

## ホワイトペーパーシリーズ：

# 大切なデータをランサムウェア被害から守る

～ LAN DISK を活用したデータ保護策のご提案 ～

2022年10月

## 内容

1. 概要.....	3
2. ランサムウェアについて.....	4
3. ランサムウェアへの対策.....	7
4. オリジナル OS 搭載 LAN DISK を活用してデータを守る.....	8
5. 設定手順.....	10
6. 最後に.....	16

本文書は、株式会社アイ・オー・データ機器（以下、「アイ・オー・データ」とします。）が、アイ・オー・データの特定の商品に関する機能・性能や技術についての説明を記述した参考資料となります。当該商品の利用という目的の範囲内で自由に使用、複製をしていただけますが、アイ・オー・データの事前の書面による承諾なしに、改変、掲示、転載等の行為は禁止されます。また、**あくまで参考資料として提供いたしますので、内容については一切保証を致しかねます。**以下の内容をご了承いただいた場合のみご利用ください。

- (1) アイ・オー・データは、本文書によりいかなる権利の移転もしくはライセンスの許諾、またはいかなる保証を与えるものではありません。
- (2) アイ・オー・データは、本文書について、有用性、正確性、特定目的への適合性等のいかなる保証をするものではありません。
- (3) アイ・オー・データは、本文書を利用したこと、または利用しなかったことにより生じるいかなる損害についても責任を負うものではありません。
- (4) アイ・オー・データは、本文書の内容を随時、断りなく更新、修正、変更、削除することがあります。最新の商品情報については、<http://www.iodata.jp/> をご覧ください。

# 1. 概要

2022 年 10 月現在、企業をターゲットとした身代金要求型不正プログラム（以下、ランサムウェア）の被害が継続しています。この被害はクライアント PC 内だけにとどまらず、ネットワークにつながっている NAS やファイルサーバーにも影響を及ぼし、保存されている業務に必要なデータが喪失してしまう危険性があります。

本ホワイトペーパーではまずランサムウェアの解説を行い、次に基礎的な対策を解説します。そのうち当社 Linux ベース OS 搭載 LAN DISK についての、ランサムウェア対策に効果的な設定をご説明いたします。



※当社 Linux ベース OS 搭載 LAN DISK とは

2022 年 10 月現在、当社 LAN DISK H シリーズ、LAN DISK X シリーズ、LAN DISK A シリーズが該当し、コストパフォーマンスに優れかつ分かりやすいユーザーインターフェースを備えた製品です。



## 2. ランサムウェアについて

### 2.1 ランサムウェアとは

マルウェアの一種で、感染したパソコンやそのパソコンに接続した USB ハードディスク、同一ネットワーク上の共有フォルダー（NAS やファイルサーバー）内のファイルを暗号化など様々な方法で使用不能にし、その復帰と引き換えに「身代金（ransom : ランサム）」を要求する不正プログラムです。

感染経路はメール添付やウェブ閲覧など多岐に渡り、現在新種や亜種が数多く出回っているためウイルス対策ソフトでも完全に防ぐことはできません。Windows の履歴管理機能であるボリュームシャドウコピー（VSS）を破壊する（過去履歴に戻れなくする）などの活動を行う高度なタイプも確認されています。

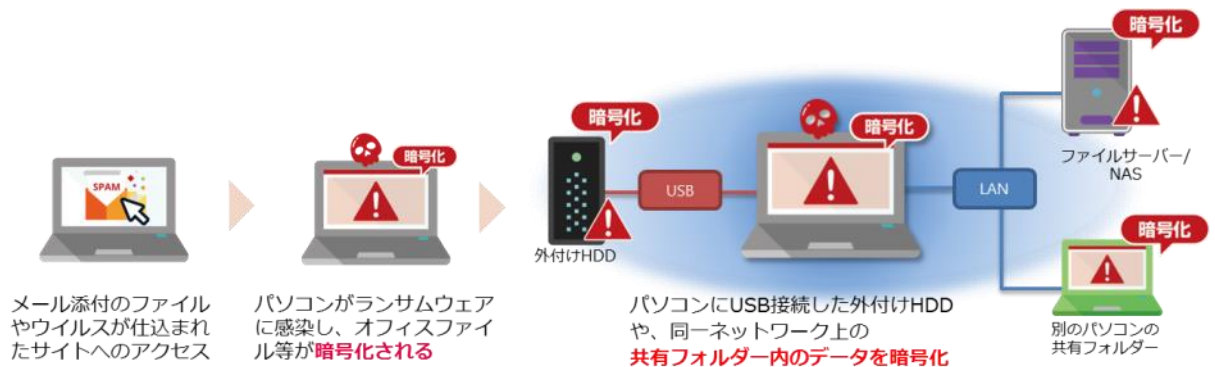
（図の出典元：セキュリティ情報 脅威と対策 | 「ランサムウェア」概要 トレンドマイクロ株式会社）

<http://www.trendmicro.co.jp/jp/security-intelligence/threat-solution/ransomware/index.html>



ランサムウェアが表示する日本語による身代金要求メッセージ例

#### ■ ランサムウェア感染イメージ



ランサムウェアの暗号化対象は、感染した PC のハードディスクだけでなく、外付けハードディスクや感染したパソコンからアクセス可能な全ての NAS やファイルサーバーが対象となります。

⚠ 当社「HDL2-XA/TM シリーズ」などに使用されている NAS のウイルス対策機能では保存されているファイルの暗号化を防ぐことができません。これは、ランサムウェアが直接 NAS に感染するのではないためです。ただし、NAS に保存されたファイルに既知のランサムウェアが含まれていた場合は検出可能です。

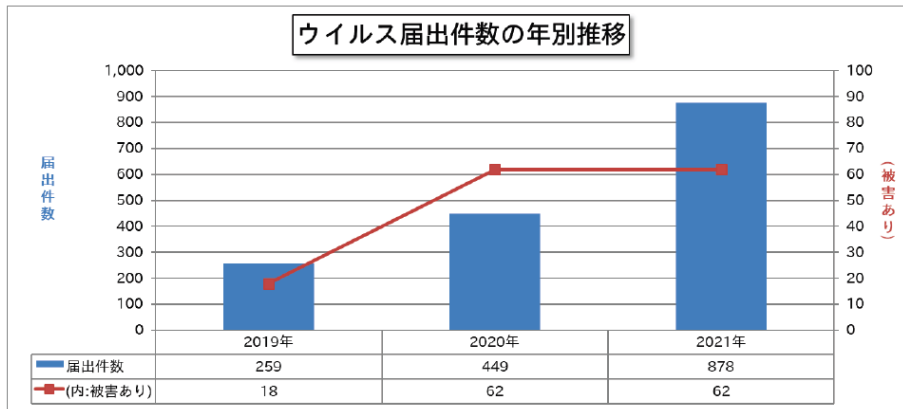


TREND MICRO Trend Micro NAS Security™

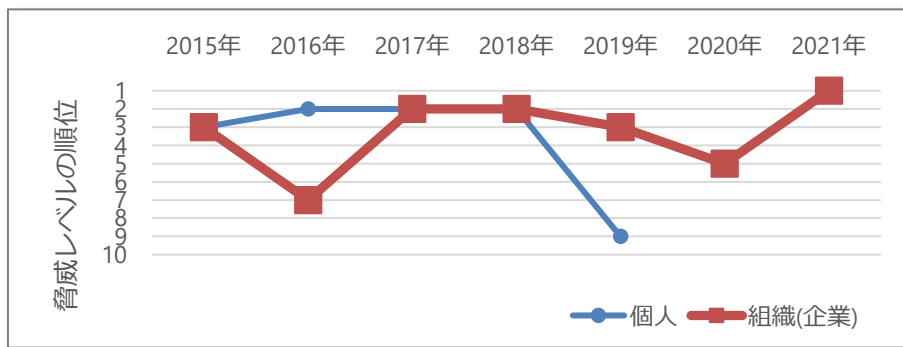
## 2.2 ランサムウェアの被害の特徴

### 感染の爆発的な広がり

ランサムウェアの被害は毎年増え続けています。図は IPA への相談件数推移となります。



### ターゲットは法人



このグラフは、IPS の情報セキュリティ 10 台脅威におけるランサムウェアの順位を抜き出してグラフにしたものです。

2021 年にはランサムウェアは法人に対する脅威の 1 位になっており、ランサムウェアのターゲットが法人にシフトしていている様子が伺えます。

## ランサムウェア被害からのデータ復旧

企業において1台のクライアントPCがランサムウェアに感染するだけで、NASやファイルサーバーに保存されている共有データが暗号化の脅威にさらされます。また、重要なファイルを暗号化された場合、ランサムウェアの被害が業務停止に直結してしまうリスクがあります。

ランサムウェアの被害を受けた場合、請求料金を支払っても暗号化が解除される保証はありませんし、反社会的勢力に資金が流れることに繋がる危険性もあります。確実なファイル復旧方法は、バックアップからの復元となります。

現在までに弊社にお問い合わせいただいた中で、実際に被害にあったユーザー様もバックアップを取られていたケースでは、85%の方がバックアップより被害ファイルを復元されています。

バックアップを行っていたものの、復旧できなかったユーザー様の状況を確認すると、いずれも設定されていたバックアップの「世代数」が少ない、或いはランサムウェア被害発生に気づくのが遅れて世代数を超えたため、バックアップデータの全てが被害後のデータに置き換わってしまっていました。

このことから、バックアップを行う際に重要な要件が浮かび上がってきます。

- 1. 世代管理のできるバックアップ方法でバックアップ設定を行うこと。**
- 2. バックアップは可能な限り多くの世代を取ること。**
- 3. バックアップで複数世代を残すため、十分な容量の外付けHDDを用意すること。**
- 4. ランサムウェア被害を受けたことを早期に把握し、対応を行うこと**

### 3. ランサムウェアへの対策

ランサムウェアへの対策は2種類あります。一つ目はランサムウェア感染防止で、もう一つがランサムウェアの被害にあった際の復旧手段の準備です。まずそれぞれの対策について説明し、次に復旧手段の準備について説明します。

#### 3.1 感染防止と復旧手段の準備

セキュリティ強化を考える際に、感染防止と、万が一セキュリティトラブルが発生した際の復旧手段の準備は分けて考える必要があります。これは、それぞれの対策を実施する対象が異なるためです。感染防止は企業が自発的かつ継続的に実施すべき内容で、社員ひとりひとりに関わる内容です。一方で復旧手段の準備はITインフラ導入時の要件かつ保守運用に関する内容で、機器選定者により検討されるべき内容です。以下に2種類の対策をまとめました。

	感染防止			復旧手段の準備	
	OSおよび利用ソフトウェアを最新の状態にする	セキュリティソフトを導入し、定義ファイルを常に最新の状態に保つ	心当たりのないメールに添付されたファイルは不用意に開かない	定期的なバックアップ	復旧手段の準備
クライアント PC	○	○	○	○	○
ファイルサーバー/ NAS	○	○	-	○	○

IPA 独立行政法人情報処理推進機構 2016 年 1 月 5 日第 16-01-345 号 今月の呼びかけより、弊社作成

<https://www.ipa.go.jp/security/txt/2016/01outline.html>

IPA が発表している「情報セキュリティ対策の基本」は過去から変わることなく、引き続き大きな効果が期待できるとのことです。感染防止策として併せてご参照ください。

攻撃の糸口	情報セキュリティ対策の基本
ソフトウェアの脆弱性	ソフトウェアの更新
ウイルス感染	ウイルス対策ソフトの導入
パスワード窃盗	パスワードの管理・認証の強化
設定不備	設定の見直し
誘導（罠にはめる）	脅威・手口を知る

(出展) : 情報セキュリティ 10 大脅威 2016

<https://www.ipa.go.jp/security/vuln/10threats2016.html>

## 4. オリジナル OS 搭載 LAN DISK を活用してデータを守る

本章では、弊社 Linux ベース OS 搭載の LAN DISK に保存されているデータをランサムウェア被害から守る設定をご案内いたします。

下図のように LAN DISK の履歴差分バックアップを社内ネットワークから直接アクセスできない設定とした外付け USB ハードディスクに行くことにより、ランサムウェア被害からデータを守る手段を用意します。



### 4.1 バックアップのポイント

ランサムウェアは、感染したパソコンから読み書きできるドライブ（内蔵 HDD、パソコンに接続した外付け HDD、共有された NAS）などに保管されているファイルの暗号化処理を試みます。しかし、感染したパソコンがアクセスできない状態のストレージに保管されているファイルには攻撃できません。そのため、バックアップ先をネットワーク経由でアクセスできないようにしておくことで、バックアップデータをランサムウェアによる被害から守ることが可能です。つまり、ファイル共有用途の NAS データを、パソコンから読み書きできない領域にバックアップすることで、ランサムウェアからの脅威を緩和することができます。

#### バックアップ先をネットワーク共有しない

- バックアップ先のネットワーク共有を「無効」にし、共有できない状態になっていることを確認してください。これにより、**感染パソコンからのアクセスがなくなる**ため、ランサムウェアからバックアップ先のファイルを守ることが可能です。

#### 世代管理のできるバックアップ方法でバックアップを行う

- バックアップに**履歴を残しておく**ことで、暗号化されてしまったファイルの前の世代（暗号化される前のファイル）を取り出すことが可能です。
- 暗号化の発覚が遅れるケースを想定して、バックアップ履歴は**可能な限り多く**取っておきます。

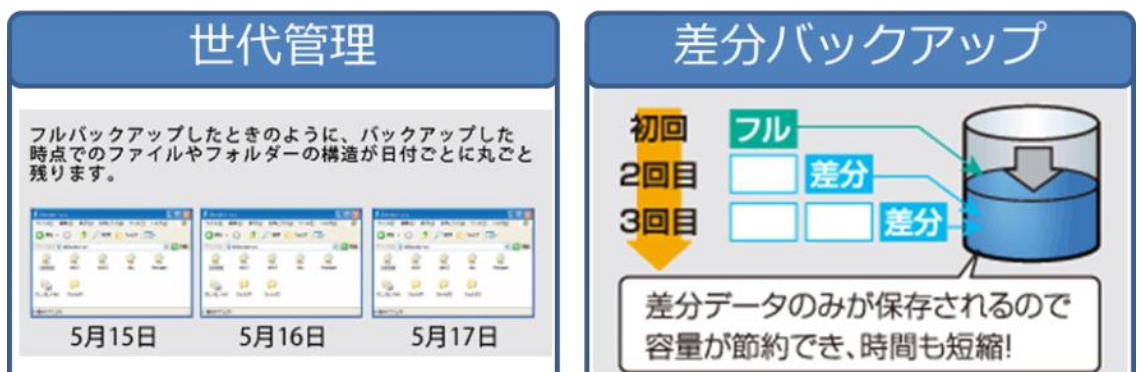


## 4.2 LAN DISK を利用するメリット

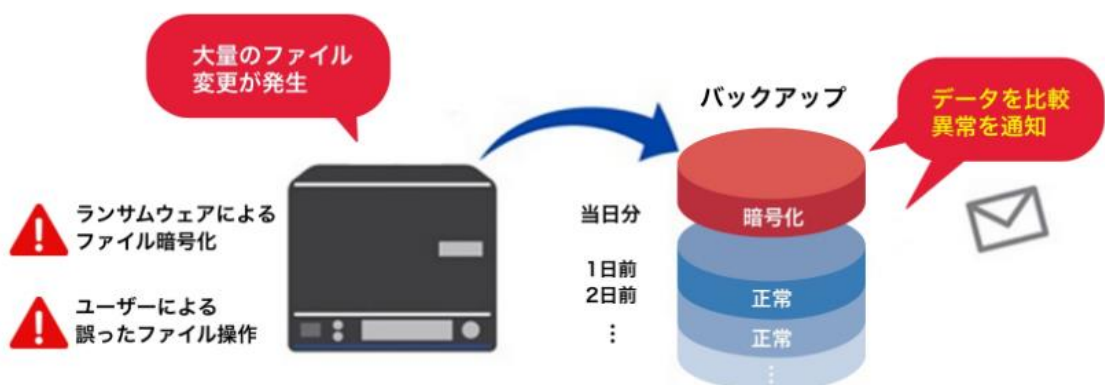
LAN DISK を利用するメリットを以下にまとめます。

導入内容	メリット
導入が容易	<ul style="list-style-type: none"> <li>LAN DISK の標準機能である「履歴差分バックアップ」機能を利用するためアプリケーション費用不要。</li> <li>バックアップ用の外付けハードディスクは比較的安価で、トータルコストを抑えることができる。</li> </ul>
履歴差分バックアップが可能	<ul style="list-style-type: none"> <li>履歴機能により世代管理が可能</li> <li>差分バックアップによりバックアップ容量節約が可能</li> <li>バックアップ先をネットワーク共有しない設定が可能</li> </ul>
ランサムウェア被害発生のアラート検出が可能	バックアップした際に、前回のバックアップデータと内容と比較し、大量の変更が確認された場合はシステム管理者へメール送信を行う「不正ファイル操作検知機能」により、ランサムウェア被害発生をいち早く把握することができます。

履歴差分バックアップ方式は LAN DISK シリーズに搭載されている当社独自のバックアップ方式です。この機能を利用することにより、世代管理とバックアップ容量の節約の両立が可能です。



「不正ファイル操作検知機能」により、ランサムウェア被害発生をいち早く把握できます。



## 5. 設定手順

それでは実際に、ランサムウェア対策のためのバックアップ設定を行っていきます。

まず外付け USB 接続ハードディスクを LAN DISK に取り付け、その後ランサムウェア対策のためのバックアップ設定を行います。最後に万が一の被害発生時に、バックアップからデータを復元する手順をご案内します。

### 5.1 バックアップ設定手順

LAN DISK に USB 接続ハードディスクを取り付けます。その後をランサムウェア対策となる設定を行い、バックアップを行います。

設定手順全体の流れは以下となります。

**[STEP.1] : バックアップ用外付けハードディスクの取り付けとフォーマット**

**[STEP.2] : ランサムウェア対策のためのフォルダー設定**

**[STEP.3] : バックアップ設定と実行**

**[STEP.4] : ランサムウェア被害発生時の復元手順**

# 1.バックアップ用外付けハードディスクの取り付けとフォーマット

最初に LAN DISK にバックアップ用外付けハードディスクを取り付け、フォーマットを行います。  
取り付け可能なバックアップ用外付けハードディスクは、以下のリストを参照してください。

<https://www.iodata.jp/pio/io/nas/landisk/hdd.htm>

フォーマットを行うと、外付けハードディスクの中に保存されていたデータは全て消去されます。外付けハードディスクの中に必要なデータがある場合は、予め取り出して別の場所に保存してください。

外付けハードディスクのフォーマット作業実施中は共有サービスが停止するため、作業前に本製品にアクセスしている方がいないことを確認してから行ってください。



例：HDL2-XA シリーズの場合



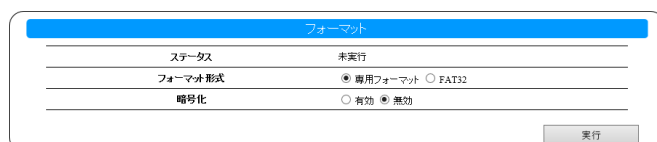
ボリューム



USB3



フォーマット



- ① 外付けハードディスクを LAN DISK 背面にある **USB3.1** ポートに取り付けます。

USB3.1 ポートは青色のポートです。  
この際に、差し込んだ USB ポートに記載している番号を記録しておきます。

左図の例では 3 もしくは 4 となります。

- ② LAN DISK の設定画面を開きます。
- ③ [ボリューム]→[USB **x**]→[フォーマット]と進みます。(※ **x** は USB 接続ハードディスクを取り付けたポート番号)
- ④ [フォーマット形式]で[専用フォーマット]を選び、[実行]をクリックします。

「フォーマットしますか？」と表示されますので、[OK]をクリックします。

フォーマットが開始されますので、完了までしばらくお待ちください。

完了したら次へと進みます。

## 2.ランサムウェア対策のためのフォルダー設定



[共有] → [フォルダー] → [変更] をクリックします。

共有	
名前	① 選択してください ▼
コメント	<input type="text"/>
基本設定	<input type="checkbox"/> 読み取り専用
	<input type="checkbox"/> 非登録ユーザーからのアクセスを拒否
	<input type="checkbox"/> AppleShareネットワーク共有
	<input type="checkbox"/> FTP共有
	② <input type="checkbox"/> Microsoftネットワーク共有

⑤ [名前]表示された選択肢の中から、USB x (※ xは USB 接続ハードディスクを取り付けたポート番号)を選択します。

⑥ [Microsoft ネットワーク共有]のチェックを外します。

ここでのポイントは、[Microsoft ネットワーク共有]のチェックを外すことです。これによりバックアップ用に取付けられた外付けハードディスクは、クライアント PC から直接アクセスすることができません。

## 3.バックアップ設定と実行

次にバックアップ設定を行い、バックアップを実行します。



[データ保守] → [バックアップ] → [追加] をクリックします。

バックアップ	
ジョブ名	① FSS400バックアップ
履歴数	② 14 設定可能範囲[0~52]。0は「制限なし」になります。 バックアップ先に十分な容量があるかご確認ください。 <a href="#">ボリューム情報</a>
スケジュール設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 <input type="checkbox"/> 日 <input checked="" type="checkbox"/> 月 <input checked="" type="checkbox"/> 火 <input checked="" type="checkbox"/> 水 <input checked="" type="checkbox"/> 木 <input checked="" type="checkbox"/> 金 <input checked="" type="checkbox"/> 土 22:00
オプション	<input type="checkbox"/> ゴミ箱も対象にする <input type="checkbox"/> 実行後にシャットダウンする <input type="checkbox"/> 強制フルコピー ③ <input checked="" type="checkbox"/> 多くのファイルに変更があった場合に通知する

① [ジョブ名]バックアップ①ジョブ名称を自由に決めて入力します。

② バックアップの履歴数とスケジュールを決め設定します。

③ [多くのファイルに変更があった場合に通知する]にチェックを入れることにより、不正ファイル操作検知機能を有効にします。

ここでのポイントは以下のとおりです。

1. 履歴差分バックアップで複数世代を残すため、バックアップ先は十分なドライブ容量を選択してください。弊社では、バックアップ元の容量の 2 倍程度を目安としてご案内しております。
2. バックアップの履歴数は、可能な限り多く取るように設定ください。  
長期休暇も想定し、履歴数は [7~14] 以上(1~2 週間以上)を目安としてください。

- ▲ バックアップ先の容量がなくなった場合、バックアップはエラーになります。
- ▲ バックアップ履歴数として設定可能な数値は最大 52 になります。
- ▲ バックアップ履歴数が設定した世代数を超えた場合、最も古い世代が削除されます。

バックアップ元	
対象種別	ローカル(全ての共有フォルダー)▼

- ⑦ [バックアップ元設定]対象種別タブから「ローカル(全ての共有フォルダー)」を選択します。

バックアップ先	
対象種別	ローカル▼
共有フォルダー	usb2▼
サブフォルダー	

- ⑧ [バックアップ先設定]共有フォルダータブから USB x (※ x は USB 接続ハードディスクを取り付けたポート番号)を選択します。

取り外し専用として設定されます。

保存

- ⑨ 最後に右下の[保存]をクリックします。

以上でバックアップの設定は完了です。設定したスケジュールに従い LAN DISK は自動的にバックアップを行います。

## 4.ランサムウェア被害発生時の復元手順

ランサムウェアに感染してしまった場合、まず感染したパソコンはネットワークから速やかに取り外し、初期化など駆除に必要な作業を実施してください。

また LAN DISK に取り付けられている外付けハードディスクも LAN DISK から取り外し、電源を切った状態で保管しておきます。

LAN DISK 内共有フォルダーのデータも暗号化されていた場合は、LAN DISK も初期化してください。

**万が一ランサムウェアが環境内に残っていた状態で復元やデータ取り出しを行おうとした場合、復元作業中に再感染が発生することによって貴重なバックアップデータが失われてしまう可能性があります。**

以下の作業は確実にランサムウェアがご利用の環境内で駆除されたことを確認したのちに行ってください。

## ■ ファイルを個別に取り出す場合

ランサムウェア感染していないパソコンにバックアップデータが保存された USB 接続ハードディスクを直接取り付けることにより、ファイルを個別に取り出すことができます。

読み出しには Windows を搭載したパソコンが必要です。

(1) LAN DISK Backup Reader をパソコンにダウンロードする

当社サポートライブラリ(<https://www.iodata.jp/lib/software/l/1655.htm>)より、読み取りソフト LAN DISK Backup Reader をダウンロードします。

(2) LAN DISK Backup Reader をパソコンにインストールする

- 1.ダウンロードしたファイルをダブルクリックし、実行します。
- 2.解凍したファイルの中にある[Setup.exe]をダブルクリックして実行します。インストールが開始されますので、画面の指示に従って完了させてください。


(3) データを読み出す

### データを読み出す

1 読み込み対象の HDD をパソコンにつなぐ

2 スタートメニューから、  
[(すべての) プログラム] → [I-O DATA] → [LAN DISK Tools] →  
[Backup Reader] → [LAN DISK Backup Reader] の順にクリック

3



①読み込み対象のHDDに  
チェック

②[実行] をクリック  
→ドライブがマウントされます。

※マウントしたドライブが専用フォーマットのボリュームではなかった場合は、ボリュームのチェックを外して [実行] ボタンをクリックしてください。

4 [コンピューター] を開き、  
割り当てられたドライブレターのディスクをダブルクリック

これでデータを読み込むことができます。

LAN DISK Backup Reader を終了させると再び上記 3 の作業を行うまでデータが読み出せなくなりますので、読み出し作業が終了してから LAN DISK Backup Reader を終了させてください。

## ■ バックアップデータの一括復元

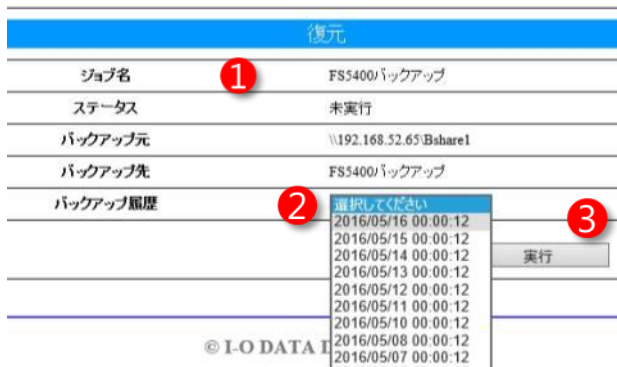
ランサムウェアの駆除が完了した LAN DISK に外付けハードディスクを取り付け、すべてのデータを一括して復元させる手順です。



[データ保守] → [バックアップ] → [一覧] をクリックします。



① 復元するバックアップジョブの右にある [復元] をクリックします。



- ① 復元内容を確認します。
- ② [バックアップ履歴] で復元するバックアップの日時を選びます。
- ③ [実行] をクリックします。

以上、で復元が実行されます。ステータスに [完了 (成功)] と表示されれば、復元完了です。

## 6. 最後に

急激に拡大したランサムウェアですが、企業がターゲットであり、さらに被害を受けた場合に事業へ多大な影響が発生するリスクがあります。さらに、企業側から見ると、全ての従業員に対して脅威への教育が必要であり、対応方法の徹底に頭を悩ませていると思われます。その中で、これまで当たり前のようにやってきたバックアップが復旧手段の最後の砦になっています。

これまで、アイ・オー・データは3つの「安心」を通じて、お客様のデータの安全運用を守る取り組みを続けてきました。この取り組みの中でバックアップの重要性や各種手法を提案してきました。バックアップを正しく行うことが、お客様の業務の安全運用に繋がるだけでなく、セキュリティ課題についても効果があるということが、本ホワイトペーパーを通じてご理解いただければ幸いです。

本ホワイトペーパーが、お客様のセキュリティ確保の一端になれば幸いです。



3つの「安心」ロゴ