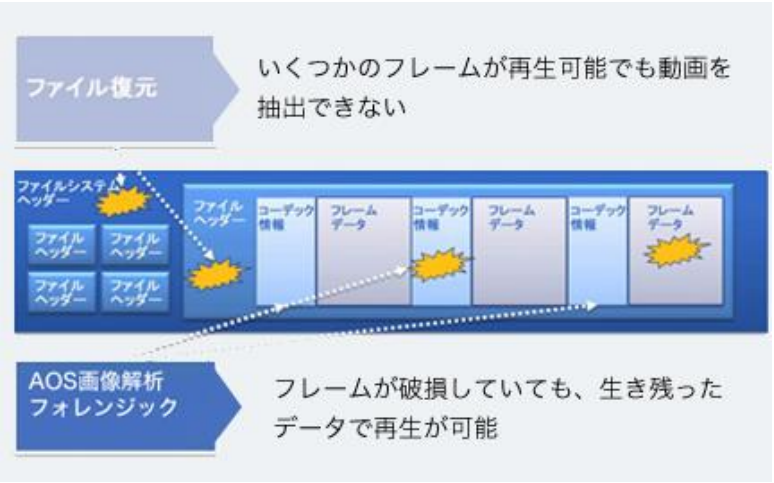
ドライブレコーダー　どういった復旧を行っているか
想定の障害：ファイルシステム障害



全データ領域から特定の拡張子と同じヘッダー情報を探す

フレーム復元

動画ファイルとして破損している場合、
フレーム単位（静止画）として切り出す。



カーナビについて

データ復旧サービスでは、筐体の特性上復旧できたとしても納品媒体を用意できないため対応不可としています。※フォレンジックサービスとしては対応可能

データ復旧サービス　問合せ案件の内容

■希望データ

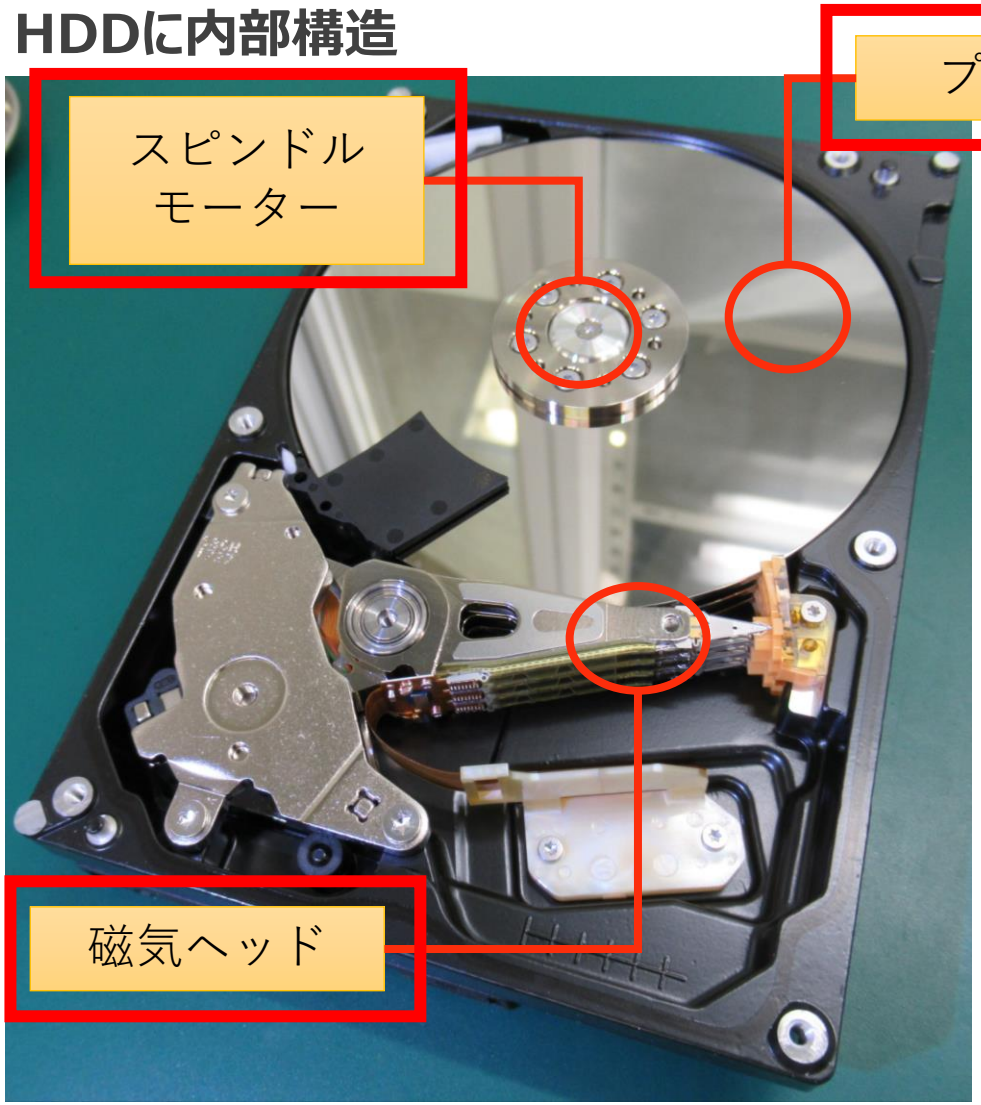
・地図データの復旧
・音楽データ

■障害内容

・カーナビの地図更新を行っていた。更新の最中に自動修復画面　になってしまった。
・カーナビをオールリセット。
・この場所を検索した履歴（日付）を知りたい
・誤削除
・マイリストに過去の行った場所が残るが自身の知らない場所が7-8箇所マイリストに入ってる。

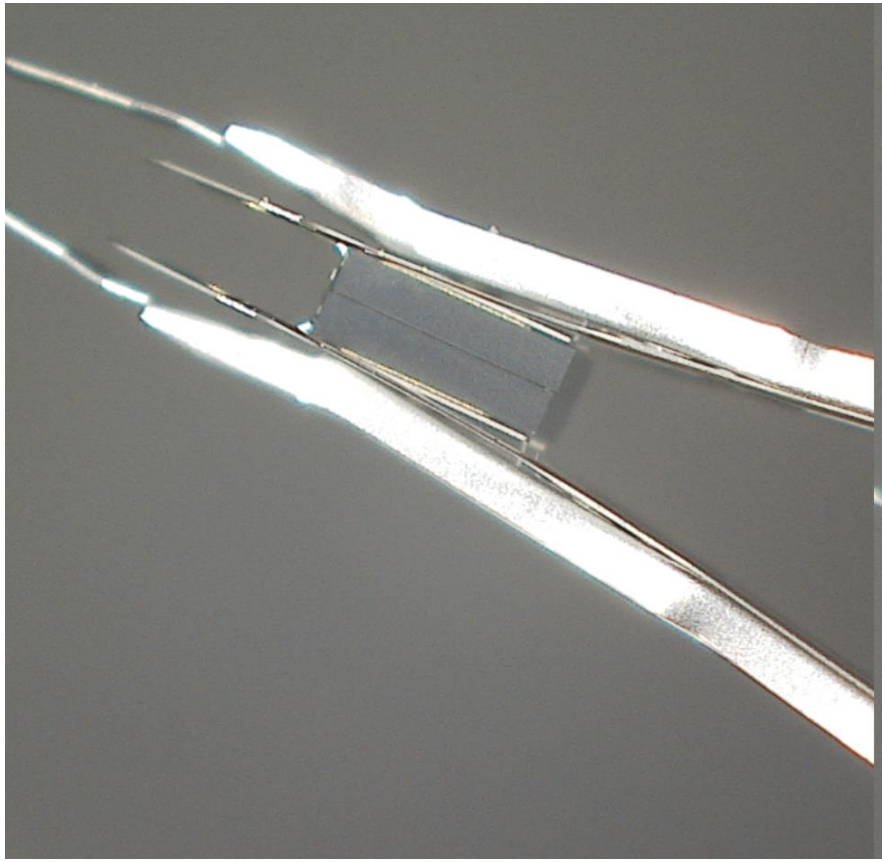
HDD、microSDについて

HDDに内部構造

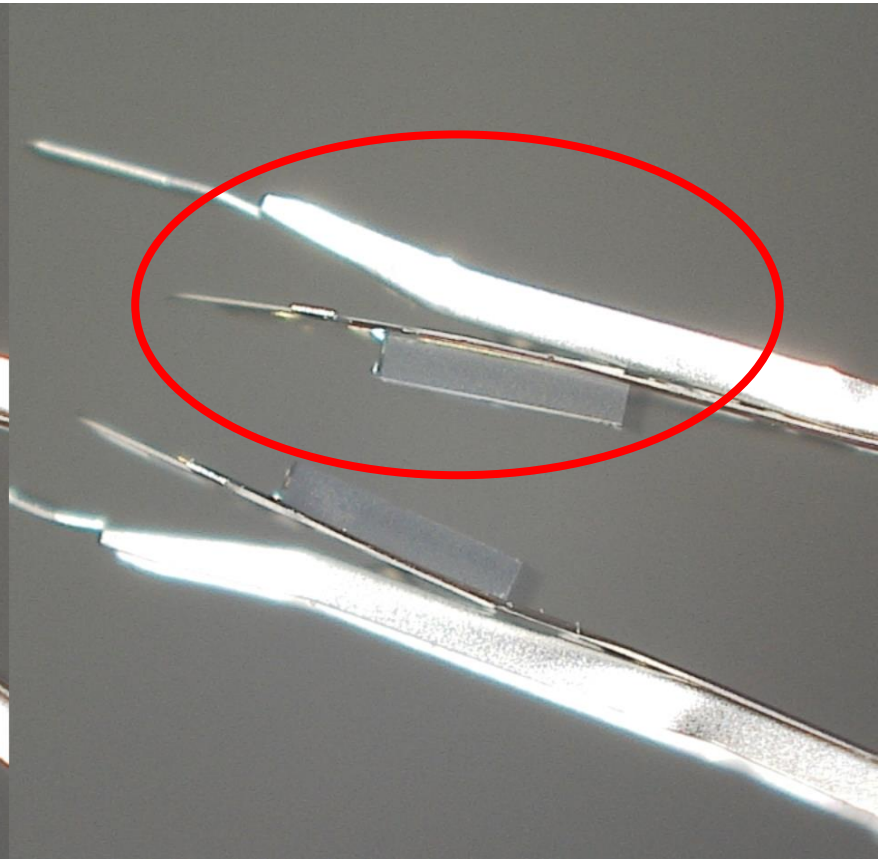


事例紹介：磁気ヘッド障害（変形）

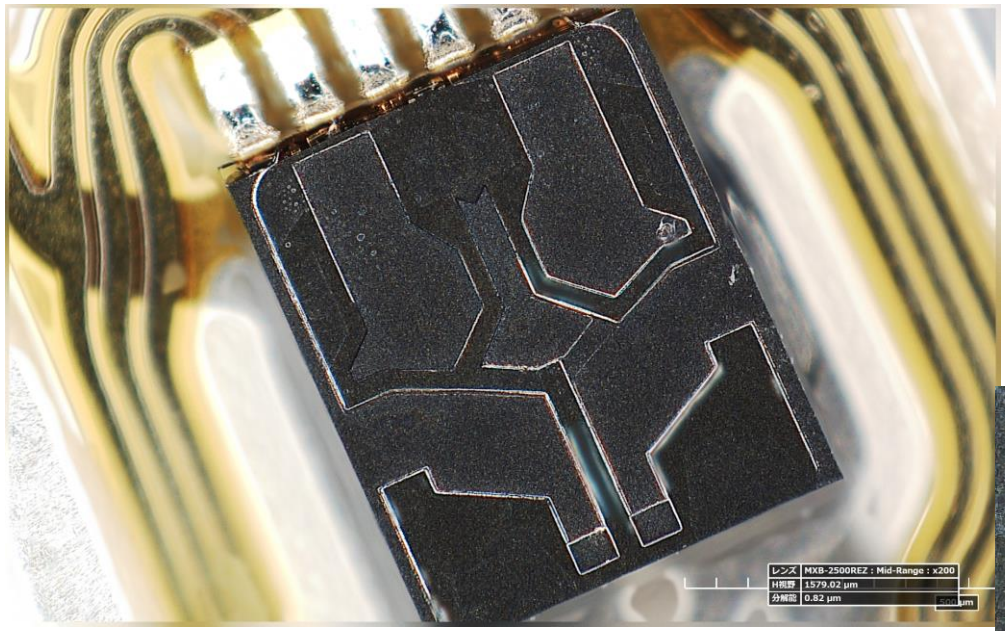
正常

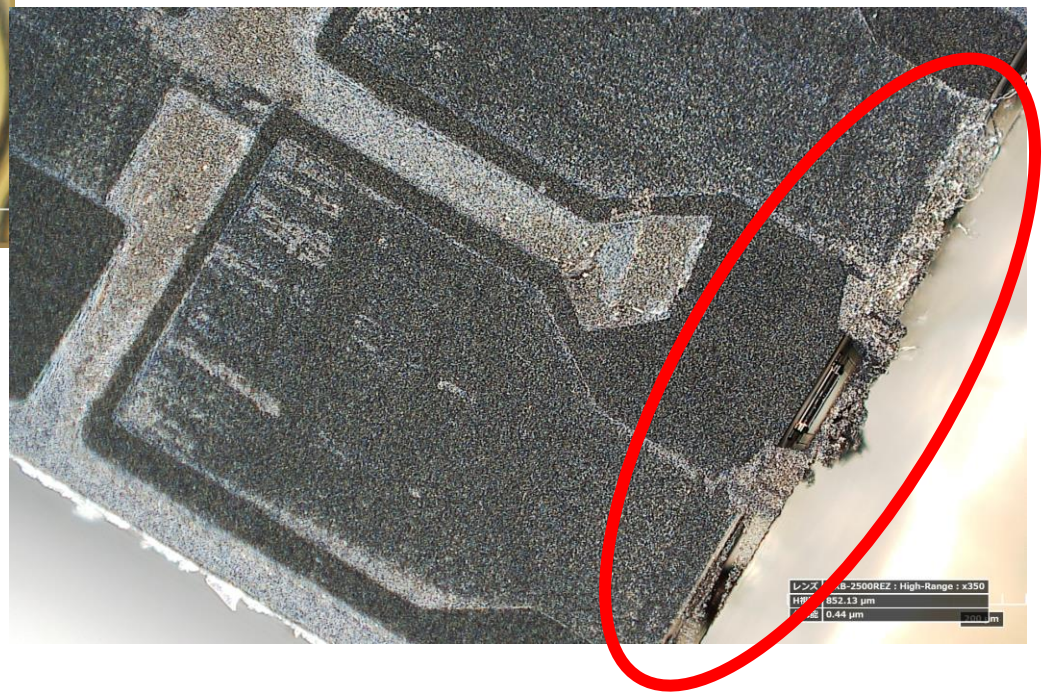


変形



事例紹介：ヘッド障害（変形）





プラッタを削った粉が付着している

事例紹介：プラッタの傷（スクラッチ）

プラッタ（正常）

プラッタ（傷あり）

事例紹介：プラッタの傷（スクラッチ）

物理復旧の作業内容

クリーンブースでヘッド交換をしている様子

AOS DATA

物理障害の復旧プロセス

診断：障害箇所の特定

どこに問題があり、どういうアプローチが最適なのか判断する。

部品交換：クリーンブースでの作業

同じ型番のHDDでも磁気ヘッドは複数種類ある。また技術者の熟練度も必要。

動作確認：ソフトウェア面での調整

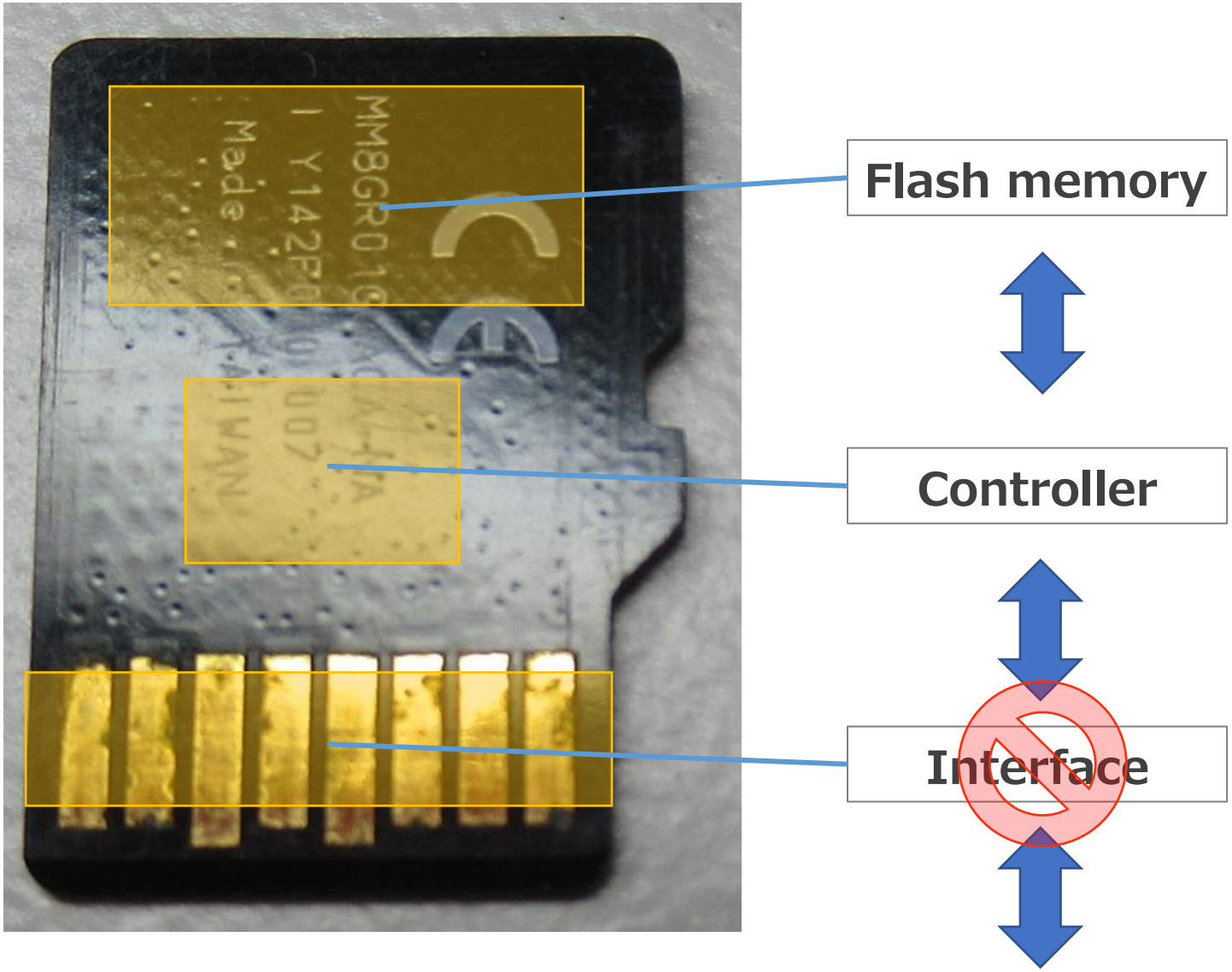
近年、HDDのSecurity対策により難易度が高くなっている

物理複製：複製媒体を作成する

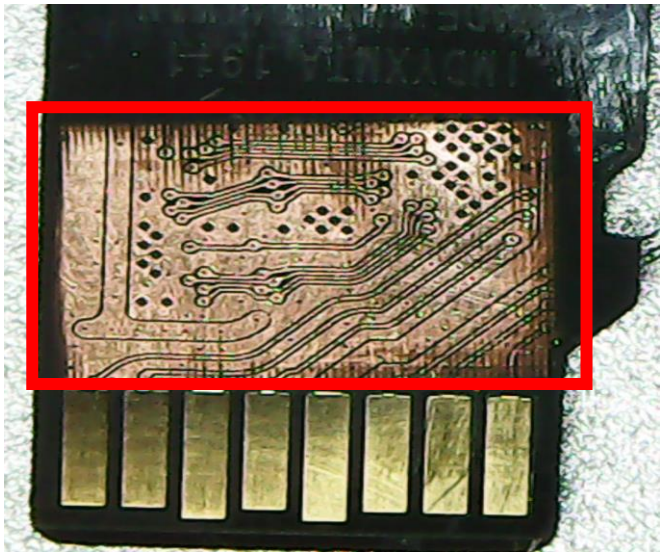
細かな設定調整を行い、最も読める状態で複製を取る

論理作業：ファイル検出作業

管理情報が破損している場合は、ファイルを探す必要がある

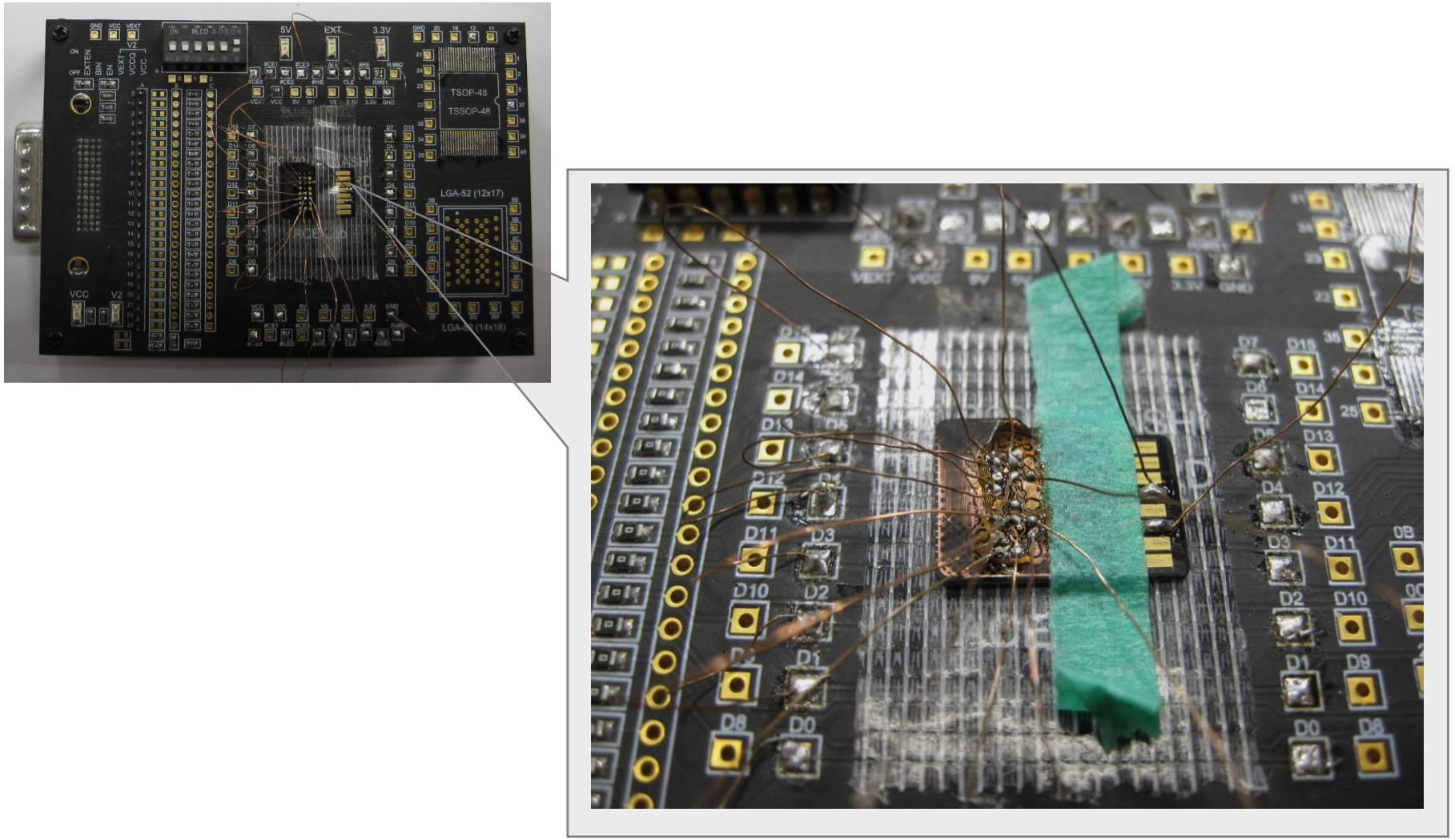


作業前のmicroSD

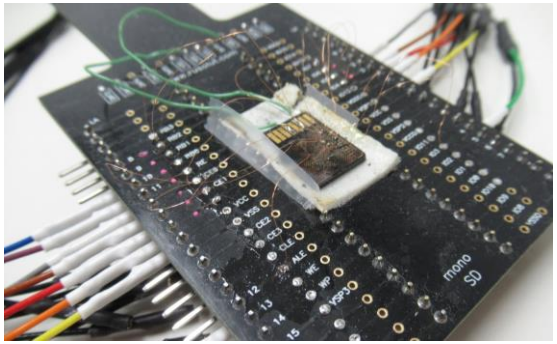


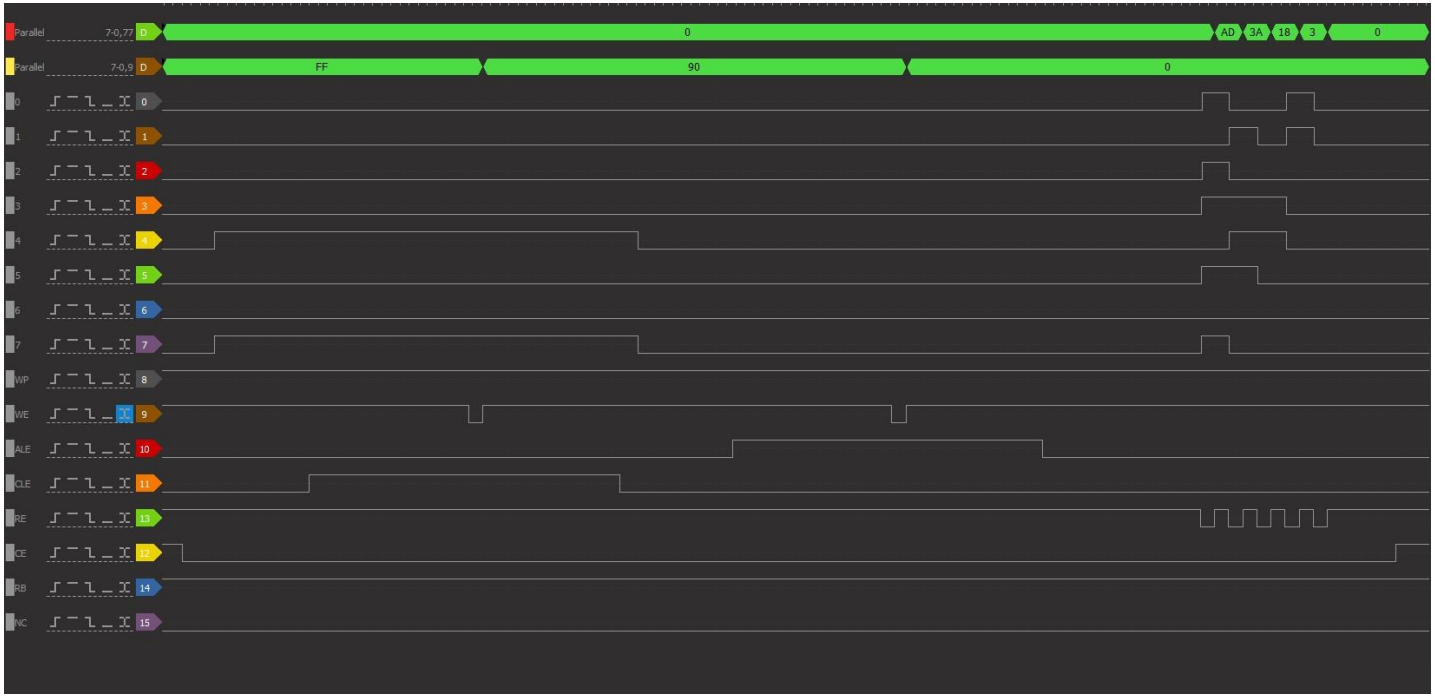
作業後のmicroSD

microSDの樹脂を剥がし、データ線を露出させる。

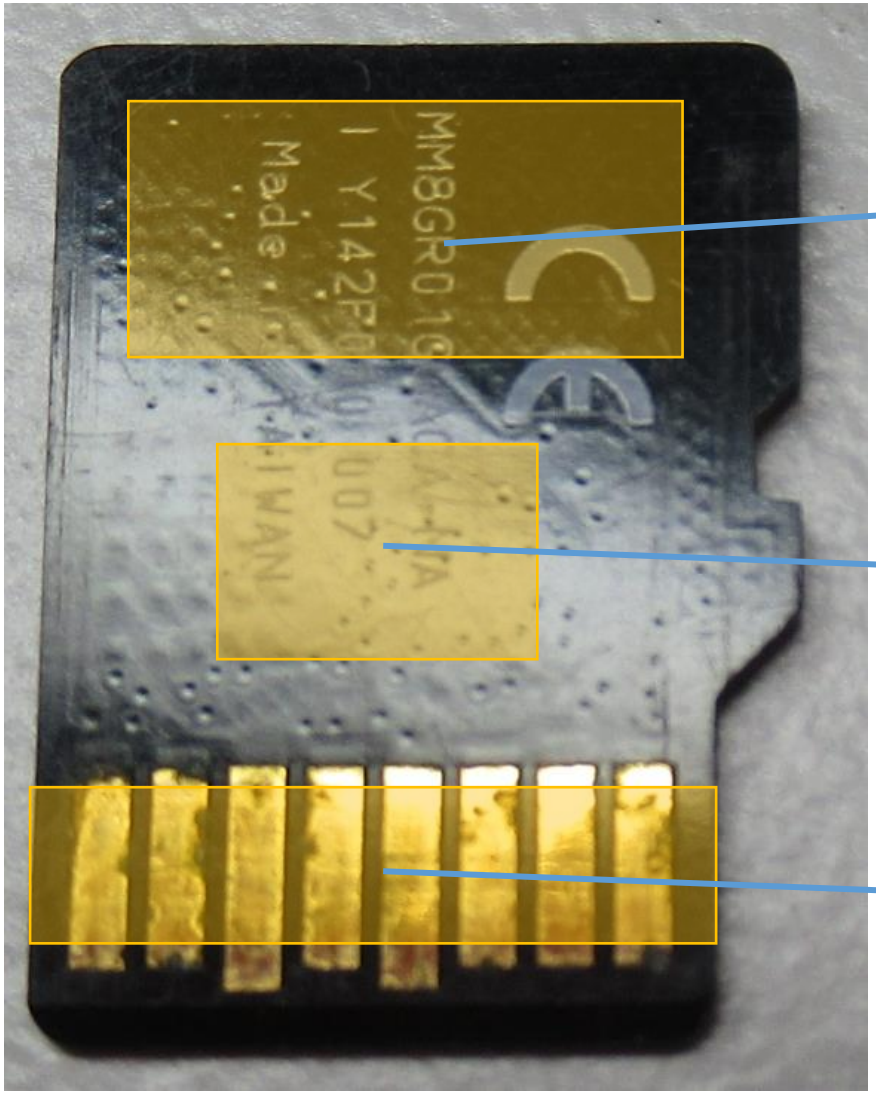


ワイヤリングを行い、データを抽出する。





データ線の特定を行う



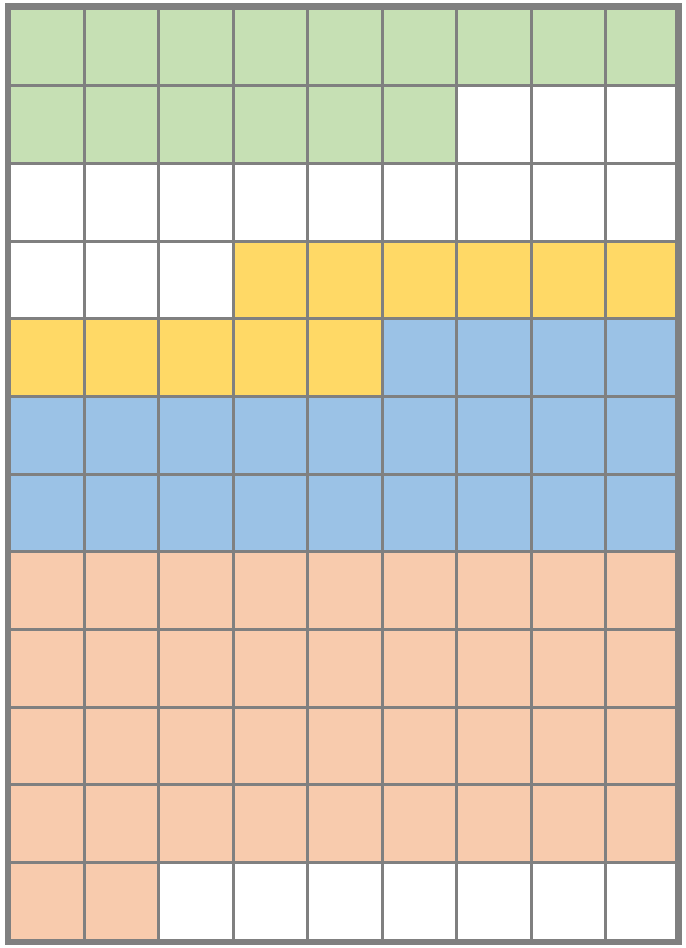
Flash memory

Controller

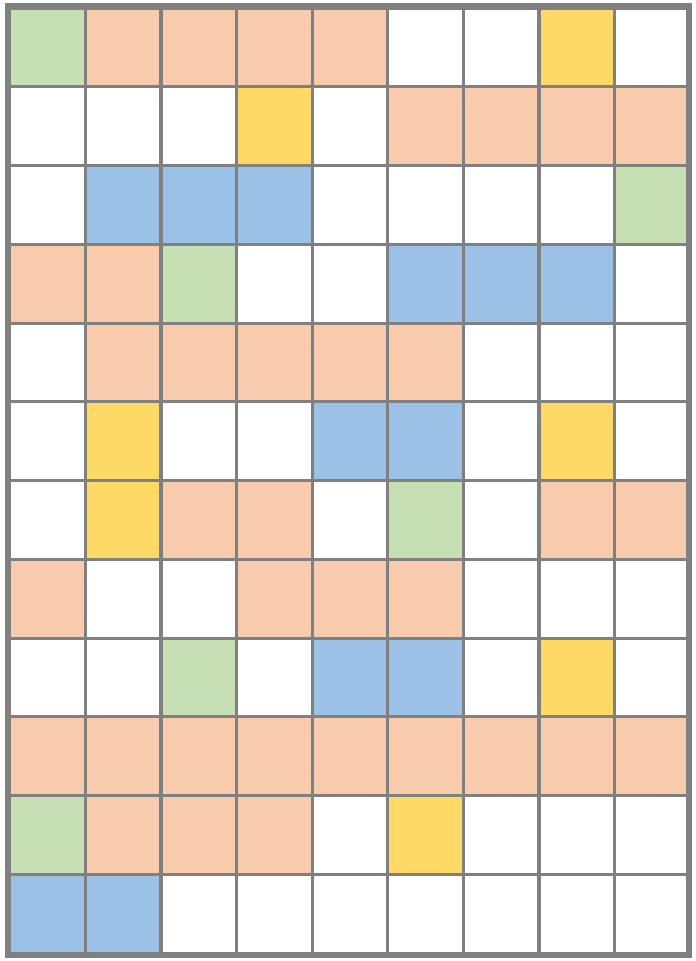
Interface

Dump !

HDDのデータ構造

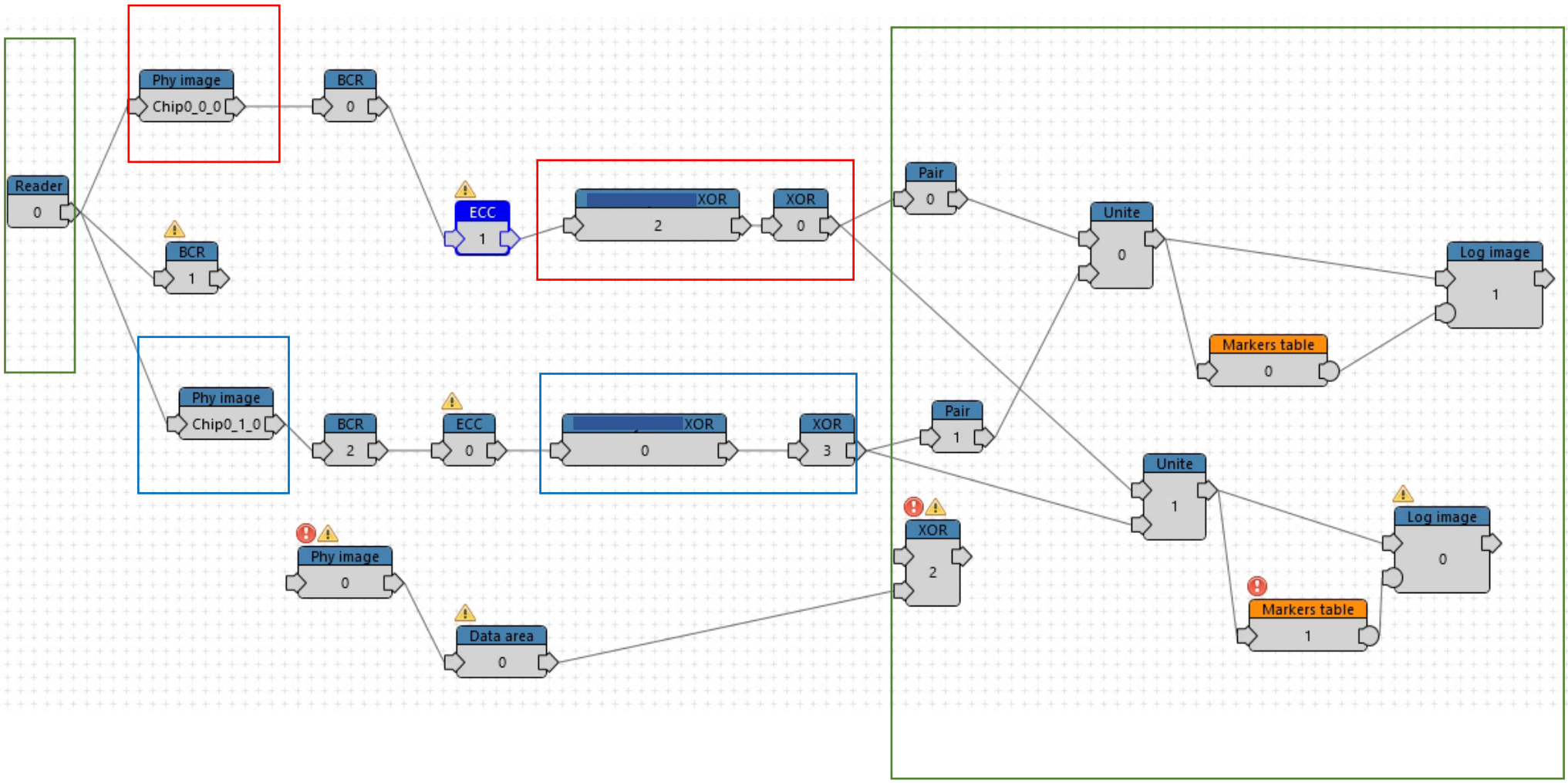


Flash mediaのデータ構造



ウェアレベリングの機能によってバラバラに保存される

（例）microSD（32GB）のDumpファイルからデータとして見えるようになるまでの論理プロセス



１．社外に持ち出せるか
　　オンサイトの場合、費用は1.5倍～３倍程度掛かる

２．絶対に復旧したいデータを把握する。
　　ファイル名・保存先・拡張子などを思い出して整理する

３．筐体を暗号化している場合は、回復キーやパスワードを把握しておく

４．信用できそうな業者を見つける
　　・故障筐体のメーカーがデータ復旧サービスを行っているか
　　・ISMSなどのセキュリティ規格を取得しているか
　　・価格が明確かつ妥当性があるか

3. デジタル･フォレンジックの概略と調査事例のご紹介

リーガルデータ事業部
営業部 マネージャー
清　利樹

講師紹介

清　利樹

Sei　Toshiki

リーガルデータ事業部　マネージャー

2016年　AOSリーガルテック（株）に入社
現：AOSデータ（株）
■データ復旧事業部に所属

2017年　リーガルデータ事業部へ部署異動

ロースクールにて法律を学んだ後、デジタル・フォレンジックやeディスカバリ支援業務、また各種ツールの販売に従事。
AOS入社当時はデータ復旧事業部に在籍していたこともあり、フォレンジックの有無に拘わらずそれぞれの調査手法に見識がある。
現在は、法律事務所や民間企業の管理部門に対し、デジタルフォレンジックほか様々なリーガルテック・ソリューションのご提案を行うとともに、警察や検察等の捜査機関への調査支援等をご提案している。

1. リーガルデータ事業部の紹介
2. デジタルフォレンジックとは
3. デジタルフォレンジックの流れ
4. 調査事例

1．リーガルデータ事業部の紹介

AOSデータ株式会社　リーガルデータ事業部

フォレンジックサービス提供
リーガルテック製品販売

政府・捜査機関

- 警察庁
- 警視庁
- 検察庁 Public Prosecutors Office
- 金融庁
- 国税庁

フォレンジックサービス・eディスカバリ支援サービス提供
リーガルテック製品販売

法律事務所

民間企業

第三者委員会

特別調査委員会

1. 強み

弊社では警察などの捜査機関や企業、弁護士からの依頼で数多くの犯罪、不正の証拠となるデジタルデータの復旧、検出、調査、開示支援を行なってきました。
その中で培われた経験により、下記のような強みがございます。

① 対応スピード

弊社には、フォレンジック調査に習熟したエンジニアが多数在籍しております。調査依頼内容に応じて、最適なスキルを持ったエンジニアを素早く割り当て、案件調査への対応を行います。また第三者委員会など大規模な調査依頼についても、対応できるだけのリソースを保持しています。

② 豊富な官公庁での実績

全国各地の警察や検察庁、税関、国税局や公正取引委員会といった官公庁との20年以上の取引実績があります。北海道から沖縄まで、フォレンジック調査ツール導入の実績がございます。

③ 様々なシステムに対応できる技術力

フォレンジック調査にあたるエンジニアには、システム運用や開発といった経験のあるエンジニアを採用しています。これにより、他社での対応が難しい「スクラッチシステムへのフォレンジック調査」といった案件にも対応しています。また、自社開発でのフォレンジックツールを設計できるほどの技術力を有しています。

2. デジタルフォレンジックとは

一言でいうと・・・

Digital forensics

デジタル 鑑識

（法科学）

2. デジタルフォレンジックとは

例えば、、、

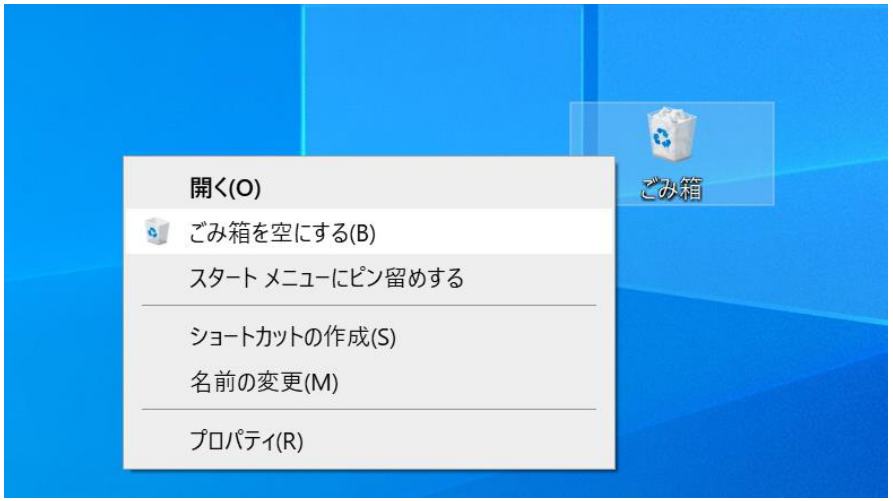
PCの中にどんなデータが入っているかを確認しようとして、パソコンの電源を入れてファイルを開く。

✓ 電源ON/ログオン → イベントログに「電源ON」、「ログオン」が記録される
✓ ファイルを開く → ファイルの閲覧履歴（LNKファイル）が更新される
⇒ さらに、これらの更新と共に古いログが削除される。

単純なパソコンの操作であってもパソコン内の情報というのはどんどん書き換えられて行ってしまう。

例えば、、、

「ごみ箱」から削除されてしまったファイルは一般のユーザーはパソコン上から確認することはできない。



電子データには特殊な解析を行わないと確認できない情報がある。

「犯罪の立証のための電磁的記録の解析技術及びその手続」

（警察白書より）

「インシデントレスポンス（コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等を言う。）や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術」

（デジタル・フォレンジック研究会HPより）

・行為者や行為事実を示す重要な証拠

・複製・消去・改変が容易である

・媒体としての有形物とは別個に独立して
成立している

・解析に特殊な技術が必要
（検察側⇔弁護側）

2. デジタルフォレンジックの三要素

①手続の正当性

デジタル証拠に関して、定められた手続きにのっとって、証拠品の収受と同様に正確かつ確実な記録を残し、取り扱い者以外の第三者がふれることのないように厳重に保管し、解析を行うために保管庫から取り出す場合や解析を中断・終了するために戻す場合には、出納状況を正確かつ確実に記録するなど、厳重な管理の下で取り扱うことが必要である。

②解析の正確性

電磁的記録の解析においては、論理的にも技術的にも正しい手法を用いた解析を実施し正しい結果を可視化・可読化し、推測や解釈を加えることなく、ありのままの事実を明らかにすることが重要である。

③第三者検証性

デジタルフォレンジックにおいて、解析に従事した者以外の解析者又は第三者が、正当な手続きの下で、かつ正しい手順で解析を行った場合には、同一の解析結果が再現可能であることが求められる。

参考：「デジタルフォレンジック概論：フォレンジックの基礎と活用ガイド」

3. デジタルフォレンジックの流れ

3. デジタルフォレンジック調査の流れ

初期対応	証拠保全	データ処理・解析	レビュー	報告
インシデントの状況を把握・評価し、その後の対応方針を決定します。	調査対象の媒体に含まれるデータを収集します。	収集したデータをフォレンジックツールを使用して解析、復元、検索、分類等を行います。	処理結果を確認し、証拠となり得る情報が含まれるか判別を行います。データ量が多い場合にはレビュープラットフォームを使用します。	報告用の最終成果物をまとめます。
当事者	当事者		当事者	当事者
弁護士			弁護士	弁護士
	DFベンダー	DFベンダー		DFベンダー

3. デジタルフォレンジック調査の流れ

初期対応ではインシデントの状況を把握・評価し、その後の対応方針を決定します。迅速な状況把握に努め、問題解決までの道筋を立てることが重要です。
デジタルフォレンジックの調査が必要と判断される場合には、調査対象の範囲を明確にする必要があります。

【調査対象の範囲】

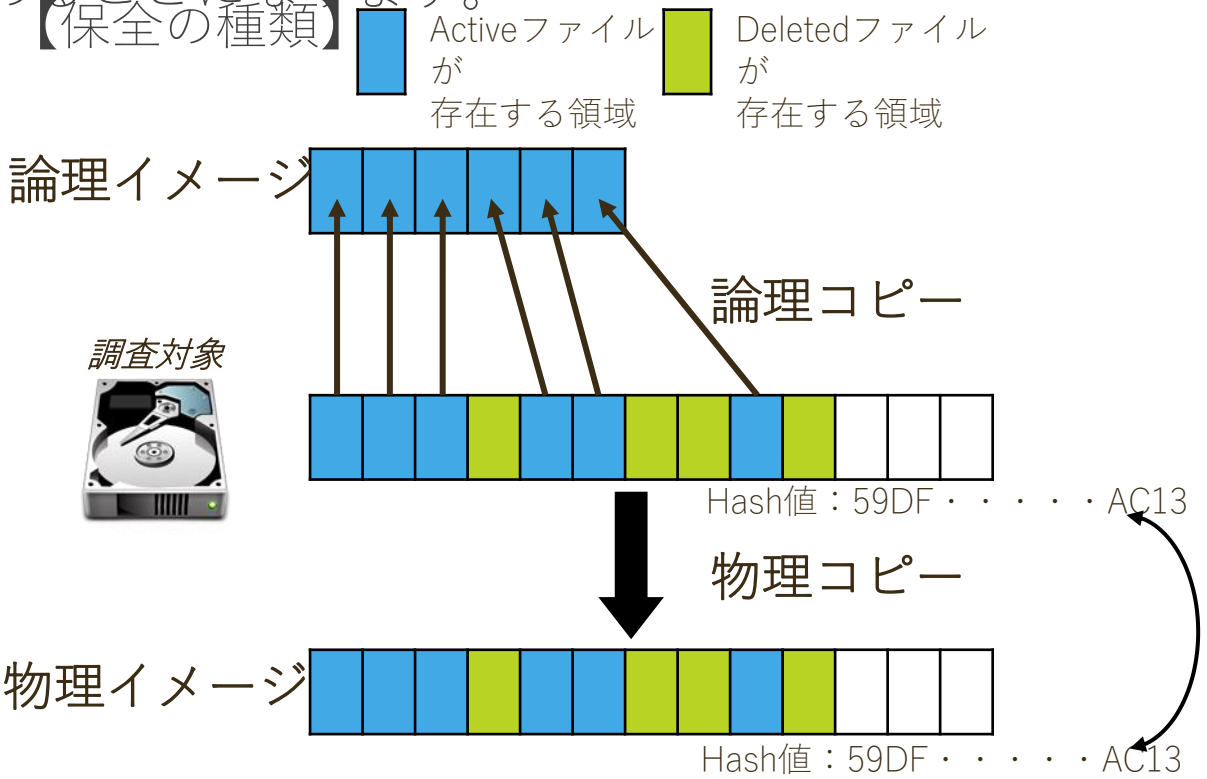
- 対象期間
- 対象人物
- 対象データの種類（メール/顧客データ/設計データ/削除データ等）
- 対象デバイス（PC/モバイル/サーバー等）

状況把握のためにPC等のデータを確認する必要がある場合には、可能な限り証拠を汚さないように注意が必要です。

3. デジタルフォレンジック調査の流れ

証拠保全とは、**「複製元の媒体に格納されているデジタルデータを書き換えることなく、かつ可能な限りデータ格納領域全体の完全な複製を作成すること」**になります。次の工程のデータ処理・解析ではこの複製したデータを使用して作業を進めることになります。

【保全の種類】



【保全時間の目安】

サイズ	時間
500GB	3時間
1TB	6時間
2TB	12時間

※USB3.0、コピー後のVerify処理含む

Hash値が一致していれば完全なコピーデータであることが証明できる。

※Hash値
電子ファイルや文字列等の電子データを、一定の計算式であるHash関数により演算し、数文字から数十文字程度の特定の長さの文字列に変換した値。Hash関数には、「同一のHashを生成する異なる2つのデータを求めることは計算量的に困難である」という性質（衝突発見困難性）がある。したがって、ある2つのデータについて、同一のHash関数を用いて得られたHash値が同一であれば、これらのデータ自体も通常は同一であると判断することができる。

3. 証拠保全の目的とポイント

① 事案発生時の状況にできるだけ近い状態で、デジタルデータの状態を固定化（維持・保持）すること

② （データを固定化することにより）調査結果の第三者検証性を確保すること

③ （物理複製をすることにより）削除データを含めた幅広い調査を可能にすること

調査に先立ち、まずはデジタルデータの保全のみを行っておく。
⇒とくに退職者のPCについてデータ保全を行うことは有用

3. 初動の重要性

嫌疑発生・不正発覚からデータ保全までの間に対象者によるデジタルデータの改変を防止することが重要

↓

例：数日後に退職を控えた社員の転職先が競合他社であると判明し、その転職先につき社員が偽っていた。また日常の業務態度から情報漏えいの嫌疑が濃厚。

↓

社員へインタビューを実施すべく日時を通告。しかし、社員はその通告によりPCのデータを抹消。

↓

嫌疑が発生した段階で業務時間外にPCを保全すべき。

※従業員の情報機器の調査にあたっては、従業員のプライバシー等の権利に配慮する必要があります。

3. フォレンジック調査の媒体一覧

ドライブレコーダー
カーナビ
ICレコーダーなど

	パソコン	外部記憶装置	サーバー	スマートフォン タブレット	その他電子機器
Web閲覧履歴	○ ブラウザでの 履歴調査	×	×	○ ブラウザでの 履歴調査	×
操作ログ	○ ファイル閲覧や イベントログの調査	△ ファイル生成・削除履歴の調査	○ アクセスログの調査	○ 各種ファイル ログの調査	○ 各種ファイル ログの調査
位置情報	△ データ保有の 位置情報	△	×	○ GPSログの調査	○ 走行軌跡の調査 （カーナビ）
メール	○ ローカルにあるメール 情報	△ 媒体に保存された PSTファイル等	○ メールサーバー の調査	○ ローカルにあるメール 情報	×
画像・動画	○ ローカルにあるデータ	○ 媒体に保存された データ	○	○ ローカル又はクラウド 上のデータ	○ 画像鮮明化（ドライブレコーダー）
その他	Windows/Macに 対応しています。	USBメモリ/ SDカード/フロッピー ディスク等を対象とします。	Windows系/ unix系/LINUX系の 調査が可能です。	上記の他に、通話履歴・連絡先等の調査 が可能です。	ICレコーダーでは、音声改ざんの 調査等が可能です。

※　調査項目は媒体の種類や状態によって異なります。

3. 主な調査項目例（PC）

調査項目	詳細説明
ファイル抽出・復元	PC 内に現在保存されているファイル、削除されたファイルを抽出・復元します。 【対象となるファイル】 Office・PDF ファイル、画像/動画ファイル、テキストファイル など
メール抽出・復元	PC 内に現在保存されているメール、削除されたメールを抽出・復元します。 【対応しているメールソフト】 Outlook、Thunderbird、Windows Live Mail など
WEB 閲覧履歴	WEB サイトの URL、アクセスした日時、ファイルのダウンロードの痕跡等、WEB ブラウザの記録を抽出します。 【対応している WEB ブラウザ】 Internet Explorer/Microsoft Edge、Google Chrome、FireFox など
ファイル閲覧履歴	ファイルを開いた日時、ファイル名、ファイルの保存場所(パス)の記録を抽出します。
USB 接続履歴	PC に接続された USB 機器について、機器の名前(デバイス名)、最初と最後に接続した日時、機器の製造番号(シリアル番号) 等の情報を抽出します。 【主な対象機器】 USB フラッシュメモリ、外付けハードディスク、スマートフォン など
USN ジャーナル	PC 内におけるファイルの作成、削除に関する履歴(ファイル名、日時)を抽出・復元します。ファイル復元で検出されなかったファイルの削除痕跡を確認できる可能性があります。
イベントログ調査	PC 内のイベントログから、ログイン/ログオフ履歴、電源 ON/OFF 履歴、リモート接続履歴などのイベントを抽出します。
アプリケーション実行履歴	PC 内における prefetch ファイルから、アプリケーションの実行履歴（実行ファイル名、実行日時）を抽出します。
キーワード検索	抽出・復元したファイルを対象に、ご指定頂いたキーワードで検索を行います。

3. フォレンジック調査の理想と現実

理想	きっとパソコン内で不正に関わるデータを作って保存していたはず！ 削除データを復元すれば見つかるはず！
現実	削除ファイルは復元できる可能性がありますが、その領域が新しいデータで上書きされてしまうと復元することはできません。復元処理は実施してみないと結果は得られませんので、復元できる確率がゼロでない限り復元の可能性はありますとお答えしております。

理想	パソコンにはどんな操作も記録が残っていて、操作内容が確認できる。
現実	デジタルフォレンジックで特定できる情報は、Windowsがシステムを稼働させるために必要なものとして記録しているものがベースとなっています。デジタルフォレンジックのために記録されているデータではありませんので、パソコンにおける全ての操作が明らかになる訳でありません。例えばUSBメモリのコピー操作そのものはWindows内に記録として残っておりませんので、USB接続履歴の日時とファイル閲覧履歴などの情報を合わせて、コピーされた可能性の有無を判断頂く形となります。

3. 主な調査項目例（モバイル）

調査項目	詳細説明
SMS	モバイル内に現在保存されているSMS、削除されたSMSを抽出・復元します。
メール	モバイル内に現在保存されているメール、削除されたメールを抽出・復元します。
通話履歴	モバイル内に現在保存されている発信履歴/着信履歴、削除された発信履歴/着信履歴を抽出・復元します。
電話帳	モバイル内に現在保存されている電話帳、削除された電話帳を抽出・復元します。
画像	モバイル内に保存されている画像、削除された画像を抽出・復元します。 iPhoneについては削除データの復元は不可となります。
WEB閲覧履歴	WEBサイトのURL、アクセスした日時、WEBブラウザの記録を抽出します。
SNSアプリ LINE,WeChat, Skype,　等	モバイル内に現在保存されている各アプリケーションデータ、削除されたアプリケーションデータを抽出・復元します。 【アプリケーションデータの内容】 メッセージの履歴、相手方の情報、チャットルームの参加者　等

3. カーナビゲーション

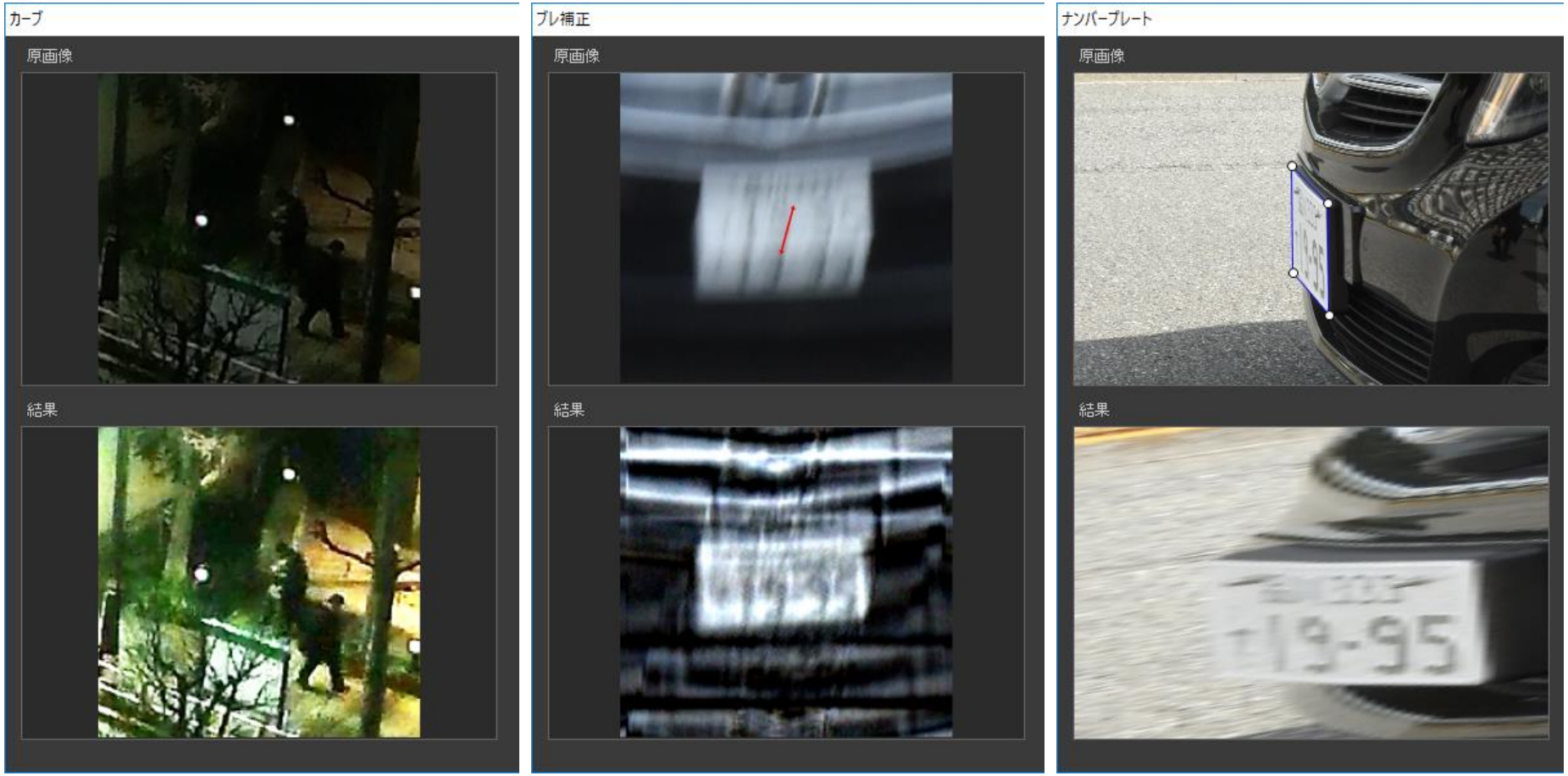
カーナビゲーションシステムから走行軌跡や目的地検索履歴のデータを抽出します。

ファイル名	日時	ポイント番号	緯度(Hex)	経度(Hex)	緯度,経度(Dec)
0001.DAT	2018-01-26 16:00:00	1	0FAC178	03D695CF	35.66304,139.74545
0001.DAT	2018-01-26 16:00:03	2	0FAC14A	03D6961D	35.66294,139.74562
0001.DAT	2018-01-26 16:00:06	3	0FAC11C	03D6966C	35.66284,139.74579
0001.DAT	2018-01-26 16:00:09	4	0FAC0E9	03D696BE	35.66273,139.74597
0001.DAT	2018-01-26 16:00:12	5	0FAC0BB	03D6970D	35.66263,139.74614
0001.DAT	2018-01-26 16:00:15	6	0FAC08D	03D6975B	35.66253,139.74631
0001.DAT	2018-01-26 16:00:18	7	0FAC05F	03D697A9	35.66243,139.74648
0001.DAT	2018-01-26 16:00:21	8	0FAC031	03D697F8	35.66233,139.74665
0001.DAT	2018-01-26 16:00:24	9	0FABFFE	03D6984B	35.66222,139.74683
0001.DAT	2018-01-26 16:00:27	10	0FABFD0	03D69899	35.66212,139.74700
0001.DAT	2018-01-26 16:00:30	11	0FABFA2	03D698E7	35.66202,139.74717
0001.DAT	2018-01-26 16:00:33	12	0FABF90	03D69948	35.66198,139.74738
0001.DAT	2018-01-26 16:00:36	13	0FABF7D	03D699AE	35.66194,139.74760
0001.DAT	2018-01-26 16:00:39	14	0FABF70	03D69A0E	35.66191,139.74781
0001.DAT	2018-01-26 16:00:42	15	0FABF5D	03D69A74	35.66187,139.74803
0001.DAT	2018-01-26 16:00:45	16	0FABF4B	03D69AD4	35.66183,139.74824
0001.DAT	2018-01-26 16:00:48	17	0FABF38	03D69B35	35.66179,139.74845
0001.DAT	2018-01-26 16:00:51	18	0FABF26	03D69B9B	35.66175,139.74867
0001.DAT	2018-01-26 16:00:54	19	0FABF18	03D69BFB	35.66172,139.74888
0001.DAT	2018-01-26 16:00:57	20	0FABF06	03D69C61	35.66168,139.74910
0001.DAT	2018-01-26 16:01:00	21	0FABEF3	03D69CC2	35.66164,139.74931
0001.DAT	2018-01-26 16:01:03	22	0FABEA0	03D69CAF	35.66146,139.74927

※メーカー、モデルによって解析できない場合があります。
※実績の無いモデルの場合には、サンプル機による事前調査を行う場合があります。

3. 画像鮮明化

動画および静止画に写っている対象に対し鮮明化処理を施し、対象が持つ特徴の判別を可能にします。



※鮮明化処理に必要な情報が画像内に記録されていなければ鮮明化処理の効果が十分に得られません。
※情報が劣化していない原本に近い画像データを収集することが重要です。

4. 調査事例

4. 代表事例

- 情報漏えい調査　（営業機密、個人情報、技術情報等）
- 労務関連調査　（競業避止違反、不就労、過労死、ハラスメント等）
- 社員不正調査　（資産横領、背任行為、キックバック等）
- 企業不祥事　（第三者委員会や社内調査委員会へサポート等）
- 刑事事件調査　（捜査機関もしくは弁護側からの依頼に基づく調査等）

相談内容

人材派遣会社A社において、幹部従業員の退職後、大量の従業員がその退職幹部が設立した新会社B社に入社。その後、既存の顧客にB社から営業攻勢があり、価格面で苦戦する。

調査方法

退職幹部のPCのHDDを保全したうえで、

1. 削除メールの復元
2. 削除ファイルの復元
3. USBデバイス接続履歴
4. ファイル閲覧履歴

について調査を実施

調査結果

1. 復元したメールデータから、在職者に新会社設立の情報と転職の勧誘メールを多数送信していたことが判明。
2. 顧客情報及び見積書を、個人のUSBメモリに格納していたことが判明。
3. 更に、そのUSBメモリが、上司のパソコンにも無断で接続されていたことが判明。
4. 後に提出されたUSBメモリの削除領域から各種情報を復元

事件の顛末

退職幹部に対して損害賠償を請求。

相談内容

東証1部上場企業のA社および、100%子会社であるB社の製品において、国土交通省大臣認定の基準に適合していない製品を出荷していたとして、外部の専門家から構成される第三者委員会が設置された。AOSは第三者委員会委員の弁護士より依頼を受け、補助者としてフォレンジック調査に参加。

調査方法

1. 委員会が必要と認めた対象者および関係パソコン のPC 70台 、ファイルサーバー2 台、メールサーバー内の電子メールファイル等を保全
2. 各種メールのデータ復元
3. 上記メールデータについて、メールアドレスで絞り込み

調査結果

抽出、復元したデータについて、事前処理（プロセッシング）を実施し、システム関連データ及び重複データを排除。さらに、プロセッシングを実施したデータに対し、委員会で定めたキーワードを用いて絞り込みを行い、30万件をレビュー対象として抽出。弁護士およびAOSのレビュワーからなるレビューチームを結成し、レビュープラットフォーム上にてドキュメントレビューを行った。
これにより判明した事実は、第三者委員会の報告書に掲載された。

事件の顛末

ドキュメントレビューの結果、関係者へのヒアリング結果の事実を裏付ける情報が確認されたことに加え、ヒアリングでは判明しなかった当事案に関する指示、認識が関係者間にあったことを強く推認されるものが確認された。

調査目的１：殺人、傷害事件捜査

調査媒体：ドラレコ、防カメ

解析内容：

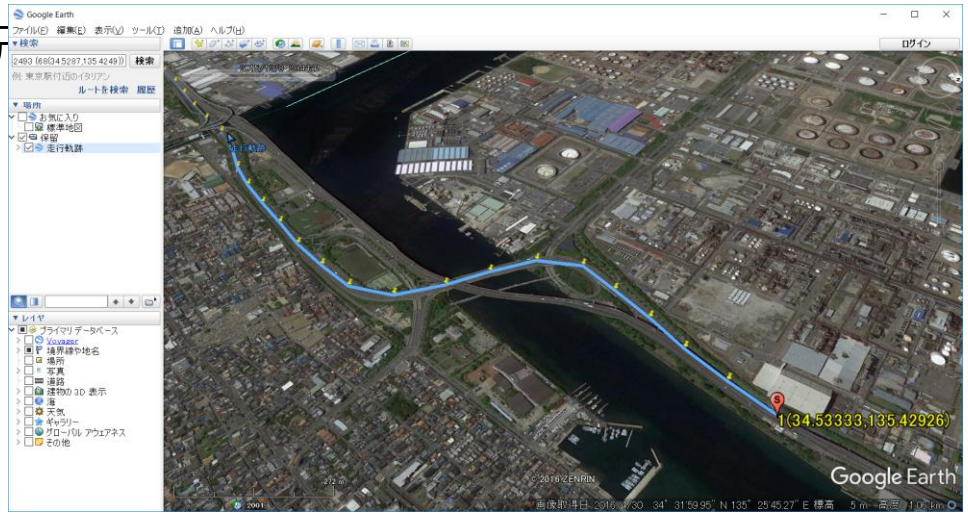
再生できない→事故当時の動画復元（ファイル復元、フレーム復元）

判別できない→画像鮮明化（コントラスト調整など）

調査目的２：盗難車両の足取り調査

調査媒体：カーナビ

解析内容：走行軌跡の抽出・復元



調査目的１：過失割合（事故状況の把握）

調査媒体：ドラレコ、防カメ

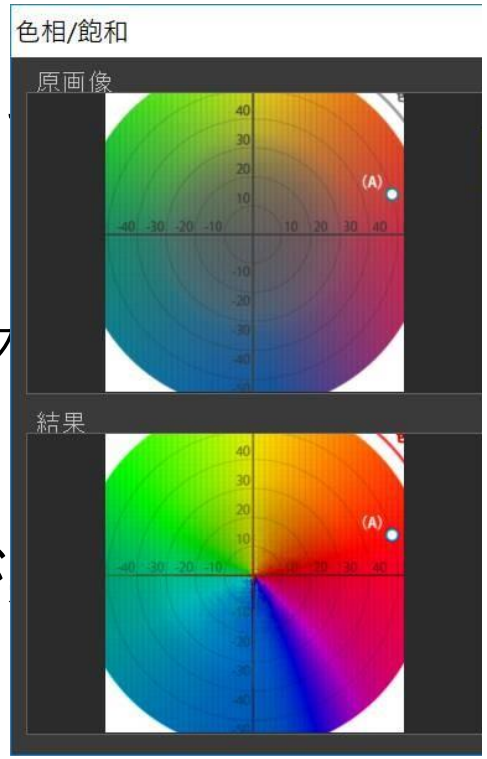
解析内容：

再生できない→事故当時の動画復元（ファイル復元、フレーム復元）

判別できない→画像鮮明化（コントラスト調整、ブレ補正、超解像など）

速度算定→各フレームにおける位置＆フレームレ
出

方向指示器の点滅や信号の色が不明瞭
→輝度/色相判定（数値傾向をグラフ



調査目的２：落下物への衝突
（前方走行トラックからの落下が

調査媒体：ドラレコ

解析内容：物体軌道解析

調査目的：死亡現場までの経緯確認（自殺が疑われる場合）

調査媒体：カーナビ
解析内容：走行軌跡の抽出・復元

調査媒体：ドラレコ
解析内容：
再生できない→事故当時の動画復元（ファイル復元、フレーム復元）
速度算定→各フレームにおける位置＆フレームレートから速度算出

調査目的１：万引き

調査媒体：防カメ

解析内容：　物体寸法計測（対照物との比較）

調査目的２：器物破損（落書き）

調査媒体：防カメ

解析内容：画像鮮明化（破損前との比較）

相談内容

高速道路を走行中、前方から何かが飛んできてフロントガラスにひびが入った。前方を走行していたトラックの荷台からの落下物であるのなら、当該トラックの運転手及びその運送会社にフロントガラスの修理代金を請求したい。

調査方法

被害者の車に設置されていたドライブレコーダーの映像から、

1. フロントガラスにぶつかった飛来物の特定
2. 飛来物が確認できるコマをすべて抽出して軌道を確認
3. 確認できている飛来物の軌道、車自体が前方へ進む速度、空気抵抗、飛来物の移動速度と落下速度の算出
4. 実際の道路状況を3Dマッピングで再現して、飛来物の起点として可能性のある場所からの飛来物の軌道をシュミレーション

といった調査を実施

調査結果

1. 前方トラックの荷台を起点とした場合に、そのままの軌道で飛んでくる場合も、道路にバウンドする場合も本件ひび割れ箇所にあたる可能性がないことが判明。
2. 更に、前方トラックが道に転がっている石を跳ね上げたとしても、本件飛来物の軌道に該当しないことが判明。
3. 軌道と走行速度との兼ね合いにより前方トラックのさらに前方を走行していた車が跳ね上げた石の軌道であれば本件ひび割れ箇所に命中する可能性が高いことが判明。

事件の顛末

前方トラックの運転手及びその運送会社への修理代金の請求はせず。
荷台からの落下物ではなく、跳ね上げられた石が原因であったため、実際に石を跳ね上げた車の運転手に対しても請求せず。

4. 質疑応答

AOS DATA

ご視聴ありがとうございました