GMO クラウド Private／ハウジングサービス

Acronis Cyber Protect Cloud

Acronis バックアップ 利用者ガイド

GMO グローバルサイン・ホールディングス株式会社
サービス運用部 インフラ SC SE グループ

■更新履歴

バージョン	日付	内容
1.0	2018/07/01	初版作成
1.1	2018/11/14	Acronis Data Cloud 7.8 による改訂
1.1.1	2019/05/09	リストア時リセット方法（Ctr+Alt+Ins）を追記
1.2	2021/07/01	クラウドストレージ利用方法の追加、UI 更新による改訂
1.2.1	2022/08/18	通知設定の新規項目について追記
1.2.2	2024/01/23	二要素認証利用時に、BootableMedia からクラウドストレージを利用できない仕様について、回避手順を追記
1.2.3	2024/02/05	・物理サーバーにおける経路設定手順を追記 ・WebUI からの復元操作を行うための経路設定手順を追記 ・WebUI からのマシン復元手順を追記
1.2.4	2024/07/25	UI 変更に伴うアカウント有効化手順、エージェントインストール手順の更新
1.2.5	2024/10/01	Acronis 社からの不具合報告による設定内容変更
1.2.6	2024/12/11	「バックアップ管理コンソール」の表記を「Cyber Protection コンソール」に変更
1.2.7	2025/06/12	アカウント名表記を変更 接続先表記を変更

はじめに

本書は、GMO クラウド Private、GMO クラウド ハウジングサービスで提供している Acronis バックアップの操作マニュアルです。

本書では Acronis バックアップを利用するに当たって必要となる下記オペレーションについて記載しています。

ーアカウントの有効化
ーバックアップエージェントのインストール
ーバックアップ計画の設定
ーバックアップデータのリストア
ーバックアップエージェントのアップデート

なお、本書では各機能の詳細については記載しておりません。必要に応じてベンダー提供の製品マニュアルをご覧ください。

ドキュメント内で記載されている[バックアップ GW]、[ストレージ GW　]、[バックアップ NW]については、サービスご利用開始時に送付させていただいている設定完了通知書をご確認ください。

目次

1. アカウントの有効化

この章ではお申込とあわせてご提示頂いたお客様指定メールアドレス宛に届く「アカウント有効化通知メール」からのアカウント有効化手順について説明いたします。

1.1 アカウントの有効化

ご契約後に提示頂いたヒアリングシートに基づき、弊社にてお客さま向けのアカウント作成を実施致します。アカウントが作成されると、指定頂いたメールアドレス宛にアカウントの有効化を促すメールが送付されますので、手順に従ってアカウントの有効化を実施して下さい。

① メール本文中の「アカウントの有効化」ボタンを押下する

② Web ページが表示され、Acronis Cyber Protect Cloud のページに接続されます

「パスワード」欄に任意のパスワードを設定して「アクティブなアカウント」ボタンを押下して下さい。

※パスワードの長さは 9 文字以上にする必要があります。また、パスワードの複雑さがチェックされ、弱／中／強いずれかのカテゴリが表示されます。

③ 契約条項の同意画面が表示されます。

エンドユーザーライセンス横の「詳細」を選択して「Acronis バックアップサービス利用約款」を確認頂き、チェックボックスにチェックを入れたうえで「同意する」を押下ください。

④ データ処理に関する補足条項が表示されます。

「許可の表示と調整」を選択いただき、各情報収集項目のオフ／オンを設定ください。
後から変更可能な設定となりますので、利用開始時点で判断がつかない場合にはオフを選択ください。

⑤ 一通りの選択が完了したら画面下部の「すべて受け入れ」を押下してください。

⑥ Cyber Protection コンソール画面が表示されます。アカウントの有効化設定はこれで完了となります。

※以降の操作を行うために Cyber Protection コンソールの URL については、ブックマークを保存いただくなどの対応を推奨いたします。

Cyber Protection コンソール	https://jp-cloud.acronis.com/login
ログイン ID	設定完了通知書に記載のあるアカウント名
パスワード	設定頂いたパスワード

2. バックアップエージェントのインストール

この章ではバックアップ対象サーバーへのバックアップエージェントインストール手順について説明しています。ハードウェア、OS 等の要件についてはベンダー提供のマニュアルを参照して下さい。本項では要件を満たしている環境へのインストールを前提としております。

2.1 インストールに際しての注意事項

① エージェントソフトウェアは Cyber Protection コンソールからダウンロード可能です。
直接外部に接続出来ない、あるいは GUI 環境がない場合にはクライアント PC にダウンロードいただき、SCP などでサーバーに転送下さい。

② インストール作業は管理者権限(root/Administrator)で実行する必要があります

③ 必ず経路設定、PROXY 設定を実施した後にインストールを実行してください

④ 文章中の[バックアップ GW]、[ストレージ GW　]、[バックアップ NW]の値については設定完了通知書にてご確認ください

2.2 Linux サーバーへのエージェントインストール

2.2.1　バックアップネットワークへの経路設定（仮想環境／物理サーバー Alma8・RHEL8 以下）

バックアップネットワーク上にある Proxy ゲートウェイおよびバックアップストレージと通信を行うため、経路設定を実施します

① 静的経路を設定する

```
# ip route add [バックアップ GW]/32 via [GW アドレス] dev [プライベート NW の I/F 名]
# ip route add [ストレージ GW　]/32 via [GW アドレス] dev [プライベート NW の I/F 名]
```

例）

```
# ip route add 192.0.2.1/32 via 10.1.4.254 dev eth1
# ip route add 192.0.2.2/32 via 10.1.4.254 dev eth1
```

② 再起動時に有効となるように経路設定ファイルに経路情報を記述する

```
# vi /etc/sysconfig/network-scripts/route-[プライベート NW の I/F 名]
[バックアップ GW]/32 via [GW アドレス]
[ストレージ GW　]/32 via [GW アドレス]
```

例）

```
# vi /etc/sysconfig/network-scripts/route-eth1
192.0.2.1/32 via 10.1.4.254
192.0.2.2/32 via 10.1.4.254
```

③ 疎通確認

```
# ping [バックアップ GW]
# ping [ストレージ GW  ]
```

※ping の応答が返らない場合には、①の設定を見直してください

2.2.2　バックアップネットワークへの経路設定（物理サーバー Alma9/RHEL9）

バックアップネットワーク上にある Proxy ゲートウェイおよびバックアップストレージと通信を行うため、経路設定を実施します。Alma8、RHEL8 については 2.2.1 の手順で実施ください。

① 静的経路を追加する

```
# nmcli connection modify [プライベート NW の I/F 名] +ipv4.routes "[バックアップ GW] [GW アドレス]"
# nmcli connection modify [プライベート NW の I/F 名] +ipv4.routes "[ストレージ GW  ] [GW アドレス]"
```

例）

```
# nmcli connection modify ens224 +ipv4.routes "192.0.2.1 10.1.4.254"
# nmcli connection modify ens224 +ipv4.routes "192.0.2.2 10.1.4.254"
```

② インタフェースに設定した経路設定を有効化して設定確認

```
# nmcli connection up [プライベート NW の I/F 名]
# nmcli connection show [プライベート NW の I/F 名] | grep IP4.ROUTE
```

例）

```
# nmcli connection up ens224
# nmcli connection show ens224 | grep IP4.ROUTE
IP4.ROUTE[1]:                           dst = 10.1.4.0/24, nh = 0.0.0.0, mt = 101
IP4.ROUTE[2]:                           dst = 192.0.2.1/32, nh = 10.1.4.254, mt = 101
IP4.ROUTE[3]:                           dst = 192.0.2.2/32, nh = 10.1.4.254, mt = 101
```

③ 疎通確認

```
# ping [バックアップ GW]
# ping [ストレージ GW  ]
```

※ping の応答が返らない場合には、①の設定を見直してください

2.2.3　管理サーバーへの Proxy 設定

バックアップ管理の通信を Proxy サーバー経由で行うため、Proxy サーバー利用設定を行います

① ディレクトリを作成後、中に設定ファイルを作成します

```
# mkdir /etc/Acronis
# vi /etc/Acronis/Global.config
```

② 設定ファイル記述内容（次の内容をコピーペーストして、[バックアップ GW]を変更ください）

```
<?xml version="1.0" ?>
<registry name="Global">
    <key name="HttpProxy">
        <value name="Enabled" type="Tdword">"1"</value>
```

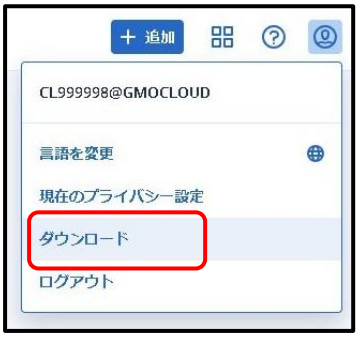
```
        <value name="Host" type="TString">"[バックアップ GW]"</value>
        <value name="Port" type="Tdword">"35088"</value>
    </key>
</registry>
```

2.2.4　エージェントのダウンロード

Cyber Protection コンソールから Linux サーバー向けエージェントのインストーラーパッケージをダウンロードします

① Web ブラウザから Cyber Protection コンソールにログインします

② 右上にある人型のユーザーアイコンから「ダウンロード」を選択します



③ チャネルをリリースの設定が「現在」になっていることを選択します

「前回のリリース」を選択すると 1 つ前のバージョンのエージェントがダウロードされます

④ 「Agent for Linux(64/32-bit)」を選択します

⑤ インストーラーがダウンロードされますので、SCP 等でバックアップ対象サーバー上の任意のディレクトリにファイルを転送してください

⑥ ダウンロードしたインストーラーに実行権限を付与します

```
# chmod +x CyberProtect_AgentForLinux_x86_64.bin                    n
```

2.2.5　エージェントのインストール

Linux 向けのエージェントをインストールするためには、kernel-devel、gcc、make など幾つかの Linux パッケージをインストールする必要があります。新しいディストリビューションの OS であれば、エージェントインストール時に自動で必要なパッケージがインストールされます。

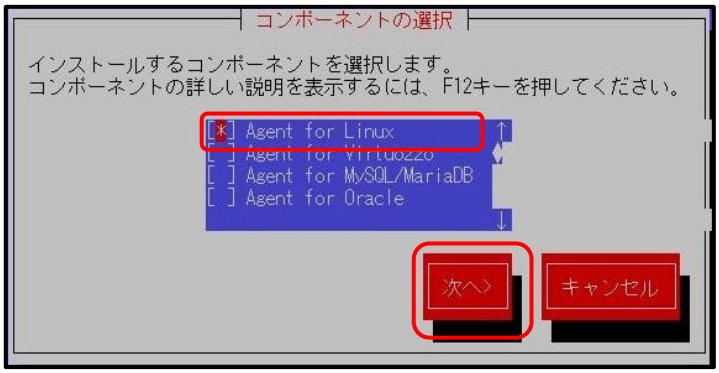
※手動でパッケージをインストールされる場合には、Cyber Protection コンソールのヘルプから「ソフトウェアのインストール」→「Linux パッケージ」の記載内容を確認ください。

※Acronis 導入先 OS において、エージェントインストール時と異なる Kernel バージョンとなった場合にエージェントの再インストールが必要となるため、当社で仮想マシン構築を代行している場合、kernel 周りのパッケージ更新を抑制するために、[/etc/yum.conf]の[main]ディレクティブへ除外設定「exclude=kernel*」を記述しております。必要に応じて解除のうえ実行ください。

① ダウンロードしたインストーラーを実行します

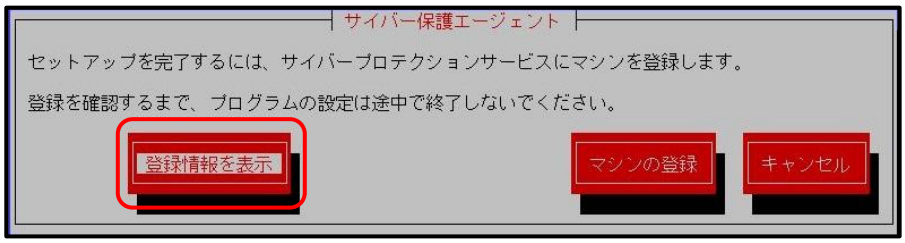
```
# ./CyberProtect_AgentForLinux_x86_64.bin
```

② コンポーネントの選択画面が表示されるので「Agent for Linux」が選択されている事を確認して「次へ」を押下します



③ インストールが開始されます

④ インストールが完了すると、エージェントの登録画面が表示されるので「登録情報を表示」を押下します



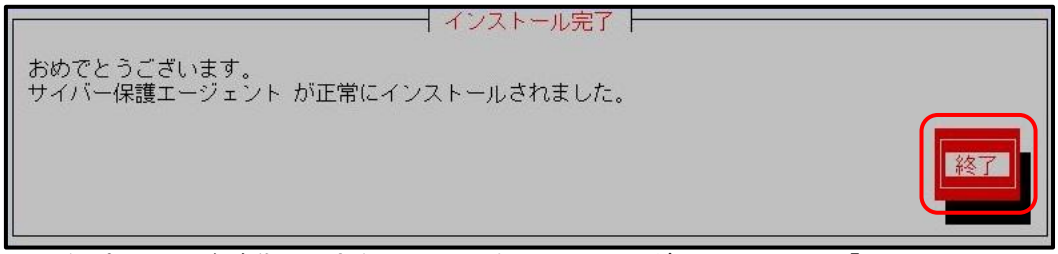
⑤ 登録コードと URL が表示されるので、ブラウザから URL を入力します

⑥ TOP メニュー「デバイス」を選択、画面右上の「＋追加」を押下してデバイスの追加ウィンドウが表示されたら「コードによる登録」セクションの「登録」ボタンを押下します

⑦ 登録コードを入力してアカウントを選択し、「コードを検証」を押下します

⑧ 検証によりワークロード（マシン名）が表示されるので確認して「登録」を押下します。

⑨ 登録が完了すると完了画面が表示されるので「終了」を押下します。



必要なパッケージが導入できなかった場合には、ベンダーマニュアル「Backup Service Web ヘルプ」の「ソフトウェアのインストール」から「Linux パッケージ」の項を確認いただき、必要なモジュールの導入を行ってください。

2.2.6　復元操作向けの経路設定

復元操作を Cyber Protection コンソールから実施する際に参照される経路設定情報をあらかじめ設定いたします。

① 経路設定ファイルの複製と編集

```
# cd /usr/lib/Acronis/BackupAndRecoveryAgent/
# cp -p media_network.config media_network.config_ORG
# vi media_network.config
ip route add [バックアップ NW] via [GW アドレス]
```

例）
```
ip route add 192.0.2.0/24 via 10.1.4.254
```
※Acronis 社より、ファイルの最終行を空白行にすると、正常に動作しないとの案内がありました。設定文字列の最後で改行をしないようにしてください。
※改行コードを含む設定内容をコピーペーストした場合には改行コードを手動で削除してください。

2.3 Windows サーバーへのエージェントインストール

2.3.1 バックアップネットワークへの経路設定

バックアップネットワーク上にある Proxy サーバーおよびバックアップストレージと通信を行うため、経路設定を実施します

① 静的経路を設定する
```
> Route -p add [バックアップ GW] mask 255.255.255.255 [GW アドレス]
> Route -p add [ストレージ GW  ] mask 255.255.255.255 [GW アドレス]
```

例）
```
> Route -p add 192.0.2.1 mask 255.255.255.255 10.1.40.254
> Route -p add 192.0.2.2 mask 255.255.255.255 10.1.40.254
```

② 疎通確認
```
> ping [バックアップ GW]
> ping [ストレージ GW  ]
```
※Ping の応答が返らない場合には、①の設定を見直してください

2.3.2 管理サーバーへの Proxy 設定

バックアップ管理のための通信を Proxy サーバー経由で行うため、利用設定を行います

① 新しいテキスト文書を作成し、メモ帳などのテキストエディタで開きます。

② 以下の内容をコピーしてファイルに貼り付け、[バックアップ GW]を変更ください。
```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE¥SOFTWARE¥Acronis¥Global¥HttpProxy]
"Enabled"=dword:00000001
"Host"="[バックアップ GW]"
"Port"=dword:00008910
```

③ ファイル名を「proxy.reg」として文書を保存します。
保存する際にファイルの種類は「すべてのファイル」を選択して保存してください。

④ ファイル「proxy.reg」をダブルクリックして実行します。

⑤ Windows レジストリを編集する事を確認します。

⑥ 「proxy.reg」ファイルを削除してください。

2.3.3 エージェントのダウンロード

Cyber Protection コンソールから Windows サーバー向けのエージェントをダウンロードします

① Web ブラウザから Cyber Protection コンソールにログインします

② 画面右上にある「＋追加」ボタンもしくは中央にある「保護するワークロードの選択」から「Windows」を選択します

③ 「ワークステーション」から「Windows」を選択します

④ インストーラーがダウンロードされますので、SCP 等でバックアップ対象サーバーにファイルを転送してください

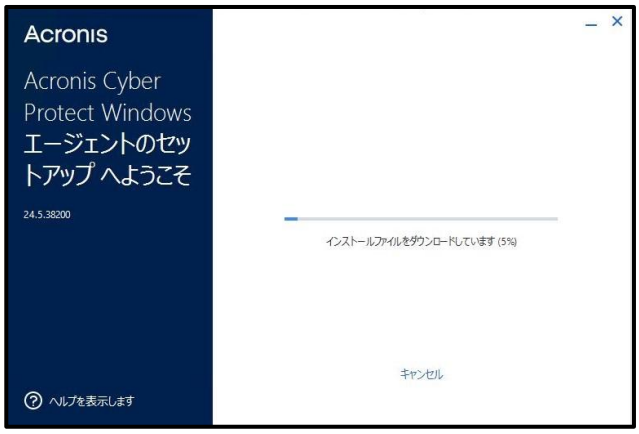
2.3.4 エージェントのインストール

① インストール対象サーバーにてダウンロードしたインストーラーを起動します

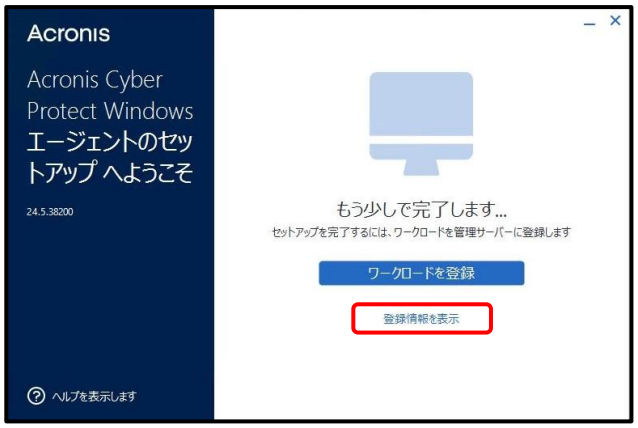
② 「インストール」ボタンを押下します

※インストールファイルを取得するため、しばらく時間がかかります。

③ インストールファイルを取得した後、自動でインストールが実行されます



④ エージェントの登録画面が表示されるので「登録情報を表示」を押下します



⑤ 登録コードと URL が表示されるので、ブラウザにて URL を入力します

⑥ TOP メニュー「デバイス」を選択、画面右上の「＋追加」を押下してデバイスの追加ウィンドウが表示されたら「コードによる登録」セクションの「登録」ボタンを押下します

⑦ 登録コードを入力してアカウントを選択し、「コードを検証」を押下します

⑧ 検証によりワークロード（マシン名）が表示されるので確認して「登録」を押下します。

⑨ 登録が完了すると完了画面が表示されます

2.3.5　復元操作向けの経路設定

復元操作を Cyber Protection コンソールから実施する際に参照される経路設定情報をあらかじめ設定いたします。

① 経路設定ファイルの複製と編集

「C:¥Program Files¥Common Files¥Acronis¥BackupAndRecoveryAgent」フォルダを開きます。

② media_network.config というファイルを開いて、以下の記載を追記します

```
ip route add [バックアップ NW] via [GW アドレス]
```

例）

```
ip route add 192.0.2.0/24 via 10.1.4.254
```

※Acronis 社より、ファイルの最終行を空白行にすると、正常に動作しないとの案内がありました。設定文字列の最後で改行をしないようにしてください。
※改行コードを含む設定内容をコピーペーストした場合には改行コードを手動で削除してください。

3. 保護計画の設定

本章では、Acronis Cyber Protect Cloud Cyber Protection コンソールにて保護計画を作成する手順を説明いたします。この作業の前にアカウントの有効化並びにエージェントのインストール、デバイスの登録が完了している必要があります。

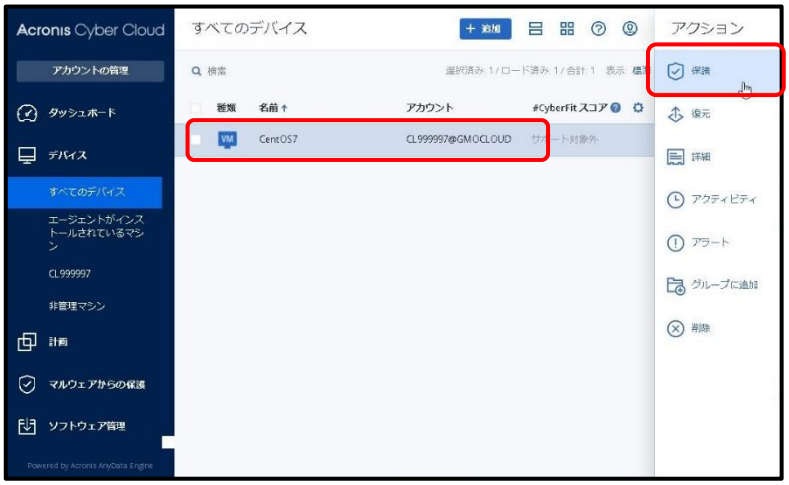
3.1 保護計画の作成

3.1.1 Cyber Protection コンソールへのログイン

① Acronis Cyber Protect Cloud の Web ページを開き、ログインして下さい

3.1.2 バックアップ対象マシンの選択

① バックアップ対象とするマシンを選択して「保護」を選択します



3.2 保護計画の作成

① 保護計画の一覧が表示されるので「計画の作成」から「保護」を選択します

② 新しい保護計画のサンプルが表示されるので、各設定値を設定します

【計画名】
「新しい保護計画」と表示されている文字の横にある鉛筆マークを押下して、この計画に名前をつけて下さい。

【バックアップ先】
初期設定では「クラウドストレージ」と表示されます。

クラウドストレージのご契約がない場合にエラーが表示されますが、無視して所定のストレージを選択してください。

以降の手順に従って、バックアップ対象、バックアップ先、スケジュール、保持する期間などを設定してください。

3.2.1　バックアップ対象の選択

バックアップ対象サーバーを丸ごとバックアップするのか、所定のファイル／フォルダのみバックアップするのかを指定下さい。

① バックアップの対象（プルダウンメニュー）から対象を選択します

対象	説明
マシン全体	全てのディスク/ボリュームを対象としてバックアップを実行します
ディスク/ボリューム	特定のディスク/ボリュームを選択してバックアップを実行します
ファイル/フォルダ	特定のファイル/フォルダを選択してバックアップを実行します

3.2.2　バックアップ先の選択

本サービスでは、バックアップデータの格納先としてローカルストレージとクラウドストレージの 2 種類の領域を提供しております。バックアップ先の選択から格納先を指定下さい。

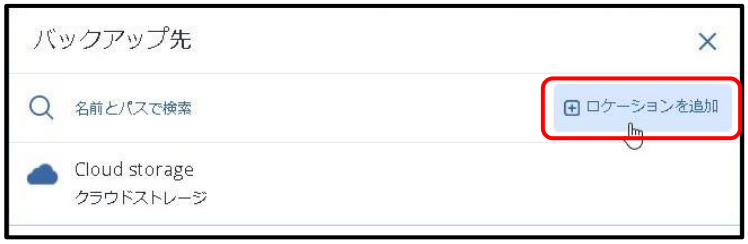
バックアップ先	設定内容
ローカルストレージ	バックアップ先にネットワークフォルダを設定
クラウドストレージ	バックアップ先にクラウドストレージを設定
ローカル＋クラウド	バックアップ先にネットワークフォルダを設定した後、ロケーションの追加を実行してクラウドストレージを設定 ※手順 3.2.5 を確認ください。

※1 つ目のバックアップ先をクラウドとした場合、ロケーションの追加は出来ません

① クラウドストレージに保存する場合にはバックアップ先に「クラウドストレージ」が選択されている事を確認ください。
※クラウドストレージに保存する場合、②以降の手順は飛ばして 3.2.3 に進んでください。

② ローカルストレージに保存する場合にはバックアップ先の「クラウドストレージ」を押下してバックアップ先の選択画面に遷移します。

③ 画面右上の「ロケーションを追加」を選択します。



④ ネットワークフォルダを選択し、入力フォームに格納先ストレージ情報を入入力して「→」を押下します。

【格納先ストレージ】　※[ストレージ GW] の値は設定完了通知書を確認ください
¥¥**[ストレージ GW]**¥**[契約番号]**

例）
¥¥**[ストレージ GW]**¥CL999998

⑤ 認証が求められたら所定のアカウント／パスワードを入力して下さい

【アカウント】
acr-svm01¥**[契約番号]**

例）acr-svm01¥CL999998

【パスワード】
設定完了通知書に記載されているパスワード

⑥ 画面下部の「追加」を押下してバックアップ先の選択画面を終了して下さい

3.2.3　スケジュールの設定

バックアップを手動で実行する場合にはスケジュール設定をオフにします。

① 「オフ／オン」スイッチでオンを選択します

② バックアップスキームを選択します

スキーム	説明
常に増分（単一ファイル）	指定した日時で常に増分バックアップを行います。最初に取得される完全バックアップとその後の増分バッ

	クアップが単一ファイル形式で保存されるため速度が速いです。
常に完全	全てのバックアップが完全バックアップで実行されます。格納先ディスクの容量にご注意下さい。
日単位で増分バックアップ、週単位で完全バックアップ	完全バックアップが週に 1 回作成され、その他は増分バックアップとなります。
月単位で完全、週単位で差分、日単位で増分（GFS）	完全バックアップが月に 1 回作成され、日単位で増分、週に一度差分バクアップが実行されます。
カスタム	完全バックアップ、差分バックアップおよび増分バックアップスケジュールを指定します。

③ 時間単位から月単位までの範囲で実行日時を設定します

単位	選択項目	説明
月単位	曜日	設定した週の特定曜日に毎月バックアップを実行
	日付	設定した日に毎月バックアップを実行
週単位	ー	指定した曜日に毎週バックアップを実行 （全ての曜日をチェックした場合は毎日実行される）
日単位	毎日	毎日指定した時刻にバックアップを実行
	月曜から金曜日まで実行	月ー金の指定した時刻にバックアップを実行（週末はバックアップなし）
1 時間ごと	ー	指定した曜日で指定した時間ごとに、「開始」から「終了」の時間内でバックアップを実行

3.2.4　保存期間の設定

取得したバックアップデータを保存する期間／数を設定します。

① データのクリーンアップを行う保持ルールを指定します

対象	説明
バックアップ期間（デフォルト）	バックアップ計画で作成されたバックアップを保存する期間を指定します。月単位や週単位などで期間の指定ができます。
バックアップの数	バックアップの最大数を指定して、保持します。
バックアップの合計サイズ別	保持するバックアップの最大合計サイズを指定して保持します。この設定は「常に増分（1 つのファイル）」バックアップスキームを指定している場合、またはクラウドストレージに保存する場合には使用できません。
期間を制限せずにバックアップを保存する	無限にバックアップを保存する事も可能ですが、バックアップ領域を大量に消費する場合があるので注意が必要です。

② クリーンナップの開始タイミングを選択します

次期	説明
バックアップ後（デフォルト）	保持ルールは新しいバックアップの作成後に適用されます。
バックアップ前	保持ルールは新しいバックアップの作成前に適用されます。

3.2.5　ロケーションの追加

バックアップストレージとしてローカルとクラウド 2 種類の契約がある場合に、最初にローカルストレージに保存したバックアップをクラウドストレージにレプリケート（複製）することができます。

※ローカル／クラウドストレージの両方を利用する場合以外は本手順をスキップ下さい。

① 「＋ロケーションの追加」を押下します

② 2 番目のロケーションとしてクラウドストレージが自動で選択されます

③ 必要に応じて 2 番目のロケーションでの保持期間を指定します

3.2.6　モジュールの適用

「バックアップ」以外の各モジュール「ウイルス対策およびマルウェア対策保護」や「脆弱性診断」などについては、必要に応じて無効化／有効化を設定ください。これらのモジュールが提供する機能については WebUI 右上のヘルプから確認ください。

3.2.7　保護計画の保存

計画の設定が完了した後に「適用」ボタンを押下して保護計画をデバイスに適用します。

4. バックアップデータの復元

本章では、取得済みのバックアップデータの復元方法を説明します。
バックアップデータの復元には大きく分けて 2 種類があり、ファイル／フォルダの復元と、バックアップ対象マシンそのものの復元となります。

バックアップ対象マシンを復元する場合、用途に応じて 2 種類の方法があります。バックアップ対象マシンが破損してしまった場合、起動しない場合には Bootable Media を利用した復元方法。対象マシンが現在正常に稼働中で、特定のバックアップ時点まで戻したいような場合には Cyber Protection コンソールからの復元方法が有効です。

4.1 ファイルの復元

ファイル／フォルダ(ディレクトリ)単位の復元は Cyber Protection コンソールから実行します。

4.1.1 ファイル、フォルダのリモート復元

① Cyber Protection コンソールにログイン後、復元したいマシンを選択してメニューから「復元」を押下します

② 復元したいバックアップを選択し、「復元」から「ファイル／フォルダ」を押下します

【バックアップロケーション】
復元対象のデータが格納されているストレージ（ローカル／クラウドストレージ）を選択します。

【n 件のバックアップ】
時系列に過去のバックアップが表示されるので、任意の日時のバックアップを選択します。

※復元するバックアップが「ファイル／フォルダ」のバックアップデータの場合には「復元」ボタンの代わりに「ファイル／フォルダの復元」ボタンが表示されます

③ 復元したいファイル、フォルダを選択して、画面右の「復元」ボタンを押下します

④ 復元先を選択したのちに「復元を開始」を押下して復元を実行します
この際、復元先として「元のロケーション」以外に「カスタムロケーション」を選択して任意の場所に復元を行う事も可能です。また、どちらの場合も上書きなどの選択が可能です。

⑤ 「実行」を押下して復元を開始します

4.1.2 ファイルのダウンロード

① ログイン後、復元したいマシンを選択してメニューから「復元」を押下します

② 復元したいバックアップを選択し、「復元」から「ファイル／フォルダ」を押下します

③ 復元したいファイルを選択し、画面右の「ダウンロード」ボタンを押下します

※100MB を超えるファイルや、フォルダを指定したダウンロードは出来ません

④ 選択したファイル、フォルダーがダウンロードされます

※お使いのブラウザ、OS 環境等によって上記画面は変更となる可能性がございます

4.2 WebUI からのマシン復元

復元対象マシンが正常に稼働中で、特定バージョンに戻したい等の復元であれば Cyber Protection コンソールから復元操作を実行することが可能です。

4.2.1　経路情報の設定

復元動作時にネットワーク接続が失われることを防ぐために、あらかじめ利用する経路情報についての設定を実施いたします。バックアップエージェントのインストール時に本手順を実行済みであれば、設定をスキップしてください。

Linux 環境の場合	2.2.6 復元操作向けの設定
Windows 環境の場合	2.3.5 復元操作向けの設定

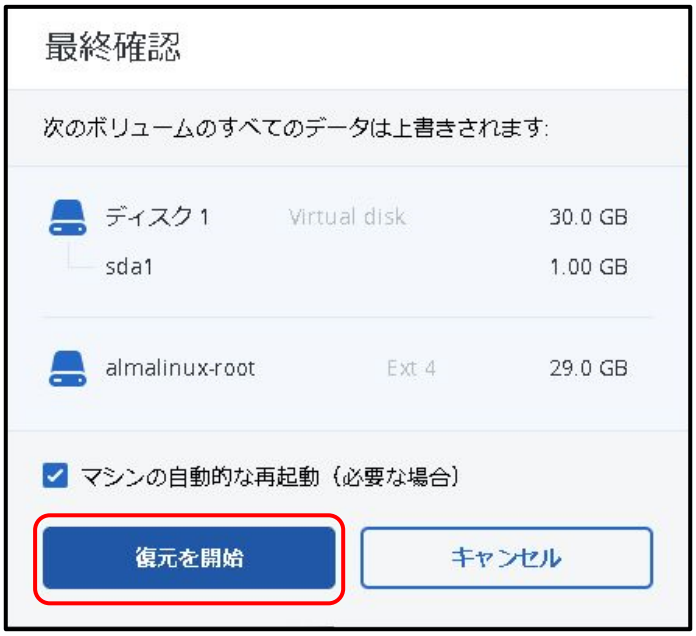
4.2.2　復元操作の実行

① 復元対象マシンを選択して「復元」→「マシン全体」を選択します

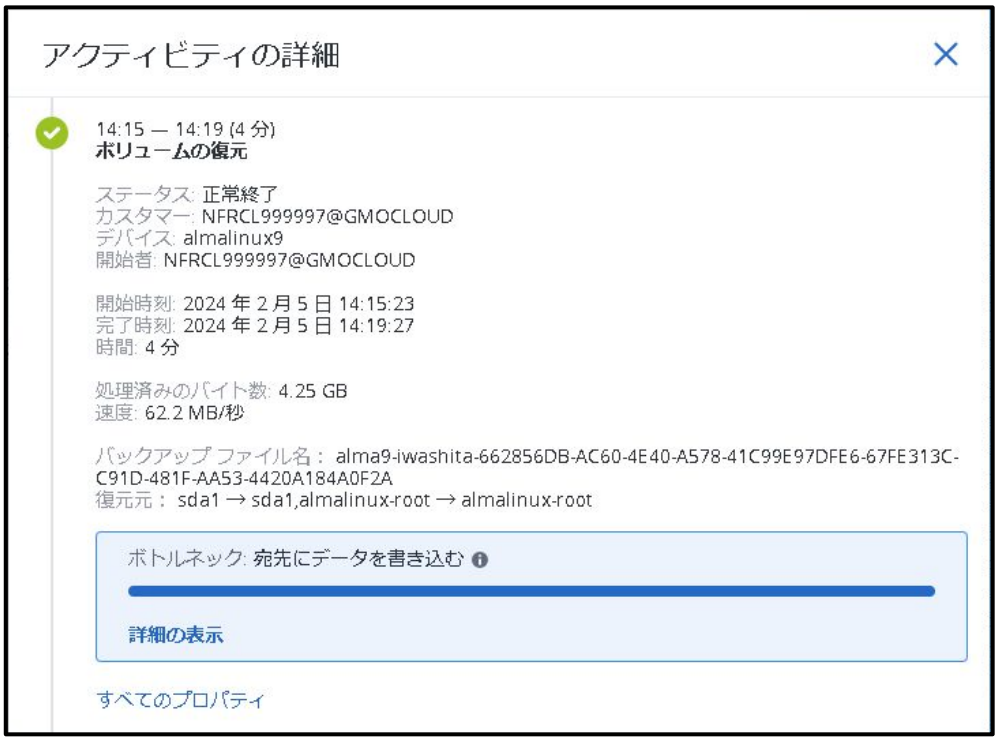
② 復元メニューが表示されるので、対象及びデバイスマッピングの内容を確認して「復元を開始」を押下します

※復元先は「物理マシン」のままで問題ありません

③ 最終確認画面が表示されるので内容を確認して「復元を開始」を押下します



④ アクティビティ画面を確認して復元タスクの完了するまでお待ちください



4.3 Bootable Media からのマシンの復元（仮想サーバ）

マシンの復元を行う際には事前に仮想サーバーをパワーオフの状態にしてください

4.3.1　ブータブルメディアのダウンロード

① Cyber Protection コンソール右上の人型アイコンから「ダウンロード」を選択します

② ツールの項目にある「Bootable media」を押下してダウンロードします

③ 操作端末に「Boot_media.iso」がダウンロードされます

④ 混乱を避けるためファイル名を「Acronis_Boot_media.iso」に変更してください

4.3.2　ブータブルメディアのアップロード

① ダウンロードしたブータブルメディアを VCD 環境にアップロードします

vCloud Director 環境へのメディアアップロード手順はメーカーサイトのドキュメントをご確認下さい。

メーカーサイト	https://techdocs.broadcom.com/jp/ja/vmware-cis/cloud-director.html

－製品ページから「VMware Cloud Director」→「テナントガイド」を選択
－「メディアファイルの操作」項にある「メディアファイルアップロード」を参照ください

4.3.3　ブータブルメディアのマウント

① vCloud Director にログインします

② リストア対象の仮想マシンの縦三点リーダーから「メディアを挿入」を選択します

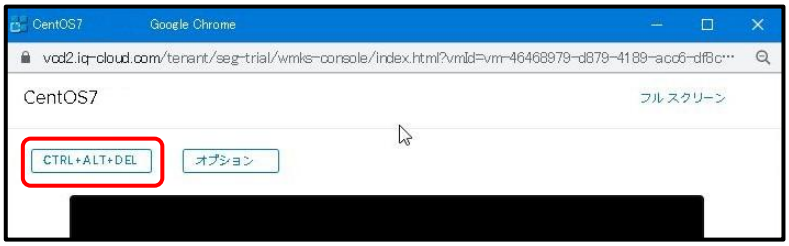
③ 「CD を挿入」ウィンドウが起動するので、名前横のろうと型のアイコンを押下すると表示される検索窓に「Acronis_Boot_meida.iso 」と入力して「×」ボタンを押下します。

④ アップロードしたメディアが表示されますので、選択して「挿入」ボタンを押下します

⑤ 縦三点リーダーから「パワーオン」を実行し、「Web コンソールの起動」を選択します

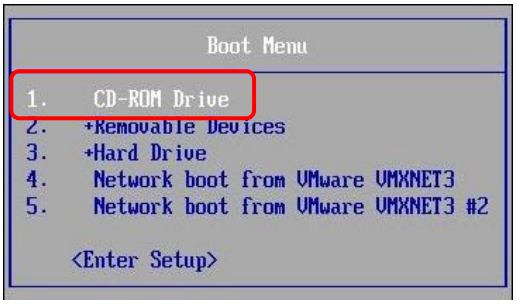
4.3.4　ブータブルメディアからのブート

① 仮想コンソールが起動したら画面上部の「CTRL+ALT+DEL」アイコンを押下します



② ブータブルメディアの起動画面が表示されます

※OS が通常起動してしまう場合には OS のブートデバイス選択順序を変更します、
Boot スクリーンが表示されたら「ESC」キーを押下して Boot Menu に入り、「↑」「↓」キーで「CD-ROM Drive」を選択して「Enter」キーを押下します



[Boot スクリーンは非常に短時間の表示となるため、タイミングを合わせて実行して下さい]

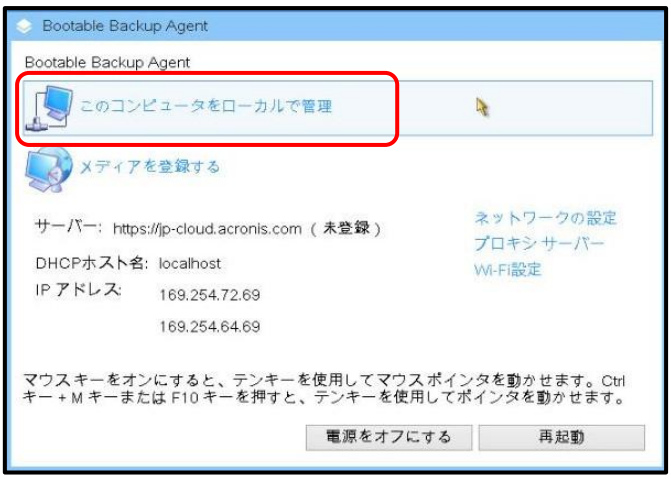
・リセットアイコンを押下する
・マウスカーソルを仮想コンソール画面内に移動してクリックして画面に入る
※仮想コンソールにマウスのカーソルを移動すると矢印から人の手のアイコンに変わり、画面上でクリックするとポインタが消えます
・vmware の表示が瞬間的に表示されるので「ESC」キーを押下する
・失敗したら「Ctrl＋Alt」で仮想コンソールから抜けて、再度リセット
※コンソールを抜けずに「Ctr＋Alt＋Ins」でリセットをかける方法も有効です

4.3.5　ブータブルメディアからの復元

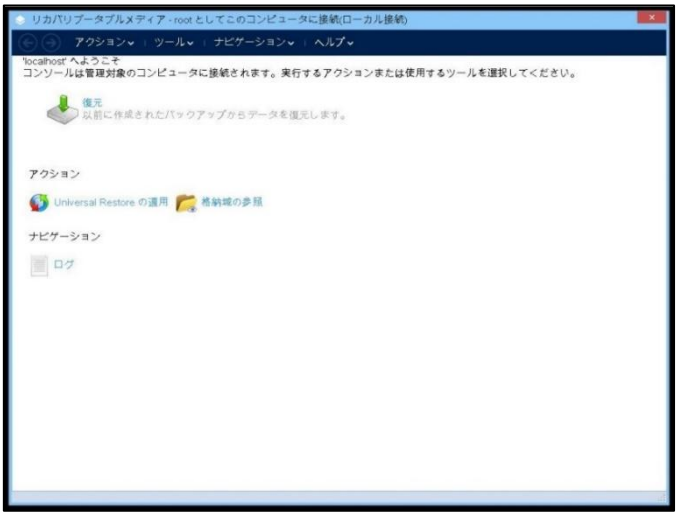
① 復元画面が表示されたら [Langurage]から日本語を選択し、「Rescure Media」を選択します

※マウスがきかない場合には
「Tab」でメニュー項目の移動、
「↑ ↓」で選択項目の操作、
「Enter」で項目の確定が可能です。

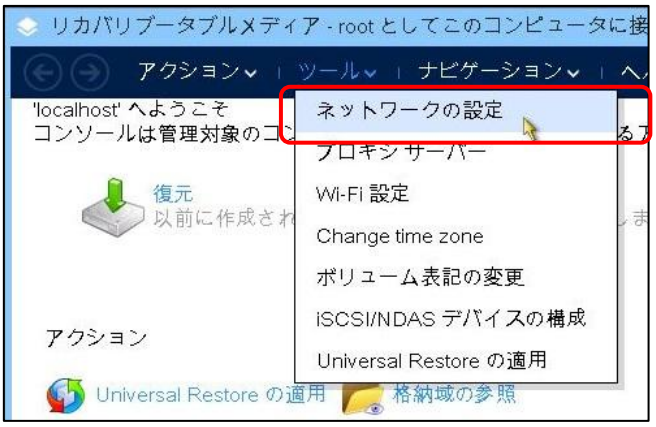
② 操作の選択画面に遷移するので「このコンピュータをローカルで管理」を選択します



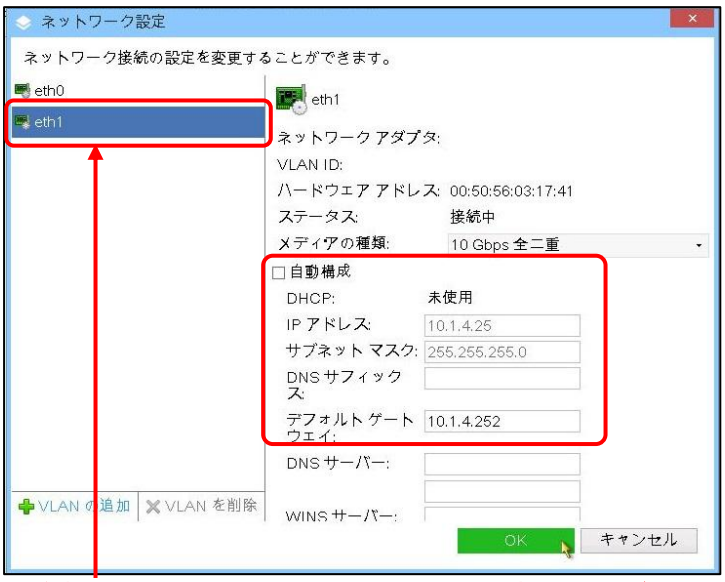
③ ブータブルメディアからの起動が始まり、TOP メニューが表示されます



④ 「ツール」→「ネットワークの設定」を選択します



⑤ ネットワーク設定を変更します



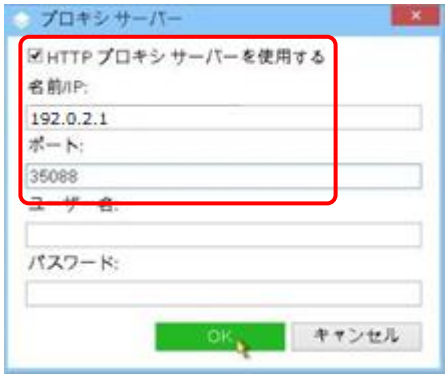
【自動構成】
チェックを外してください

【IP アドレス】
バックアップネットワークにつながる VLAN の IP アドレスを入力してください

【デフォルトゲートウェイ】
エージェント導入時の経路設定で指定したゲートウェイ IP を入力して下さい

※複数のネットワークインターフェースを持つサーバーでは、必ずバックアップネットワークにつながるネットワーク I/F を指定してください

⑥ クラウドストレージからの復元を実行する場合は「ツール」→「プロキシサーバー」からプロキシ設定を実施ください。　※[バックアップ GW]の値は設定完了通知書を確認ください

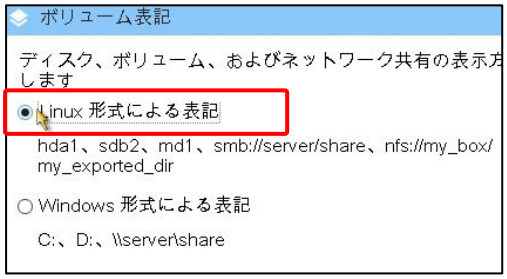


【HTTP プロキシサーバーを使用する】
チェックを入れる

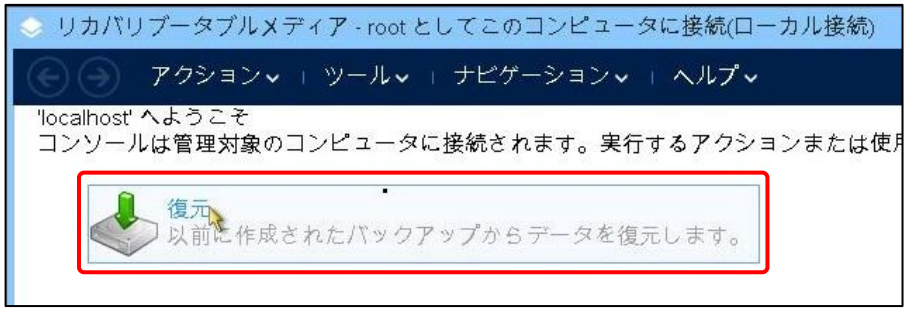
【名前/IP】
[バックアップ GW]

【ポート】
35088

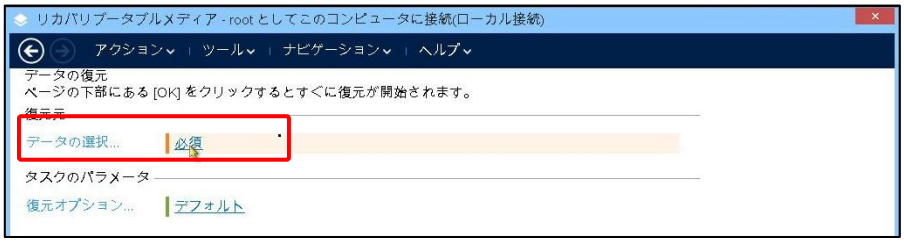
⑦ LVM を使用してるLinux サーバー復元時には「ツール」→「ボリューム表記の変更」から「Linux 形式による表記」を選択して下さい。
※表記変更時に手順②の画面に戻ることがありますが、以降の手順に進んでください



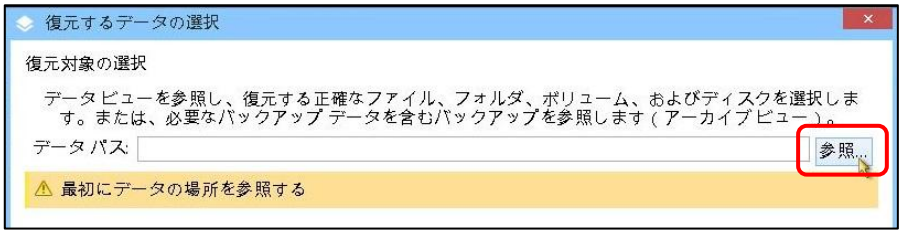
⑧ 「復元」を押下します



⑨ 「データの選択」を押下します



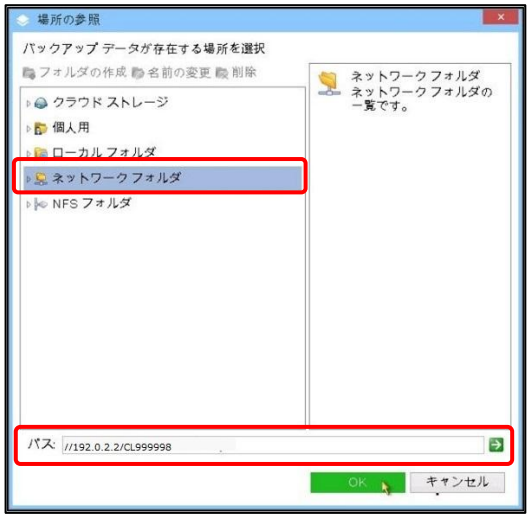
⑩ 復元データの選択ウィンドウが表示されたら、「参照」を押下します

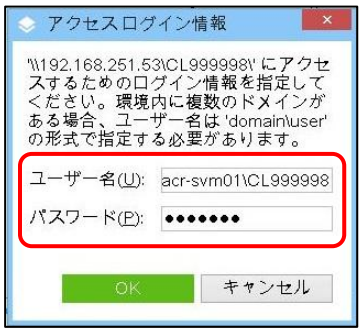


⑪ 場所の参照ウィンドウが表示されたらデータ格納場所を選択して、必要な認証を行います

［ネットワークフォルダの場合］　※[ストレージ GW] の値は設定完了通知書を確認ください

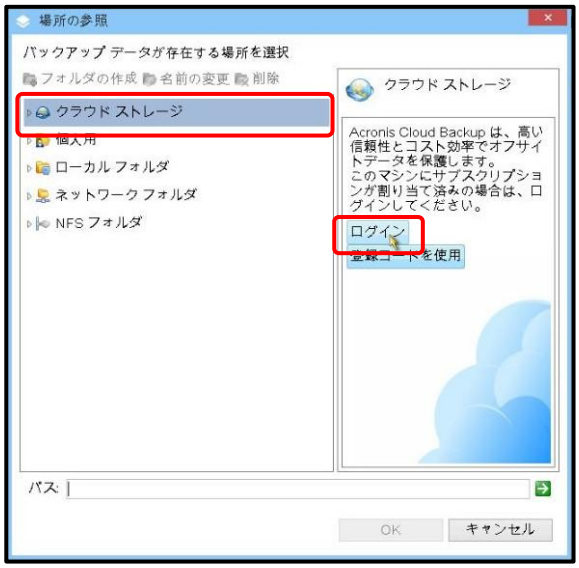
【　パス　　】保護計画作成時に設定した格納先ストレージの情報を入力して下さい
［格納先ストレージ］ ¥¥**[ストレージ GW]**¥**[契約番号]**
例）¥¥192.0.2.1¥CL999998
※画面表示上「¥」は「＼」として表示されます
【ユーザー名】acr-svm01¥**[契約番号]**　　例）acr-svm01¥CL999998
【パスワード】設定完了通知に記載されているパスワード





［クラウドストレージの場合］
「ログイン」を押下して認証を行います。

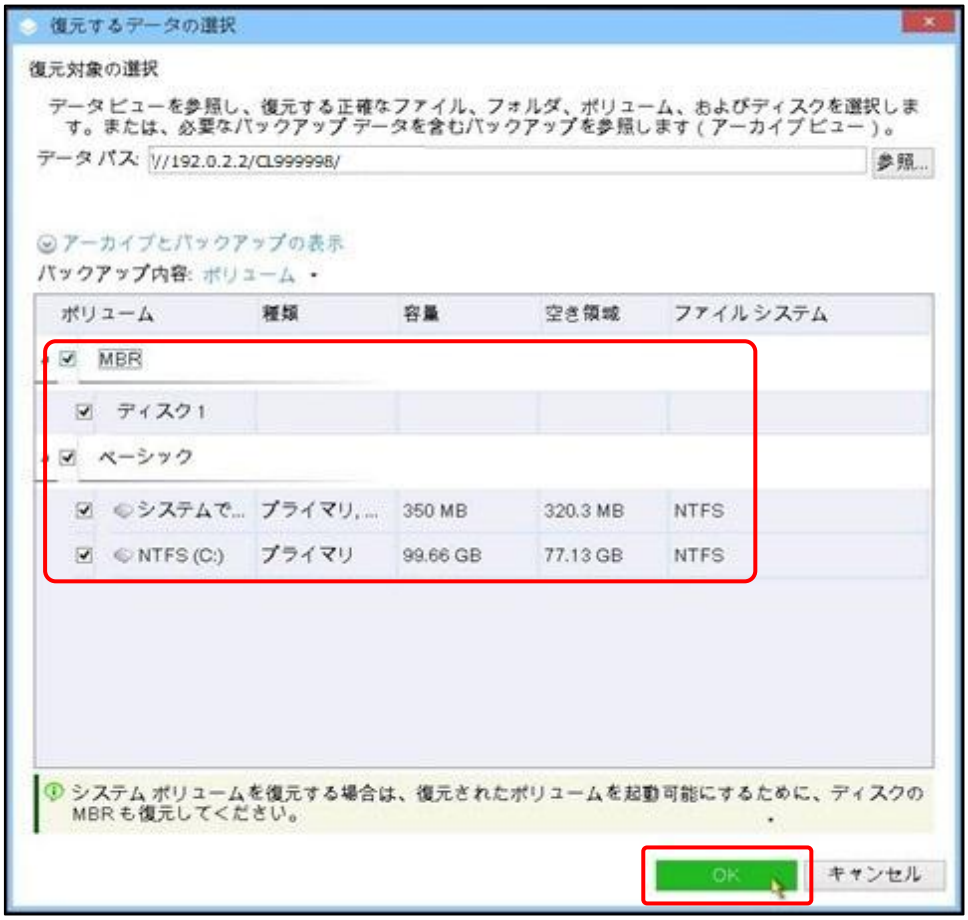
【ログイン　】[契約番号]@GMOCLOUD
【パスワード】ご自身で設定したログインアカウントのパスワード



※セキュリティの設定で二要素認証を有効にしている場合、上記の手順による認証が通らない仕様となっております。「4.2.6. 登録トークンを利用したメディアの登録」を実行してください。

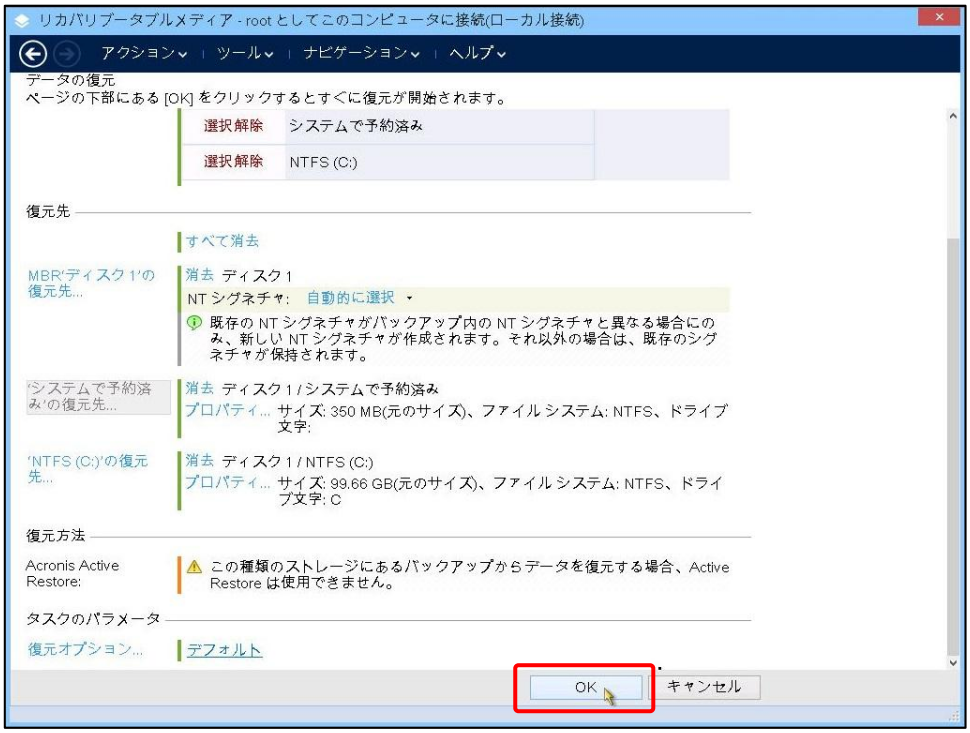
⑫ バックアップの一覧が表示されるので「表示：」から「ディスクアーカイブ」を選択した後に復元したいバックアップを選択して「アーカイブとバックアップの非表示」を押下します

⑬ 対象ボリュームのバックアップ内容が表示されるので、復元したいデータを選択して「OK」を押下します

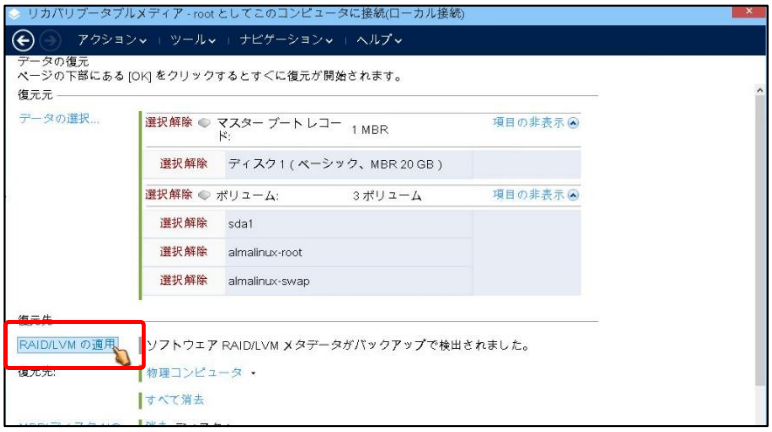


※システム丸ごとの復元であれば、全てのチェックボックスにチェックを入れてください

⑭ 準備ができたら「OK」を押下して復元を開始します

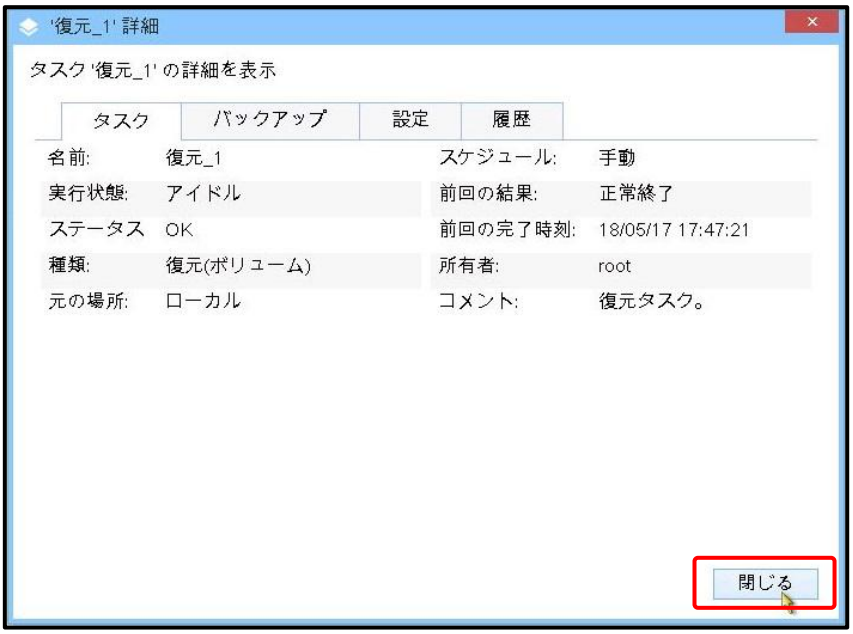


※LVM 利用時の注意
LVM 利用環境の復元時には「RAID/LVM の復元」が表示されるので、リンクを押下後以降の手順を進めてください。



⑮ 復元が完了するまでの時間はデータ量や環境によって変化します

⑯ 復元終了後、「閉じる」ボタンを押して復元タスクの画面を閉じます



⑰ 画面上のメニューから「アクション」→「終了」を選択します。

⑱ 「電源をオフにする」で処理を終了してサーバーの電源をオフにします。

※再起動した場合に、再度復元プログラムが起動する可能性がありますので、
忘れずにブータブルメディアを取り出してください。

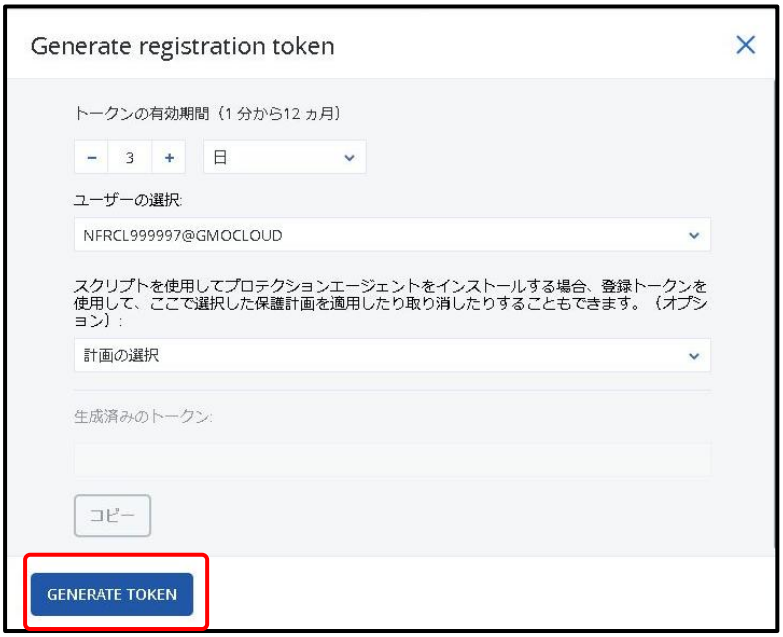
4.3.6　登録トークンを利用したメディアの登録

この手順では、Bootable Media を利用したバックアップの復元時に、クラウドストレージからデータを復旧するための認証の流れを記載いたします。

① Cyber Protection コンソールの TOP メニュー「デバイス」からデバイス表示画面に遷移して「＋追加」を押下する

② 登録トークンというセクションにある「生成」ボタンを押下する

③ 画面下部の「GENERATE TOKEN」を押下してトークンを生成する



④ 生成したトークンをテキストなどにコピーする

※あとからこの文字列を確認する方法がないため、消失してしまった場合は新たにトークンを作成してください。

⑤ 復元画面の TOP から「ツール」→「バックアップサービスでメディアを登録」を選択

⑥ 先ほど取得したトークンを入力して「登録」を押下する

⑦ 復元対象の選択からクラウドストレージを選択すると、認証済みのアカウントが表示されるので操作を継続する

4.4 Bootable Media からのマシン復元（物理サーバ）

4.4.1　レンタルサーバーの復元

当社よりレンタル提供しているサーバーで障害が有った場合、お客さまリクエストによる復元が必要となった場合には、必要な情報を提示頂いた上で弊社スタッフが本作業を代行致します。

① サポート窓口に以下の情報を添えてご依頼下さい

1. 契約会社名
2. 契約番号
3. 担当者名
4. ご連絡先（電話及びメール）
5. 復元対象となる物理サーバーの機材管理番号
6. 復元対象ホスト名
7. 復元対象ホストの IP アドレス、ネットマスク
8. 復元したいデータ（ホスト名とバックアップ取得日時）

② 弊社スタッフにて復元作業を実施いたします

復元にかかる時間はデータ量（サイズ、数量）にもよりますが、5GB の OS バックアップデータからのマシン復元で 30 分～60 分程度となります。

③ サーバーを起動し、ログイン画面が表示されましたら折り返しのご連絡をさせて頂きます

指定頂いたバックアップが見当たらない、復元後にサーバーが起動しないなど、何らかの問題が発生した場合においても、ご判断を仰ぐために連絡させて頂きますのでご承知おきください。

4.4.2　お客さま持込みマシンの復元

当社 IDC でお預かりしているお客さま持ち込みサーバーで復元を実施される場合には次の手順に従って復元を実施ください。

① リカバリメディアの用意

Cyber Protection コンソールから「ISO イメージのダウンロード」を実施いただき、メディアを作成してご持参ください。
※機種・構成によっては通常のブータブルメディアでは起動しない場合があります。
　事前に検証サービスをご契約頂いている場合には、当社から提供させて頂いたメディアをご持参ください。

② IDC への入館申請

ハウジングサービスご契約時に案内させて頂いている入館手続きを実施ください。

③ 入館と作業準備

データセンターまでお越しください。弊社スタッフがアテンドさせて頂きます。
お客さまマシンに DVD ドライブが無い場合にはポータブルドライブの貸与が可能です。

④ ブータブルメディアからの復元

以降の手順は「4.2.3」同様となります。

5. エージェントのアップデート

本章では、バックアップ対象サーバーにインストールしたエージェントの手動アップデート方法について記載いたします。

※ご提供中の環境では、エージェントの自動更新が有効になっているため手動でのアップデートは原則不要となりますが、トラブルなどで自動更新が上手くいかない場合などはこちらの手動更新をお試しください。

5.1 エージェントのアップデート

① Acronis Cyber Protect Cloud の Web ページを開き、ログインして下さい

② TOP メニュー「設定」→「エージェント」にてアップデート対象ホストを選択して「エージェントのアップデート」を押下します

※「エージェントのバージョン」横の「!」マークを押下しても同様の操作が可能です

③ アップデートの確認が表示されるので「はい」を押下します

④ エージェントのアップデートが実行され、完了するとバージョン表示が変わります

6. 管理ポータルでの設定変更

本章では、管理ポータルを利用したメール通知の設定変更や、管理 UI への接続元 IP 制限設定の変更方法などについて記載いたします。

6.1 管理ポータルへのログイン

管理ポータルには、Cyber Protection コンソールの TOP メニューにある「アカウントの管理」ボタンから遷移します。

6.2 通知メールアドレスの変更

① 管理ポータルにログインします

② 「ユーザー」からユーザーを選択して「一般情報」横の鉛筆マークを押下します

③ 電子メール欄のメールアドレスを変更したい内容に変更して「完了」を押下します

④ 変更についての確認が表示されるので「はい」を押下します

※この操作により、指定したメールアドレスに「登録電子メールの変更確認」という件名のメールが送付されます。このメールを承認すれば完了となります。

6.3 通知設定の変更

① 管理ポータルにログインします

② 「ユーザー」からユーザーを選択して「設定」横の鉛筆マークを押下します

③ 必要箇所を変更して「終了」を押下します

項目名	説明
メンテナンスに関する通知	製品提供元からのメンテナンス通知（有効を推奨）
クォータの超過に関する通知	ライセンス超過、ディスク容量超過などのアラート通知
定期使用状況レポート	月次利用状況のサマリレポートを送信するか
失敗に関する通知	バックアップの失敗時の通知
警告通知	バックアップが警告を伴って正常に終了した際の通知
成功の通知	バックアップが正常に終了した際の通知
アクティブなアラートの日次サマリ	アクティブなアラートの日次サマリを送信するか
デバイス制御通知	制限対象デバイス等の利用が施行された際に通知を行うか
復元通知	通知対象機能の提供なし（無効を推奨）
データ漏洩防止通知	通知対象機能の提供なし（無効を推奨）
マルウェア検知通知	マルウェアが検知された際に通知を行うか
インフラストラクチャの通知	通知対象機能の提供なし（無効を推奨）

6.4 IP アドレス接続元制限設定の変更

① 管理ポータルにログインします

② 「設定」→「セキュリティ」を選択します

※IP アドレス接続元制限設定が未設定の場合には上記画面になりますのでスライダーを右にスライドして「ログイン管理」を有効にしてください。

③ 制限設定を入力して「保存」を押下してください

【許可された IP アドレス】
- 複数ある場合はセミコロンで区切って入力してください
- ハイフン"-"でつないで範囲指定も可能です
- "/"でサブネットマスクでの指定も可能です

以上