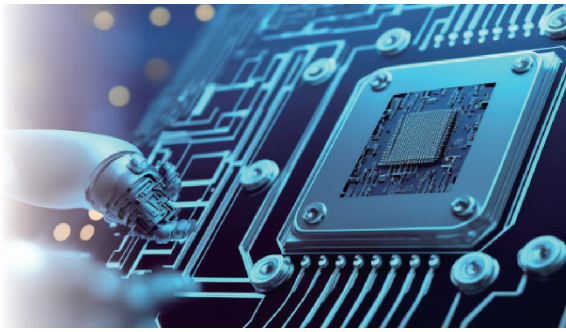
データ復旧事業者を選定する際の注意点
～チェックシートの解説～

応般



北條孝佳 西村あさひ法律事務所
下垣内太 アイフォレンセ日本データ復旧研究所（株）

背景

近年データ復旧に関するトラブル事例が複数発生していたことから，日本のサイバーセキュリティを支える以下の5団体は，**「データ被害時のベンダー選定チェックシート」**[1]（以下**「チェックシート」**という）を作成し，2022年12月16日に各団体のWebサイトにて公開した．また，同日，「NCA Annual Conference 2022」[2]において各団体の代表者が登壇し，パネルディスカッションを行い，周知活動も実施した．

- **（一社）日本データ復旧協会**
- **NPOデジタル・フォレンジック研究会**
- **NPO日本ネットワークセキュリティ協会**
- **（一社）日本コンピュータセキュリティインシデント対応チーム協議会**
- **（一社）ソフトウェア協会**

本稿ではこのチェックシートについて解説する．

データ復旧のトラブル

サイバー攻撃の被害

毎日のように報道されているとおり，企業や病院等（以下**「組織」**という）がサイバー攻撃を受け，甚大な被害が相次いで発生している．しかも，インターネットの特殊性も相まって組織の規模や地域を問わず，サイバー攻撃が可能な脆弱な組織に対する被害が発生しており，すべての組織がサイバー攻撃の対象となっている．その中でも組織が保有するデータを窃取した上で，当該データを暗号化し，データを人質のように見立て，「復号鍵がほしければ身代金を支払え，さもなければ暗号化されたデータは元に戻らず，盗んだデータも公開するぞ」と脅迫するランサムウェア攻撃が後を絶たない．組織が保有する重要なデータが暗号化されてしまい，復号鍵がなければ暗号化されたデータは消滅したのと同じであることから，当該データを業務として活用していた被害組織は，業務停止に追い込まれることになる．

こうした業務停止の被害に陥った状況を打破するには，暗号化されたデータを元に戻し，システムが稼働可能なように復活させて事業を再開する必要がある．このとき，バックアップデータがあれば元通りに戻すこともできるが，ランサムウェア攻撃によってバックアップデータも含めて暗号化されることも多い．そのため，ランサムウェア攻撃を受けた組織は，業務を再開させるためにバックアップデータのない状況下において**「データ復旧」**に取り組むことになる．

データ復旧の問題

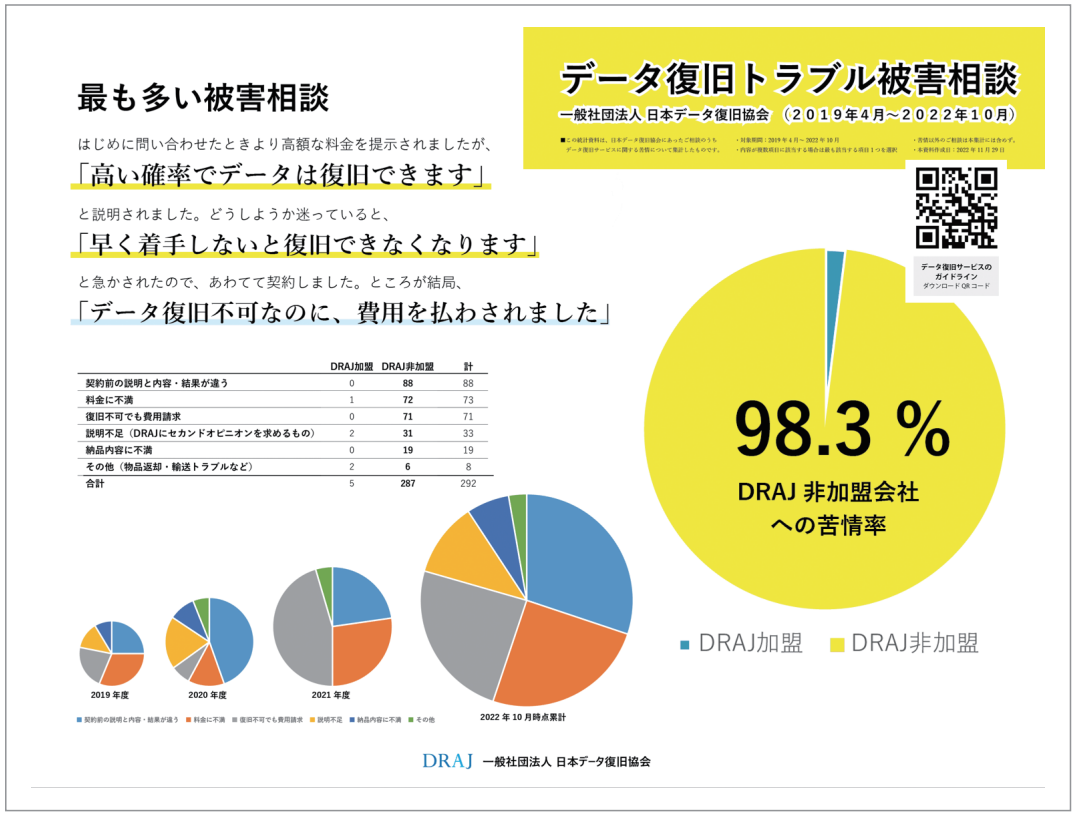
「**データ復旧**」とは，ランサムウェア攻撃によるデータが暗号化される被害に限らず，他のサイバー攻撃，犯罪捜査，不正調査におけるデジタル・フォレンジック調査でも用いられるデータ解析技術の1つである．このような調査等以外にもサーバやパソコンの故障，誤操作により削除されてしまったファイルを復元する際にも活用される．

ところが，データ被害を受けた組織の担当者が，データ復旧事業者に復旧作業を依頼するにあたり，データ復旧事業者が提示する「**復旧率**」や「**復元率**」などの表記の解釈をめぐってトラブルに陥るケースも年々増加している．そのようなトラブルのうちいくつかは，被害に遭った組織の担当者の知識不足というよりも，データ復旧事業者が合理的な根拠のないまま，高いデータ復旧率を提示して広告宣伝を行っていることや，その復旧率について，データ復旧サービスを利用しようとする担当者に理解しやすい説明を行わないまま契約を締結し，利用者の想定する結果が得られないといったことに起因すると，（一社）日本データ復旧協会（以下「**DRAJ**」という）から公表された「データ復旧サービスのガイドライン」[3] に記載がある．

DRAJ には多くの問合せまたは相談が届いているが，そのほとんどはデータ復旧サービスそのものに対する問題である．このデータ復旧サービスの問題に関するもののみを集計したものが図 -1 である．

データ復旧サービスの問題として多いトラブル事例の主な流れは次のとおりである．

1. **最初にデータ復旧サービスを希望する相談者が，データ復旧事業者に電話にて問い合わせると安い金額が提示される．**
2. **相談者は，提示された安い金額での対応を期待して当該事業者にパソコンを預ける．**



	DRAJ加盟	DRAJ非加盟	計
契約前の説明と内容・結果が違う	0	88	88
料金に不満	1	72	73
復旧不可でも費用請求	0	71	71
説明不足（DRAJにセカンドオピニオンを求めるもの）	2	31	33
納品内容に不満	0	19	19
その他（物品返却・輸送トラブルなど）	2	6	8
合計	5	287	292

図 -1
DRAJ へ寄せられた相談

3. 相談者は，パソコンを受領したデータ復旧事業者から，想定以上の見積額を提示される．
4. 相談者が迷っていると，当該事業者から「高い確率でデータは復旧できる」「早く着手しないと復旧できなくなる」などと催促される．
5. 相談者は，大切なデータを復旧してもらうためなら仕方がないと思い，あわてて契約を締結してしまう．
6. 契約締結後，データ復旧事業者から「あいにく今回はデータが復旧できない」等と伝えられ，相談者は，想定以上の金額を請求されてしまう．

このような状況に不満を抱いた方から，DRAJに対して「データの復旧ができないのに，費用を払わされた」「契約前の説明と内容・結果が違う」「他のデータ復旧事業者でも同様なのか」といった相談が寄せられている．

この問題は，データ復旧サービスの料金が高いという側面だけが捉えられがちだが，実はそうではない．「料金が高すぎる」あるいは「料金に不満」ならば，そのデータ復旧事業者のサービスを利用しないという選択も可能である．それにもかかわらず，利用者からDRAJへの相談が減らないのは，金額を考慮してもトラブルを回避できないからである．一番の問題は，利用者が「データは復旧できる前提」で「復旧不可でも費用を支払う内容の契約」を締結してしまうから，データが復旧できない結果となったときに「契約前の説明と内容・結果が違う」という状況になってしまうのではないかと考えられる．

チェックシートの活用

チェックシートの目的

前述したデータ復旧のトラブルに加え，IPA（(独)情報処理推進機構）が毎年発表している情報セキュリティ10大脅威（組織）において，ランサムウェアによる被害が3年連続1位[4]であることが示すように，サイバー攻撃によるデータ被害事例は後を絶たない．ランサムウェアを含むマルウェア等に感染した端末内の削除等がされたデータを復旧するにあたり，利用者がデータ復旧事業者を選定して契約を締結する前に，チェックシートを活用することによって，データ復旧事業者とのトラブルを未然に防止することが可能になると考えられる．もっとも，すべてのトラブル事例を回避できるわけではないため，その点は留意いただきたい．

チェックシートの構成

「データ被害時のベンダー選定チェックシート」はエクセル形式のファイルとして提供しており，誰でも無償でダウンロードが可能である．チェックシートはランサムウェア版と通常版のシートに分かれていて，データ被害の原因がランサムウェア攻撃ではない場合，通常版のシートを活用することになる．

このチェックシートの通常版にはチェック項目が15個あり，ランサムウェア版には19個ある．いずれも利用者がチェックシートを活用するタイミングは，データ復旧事業者を選定する「前」と「後」の2局面に分けて作られている．一般的に，データ被害が発生し，利用者がデータ復旧事業者にデータ復旧を依頼するには，まずデータ復旧事業者を選定することになる．そして，被害データが保存されているパソコン等をデータ復旧事業者に送付する等して契約の締結に向けた段階へ進むことになる．そうした各段階において参照されることを想定し，チェックシートは「依頼前・事業者選定・問い合わせ」におけるチェック項目と「データ復旧着手の事前確認・契約前」におけるチェック項目から構成されている．なお，通常版のチェック項目はすべてランサムウェア版にも含まれているため，以降はランサムウェア版を前提として解説する．

チェックシートの活用方法

各チェック項目に回答欄があり，選択肢は「はい」，

「いいえ」に加え「不明・対象外」の3つが用意されている（図-2）．利用者が，いずれかの回答を選択すると，それに応じてチェックシート最下部にあるリスク判定結果が自動的に集計されて点数で表示される仕組みである．なお，「不明・対象外」を選択した場合は，点数が反映されないことになっている．

各チェック項目には，当該項目が設けられた理由や対応策も解説している．チェックシートは，データ被害が発生した後に活用されることを想定しているが，データ被害が発生した直後は迅速な対応が求められ，チェックシートを活用できない可能性もある．そこで，あらかじめ平時に解説に目を通しておけば，いざというときに，より適切な対処が期待できる．

たとえば，「データ復旧率の高さをデータ復旧の事業者選定の基準にしましたか？」という質問の解説には，「データ復旧率の定義は各社バラバラです．データ復旧率については定まった基準がないため，復旧率だけを鵜呑みにしないように気をつけましょう」との注意喚起を記載し，前述のDRAJが公表した「データ復旧サービスのガイドライン」も紹介している．利用者は，このことを事前に把握しておけば，データ復旧率の高さをデータ復旧事業者の選定基準から除外しておくことができる．

チェックシートの最下部にあるリスク判定結果は100点満点であり，各チェック項目を選択することで当該項目の重要度に基づいて重みづけをした点数が減点される．すべてのチェック項目に回答した後の点数が75点未満の場合，合計点数欄の背景色が黄色に変わり，50点未満の場合は赤色に変わる．これは，利用者が，黄色や赤色になる応対をしたデータ復旧事業者との間で契約を締結してしまうと，トラブルに遭遇する危険性が高いことを示している．特にランサムウェア被害の場合，犯行グループと交渉しないことや身代金を支払わないことを利用者が決定していた場合であっても，データ復旧事業者との間においてこれらの決定事項が示されていなければ，当該事業者が利用者の意思に反して勝手に犯行グループと交渉や身代金の支払いをしてしまうおそれもある．被害組織は，データ被害という大惨事において，他の偶発的なシステム障害と同様の対応をしがちだが，ランサムウェア被害の場合はそ

データ復旧を依頼する前に確認すべきこと(ランサムウェア版)

No.	時期	キーワード	質問	回答選択肢
1	依頼前・事業者選定・問い合わせ	データ復旧	どういう場合にデータが復旧できたといえるかを理解していますか？	いいえ
2		データ復旧	データ復旧は、依頼組織が復旧を希望するデータが復旧しない場合でも、「データは復旧した」とされることがあることを理解していますか？	いいえ
3		復旧率 広告 宣伝	データ復旧率の高さをデータ復旧の事業者選定の基準にしましたか？	はい
4		問合せ 口頭説明	復旧事業者に問い合わせた際に、復旧事業者から、契約前に「復旧できます」などと口頭だけの説明を受けましたか？	はい
5		問合せ 催促	復旧事業者に問い合わせた際に、HDDやSSDをパソコン等から取り外している、または電源を落としているのに、時間の経過とともに、復旧が難しくなると言われましたか？	はい
6		ランサムウェア 復号鍵	ランサムウェア対策サイトで、暗号化されたファイルの復号鍵を入手する方法を試しましたか？	いいえ
			データ復旧の事前確認として、契約前に復旧事業者に対象機器を送付して確認しても	

■図-2　データ被害時のベンダー選定チェックシート（一部抜粋）

うではない．データ復旧事業者の選定および契約締結前において，特に契約内容の確認を怠ったばかりに後になって不要なトラブルに発展しかねないことは誰もが避けたいことであろう[5]．

リスク判定の結果，背景色が変わらない応対をした（トラブルに遭遇する危険性が高くない）データ復旧事業者であっても，トラブルがまったく発生しないわけではない点には注意してほしい．チェックシートはあくまで注意すべき項目を分かりやすく示すために設計された基準であり，万能ではないからである．データ被害の発生時は緊急事態であり，平常心を保った判断が困難なことも少なくなく，時間的にも精神的にも余裕がない状況である．そうであるからこそ，データ復旧事業者との契約を締結するまでの限られた時間内に，利用者が短時間のうちにリスクを判断できるよう設計されたのがこのチェック項目であり，チェックシートである．

繰り返しになるが，データ被害時におけるデータ復旧事業者とのトラブルを避ける最大のポイントは，契約を締結する前にデータ復旧事業者をチェックすることである．多くの相談事例では契約を締結した後に，トラブルに発展したことを認識するが，契約内容を理解した上で契約を締結しているのであるからこれに従う必要があり，手遅れとなるケースも多い．しかも，利用者からの相談事例は年々増加傾向であるにもかかわらず，このような問題が発生していること自体あまり知られていないため，周知すべきという課題もある．

チェックシートの活用に期待すること

データ被害時のトラブルをできるだけ減らすには，より多くの利用者へ周知することが肝要である．そのため，このたび，日本のサイバーセキュリティを担う5団体が，初の合同連携により「**データ被害時のベンダー選定チェックシート**」を作成し，公開するに至ったものである．本稿を含め，このチェックシートをより多くの組織に活用していただけるよう，さまざまな呼びかけを実施していきたいと考えている．そして，このチェックシートを活用することによって，1件でもデータ復旧に関するトラブルに遭う組織が減ることを願っている．

参考文献

1) 2022年12月16日「データ被害時のベンダー選定チェックシート Ver.1.0」https://digitalforensic.jp/higai-checksheet/
2) 2022年12月16日「Nippon CSIRT Association Annual Conference 2022」にて「パネル：インシデント発生時のデータ復旧の課題と対応」https://annualconf.nca.gr.jp/program/day2/1600_1650/
3) 2022年6月28日「データ復旧サービスのガイドライン」https://www.draj.or.jp/wp-content/uploads/Data_recovery_service_guidelines.pdf
4) IPAが公表した「情報セキュリティ10大脅威2023」(https://www.ipa.go.jp/security/10threats/10threats2023.html),「情報セキュリティ10大脅威2022」(https://www.ipa.go.jp/security/10threats/10threats2022.html),「情報セキュリティ10大脅威2021」(https://www.ipa.go.jp/security/10threats/2021/2021.html)の各組織に対するランサムウェアの脅威は1位である．
5) 2023年1月20日に実施された静岡県保険医協会セミナーの「医療機関に対するサイバー攻撃の実態と，事例から見える教訓，直ちに行うべき対策について」資料58-61ページでは，徳島県半田病院のランサムウェア事件において，同病院は犯行グループに対して身代金を支払わない方針を決めており，身代金を支払った事実もないとしながらも，委託先事業者が身代金を支払った可能性があるとされている．https://www.shizuoka-hk.org/cmsdesigner/dlfile.php?entryname=news&entryid=00389&fileid=00000001

(2023年4月10日受付)
(2023年5月15日note公開)

■北條孝佳

弁護士．前職は警察庁技官として多数のサイバー攻撃事案の解析，支援，研究業務に10年以上従事．サイバーセキュリティに関する知見を幅広く持ち，企業内における不祥事対応，危機管理対応などを中心に数多くの案件を取り扱う．(一社) 日本コンピュータセキュリティインシデント対応チーム協議会 専門委員，国立研究開発法人情報通信研究機構 招聘専門員，埼玉県警察 サイバー犯罪対策技術顧問，NPO デジタル・フォレンジック研究会 理事等を務める．

■下垣内太

1998年にアイフォレンセ日本データ復旧研究所（株）を創業．消失データの復元・社内不正のデジタル証拠解析・データ消去検証が専門．2018年にはNPOデジタル・フォレンジック研究会から技術開発賞を受賞．CODE BLUEやHTCIAでの研究発表や裁判所・検察・警察での講演実績も豊富．(一社) 日本データ復旧協会 常任理事．