

データ復元の達人による 最先端デジタルフォレンジック技術

AIFORENSE JAPAN DATA RECOVERY, INC.
Dai Shimogaito (下垣内 太)

2021年10月21日@zoomウェビナー

主催・共催：SYSCOM GLOBAL SOLUTIONS INC. 様、日本クラブ様、JCCI NY様

データ復旧とは

通常の方法ではアクセス不能なデータを救出すること



講師略歴 – 下垣内 太 （しもがいと だい）

・ アイフォレンセ日本データ復旧研究所（株） 代表取締役

- ・ 大阪データ復旧 - 梅田・大阪駅前第4ビル（創業1998年）
- ・ New York, U.S.A. – AIFORENSE JAPAN DATA RECOVERY, INC.

・ 一般社団法人 日本データ復旧協会 常任理事

・ デジタル・フォレンジック研究会 会員

- ・ データ消去分科会、医療分科会、DF人材育成分科会

・ 特許&受賞

- ・ ハードディスクの動作を制御するための方法及びハードディスクドライブ（特許第6398023号）
- ・ デジタル・フォレンジック研究会「研究開発賞」受賞（2018年）

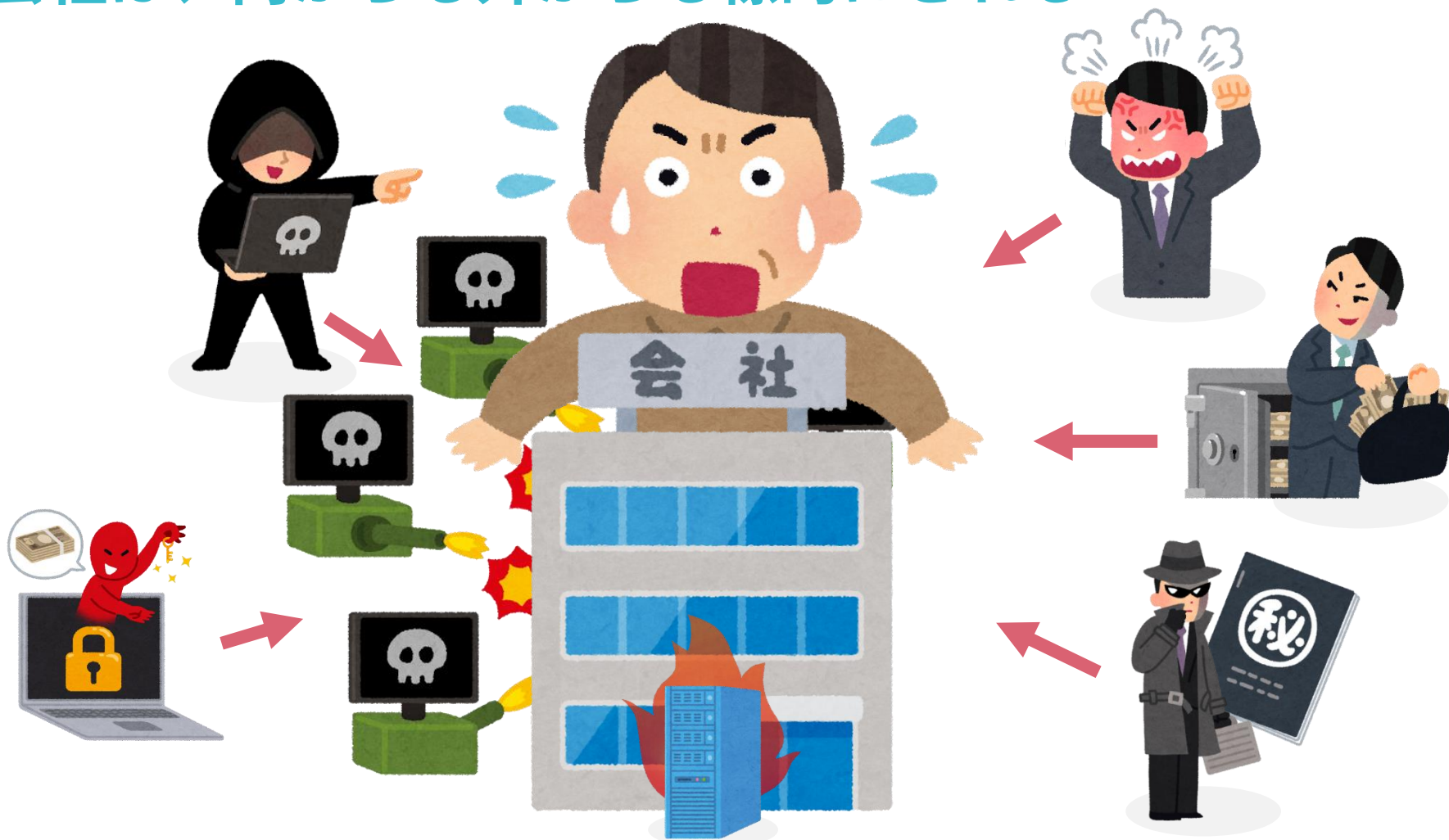
・ 主な講演歴

- ・ 国際カンファレンス（CODE BLUE、HTCIA）、国内カンファレンス（SECCON、IDFコミュニティ）、地域勉強会及び捜査機関での講演など



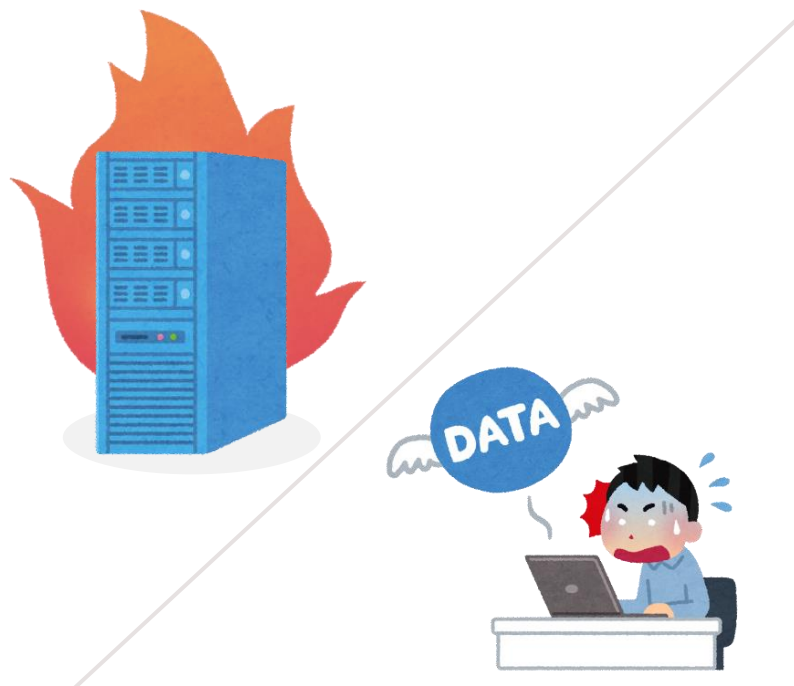
データ復旧：味方だった敵に対峙する武器を得る

会社は、内からも外からも標的にされる



企業におけるデータ復旧の必要性

システム障害・事故



業務の復活

不正・労使トラブル



裁判の証拠

相談：消えたエクセルを復旧してほしい



相談：消えたエクセルを復旧してほしい

無事復旧に成功 & 依頼者の潔白も証明

デジタルフォレンジック 解析調査報告書

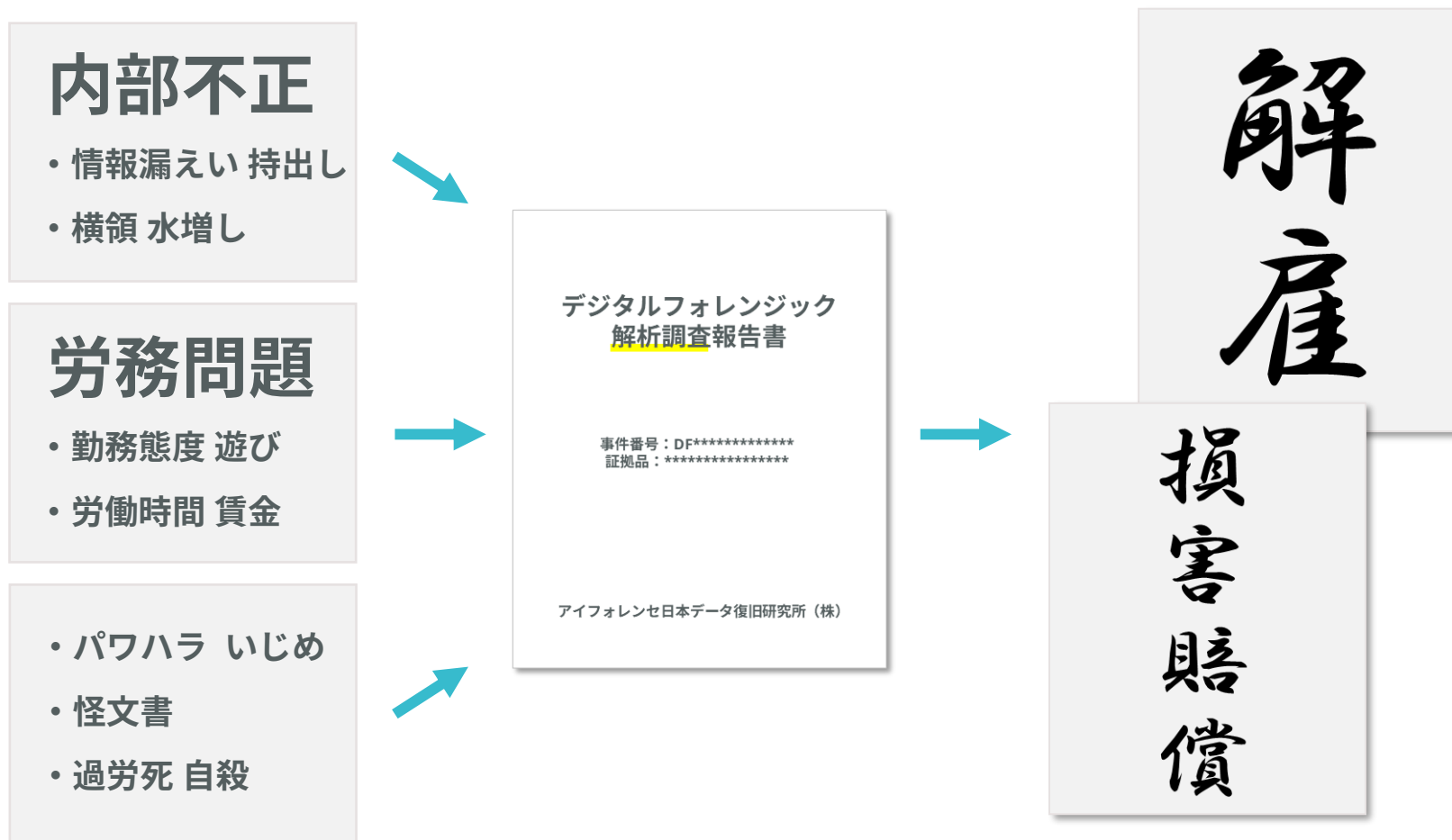
事件番号：DF*****
証拠品：*****

アイフォレンセ日本データ復旧研究所（株）



企業、官公庁、大学、医療機関での不正調査

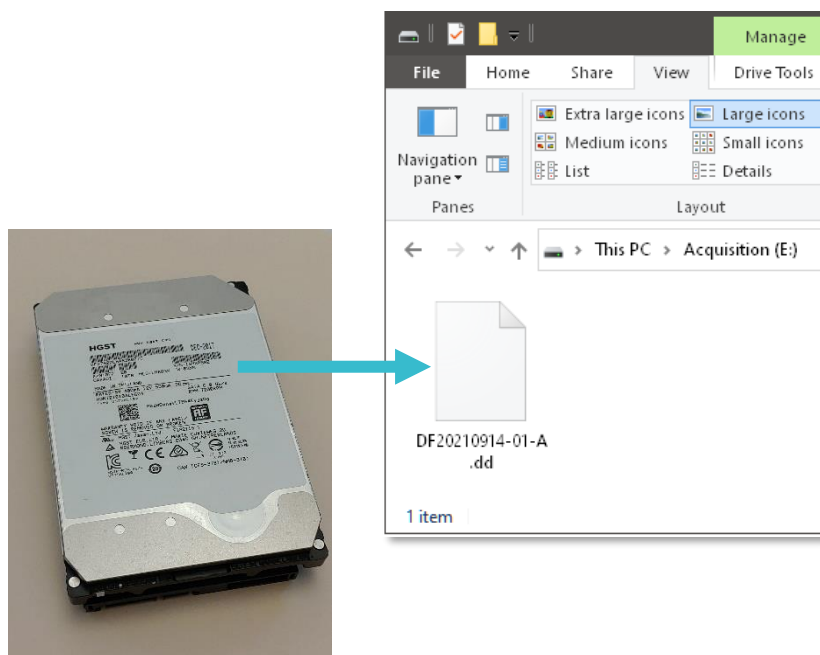
調査報告書は、解雇や損害賠償の根拠



ディスク保全（証拠保全）

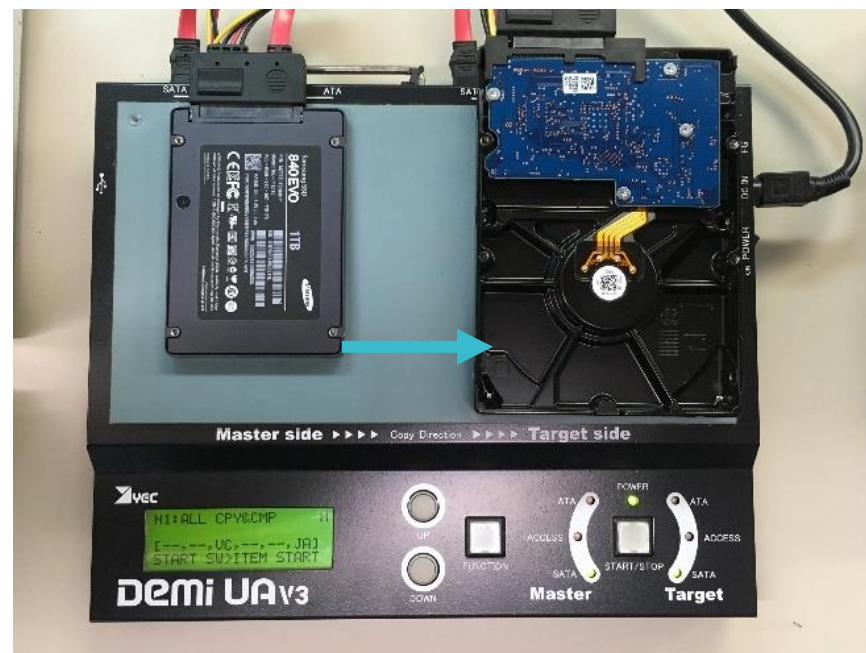
ディスク イメージ

- HDDやSSDをファイル化



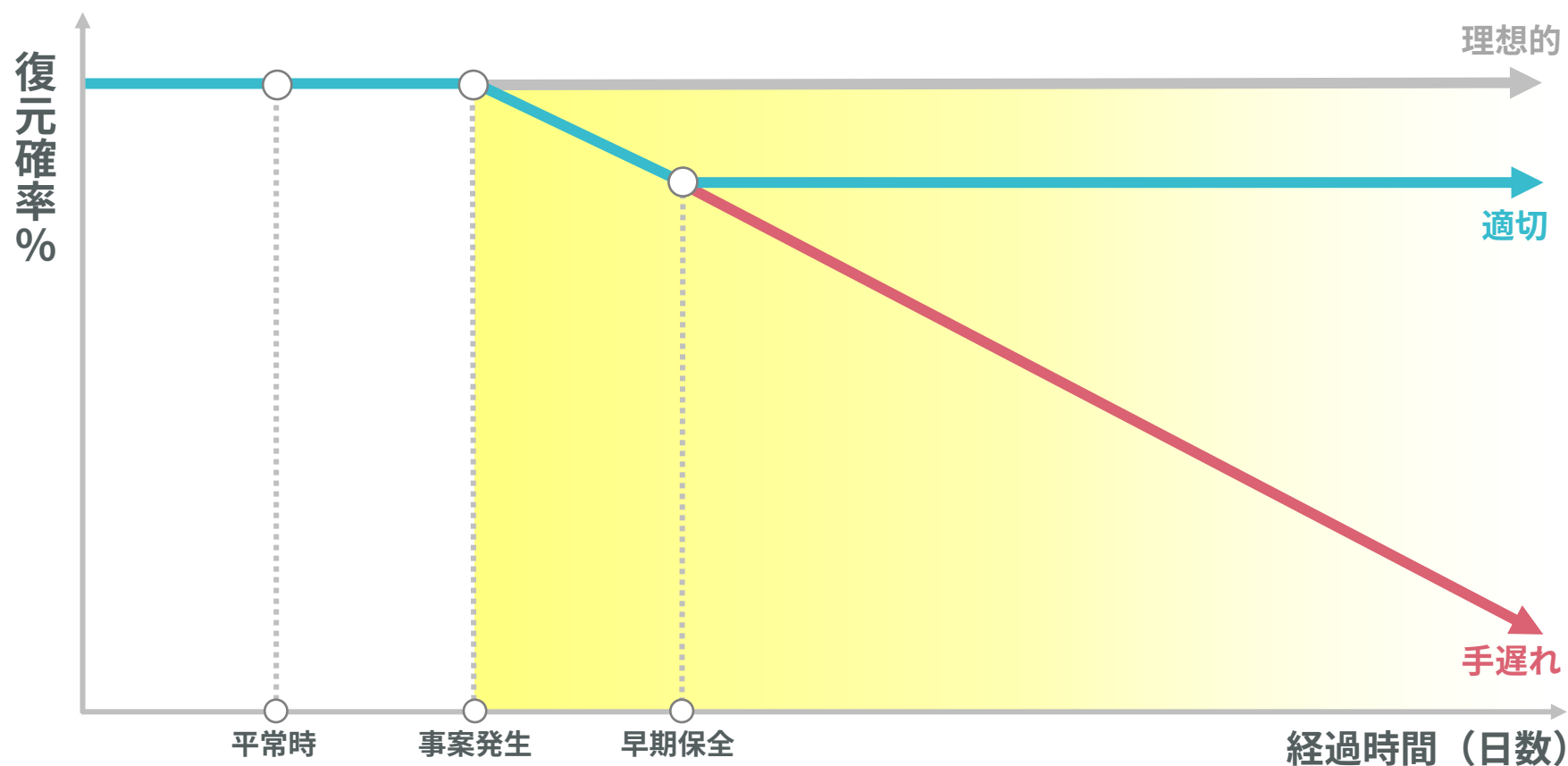
ディスク クローン

- HDDやSSDを別ドライブに複製



ディスク保全（証拠保全）

時間の経過によるデータの劣化を止める



経営判断の原則

証拠（ディスク）保全のタイミングは事実認識に影響する

取締役の判断の前提となった事実認識に不注意な誤りがなく、判断の内容に著しく不合理なものがない限り、善管注意義務違反または忠実義務違反を認定すべきでないとする考え方

取締役は善管注意義務を怠った場合、損害を賠償する責任を負う

ランサムウェア被害によるデータ消失

サイバー攻撃：ランサムウェア犯罪の増加

- 「情報セキュリティ 10大脅威 2021」

IPA 情報処理推進機構

<https://www.ipa.go.jp/security/vuln/10threats2021.html> ※閲覧日：2021年8月31日

順位	組織	昨年 順位
1位	<u>ランサムウェアによる被害</u>	5位
2位	標的型攻撃による機密情報の窃取	1位
3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
4位	サプライチェーンの弱点を悪用した攻撃	4位
5位	ビジネスメール詐欺による金銭被害	3位



ランサムウェア被害（サイバー攻撃）

奈良県宇陀市立病院 2018年10月16日 発生

- ・ 影響した患者数：1,133名
- ・ データのバックアップはとられていなかった（ミス）



調査報告書 P.12 「有識者会議の見解」より抜粋

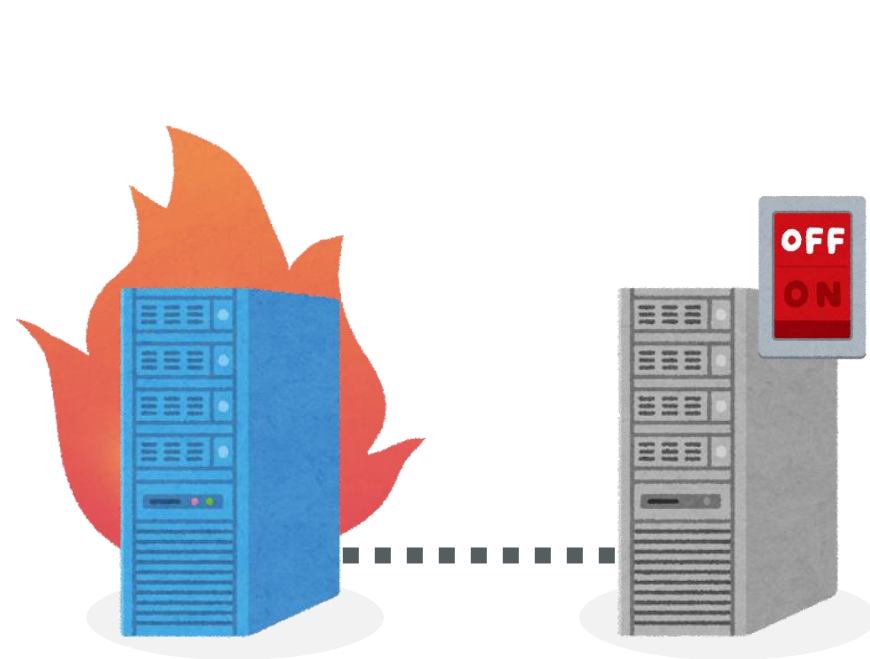
“初期対応が不適切であり、**証拠保全の観点**が欠落していた
との指摘”

データのバックアップ体制

災害級の障害 & ランサムウェア被害を前提に構築



遠隔地



オフライン

ランサムウェア被害（サイバー攻撃）

奈良県宇陀市立病院 その後

- ・ 暗号化されたカルテデータは2019年3月に復元に成功
- ・ 身代金は支払わず
- ・ データ情報システム管理室長が2019年10月に自殺



調査報告書 P.16 「2 本件の原因等」より抜粋

“遺書の内容から私的な問題ではなく、**職場の業務、職責に関するものである**と思われる。”

データ消失の初動対応の流れ

ディスク保全是鉄則 & 予備解析や復旧計画を立案

1. データ消失事案 発生
2. ディスク保全
消失した状態を、そのまま複製
3. 予備解析
事故環境の再現データで予備解析
4. 復旧計画の立案
IT担当者からの情報に基づき意思決定
5. 被害データ解析・復旧に着手



本番機で実験して
失敗すると
取り返しがつかない



データ消失：よくある失敗後の相談

ディスク保全せずに、データ復旧ソフト使用



不正調査：機密情報を社外で開示

社外秘のデータを転職活動に活用

- ・ 面接日の行動を裏付ける証拠を探してほしい
- ・ 結果：社外WiFi接続とパワポの操作履歴を解明



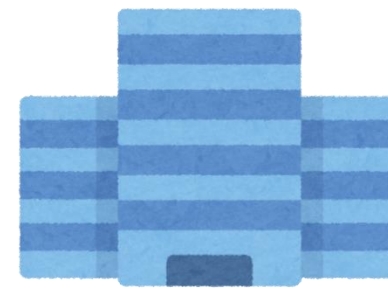
不正調査：営業データの持ち出し

現社員 & 元同僚が価格情報を不正利用

- ・ 損害賠償請求と刑事告訴に使える証拠を復元してほしい
- ・ 結果：ファイルのアクセス履歴とデータ持ち出し経緯を解明



元 勤務先



現 勤務先

不正調査：詐欺・横領

元社員による不正な不動産売買契約

- ・ 削除されたワード文書を復元してほしい
- ・ 結果：署名&押印済み契約書のスキャン画像を復元

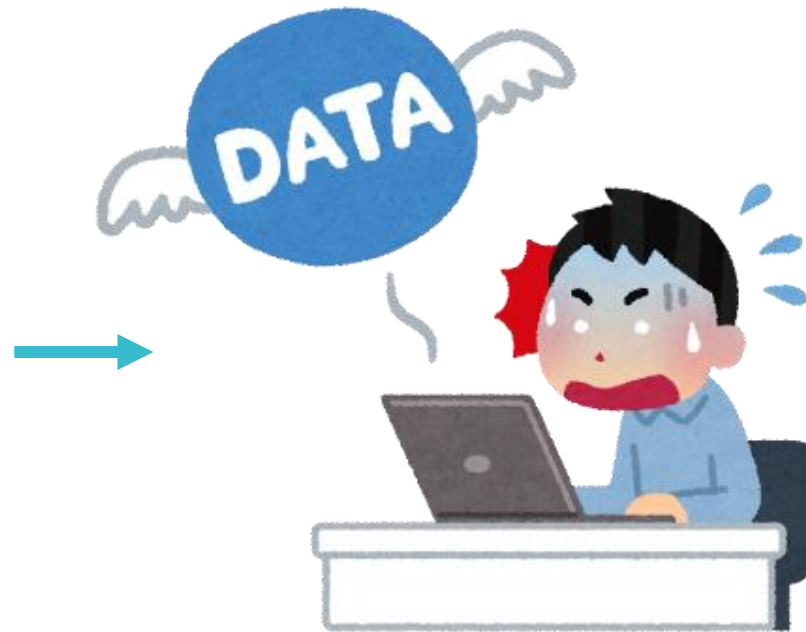


不正調査以外：デジタルデータ解析事例

プロカメラマンの消失データ復旧



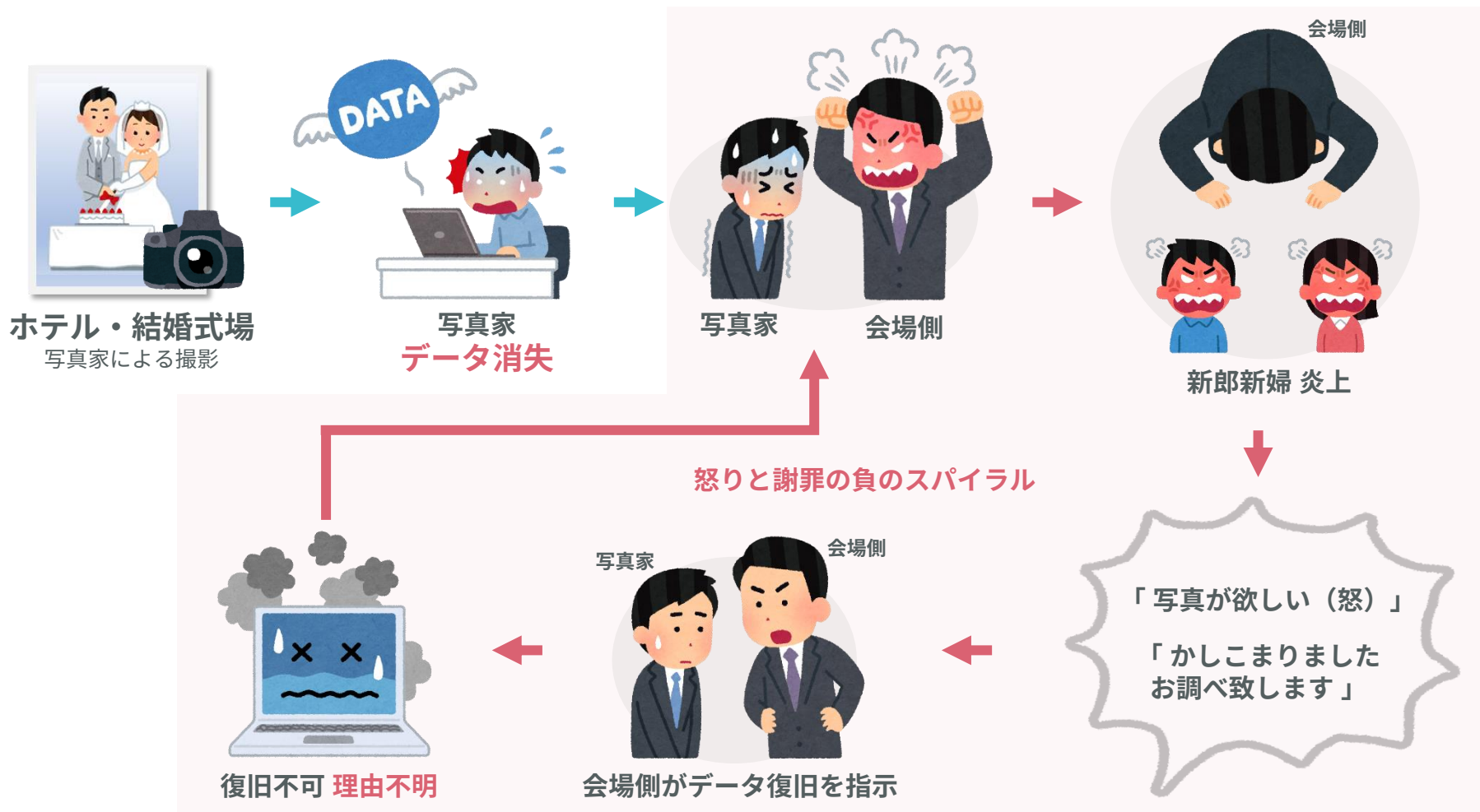
ホテル・結婚式場
写真家による撮影



写真家
データ消失

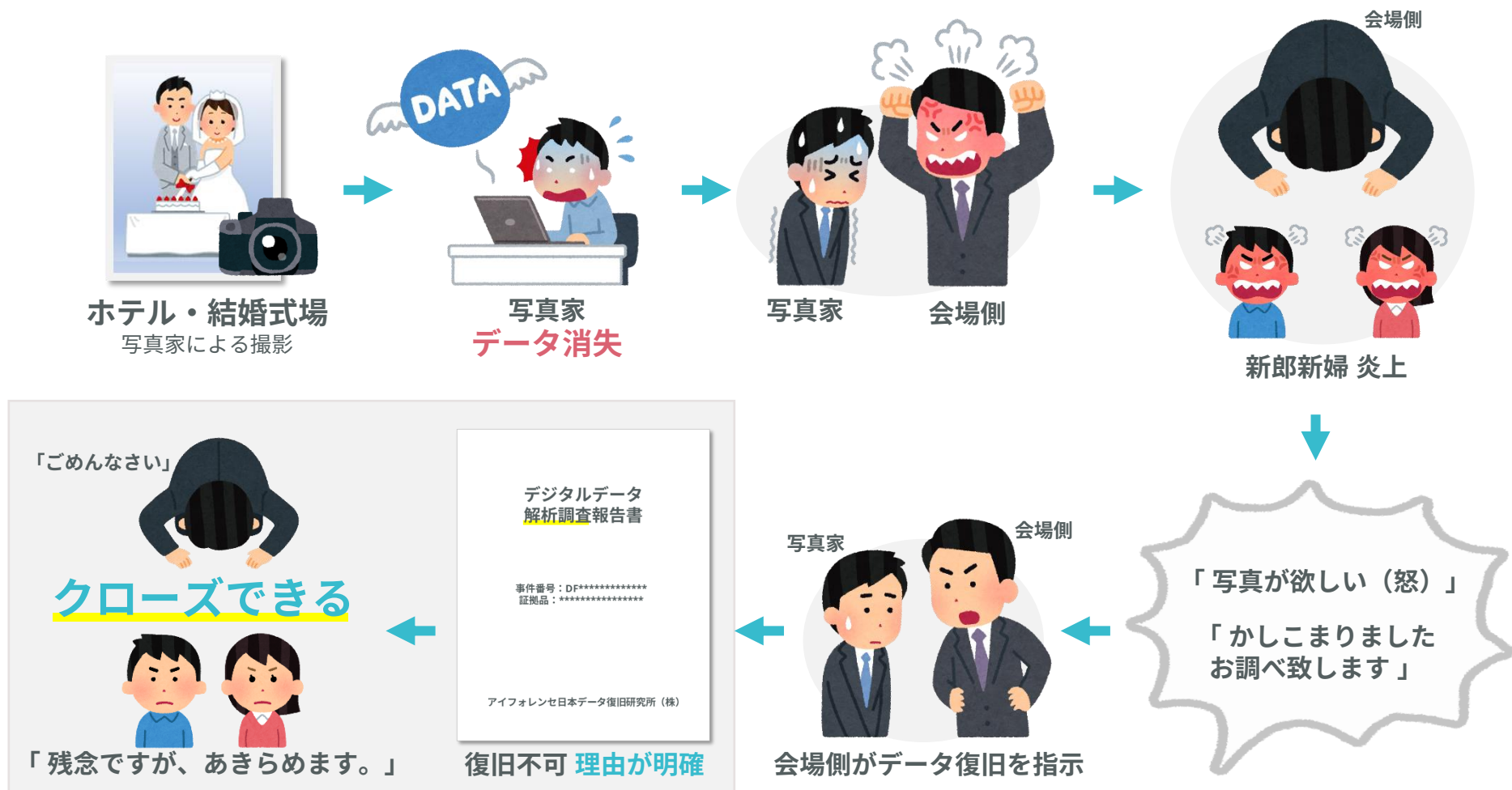
不正調査以外：デジタルデータ解析事例

データ復旧できない理由が不明なとき



不正調査以外：デジタルデータ解析事例

データ復旧できなくても、理由が明確なとき



労使問題：過剰な残業代の不正請求

経費や残業代の水増し請求を退ける証拠

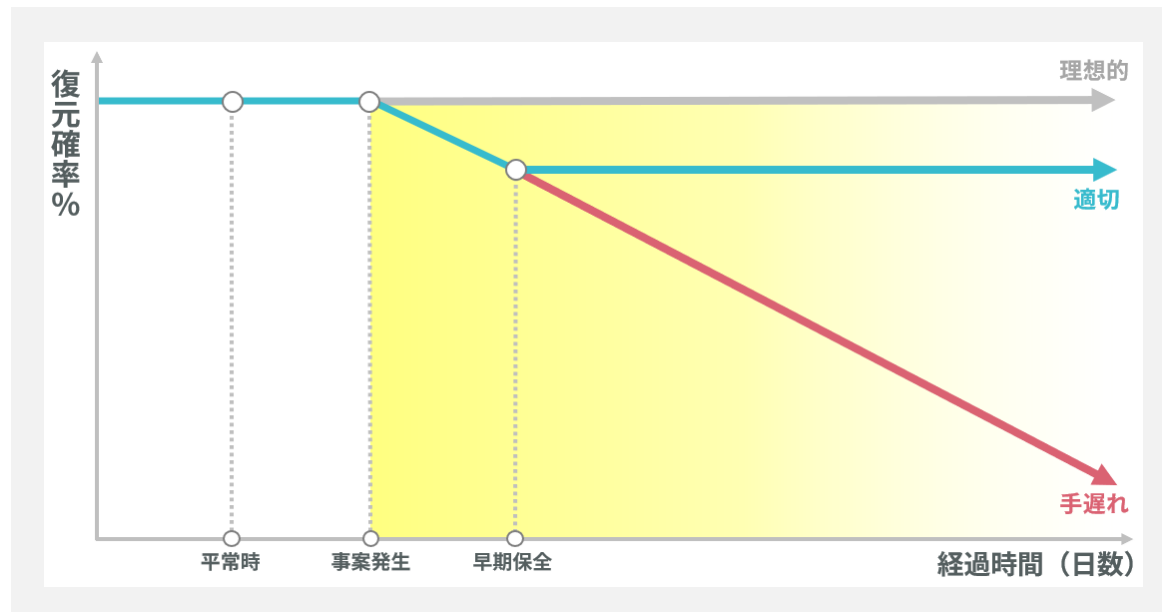
- ・ 就労実態を調べて欲しい。
- ・ 結果：職務専念義務違反の証拠を集めて、立場逆転



労使問題：自殺、過労死、いじめ、ハラスメント

会社は証拠を隠滅した疑いをかけられる

- 原因を知りたい。真実を知りたい。
- 傾向：被害者はもちろん、会社も、かなり疲弊する。長期化しがち。



デジタルデータの解析調査

トラブル対応の切り札

デジタルデータ 解析調査報告書

事件番号：DF*****

証拠品：*****

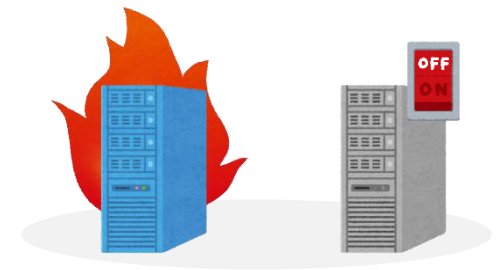
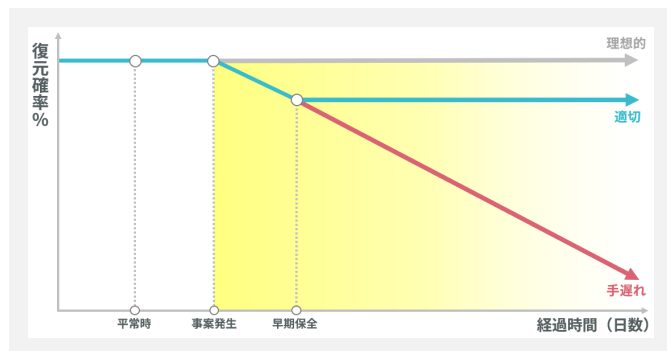
アイフォレンセ日本データ復旧研究所（株）



本日のまとめ

データ消失・不正事案の対策と初動対応

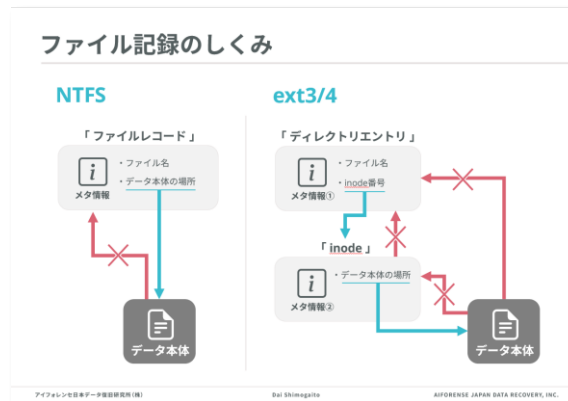
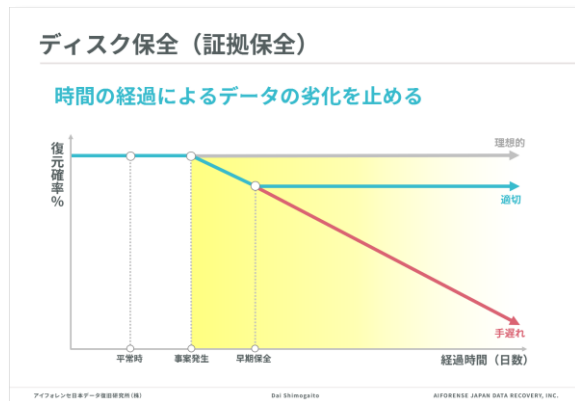
1. ディスク保全（証拠保全）は鉄則。早期ほど有益。
2. 小さな事件、大きな事故、トラブルの規模は関係なし。
3. ランサムウェア被害も前提としたバックアップを。



講義：経営者＆管理者・IT技術者・法律＆弁護士

各分野の専門家を対象としたデータ復旧・DFの講義

どうぞお気軽にお問合せください。講演時間は柔軟に対応致します。



ランサムウェア攻撃によるデータ消失

ファイルサーバの主なファイルシステム

- ・NTFS
Windows
- ・ext2/3/4
Linux（QNAPなど）
- ・XFS
Linux（NAS：Buffalo LinkStation, TeraStation, IO-DATA LAN DISKなど）

- ・ファイルシステムにより、削除のしくみが異なるので、復旧の見込みも変わる。
- ・弊社での対応実績では、NTFS、XFS、ext3、ext4の計4種がほとんど。
- ・被害側からの相談時には、ファイルシステム種別が明確でないことが多い。
- ・物理サーバだけでなく**仮想サーバの被害相談も**。

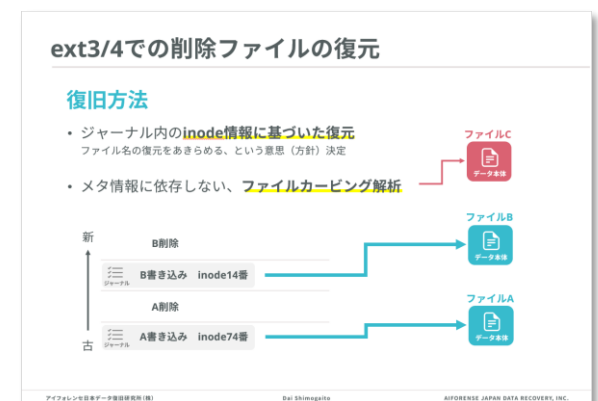
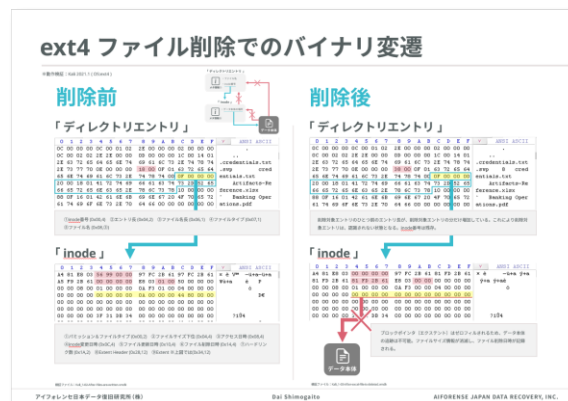
アイフォレンセ日本データ復旧研究所（株） Dai Shimogaito AIFORENSE JAPAN DATA RECOVERY, INC.

不正調査：開発データの持ち出し

製品の図面データを開発担当者が社外へ持ち出し

- ・図面データの流出や不正な複製がないかを知りたい
- ・外部デバイスへのファイル転送経緯を解明

アイフォレンセ日本データ復旧研究所（株） Dai Shimogaito AIFORENSE JAPAN DATA RECOVERY, INC.



講演・面談・取材について

お気軽にお問い合わせください

- **ご所属の組織向けの講演や講義も承ります。**

テーマ：データ復旧、デジタル・フォレンジック、データ消去、不正調査

対象：経営層、法律専門家、捜査機関、金融機関、カメラマン、IT専門家など

※講演時間や内容は調整可。

- **将来的なトラブルに備えた事前面談**

個別のご挨拶と事案対応の流れや料金のご説明

- **お困りごとのご相談**

現在発生している事案対応のご相談

セカンドオピニオン

- **新聞、TV、ネット等、マスコミ取材**

お気軽にお問い合わせください

アイフォレンセ日本データ復旧研究所（株）

大阪市北区梅田1-11-4-1000 大阪駅前第4ビル10F

<https://www.daillo.com/>

AIFORENSE JAPAN DATA RECOVERY, INC.

171 East 74TH ST. C4, New York, NY 10021

<https://aiforense.com/>

本日の講演者：下垣内 太（しもがいと だい）

dai.shimogaito@aiforense.com

<https://www.facebook.com/dai.shimogaito/>

主な講演実績 (敬称略)

国際カンファレンス (開示可のみ)

• CODE BLUE 2013

世界トップクラスの専門家による情報セキュリティ国際会議「CODE BLUE」で研究発表「ハードディスクのディザスタリカバリとファームウェア改竄攻撃への対応策」

• HTCIA 2016

ハイテク犯罪捜査に関する国際会議 (HTCIA、米国) にて研究発表「EXOTIC DATA RECOVERY & PARADAIS」

• CODE BLUE 2016

世界トップクラスの専門家による情報セキュリティ国際会議「CODE BLUE」で2回目となる研究発表「EXOTIC DATA RECOVERY & PARADAIS」

国内での主な講演など (開示可のみ)

• デジタル・フォレンジック研究会

第11期総会「安全性の高いデータ復旧技法 (HiDR) とディザスタデータリカバリ」2014年5月

• ディアイティ

フォレンジック最前線セミナー【フォレンジックを極める】にて講演「デュプレータで読めないデータを獲得する方法」2014年8月

• 兵庫県警察本部

「サイバー攻撃の解析及び犯罪捜査 (デジタルフォレンジックス) へのデータ復旧技法 (HiDR) の活用」2015年10月

• 三重県警察本部

「世界最先端のデータ復旧技術と徹底的なデジタルデータ解析法」2016年2月

• 警察庁情報通信局情報技術解析課

「HDDの完全データ消去が不可能な理由としくみ」2016年12月

• 第14回デジタル・フォレンジック・コミュニティ2017 in TOKYO

パネリストとして登壇。「攻めのフォレンジック」2017年12月

• 一般財団法人 関西情報センター (KIIS)

サイバーセキュリティ研究会第10回サロンに招へいされ講演「リスクマネジメントと危機管理のためのデータ復旧」2018年6月

• 滋賀県警察本部

「故障したデジタル証拠品解析の実例紹介とHDDの完全消去 (保全) に関する誤解」2019年2月

• デジタル・フォレンジック・コミュニティ2019 in 関西

「不正解明の可否が分かれたデジタル・フォレンジック基点での境界線」2019年2月

• 警察庁情報通信局情報技術解析課

「故障したデジタル証拠品や消去済みデータ解析の実例紹介」2019年2月

• 大阪地方検察庁DFセンター

「故障したデジタル証拠品や消去済みデータ解析の実例紹介」2019年7月

• 兵庫県警察本部

「事件性のある壊れたデジタル証拠品や消失データ復元の解析実例」2019年8月

• SECCON 2019

パネリストとして登壇。「セキュリティ業界におけるフォレンジックという仕事のいまとこれから」2019年12月

• デジタル・フォレンジック・コミュニティ2020 in 関西

講演「災害復興支援とフォレンジック」2020年2月

• データベース・セキュリティ・コンソーシアム

第16回DBSC春のセミナーにて基調講演「ハードディスクドライブの完全データ消去が不可能な理由を知る」2020年6月

• 第17回デジタル・フォレンジック・コミュニティ2020 in TOKYO

「HDD、SSD等のデータ消去の課題とフォレンジック」2020年12月

• FISC (金融情報システム監査等協議会)

「ランサム被害・データ消失・不正の証拠隠滅・情報流出の対処に役立つデータ復旧の基礎知識」2021年9月

• 兵庫県弁護士会 姫路支部

「証拠の復元」2021年9月

主なメディア掲載 (敬称略)

- **産経新聞** 2011年5月
東日本大震災のデータ復旧対応に関する取材対応と記事掲載「高い技術必要 関西でも需要増」
- **日経産業新聞** 2013年9月
関西大学に技術協力した損傷ハードディスクからのデータ復旧に関する記事が掲載「データ 9割以上復旧」
- **読売新聞** 2014年2月
“サイバー犯罪捜査に欠かせない科学捜査、デジタルフォレンジックの世界では有名な技術者”として紹介される
- **NHKラジオ** 2014年2月
セキュリティ専門家として出演
- **共同通信社** 2014年4月
『被災 HDD のトリアージおよび初動対応ガイドライン』について取材され、東奥日報、岩手日報、福島民報、四国新聞で記事が掲載。「被災データ保全へ指針」
- **FNSドキュメンタリー大賞** 2017年9月
『じゃあな、親父～あの川が奪ったもの～』で、被害者のデジカメ写真画像復旧の技術協力と番組出演
- **NHKテレビ クローズアップ現代** 2018年8月
「消えたデータがよみがえる！？ “デジタルフォレンジック”の光と影」に、“データ復旧の達人”として取材協力と出演
- **毎日新聞** 2018年12月
第一面で“警察や国税局からの依頼も舞い込む”、“業界では達人と呼ばれ”と紹介された特集記事が掲載される
- **産経新聞** 2018年12月
同年7月に発生した西日本豪雨で被災したパソコンからのデータ復旧に関する取材依頼と記事掲載
- **朝日新聞、毎日新聞** 2019年12月
神奈川県庁のHDD流出事件について各紙取材対応。朝日新聞や毎日新聞の紙面にコメント掲載。朝日新聞デジタルではトップニュースタイトルにコメント掲載。(2019/12/07 他)
- **読売新聞** 2020年5月
「データ消しても悪事残る、デジタル・フォレンジックの裏側」特集記事に解析作業の写真とコメント掲載 (2020/05/13)
- **毎日新聞** 2021年3月
「消された証拠を追え！捜査に威力 デジタル鑑識」専門企業、破壊PCの検索履歴も復元 (2021/03/08)

主なメディア掲載 (敬称略)



NHKクロズアップ現代+
<https://www.nhk.or.jp/gendai/schedule/>
 Accessed:2018/7/26



読売新聞 (2014年2月16日)



毎日新聞 (2018年12月1日)



読売新聞 (2020年5月13日)