進化する明日へ Continue thinking

I-O DATA

ホワイトペーパーシリーズ：

バックアップから始めるセキュリティ

～ ランサムウェア対策のご提案 ～

2016 年 5 月

内容

1. 概要

2016 年 3 月以降、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）の被害が拡大しています。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ます。1 台の PC が感染した結果、全社の業務継続に大きな影響を与えるリスクがあります。

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。最後に既存のファイルサーバーに対して、実業務を止めずに導入できるランサムウェア対策をご提案いたします。

2. ランサムウェアについて

2.1 ランサムウェアとは

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

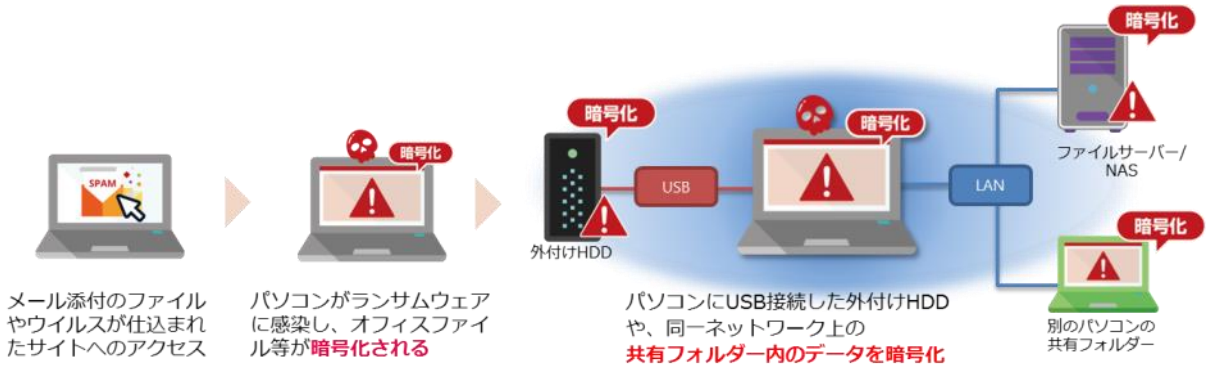
マルウェアの一種で、感染したパソコンやそのパソコンに接続した USB ハードディスク、同一ネットワーク上の共有フォルダー（NAS やファイルサーバー）内のファイルを暗号化など様々な方法で使用不能にし、その復帰と引き換えに「身代金（ransom：ランサム）」を要求する不正プログラムです。

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。

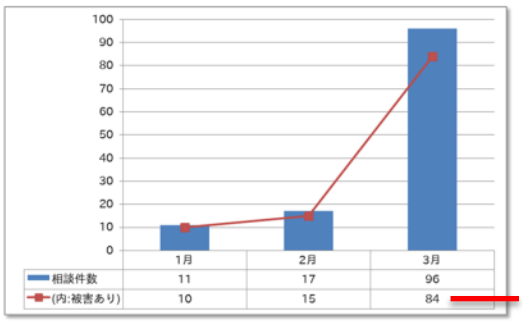
⚠ 当社「HDL2-H/TM シリーズ」などに使用されている NAS のウイルス対策機能では保存されているファイルの暗号化を防ぐことができません。これは、ランサムウェアが直接 NAS に感染するのではないためです。ただし、NAS に保存されたファイルに既知のランサムウェアが含まれていた場合は検出可能です。

LAN DISK H
TREND MICRO
Trend Micro NAS Security™

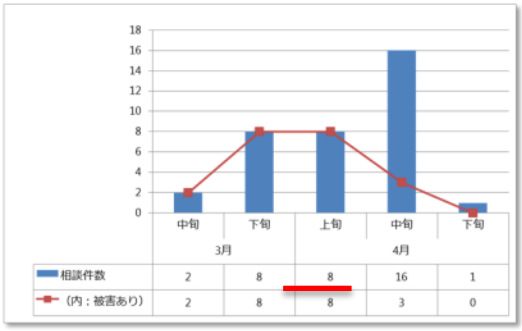
2.2 ランサムウェアの被害の特徴

1. 感染の爆発的な広がり

ランサムウェアの被害は 2016 年 3 月より爆発的に広がりました。IPA への相談件数はもちろん、当社サポート窓口への問い合わせ件数も 3 月を境に急増しています。



IPAランサムウェアに関する相談の月別推移
（2016年1月～3月）

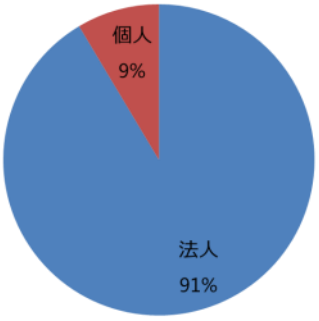


IODATA ランサムウェアに関する相談の月別推移
（2016年3月～4月）

2. ターゲットは法人

弊社への問合せの 9 割が法人でした。このことからランサムウェアは法人を主なターゲットにしている可能性があります。

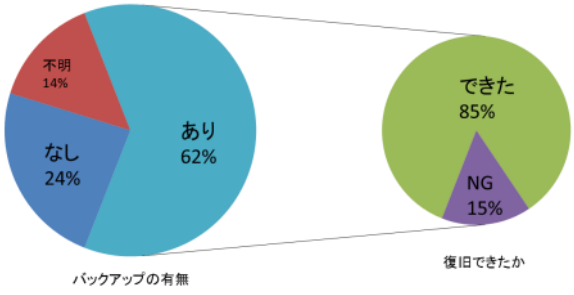
企業において 1 台のクライアント PC がランサムウェアに感染するだけで、NAS やファイルサーバーに保存されている共有データが暗号化の脅威にさらされます。また、重要なファイルを暗号化された場合、ランサムェアの被害が業務停止に直結してしまうリスクがあります。



IODATA ランサムウェアに関する相談比率
（2016年3月～4月）

3. ランサムウェア被害からのデータ復旧

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。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。



IODATA バックアップ率・復旧率（2016年3月～4月）

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の 6 割がバックアップを取られており、そのうち 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以下のケースでした。

- ⚠ フルバックアップ 1 回分しか取っていなかった。気がつくのが遅れ、バックアップが暗号化された状態で上書きされた。
- ⚠ バックアップを 2 世代しか取っていなかった。気がつくのが遅れ、バックアップが暗号化された状態で上書きされた。

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。

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の脅威への対策で、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。最後に既存のファイルサーバーを対象とした復旧手段の提案をいたします。

3.1 脅威への対策と復旧手段の準備

セキュリティ強化を考える際に、脅威そのものへの対策と、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。脅威に対する対策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。

	脅威に対する対策			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

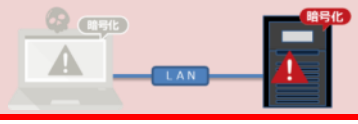
IPA が発行している「情報セキュリティ 10 大脅威 2016」によると、「情報セキュリティ対策の基本」は過去から変わることなく、引き続き大きな効果が期待できるとのことです。脅威への対策として併せてご参照ください。

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

3.2 復旧手段の準備

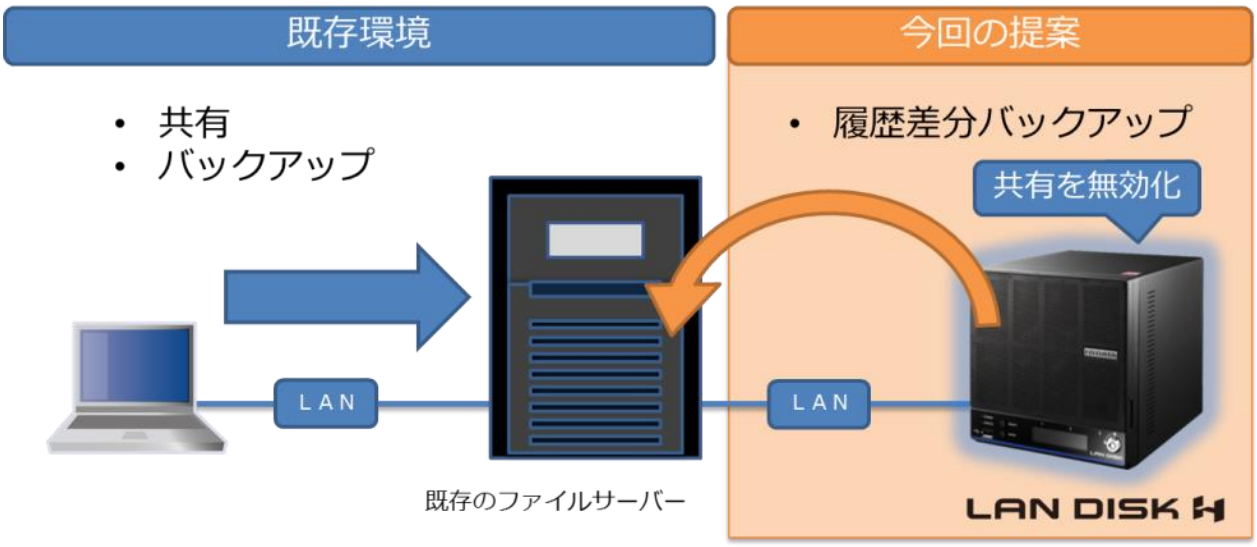
ランサムウェア被害からの復旧手段としてバックアップが有効です。その際、セキュリティ問題が発生したときに、その問題が発生した時点より前のバックアップデータ、つまり暗号化されてしまう前のバックアップデータが残っている必要があります。以下に、バックアップ対象機器と、これまで弊社でご紹介したバックアップ手段をまとめました。

バックアップ対象	復旧手段のご提案
クライアント PC 	【ホワイトペーパー】LAN DISK H を活用したクライアント PC のバックアップ http://www.iodata.co.jp/biz/whitepaper/
LAN DISK シリーズ 	【特集ページ】ランサムウェア対策のご案内 http://www.iodata.co.jp/biz/ransomware/index.htm 【商品別設定内容】 ● LAN DISK Z シリーズ http://www.iodata.co.jp/news/2016/information/ransomware/landiskz.pdf ● LAN DISK H シリーズ http://www.iodata.co.jp/news/2016/information/ransomware/landiskh.pdf ● LAN　DISK XR、XV シリーズ http://www.iodata.co.jp/news/2016/information/ransomware/landiskxr.pdf ● LAN DISK A シリーズ http://www.iodata.co.jp/news/2016/information/ransomware/landiska.pdf
既存のファイルサーバー 	**今回の内容**

本、ホワイトペーパーでは、既存のファイルサーバーの復旧手段について解説します。

4. 既存のファイルサーバーの復旧手段

本章では、運用中のファイルサーバーに対して弊社 NAS 製品の LAN DISK H をバックアップ先として提案いたします。これは、LAN DISK H の履歴差分バックアップを利用することにより、ネットワーク上のクライアント端末からバックアップ先を隠して、世代バックアップを取ることが可能だからです。まず、ランサムウェアに対するバックアップのポイントを説明します。次に、LAN DISK H をバックアップ先として利用するメリットを解説します。



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、ファイルサーバーのバックアップ先を読み書き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 やファイルサーバーのデータを、パソコンから読み書きできないドライブ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出来なくなるため、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ひとつ前の世代（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。

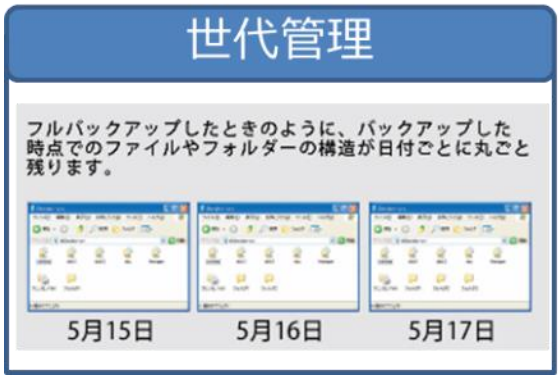
4.2 LAN DISK H をバックアップ先として利用するメリット

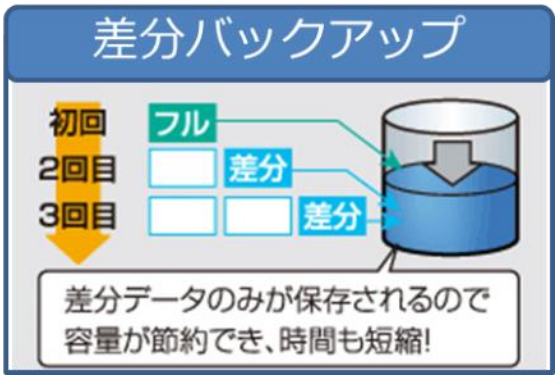
既存のファイルサーバーのバックアップ先として LAN DISK H を利用するメリットを以下にまとめます。

導入内容	メリット
既存の環境に影響を与えない。	■ 外付け HDD のように、ファイルサーバーに直接接続しないため、既存環境や機器構成を変更することなく導入が可能。 ■ LAN DISK H の標準機能である「履歴差分バックアップ」機能を利用することが可能。 ■ LAN DISK H がファイルサーバー内のファイルを引き取るため、ファイルサーバーにバックアップ用のアプリケーションのインストールが不要。
履歴差分バックアップが可能	■ 履歴機能により世代管理が可能 ■ 差分バックアップによりバックアップ容量節約が可能 ■ バックアップ先をネットワーク共有しない設定が可能
大容量	最大48TB（拡張ボリューム利用時の実効容量24TB）までラインナップ。複数の履歴を残すことが可能。

■ 履歴差分バックアップについて

履歴差分バックアップ方式は LAN DISK H 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。

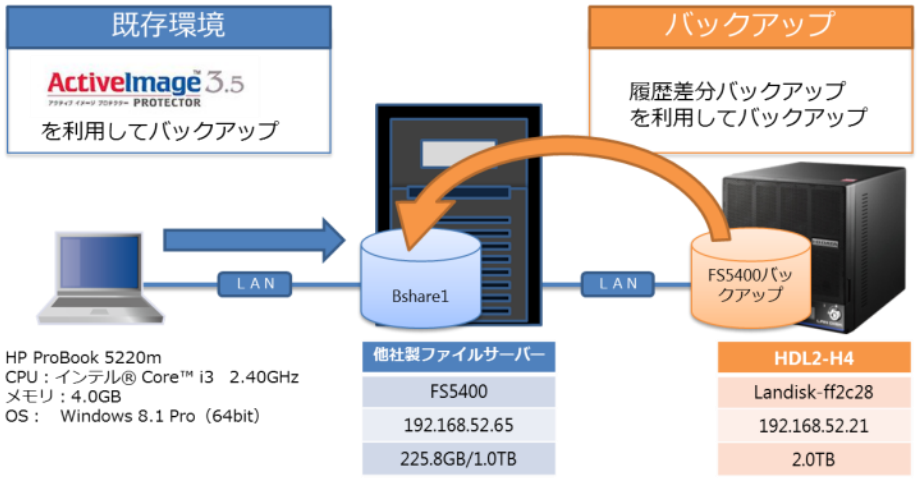




5. LAN DISK H を利用したファイルサーバーバックアップの実際

本章では、実際に既存のファイルサーバーを LAN DISK H にバックアップする手順についてご紹介します。また、合わせて LAN DISK H シリーズに標準添付しているイメージバックアップツール『ActiveImage Protector』を利用し、ファイルサーバーにクライアント PC のイメージバックアップを取り、クライアント・ファイルサーバー共にランサムウェアに対する備えを準備します。

6. テスト環境と既存環境



今回、既存の環境に、LAN DISK H を追加してファイサーバーのバックアップを行います。既存環境の特徴は以下の通りです。

- ファイルサーバー上の「Bshare1」をクライアント PC 用の共有フォルダーとして利用。
- クライアント PC にイメージバックアップソフト；ActiveImage Protector 3.5 Desktop Edition（以下、AIP3.5）をインストールし、Windows OS、アプリケーションを含む全てのデータをファイルサーバーにイメージバックアップ。
- AIP3.5 を利用して、一日一回「Bshare1」をバックアップ先として増分バックアップを実行。
  ※ AIP3.5 の設定方法や運用手順は以下のホワイトペーパーを参照ください。

※ホワイトペーパー「LAN DISK H を活用したクライアント PC のバックアップ

http://www.iodata.co.jp/biz/whitepaper/pdf/landiskh_backup.pdf

6.1 バックアップ環境の増設と手順

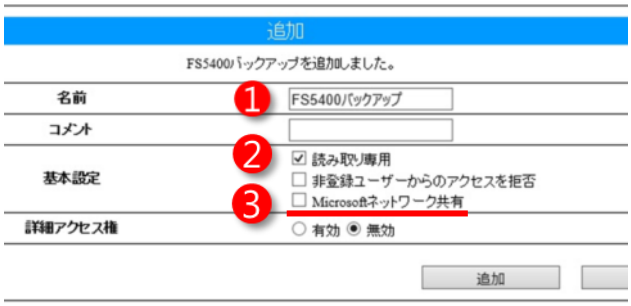
既存環境に、LAN DISK H を追加してファイサーバーのバックアップを行います。この際、バックアップ設定は LAN DISK H のみで行います。稼働中のファイルサーバーに対して機器増設および、アプリケーションのインストールはいたしません。そのため、運用を止めずにバックアップ環境導入が可能です。設定手順は以下のとおりです。

STEP.1	バックアップ用共有フォルダーの作成
STEP.2	バックアップの設定・実行
STEP.3	トラブル時のデータアクセス・復元

1. バックアップ用共有フォルダーの作成

最初に LAN DISK H にバックアップ用の共有フォルダーを作成します。

［共有］→［フォルダー］→［追加］をクリックします。



① [名称]共有フォルダーの名称を入力します。今回の例では「FS5400 バックアップ」としています。
② [読み取り専用]をチェックします。
③ [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、新規作成したバックアップ用の共有フォルダーは、設定変更しない限りクライアント PC からアクセスすることができません。

2. 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。

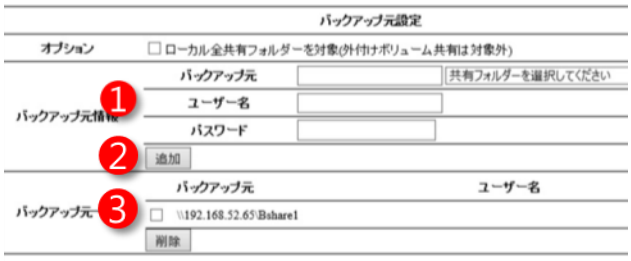
［データ保守］→［バックアップ］→［追加］をクリックします。

① [ジョブ名]バックアップジョブ名称を入力します。今回の例では「FS5400 バックアップ」としています。
② バックアップの履歴数を決定します。
③ [スケジュール]を決め設定します。

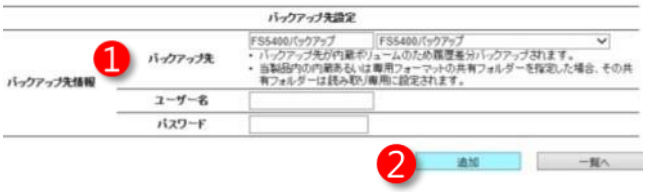
ここでのポイントは以下のとおりです。

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。
   履歴数は［7～14］程度（1～2 週間）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 31 になります。
⚠ バックアップ履歴数が設定値を超えた場合、古い履歴から削除します。



① [バックアップ元情報]バックアップ元情報を入力します。今回の例では既存のファイルサーバーの共有フォルダーを対象としました。
『¥¥192.168.52.65¥Bshare1』
② [バックアップ元情報]を入力完了後、[追加]をクリックします。
③ 追加した共有フォルダーが一覧に表示されていることを確認します。



① [バックアップ先情報]バックアップ先情報を入力します。今回の例では、先ほど作成した共有フォルダー「FS5400 バックアップ」を指定しました。
② [追加]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 H よりバックアップが実行されます。

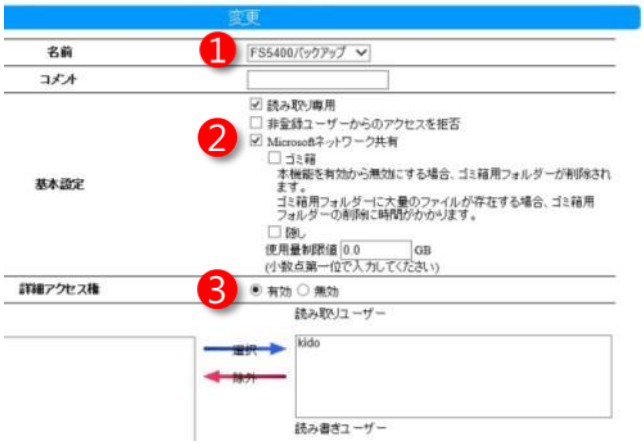
3. トラブル時のデータアクセス・復元

ランサムウェアに感染してしまった場合、感染したパソコンはネットワークから取り外し初期化してください。パソコンの初期化後、必要なファイルを事前に取得しているバックアップから復元してください。AIP3.5 のようなイメージバックアップソフトを利用することで、個別にファイルを戻すことなく、感染前のバックアップデータを基に OS・アプリケーション・データ全てを復元することができます。

■ ファイルを個別に取り出す場合

トラブル発生時のファイル復元のために、バックアップデータにアクセスし、ファイルを個別に取り出せるようにします。これは、LAN DISK H のネットワーク共有を有効にすることにより実現します。

［共有］→［フォルダー］→［変更］をクリックします。



① 変更する共有フォルダーを選びます。
② [Microsoft ネットワーク共有]をチェックし、ネットワーク共有を有効にします。
③ [詳細アクセス権]を有効にし、適切なアクセス権を設定します。
④ [変更]をクリックします。

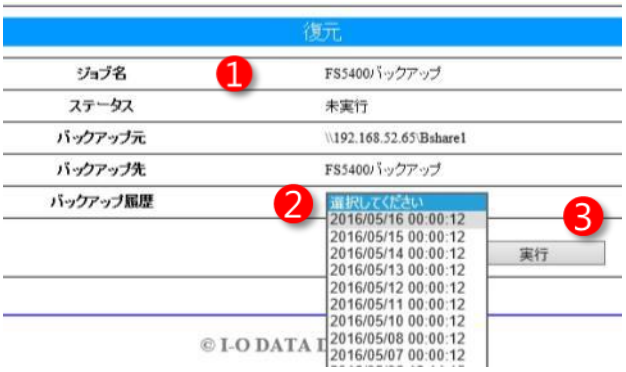
[Microsoft ネットワーク共有]にすることにより、これまでエクスプローラーで確認できなかった LAN DISK H のバックアップデータにアクセスすることができるようになります。この際、必ずランサムウェアに感染していないことが確認されている端末からアクセスしてください。ランサムウェアに感染しているパソコンからアクセスすると、大事なバックアップデータを破損するリスクがあります。また、[読み取り専用]をチェックのままにしておくことで、万一ランサムウェアに感染しているパソコンが残っていた場合でも、バックアップデータが暗号化されることを防げます。

■ バックアップデータの一括復元

LAN DISK H に保存されたバックアップデータをファイルサーバーに一括して復元します。

［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。



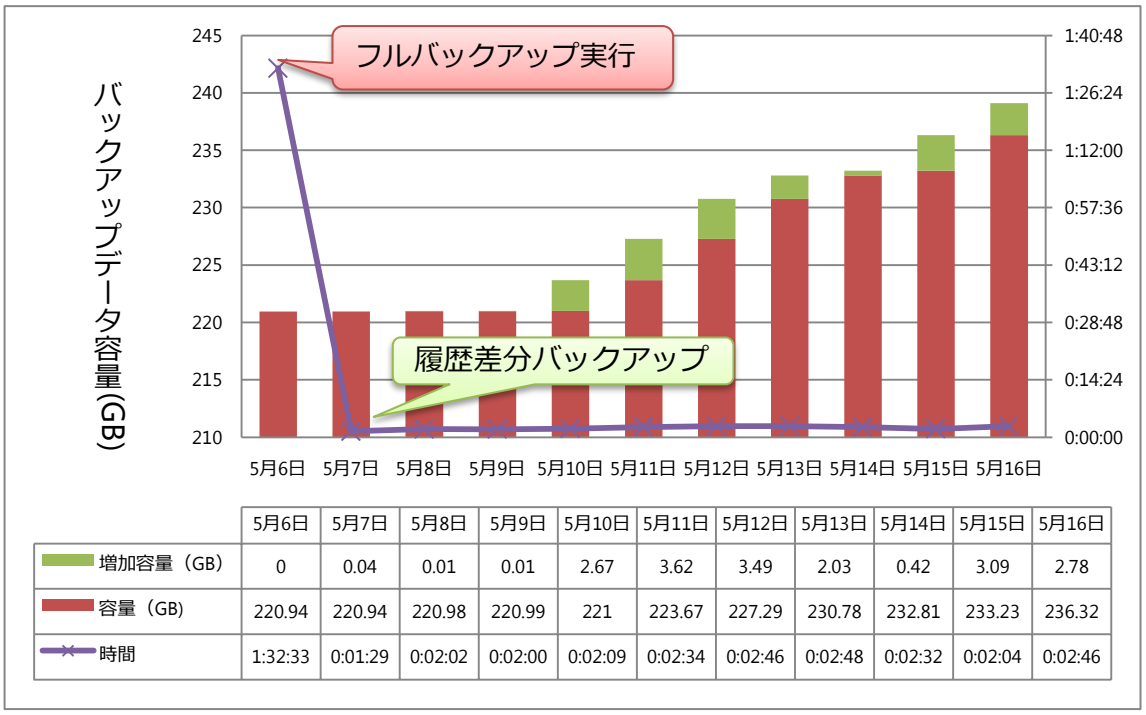
① 復元内容を確認します。
② ［バックアップ履歴］で復元するバックアップの日時を選びます。
③ [実行]をクリックします。

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

6.2 実行結果

上記設定内容で実行した、実測結果を以下に示します。

■ 履歴差分バックアップ時間



	5月6日	5月7日	5月8日	5月9日	5月10日	5月11日	5月12日	5月13日	5月14日	5月15日	5月16日
増加容量（GB）	0	0.04	0.01	0.01	2.67	3.62	3.49	2.03	0.42	3.09	2.78
容量（GB）	220.94	220.94	220.98	220.99	221	223.67	227.29	230.78	232.81	233.23	236.32
時間	1:32:33	0:01:29	0:02:02	0:02:00	0:02:09	0:02:34	0:02:46	0:02:48	0:02:32	0:02:04	0:02:46

初回のフルバックアップで 1 時間 32 分かかっていますが、その後の履歴差分バックアップでは増加分のデータ（約 3GB 程度）に対して、3 分程度の短時間で完了しています。

■ バックアップデータの復元時間

上記履歴差分バックアップを行ったデータよりバックアップデータの復元を行いました。

- LAN DISK H のバックアップ容量：239.1GB
- ファイルサーバーへの復元時間：1 時間 12 分 17 秒

7. 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継続してきました。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