Arcserve UDP Cloud Direct スタートアップ ガイド

【Windows 編】

本資料は、Arcserve UDP Cloud Direct の製品概要をご理解した方向けに、
物理の Windows 環境を保護するための設定手順を記載したガイドです。
他の構成のためには以下のガイドもご用意をしています。

- ◆ Arcserve UDP Cloud Direct スタートアップ ガイド 【仮想エージェントレス編】
  https://www.arcserve.com/wp-content/uploads/2019/09/ucd-startup-guide-agentless.pdf
- ◆ Arcserve UDP Cloud Direct スタートアップ ガイド 【Linux 編】
  https://www.arcserve.com/wp-content/uploads/2019/09/ucd-startup-guide-linux.pdf

Arcserve UDP Cloud Direct の製品概要については、下記をご参照ください。

◆Arcserve UDP Cloud Direct 紹介資料
https://www.arcserve.com/wp-content/uploads/2019/08/ucd-presentation.pdf

改訂履歴

2019 年 8 月　Rev1.0 リリース

2019 年 9 月　Rev1.1 リリース

- 表紙に他のガイドの案内追記
- 画面ショット更新

2019 年 11 月　Rev1.2 リリース

- クラウド側のストレージ消費量についての表記修正

2020 年 3 月　Rev1.3 リリース

- フェイルバックに関する追記
- トライアル開始方法の変更に伴う修正

2020 年 4 月　Rev1.4 リリース

- ライセンス購入時にも[トライアル開始]をクリックする旨を追記

2020 年 7 月　Rev1.5 リリース

- 東日本リージョン開設に伴う修正
- タスクの設定に機能追加
- 一部 URL のリンク切れ修正

2020 年 10 月　Rev1.6 リリース

- SPEED TEST サイトに東日本リージョンが追加されたことに伴う修正
- Arcserve UDP 変更トラッキングドライバとの競合についての情報追加
- エージェントの Web プロキシ設定追加
- UI に Exchange が追加されたことに伴う修正

2021 年 3 月　Rev1.7 リリース

- UI の全体的な変更にともない手順の文言変更、スクリーンショット貼り替え
- トライアルについて注意書きを追記

2021 年 7 月　Rev1.8 リリース

- 利用する通信ポートの追記、表現修正
- BaaS の保存期間に 2 か月、 3 か月、 6 か月を追加
- BaaS のディスク全体バックアップの増分で時間がかかる場合があることを記載
- DRaaS のプロビジョニングによりバックアップ運用が停止する旨を追記
- [トライアル版の開始]についての注意の文言微修正

2021 年 11 月　Rev1.9 リリース

- 2 要素認証に関する記述追加
- プロキシのアカウント設定について補足
- リストアの補足として、システムブートは不可な旨を追記
- アイコン変更
- UNC パス指定によるバックアップが可能なことを追記

2022 年 1 月　Rev1.91 リリース

- ライセンス登録の時差計算の誤りを修正

目次

1　用語と構成例

1.1 用語の説明

- Arcserve Business Continuity Cloud

Arcserve が提供するデータ保護サービスの総称です。Arcserve UDP Cloud Direct と Arcserve UDP Cloud Hybrid の 2 種類のサービスで構成されています。「Arcserve クラウド」と省略されることもあります。

- Arcserve UDP Cloud Direct

本書で説明するバックアップ サービスです。「Cloud Direct」と省略されることもあります。

- BaaS（Backup as a Service : バックアップ サービス）

Arcserve UDP Cloud Direct のバックアップ/リストア機能だけを使う方式です。

- DRaaS（Disaster Recovery as a Service : 惨事復旧サービス）

バックアップ/リストアに加えて、本番システムの代替仮想マシンを Arcserve クラウド上で起動できる方式です。

1.2 使用するコンポーネント

◆BaaS/DRaaS 共通

- Arcserve Business Continuity Cloud コンソール（以下 Cloud Console）

Web ブラウザで利用するクラウド ベースの管理 UI です。
ライセンス管理、コンポーネントのダウンロード、バックアップ設定、リストア、ジョブ監視等の管理機能を提供します。

- Arcserve UDP Cloud Direct Agent（以下 Cloud Direct エージェント）

バックアップ対象に導入するプログラムで、バックアップ データを Arcserve クラウドに転送します。Windows 用と Linux 用があります。Replication Agent と呼ぶ事もあります。

◆ DRaaS 利用時のみ

- VPN サーバ

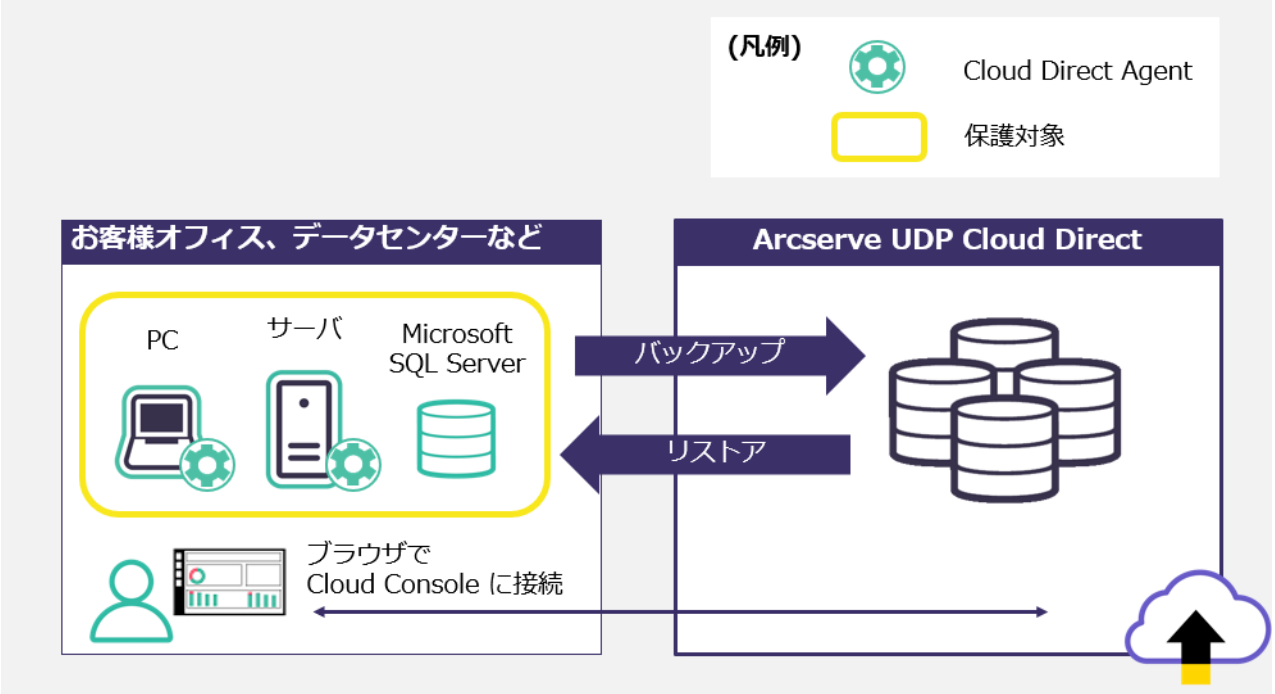
DRaaS の利用時に Arcserve クラウド内に用意されます。オンプレミスから Arcserve クラウドにポイント対サイトの VPN 接続を行う際に使用します。

- Active Directory サーバ（オプション）

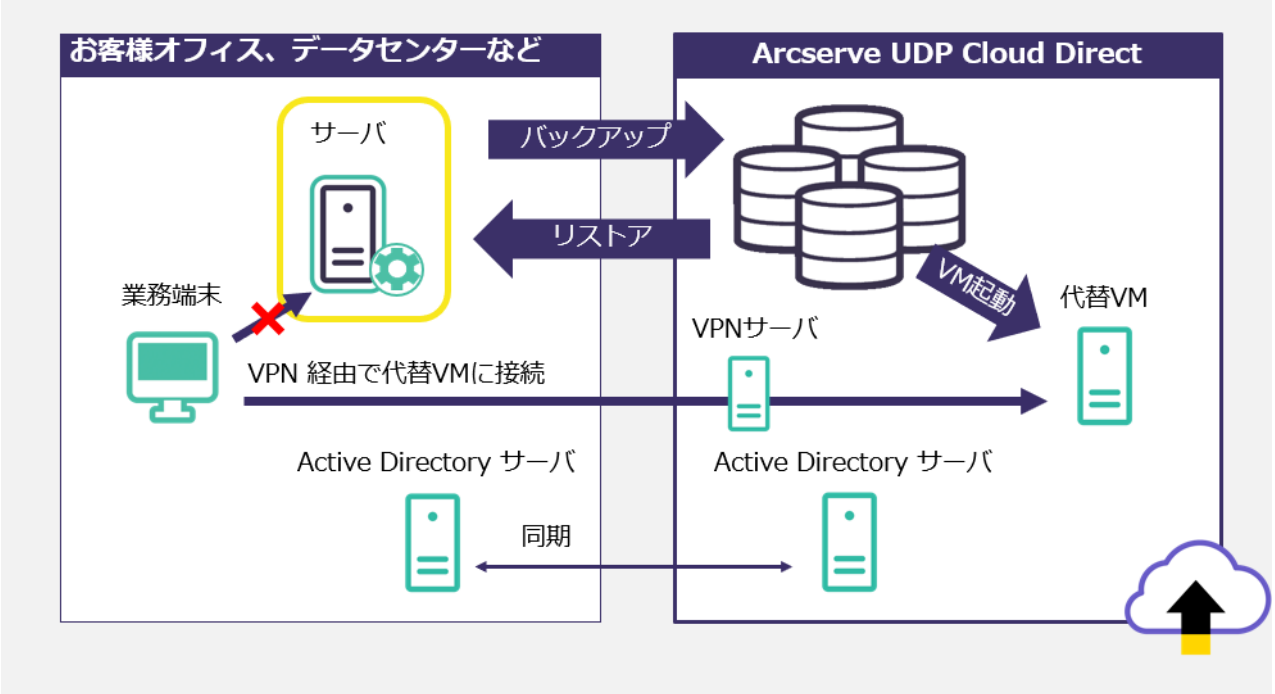
DRaaS の利用時にオプションで Arcserve クラウド内にご用意します。オンプレミスの Active Directory サーバから Active Directory 情報をあらかじめ同期しておくことで、災害発生時でもドメイン環境でシステムを継続運用することができます。

1.3 Windows 環境のバックアップ構成例

以下は Backup as a Service（BaaS） 構成の一例です。



以下は Disaster Recovery as a Service（DRaaS） 構成の一例です。



2 事前確認

2.1 Arcserve UDP Cloud Direct 環境構築の流れ

この資料では、以下の流れで環境構築の流れに沿って手順を説明します。

2.2 動作要件、その他要件の確認

サブスクリプションの購入前に、保護対象サーバが Arcserve サポート ポータルの動作要件に記載され、ご利用いただくネットワーク環境が要件を満たしていることをご確認ください。

○ 動作要件

https://support.arcserve.com/s/article/115003836346?language=ja

○ その他の要件

◆ BaaS/DRaaS 共通

- 各コンポ―ネットを導入する環境にインターネット接続環境をご用意ください。
- Arcserve UDP Cloud Direct は通信のために以下のポートを利用します。

443/TCP（送信）、8443/TCP（送信）

Arcserve UDP Cloud Direct Agent 利用環境にて、以下のホスト名やサブネットに対して上記ポートで通信できる必要があります。必要に応じて組織のファイア ウォールにポート開放のための設定を行ってください。

・admin.zetta.net
・dataapi.zetta.net
・smpping.zetta.net
・smpstatus.zetta.net
・cloud.arcserve.com
・ccapi.arcserve.com

・210.162.185.0/24（東日本リージョンの場合）
・74.114.124.0/22（Santa-Clara リージョンの場合）

◆ DRaaS 利用時は、以下もご留意ください。

- DRaaS は東日本リージョンでは未提供となります。
- Arcserve テクニカル サポートへの事前お申込みが必要です。詳細は、3.3 DRaaS 設定のサポート依頼をご覧ください。
- ポイント対サイト VPN の利用のために OpenVPN ツールを使用する時、以下のポート開放が必要です。

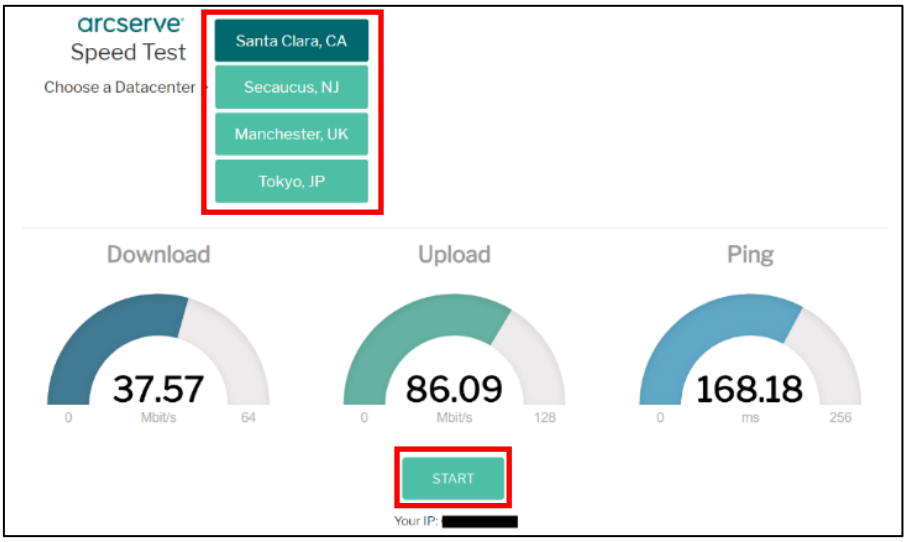
・1194/UDP（送信/受信）

◆ （任意）通信レートの確認

下記の Arcserve Speed Test サイト URL にアクセスすると、お客様環境と Arcserve データセンター間のダウンロード/アップロードの通信レート、Ping の応答遅延時間を測定できます。計測を開始するにはご利用になるデータセンター（Santa Clara, CA もしくは Tokyo, JP）を選択し、ページ内の[START]をクリックします。

<ご参考>

Arcserve Speed Test サイト　http://speedtest-sc.arcserve1.com/



注意：実際のバックアップやリストアの速度はソースの読み取りや圧縮、管理のための付加的な処理等さまざまな要因の影響を受けるため、必ずしもここで測定した結果とは一致しません。傾向を確認するためにご利用ください。

3 管理用アカウントの登録とライセンス有効化

3.1 管理用アカウントの登録

サブスクリプションの購入後には、管理者アカウントの登録を行ってください。

1. はじめてご利用いただく方は、Arcserve UDP Cloud Direct の管理用アカウントを登録するため、Web ブラウザより以下の URL にアクセスしてください。
   既にアカウント登録済の方は" **3.2　Cloud Console へのアクセスとライセンスの有効化**"に進んでください。
   https://cloud.arcserve.com/enroll

2. 画面右側の空欄をすべて入力します。電子メールアドレスは、Cloud Console へのログイン ユーザ名として使用されます。入力後「サービス規約に同意します」にチェックを入れ、[次へ]をクリックします。

3. バックアップ先のデータセンターとして**以下のいずれかから購入したストレージ サブスクリプション対応するものを選択してください。**

   ・「カリフォルニア州サンタクララ」（BaaS、DRaaS 対応）

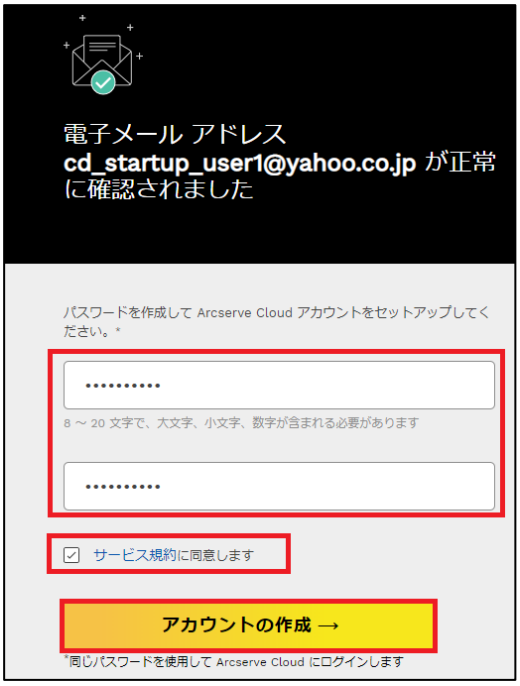
   ・「東日本」（BaaS のみ対応）

   [次へ]をクリックすると、指定したメールアドレスにアカウントをアクティブ化するためのリンク情報を記載したメールが送信されます。

4. 指定したメールアドレスを HTML メールで受信し、メール本文中の [アカウントの作成]をクリックすると、アカウントのアクティブ化と、ブラウザの自動起動によりパスワード入力画面が表示されます。

   注意：メールが届かない場合は、noreply@arcserve.com からのメールが迷惑メールとしてブロックされていないかをご確認ください。

5. [パスワード]入力と[サービス規約に同意します]チェック後、[アカウントの作成]をクリックします。



6. 画面上部に［トライアル版の開始］が表示されている場合はクリックして、ご利用リージョンを選択してください。

注意：ライセンスをご購入いただいている場合もこの操作は行ってください。

注意：Cloud Direct のトライアルを下記のサイトから登録して行っていた場合、[トライアル版の開始]リンクは表示されず、クリックする必要はありません。

https://www.arcserve.com/jp/cloud-direct-free-trial/

注意：トライアル期間は 15 日間です。トライアル終了後も継続してご利用いただく場合は、ライセンスのご購入、アクティブ化の操作が必要です。トライアル終了から 30 日以内にアクティブ化を行ってください。30 日以後はクラウド上のボリュームが削除されるため、実運用環境への移行はできなくなります。

3.2 Cloud Console へのアクセスとライセンスの有効化

Cloud Console 上でライセンスの有効化（アクティベーション）を行います。サブスクリプションのご連絡先メールアドレス宛に届くライセンス プログラム証書をご用意ください。

※メールは送信元が「License Program (licenseprogram@arcserve.com) 」、件名が「Arcserve - License Order Confirmation #xxxxxx」（#xxxxx は Order ID）となります。

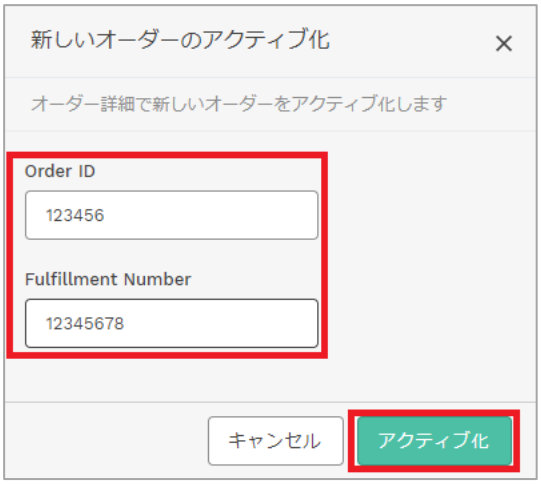
1. ライセンスを有効化（アクティベーション）するには以下 URL より Cloud Console に登録済みの電子メールアドレス、[パスワード]を入力しログインします。

   https://cloud.arcserve.com/login

※こちらのサイトはバックアップやリストア設定など、今後の管理を行う際の Cloud Console へのログイン画面となりますので、Web ブラウザへのブックマークをお勧めします。

2. 画面左のアイコンの中から[設定]、[エンタイトルメント] と順にクリックし画面右上の、[新しいオーダーのアクティブ化]をクリックします。

3. ライセンス プログラム証書に記載されている [Order ID]、[Fulfillment Number]を入力し、[アクティブ化]をクリックします。



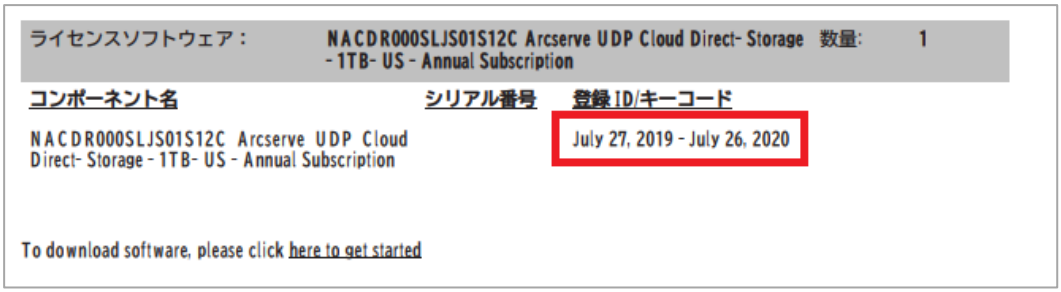
[オーダーは正常に処理されました]と表示され、ライセンス情報が画面に反映されます。

登録日が購入ライセンスの開始日当日の場合、ライセンスの反映はサービス開始日のカリフォルニア州 サンタクララ時刻の 0:00 以降となるため日本時間では以下の時刻に反映されます。

- サマータイム期間： 日本時間の 16:00
- サマータイム期間外： 日本時間の 17:00

に反映されます。

サブスクリプションの開始日は ” ライセンス プログラム証書” PDF に記載されています。



3.3 DRaaS 設定のサポート依頼

DRaaS の利用には Arcserve テクニカル サポートへの事前お申込みが必要です。お申込みいただくとご購入いただいているストレージ サイズ範囲内で利用可能な DRaaS 専用ボリュームを追加します。

下記、Arcserve サポート ポータルにて DRaaS の有効化を依頼します。

Arcserve サポート ポータル：https://support.arcserve.com/s/?language=ja

サポートポータルの利用方法については以下 URL のポータルマニュアルをご覧ください。

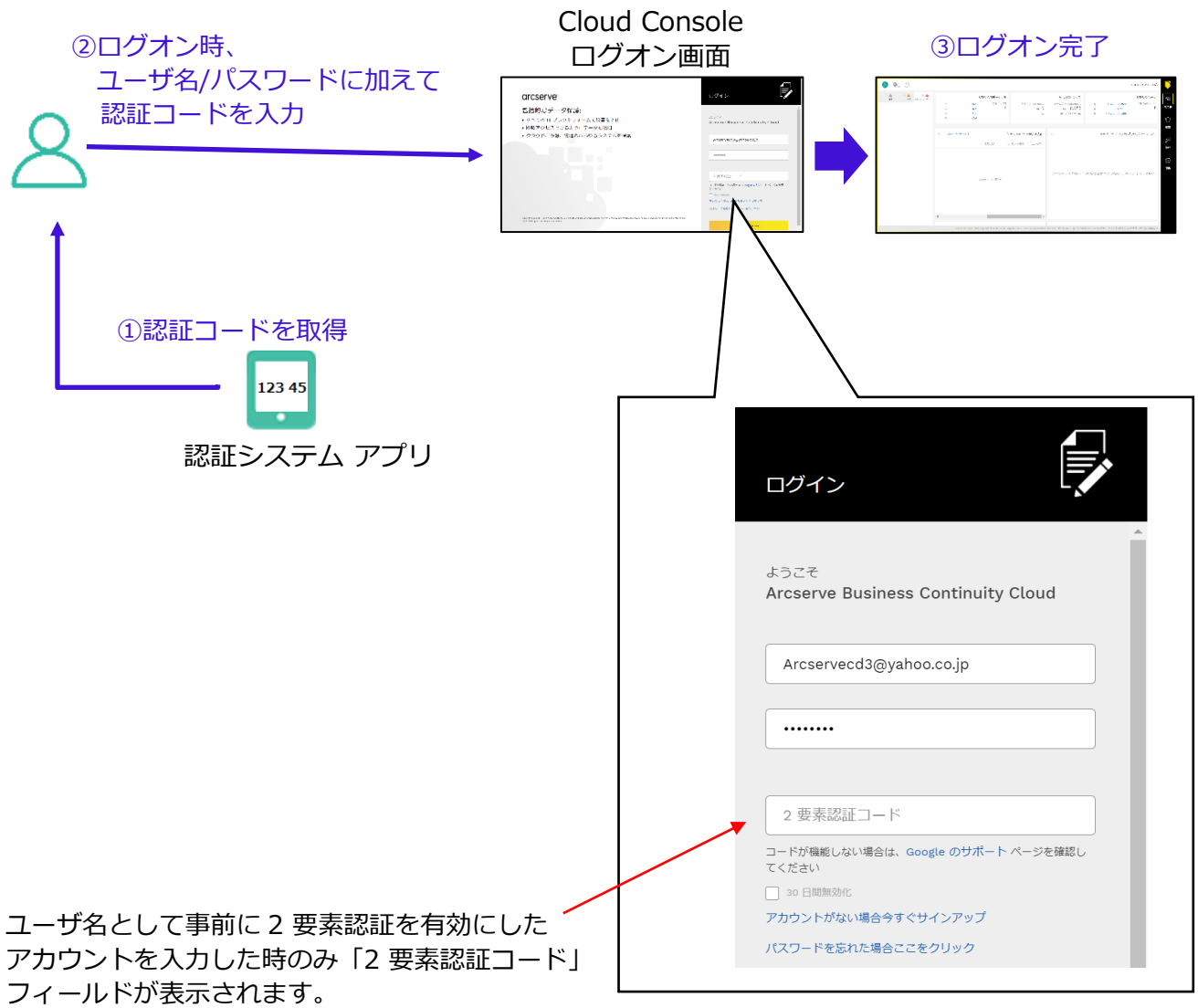
https://support.arcserve.com/s/article/202937699?language=ja

3.4　2 要素認証の利用（オプション）

Cloud Direct のログオン アカウントに対して 2 要素認証を有効化することで、Cloud Console への不正なログオンのリスクを軽減し、セキュリティを向上させることができます。

デフォルトでは 2 要素認証は無効になっており、ログオン アカウント名とパスワードを入力してログオンしていただく「パスワード認証」のみが使用されます。アカウントに対して 2 要素認証を有効にしていただくことで、そのアカウントでログオンする際には、パスワードに加えて「認証コード」と呼ばれるワンタイム パスワードの入力が追加で求められるようになります。

認証コードはスマートフォンなどのモバイル端末にインストールした Microsoft 社製や Google ブランドの認証システム アプリで取得します。



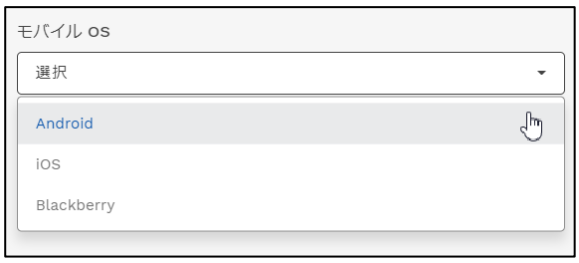
3.4.1.2 要素認証の有効化（オプション）

2 要素認証を利用するためには、以下の手順で事前に機能を有効化しておく必要があります。

1. 2 要素認証を利用したいアカウントで Cloud Console にログオンし、右上のアイコンをクリックし、[ユーザ プロファイル]を選択します。

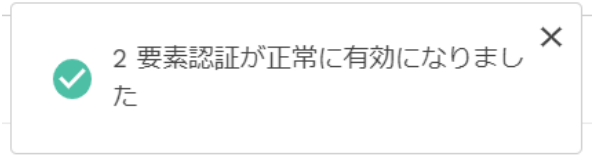
2. 画面を下にスクロールします。2 要素認証の設定として、ログオンしているアカウントの現在のパスワードを入力し、[2 要素認証を有効にする]をクリックします。

3. 使用するモバイル端末の種類を選択します。



4. モバイル端末に認証システム アプリを導入する方法が表示されるので、指示に従いアプリをインストールしてください。また、認証システム アプリ上に「アカウント」を登録するために、画面の指示に従い、表示された QR コードを読み込んでください。

5. Cloud Console の画面を下にスクロールし、[生成されたコードを入力]欄に認証システムアプリに表示されるワンタイムパスワードを入力し、[保存]をクリックします。



注意：

・モバイル端末の認証システム アプリ上のアカウントは、認証システム アプリの解説をよく読んだうえで、**必ずバックアップを取ってください**。アカウントを設定したモバイル端末の故障/紛失、機種変更、アカウントの誤消去などにより、認証コードの確認ができなくなる場合があります。また、登録時に QR コードの下に表示されたシークレットキーも保管しておいていただくと、アカウントの再登録にご利用いただけます。

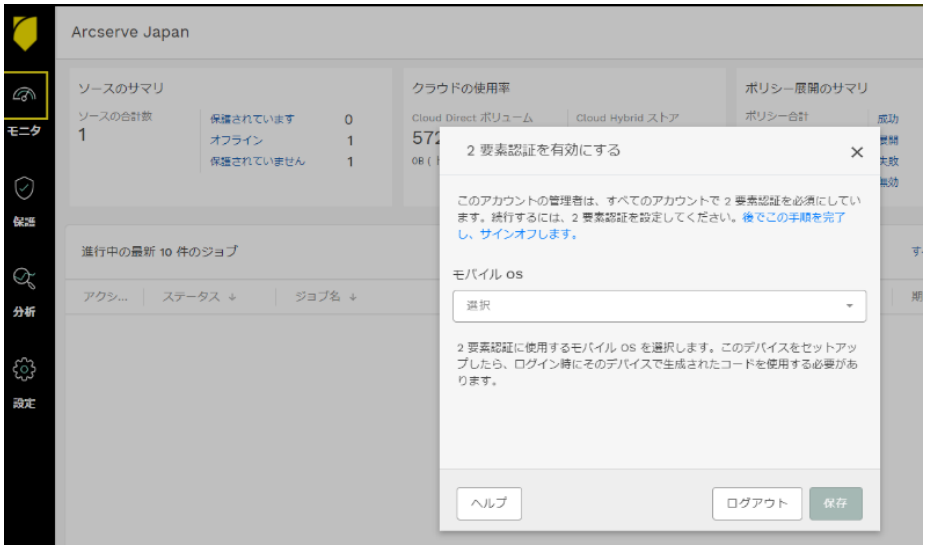
・モバイル端末は時刻を正確に合わせてください。

ワンタイム パスワードは、Cloud Direct 環境とモバイル端末、それぞれの環境で時刻を元に生成しています。両者の時刻が一致していないと、生成されるパスワードが食い違うことで認証が通らない場合があります。

3.4.2. すべてのユーザに対して 2 要素認証の利用を必須に設定する（オプション）

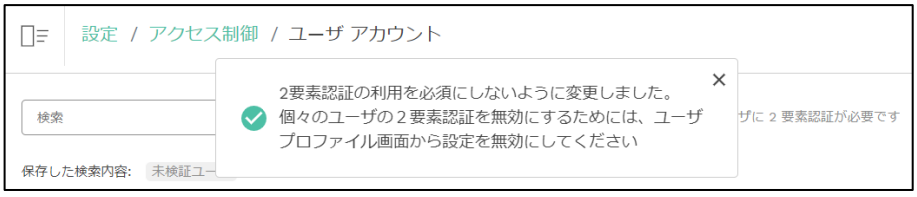
Cloud Direct では Cloud Console に複数のユーザ アカウントを登録できますが、そのすべてのユーザ アカウントに対して 2 要素認証の利用を必須にするよう設定ができます。[設定] – [ユーザアカウント] 画面で、[すべてのユーザに 2 要素認証が必要です]のチェックを入れます。

次回、ユーザが Cloud Console にログオンすると自動的に設定画面が表示されます。



注意：

[設定] – [ユーザアカウント] 画面で、[すべてのユーザに 2 要素認証が必要です] のチェックを外せば、以後、2 要素認証の利用は必須ではなくなります。ただし、この時点で既に 2 要素認証が有効になっているアカウントの 2 要素認証が無効になるわけではありません。別途、ユーザ プロファイル画面からアカウントごとに 2 要素認証を無効にする必要があります。



4 コンポーネントの導入

4.1 必要なコンポーネントのダウンロード

Windows 環境のバックアップに必要な Cloud Direct エージェントをダウンロードします。

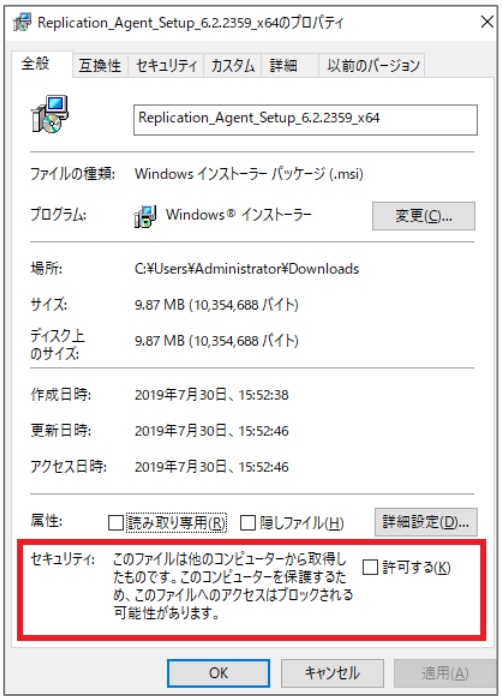
6. Cloud Console にログインし、画面左側のアイコンから[保護]を選択し、[エージェントのダウンロード]をクリックします。

7. 導入する OS 環境に合致するエージェントの [ダウンロード] リンクをクリックします。

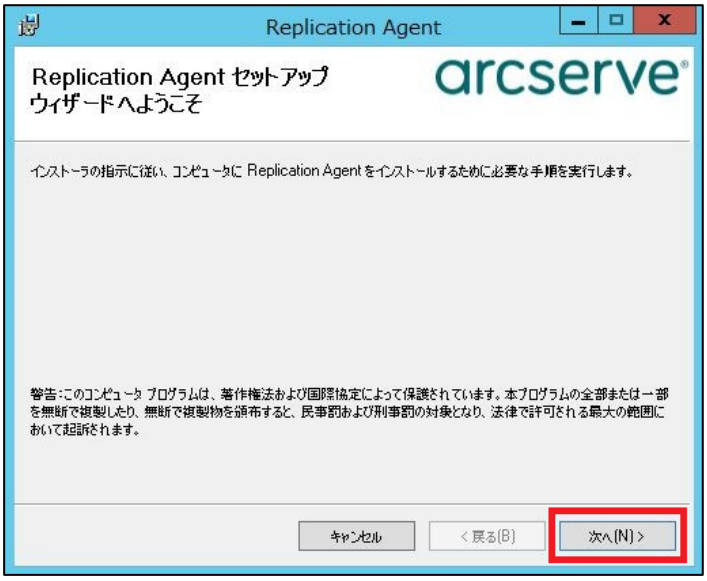
ブラウザのダウンロード フォルダにエージェントがダウンロードされます。

4.2 Windows 用 Agent のインストール

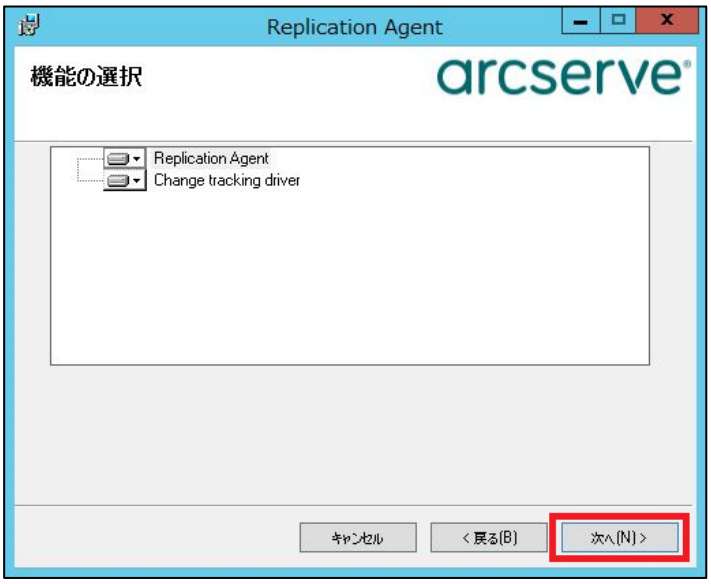
1. 保護対象マシンに管理者権限を持つアカウントでログインし、インターネットに接続できることを確認して、ダウンロードされたインストーラ ファイルを実行します。Windows によって PC が保護された旨のメッセージが表示された場合は、インストーラ ファイルを右クリックし、プロパティをクリックします。他のコンピュータから取得したファイルの実行のブロックを解除するために、セキュリティの設定で「許可する」にチェックを入れて[OK]をクリックします。



2. セットアップ ウィザードが起動します。[次へ] をクリックします。



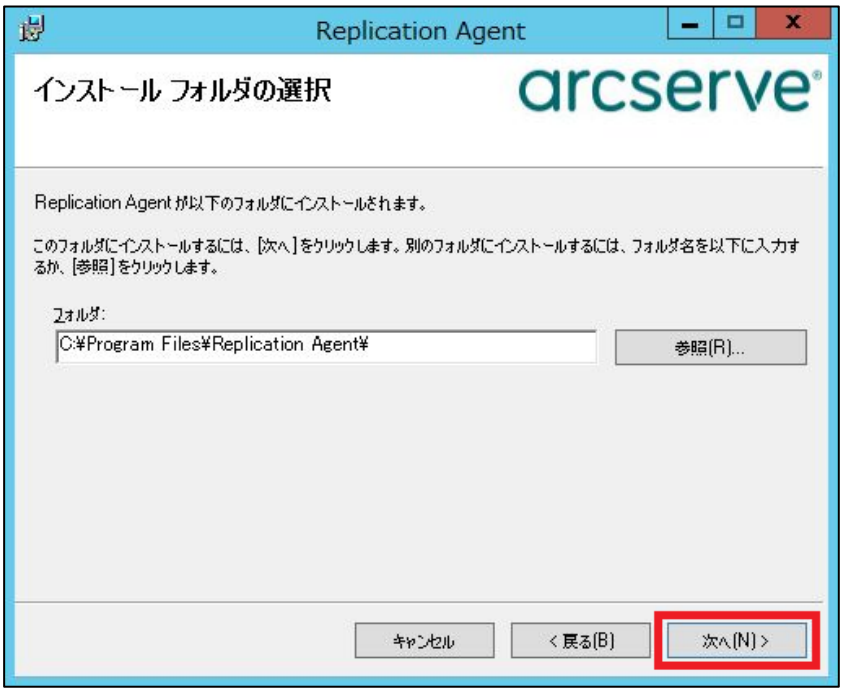
3. 機能がすべて選択されていることを確認し、そのまま [次へ]をクリックします。



注意：Arcserve UDP のエージェントがインストールされている環境では、”Change tracking driver“ についてはインストールを行わないでください。詳細は下記サイトの「4. DRaaS は Arcserve UDP によるエージェントベース Windows バックアップと併用することはできません。」および「5. BaaS は Arcserve UDP との併用が可能です。Arcserve UDP Cloud Direct (BaaS) は、Arcserve UDP の変更ブロック トラッキング ドライバは使用しません。」をご参照ください。

ARCSERVE UDP CLOUD DIRECT 注意/制限事項
https://support.arcserve.com/s/article/2019081401?language=ja

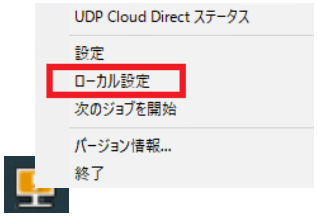
4. インストール先フォルダを確認し、[次へ] をクリックします。



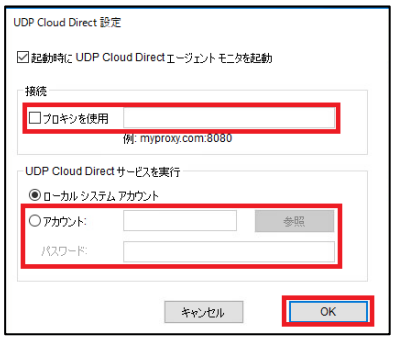
5. インストールを開始するため、[次へ]をクリックします。

6. 正常にインストールされたことを確認し、[閉じる]をクリックします。

注意：お客様の環境でインターネット接続のためにプロキシ設定が必要な場合は、Windows のタスク トレイで Arcserve UDP Cloud Direct のエージェント アイコンを右クリックし、[ローカル設定]をクリックします。



[プロキシを使用]にチェックを入れ、プロキシ サーバ及びポートを指定します。認証が必要な場合は、下の[アカウント]にチェックを入れてアカウント情報を入力し、[OK] をクリックします。



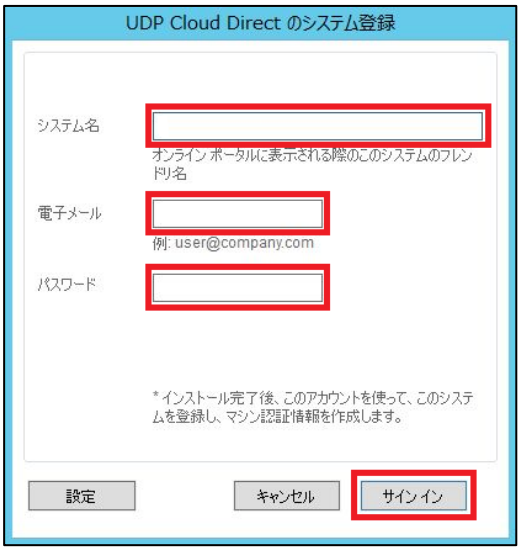
注意：

ここでの設定は Arcserve UDP Cloud Direct のサービスを実行するアカウントや、CIFS 共有フォルダをバックアップする際のアクセス アカウントとしても利用されます。

7. Cloud Console にバックアップ対象の情報を登録するためのポップアップが表示されます。

・システム名：Cloud Console 上でこのシステムを固有に認識するための、ホスト名（フレンドリ名）が自動入力されます
・電子メール：Cloud Console アカウント作成時に指定したメールアドレスを入力します。
・パスワード：Cloud Console アカウントへのログインパスワードを入力します。

入力完了後、[サイン イン]をクリックします。



8. Cloud Console で、[保護] – [ソース] の一覧に指定ノードが登録されたことを確認します。

5 バックアップの設定

5.1 バックアップ先ボリュームの作成

デフォルトでは BaaS 用のボリュームが 1 つ作成済みですが、このボリューム名は変更できないので、任意の名前を持つボリューム名をバックアップ先として利用する場合はボリュームを新規に作成します。この資料では、新しいボリュームを作成する手順を説明します。

※BaaS 用のボリュームは Cloud Console で作成できます。DRaaS 用ボリュームは Arcserve テクニカルサポートへ作成を依頼してください。詳細は「3.3 DRaaS 設定のサポート依頼」をご参照ください。

1. Cloud Console において、[保護] – [Arcserve Cloud]を開き、 右上の [クラウド ボリュームの追加] をクリックします。

2. クラウド ボリュームの追加画面が表示されます。コメント以外のすべての情報を入力すると [クラウド ボリュームの追加] を押し、ボリューム追加ができるようになります。

・ボリューム名　※作成するボリュームに任意の名前を入力してください。

・データ センター　※[カリフォルニア州サンタクララ] もしくは [東日本] のうち、購入したストレージ サブスクリプションに対応するものを選択してください。

・コメント　※任意のコメントです。

・保存　※ここで指定した期間、バックアップデータは Arcserve クラウド上に保持されます。BaaS 用ボリュームでは 7 日、14 日、1 か月、2 か月、3 か月、6 か月、1 年、2 年、3 年、7 年、10 年、無期限から選択できます。DRaaS 用ボリューム（Arcserve テクニカル サポート経由で作成）は 7 日、14 日、1 か月から選択となります。

3. Cloud Console 上のポップアップから、ボリュームが作成されたことを確認できます。

5.2 ポリシー作成の開始

Arcserve UDP Cloud Direct ではバックアップの設定を「ポリシー」として作成し、これをバックアップ対象マシンに割り当てることでバックアップを行ないます。

デフォルトではコンピュータ全体をバックアップするポリシーが 1 つ作成済みです。

名称を変更して利用することも、新しいポリシーを作成することもできます。

今回は、新しいポリシーを作成する手順を確認します。

1. Cloud Console において、[保護] – [ポリシー]の順にクリックし、画面右上、[ポリシーの追加] をクリックします。

5.3 基本情報の設定

[基本情報] タブが自動的に選択されるので、[ポリシー名] を入力し、[保護タイプ]を指定すると、[ソース(オプション)] タブ、[タスク] タブの設定に進むことができます。

[基本情報]タブ設定には、以下の項目を設定します。

・ポリシー名　※ ポリシー名を入力します。入力必須です。

・保護タイプ　※ 入力必須です。

- Arcserve Cloud へのエージェント ベースの直接バックアップ

※ BaaS タイプの保護をおこないます。

- 惨事復旧のための Arcserve Cloud へのエージェント ベースのバックアップ

※ DRaaS タイプの保護を行います。

・説明（オプション）　※ 任意の説明を入力できます。

5.4 ソースの設定

1. [ソース(オプション)]タブをクリックします。画面右上の[ソースの選択]をクリックすると、ノードリストが表示されます。

2. 表示されたリストから保護対象マシンの左横のチェックボックスにチェックを入れ、右上の[ソースの追加] ボタンをクリックすることで、ポリシーがマシンに割り当たります。

※ノードへのポリシーの割り当ては、ポリシー作成後に行うことも可能です。

5.5 タスクの設定

[タスク] タブをクリックします。ここでは、以下の 4 つの詳細タブで保護対象や保護する場所（バックアップ先）、タイミング（スケジュール）などの設定を行います。

- [1. 保護対象]
- [2. 保護する場所]
- [3. 保護するタイミング]
- [追加の設定]　※ 保護対象に[Cloud Direct ファイル フォルダ バックアップ]を選択した場合のみ

5.5.1. 保護対象の設定

[1. 保護対象] タブでは、[アクティビティのタイプ] を選択します。

※[基本情報] タブで選択した保護タイプにより選択肢が異なります。

アクティビティのタイプには以下があります。

※[Exchange] については日本では未サポートとなります。

- **[Windows イメージ (ディスク ドライブ全体)]　※BaaS/DRaaS で選択可**

  システム全体もしくはディスク全体のイメージ バックアップを行います。

  初回のバックアップ時には未使用領域を含めたディスク全体に対して読み込み処理が行われるので、その分の時間がかかることにご注意ください。

  例えば 100 GB バイト容量のバックアップ対象ディスクに 30 GB のデータが格納されている場合、初回のバックアップでは 100 GB 分に対して読み込みが行われます。

  ただし、Cloud Direct ストレージには、30 GB 分のバックアップが保存されます。

  また、BaaS 用ボリュームへの Windows イメージ バックアップでは、増分バックアップ時にファイルのタイムスタンプに変更があったファイルを確認した上で、該当ファイルの変更ブロックを抽出してバックアップを行うという、2 段階の処理が行われます。

  そのため、バックアップされる容量は小さくなるものの、増分バックアップ時間はフルバックアップより長くなることがあります。

  [フル システム] を選択した場合、システム上に存在するすべてのドライブがバックアップされます。 [ドライブの選択] を選択した場合、任意のドライブのバックアップができます。バックアップしたいドライブ文字のチェック ボックスを選択してください。

※　DRaaS により Arcserve クラウドに復旧を行うためには、システム ドライブとブート ボリュームを保護対象に含めてください。

- **[Cloud Direct ファイル フォルダ バックアップ]　※Baas のみ選択可**

  特定のフォルダを指定してバックアップを行います。

  バックアップしたいフォルダへのフル パスを入力してください。

UNC パス（¥¥サーバ名¥共有名）を指定することで、NAS や共有フォルダ上のデータのバックアップも可能です。※その場合はエージェントのアイコンから、[ローカル設定]画面を開き、共有にアクセスのためのアカウント情報を指定してください。

複数のフォルダをバックアップする場合は、[追加] ボタンによりパス フィールド行を追加できます。

- **[SQL Server]　※BaaS のみ選択可**

Microsoft SQL Server のデータをオンラインでバックアップしたい時に使用します。
SQL Server をバックアップする際には、一次バックアップとしてローカル ディスクにバックアップを行い、その後 Arcserve クラウドにバックアップを行うという、２段階（”ステージング”方式）での処理となります。

[ステージング ドライブまたはパス]に、一次バックアップ先となるドライブ、もしくはパスを指定します。
デフォルトでは既定のインスタンス（MSSQLSERVER）をバックアップします。

既定のインスタンスのバックアップが不要な場合は [デフォルト SQL Server インスタンスのバックアップ] のチェックを外してください。

インスタンス 名を指定してバックアップする場合は [名前付き SQL Server] にバックアップ対象のインスタンス名を入力します。複数のインスタンス名を入力する場合は、';'（セミコロン）で区切って入力をしてください。

※SQL Server のインスタンス名は、Windows のサービス画面で確認できます。"SQL Server（インスタンス名）" サービスの括弧内の文字列がインスタンス名です。

[SQL バックアップの検証] にチェックを入れることで、SQL Server の機能を利用して SQL バックアップ データの整合性を検証することができます。

<参考：アクティビティのタイプとリストア単位>

バックアップの取り方により、リストアできる単位が異なります。

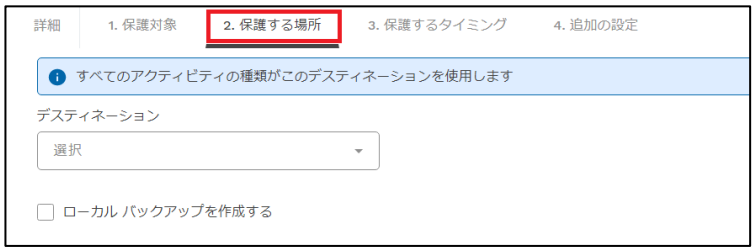
	バックアップ単位	リストア単位 （お客様サイトへのリストア）	プロビジョニング単位 （Arcserve クラウドでの VM 起動）
BaaS	フル システム	ディスク イメージ ※1	-
	ディスク ドライブ	ディスク イメージ ※1 /フォルダ/ファイル	-
	ファイル フォルダ	フォルダ/ファイル	-
	SQL Server	データ ファイル、ログ ファイル ※2	-
DRaaS	フル システム	ディスク イメージ/フォルダ/ファイル	フル システム
	ディスク ドライブ	ディスク イメージ/フォルダ/ファイル	フル システム （バックアップしたディスクのみ）

※1 ディスク イメージは、img、vhdx 形式となります。img 形式のファイルは Raw Disk Image 対応のツールでディスクとしてマウントできます。vhdx ファイルは Windows Server 2012 以降で、マウントできます。
ただし、いずれの形式のファイルもブート ボリュームとしてマウントする事はサポートされません。

※2 SQL Server のバックアップデータはリストア時に bak 形式のファイルとなります。リストア後に SQL Server の機能でデータベースとして利用できるように復元できます。データベースの復元手順の詳細はマイクロソフト社の情報をご参照ください。

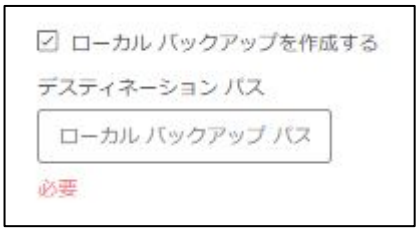
5.5.2. 保護する場所の設定

[2. 保護する場所] タブを開き、バックアップ先となる Arcserve クラウド上のボリュームを指定します。



[デスティネーション] 下の [選択] ボタンをクリックし、プルダウンメニューから作成済みのクラウド ボリュームを選択します。

[ローカル バックアップを作成する] にチェックを入れると、Arcserve クラウドへのバックアップとは別に、ローカル ディスク上にバックアップデータを残すことができます。
ローカル バックアップを行なう場合は [ローカル バックアップ パス] に格納先フォルダのパスを指定してください。



注意：ローカル バックアップではバックアップ方式として[Windows イメージ (ディスク ドライブ全体)]を選択し、”フル システム”を保護対象とした場合、ローカルディスクにフル バックアップと同等サイズのテンポラリデータが作成されます。そのため、フル バックアップ 2 回分以上の空き領域を持つドライブをローカル バックアップの作成先として指定してください。

5.5.3. 保護するタイミングの設定

[3. 保護するタイミング] タブを開き、バックアップ スケジュールを設定します。

バックアップスケジュール間隔は BaaS では[1 日ごと] で固定です。

DRaaS では「15 分ごと」、「1 時間ごと」、「6 時間ごと」、「1 日ごと」のいずれかを指定できます。

注意：DRaaS のデフォルトでは「15 分ごと」が選択されています。必要に応じ変更してください。

[開始時刻]には最初にバックアップを実行するタイミングを指定してください。

[バックアップ スケジュール]では実行する曜日を指定できます。青い色がついている曜日にはバックアップが実行されます。クリックで変更できます。

スロットル スケジュールで [追加] をクリックすると、帯域制御設定が追加できます。例えば、平日日中のバックアップによるインターネット使用量を制限し業務への影響を抑えたい、という場合に設定してください。

[スループット制限]では、各ポリシーがバックアップに使用できる帯域幅の上限値を設定します。

[実行予定日]では、帯域制御を行なう曜日を指定します。

[開始時刻]と[終了時刻] で帯域制御を行なう時間帯を指定します。

5.5.4. 追加の設定

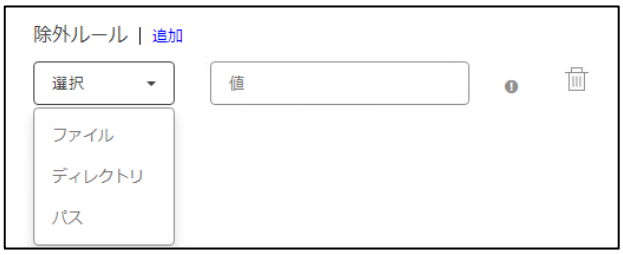
[キャッシュの場所]で転送を効率化するためのローカル キャッシュの保存場所を指定できます。バックアップデータの 1%程度の領域が必要です。

[バックアップ前のスクリプト][バックアップ後のスクリプト]では、バックアップの前後に任意のスクリプトを実行するように指定できます。（ファイル/フォルダ バックアップ時のみ）

[除外ルール]でバックアップ対象から任意のファイルやディレクトリを除外するための設定が行えます。[除外ルール] の下の [選択] を開き、ルールを追加します。

「ファイル」、「ディレクトリ」では、[値] 欄に入力した名前が一致したファイルやディレクトリを全てバックアップ対象から除外します。「パス」では、入力したパスが一致したファイルやフォルダのみをバックアップ対象から除外します。

※１文字以上の任意の文字を置き換えるワイルドカード（*）も使用可能です。



5.6 ポリシー設定の完了

[ポリシーの作成] をクリックして設定を保存します。

これでバックアップの設定は完了です。

ポリシーで設定したスケジュールに基づき、バックアップが実行されます。

5.7 バックアップ結果の確認

バックアップの進捗や実行結果は [分析]-[ジョブ]をクリックし、確認したいジョブ名をクリックすることで確認できます。

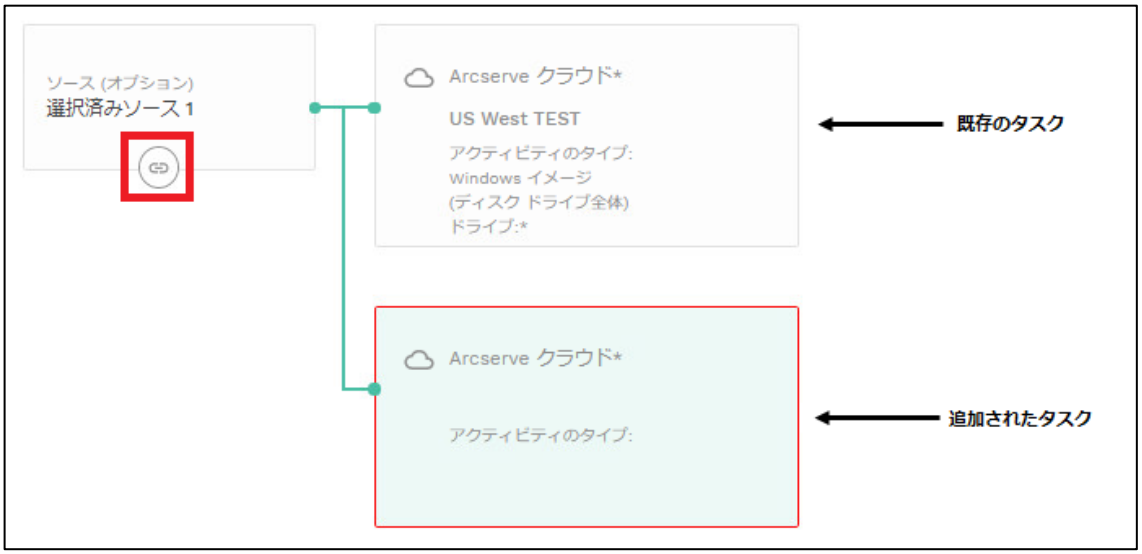
5.8 タスクの追加、変更、削除

ポリシーの [タスク] タブでは画面上部にタスクの構成が図示されます。

ポリシー画面上ではタスクの変更と追加が可能です。

5.8.1. タスクの追加方法

ソース（オプション）の下のアイコンをクリックすることで、タスクを追加することができます。



例えば、 1 つのマシンでディスク全体のバックアップと SQL Server のオンライン バックアップを併用したい時はデスティネーションを追加することで実現できます。

5.8.2. タスクの削除方法

既存のタスクを選択しているときに画面下部の[デスティネーションの削除]をクリックすることで、タスクを削除できます。

6 データのリストア

6.1 フォルダのリストア

ここでは、ディスク イメージのバックアップから、特定のフォルダをリストアする例を説明します。

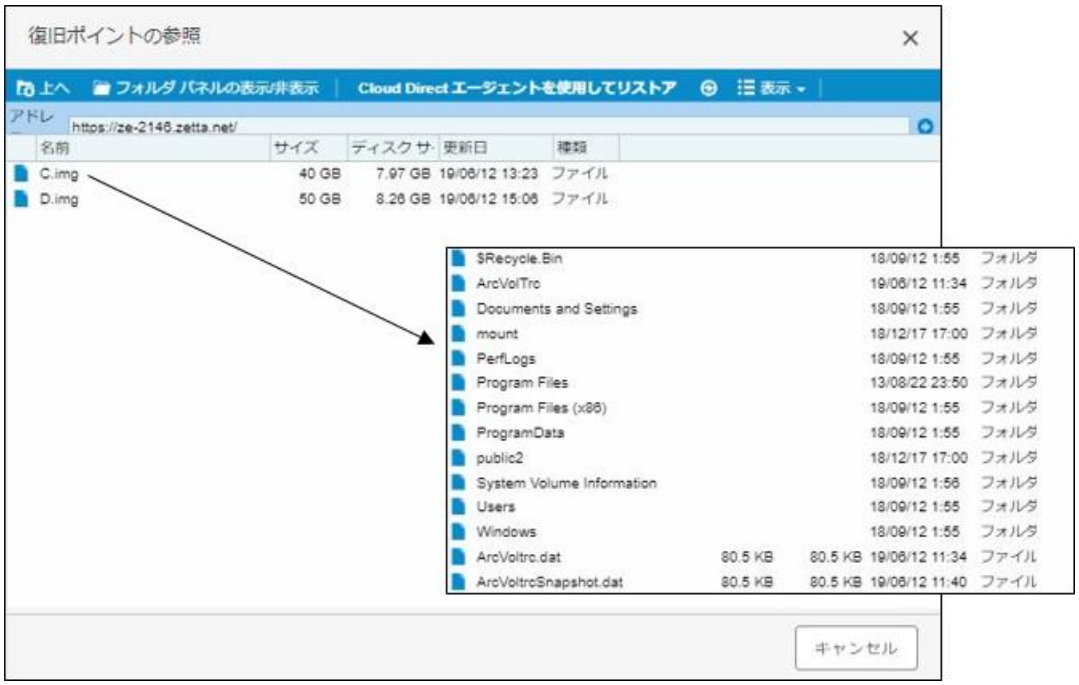
1. [保護] – [ソース]をクリックします。

2. リストアしたいマシン名のリンクをクリックします。

3. [復旧ポイント]タブをクリックすると、復旧ポイントがドライブ単位でリスト表示されます。リストアしたい復旧ポイントの [アクション] カラムでプルダウンから [復旧] をクリックします。

4. 特定のフォルダをリストアするためには、[復旧ポイントの参照]をクリックします。

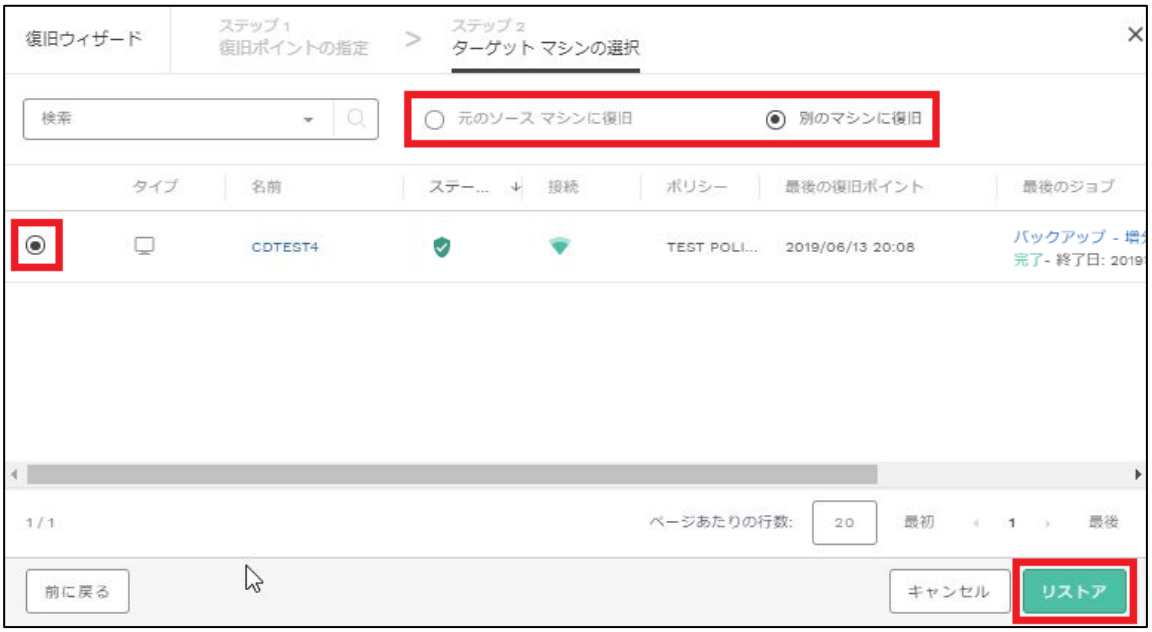
5. リストアしたいフォルダやファイルをブラウズできます。



6. リストア対象フォルダを右クリックして[Cloud Direct エージェントを使用してフォルダをリストア]クリックします。

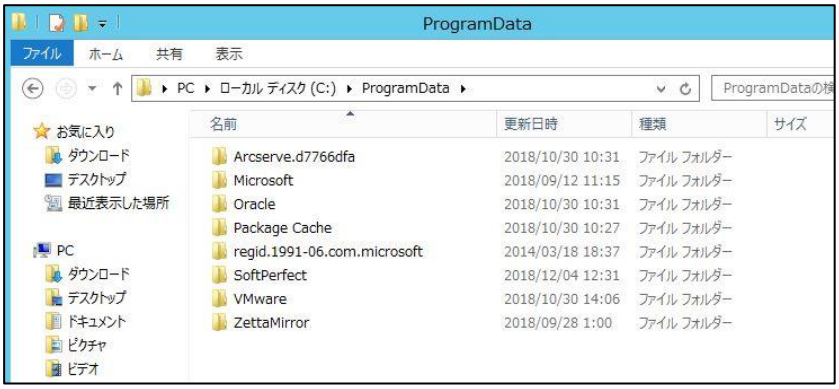
7. 復旧元とデスティネーション パスを確認し、右下の [次へ] をクリックします。

8. [元のソース マシンに復旧]を選択するとバックアップ元のマシンにリストアします。[別のマシンに復旧]を選択した場合は、リストからリストア先マシンを指定します。
右下の [リストア] をクリックし、リストアを開始します。



9. リストアの開始がポップアップメッセージで表示されます。

10. リストア結果はログで確認できます。リストアしたフォルダを開き、正常に復旧が完了したことを確認してください。



6.2 イメージのリストア

ディスク全体をバックアップしていた場合、ボリュームのイメージ単位でリストアすることも出来ます。以下の図のようにイメージのフォーマットを指定できます。

7 Arcserve クラウドに復旧された VM へのアクセス

7.1 プロビジョニングの実施

DRaaS 用ボリュームにバックアップを行うと、復旧ポイントを Arcserve クラウド内で本番システムの代替 VM としてすぐに起動できます。障害発生時に代替 VM を起動するには以下の要領でプロビジョニングを行います。

注意：プロビジョニング後はバックアップ運用が停止します。運用を再開したい場合は、代替 VM の電源をオフにした後でプロビジョニングを解除してください。

1. Cloud Console にログインし、[保護]-[DRaaS]をクリックします。
2. プロビジョニング対象マシン名の [アクション] カラムでプルダウンし、[ターゲット VM 環境設定]から、起動する VM のメモリを調整できます。

ご契約いただいている DRaaS のコンピュート リソースから、2GB～128GB（偶数）のメモリを割り当てることができます。

3. プロビジョニング対象マシン名の [アクション] カラムでプルダウンし、[プロビジョニング]をクリックします。

4. プロビジョニングが開始された旨のメッセージが表示されます。対象マシンの [状態]フィールドが「実行」となるまで数分お待ちください。

7.2 復旧された VM へのリモート デスクトップ接続

プロビジョニングが完了した VM には、リモートデスクトップで接続が可能です。以下の手順で接続します。

1. Cloud Console にログインし、[保護] - [DRaaS] をクリックします。
2. 接続する VM の[アクション] カラムでプルダウンし、[リモート コンソール]をクリックします。

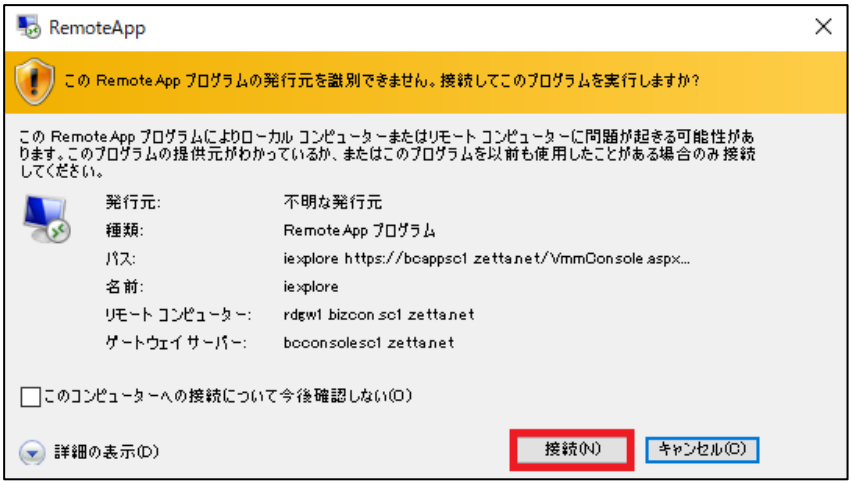
3. Web ブラウザで設定されているダウンロード保存先に、「RemoteConsole.rdp」ファイルがダウンロード/保存されます。

4. また、画面上部に、接続に使用するための認証情報が表示されます。
[パスワード]フィールドの文字列を選択し、コピーします。

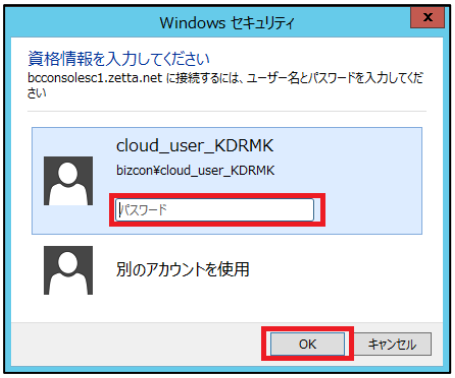
5. ダウンロードされた「RemoteConsole.rdp」を実行します。
ご利用の環境によっては、セキュリティの警告メッセージが表示されます。

※接続先のパスやリモートコンピュータ、ゲートウェイとして”zetta”を含む文字列が表示されていますが、これは Cloud Direct の開発部門の旧称です。

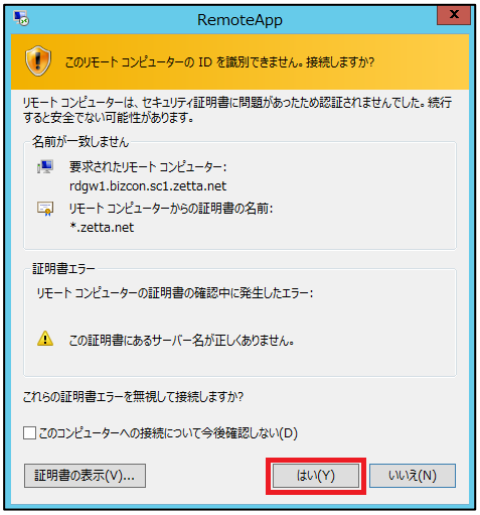
[接続]をクリックします。



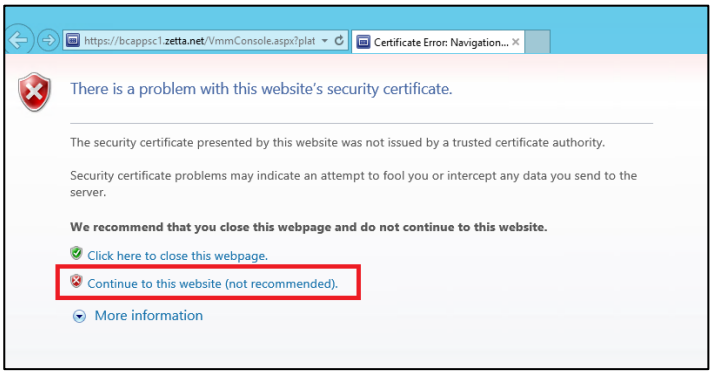
6. 資格情報の入力を促す画面が表示されます。フィールドに手順 2.でコピーしたパスワードを貼りつけて、[OK]をクリックします。



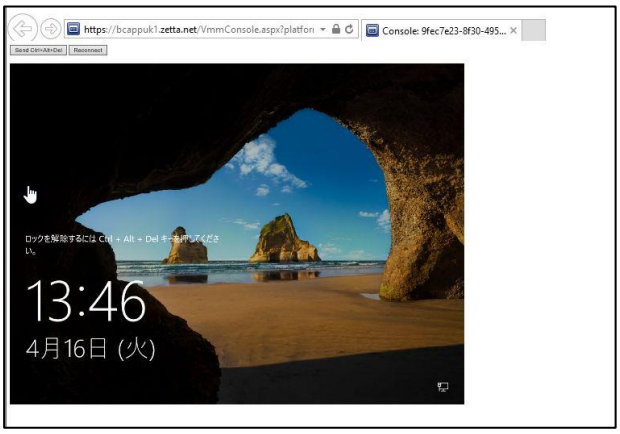
7. セキュリティ証明書に関するメッセージが表示されます。
正しくサーバ証明書を用意いただいたうえでリモートデスクトップに接続します。この資料では評価目的のためそのまま[はい]をクリックしエラーを無視して接続します。



8. 環境によってはブラウザに以下の証明書に関するメッセージが表示される場合があります。この資料では評価目的のためそのまま [Continue to this website (not recommended)] をクリックします。



9. 接続が完了し、ログオン画面が表示されます。ログオンして動作を確認してください。



7.3 ポイント対サイト（Point to Site）の VPN 接続

ポイント対サイトの VPN 接続により、単一のノードから Arcserve クラウド上の環境に対してセキュアな仮想プライベート ネットワーク接続が可能となります。お客様環境のコンピュータから Arcserve クラウド上に復旧された VM と通信をする場合に利用できます。

ポイント対サイトの VPN 接続には「OpenVPN」ツールを利用します。

1. Cloud Console にログインし、[設定]-[ネットワーク設定]を開きます。
   [説明の表示] をクリックします。

2. Open VPN の利用方法の解説ページが表示されます。説明に従い、ツールのインストールおよび設定を行ってください。

Point-to-Site VPN

Point-to-Site VPN では、VPN クライアントとクラウドの間でセキュアなネットワーク接続を確立して、クラウドでアクティブ化されているビジネス上の重要なサーバにアクセスできます。

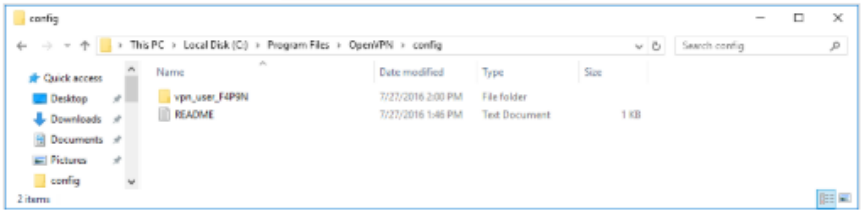
Windows　Mac　Linux

OpenVPN クライアントのダウンロードとインストール

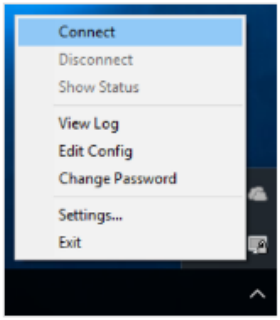
Windows OpenVPN クライアントのダウンロード に連絡してインストールすることもできます。

設定ファイルのダウンロードと展開

1. Windows 用の設定のダウンロード
2. 解凍した設定フォルダを以下に移動: `C:\Program Files\OpenVPN\config`

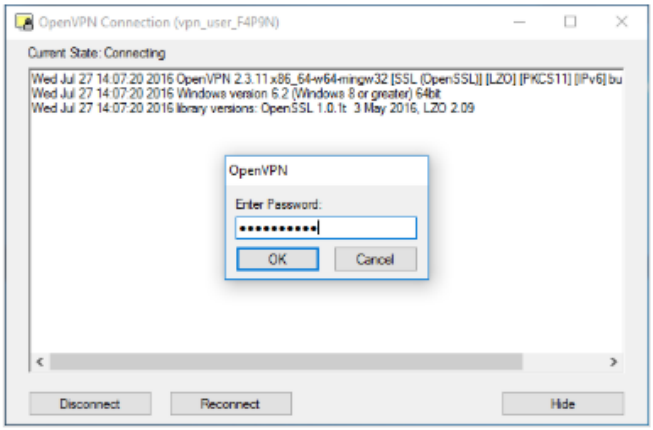


3. OpenVPN GUI を右クリックします。[接続] をクリックします (OpenVPN クライアントが現在実行中であることを前提としています)。



※画面上の「表示」をクリックすると
パスワードを参照できます。

4. VPN パスワードを入力してください: ********** 表示



8 通常運用環境への切り戻し

8.1 フェイルバックの実行

フェイルバックは DRaaS において、クラウドから本番環境への切り戻しに使用する機能です。

ユーザが代替 VM 上で業務を行うことで、この VM には最新の業務データが蓄積されます。

代替 VM からオンプレミスに運用を切り戻すには、代替 VM 上の最新業務データを含むイメージを本番環境にダウンロードする必要があります。

※ダウンロードしたイメージは既存環境にマウントしてデータを参照できます。

この、最新イメージのダウンロードの操作を「フェイルバック」と言います。

フェイルバックは、以下の 3 つのステップで実行されます。

STEP1.オンライン フル ダウンロード

クラウド上の代替 VM のスナップショットを取得し、フル イメージをダウンロードします。この処理は、VM の大きさに応じて時間がかかります。

STEP2. オンライン 増分ダウンロード

STEP1 のスナップショット取得以降の増分をダウンロードします。

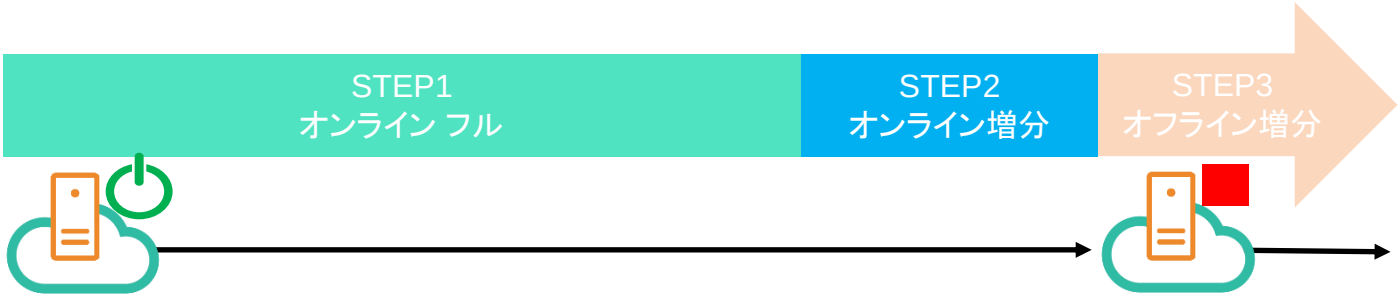
この処理は、STEP1 の後に自動的に実行されます。

STEP1 の実行中に行われた変更量に応じて時間がかかります。

STEP3. オフライン 増分ダウンロード

クラウド上の代替 VM をシャットダウンしてユーザアクセスを遮断し、STEP2.以降の増分をダウンロードします。

シャットダウン以降は代替 VM に変更が加えられないため、この処理は STEP2 実行からシャットダウンをするまでの変更分のみのダウンロードとなります。



以下は、フェイルバックの実行手順です。

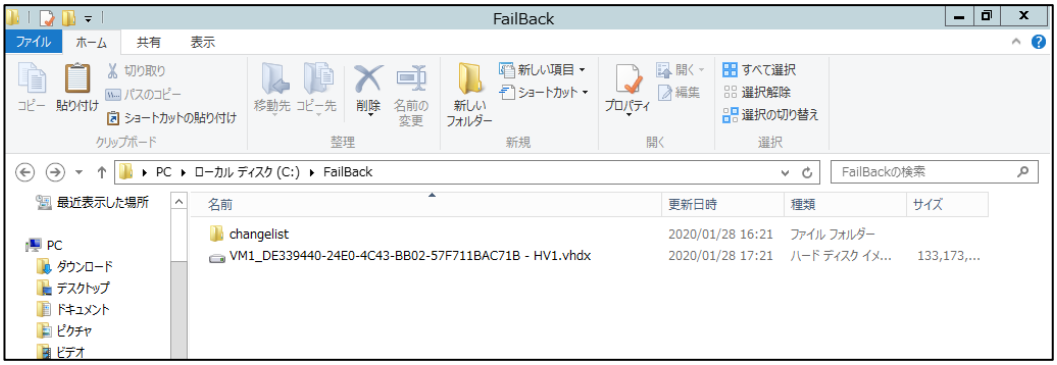
STEP1.オンライン フル ダウンロード、および STEP2. オンライン 増分ダウンロード の実行

1. [保護]-[DRaaS]をクリックし、フェイルバックを実行したいクラウド上の VM の[アクション]カラムでプルダウンし、[フェイルバックを開始]をクリックします。

[デスティネーション システム]で、ダウンロード先となるシステム、[デスティネーション パス]として、デスティネーション システム上のリストア先となるディレクトリへのパス、[イメージ フォーマット]としてリストアされるイメージ ファイルの形式を指定し、[フェイルバックを開始]をクリックします。

※リストアするイメージ ファイルの利用方法については、5.5.1 保護対象の設定内の、 <参考：アクティビティのタイプとリストア単位>をご参照ください。

フェイルバック実行開始時点のフル イメージ、およびそれ以降の増分のダウンロードが行われます。※増分イメージはフルイメージに合成されます。



STEP3. オフライン 増分ダウンロード の実行

2. ダウンロードが完了したことを確認し、クラウド上の VM をシャットダウンします。
3. アクションカラムでプルダウンし [最終フェイルバック手順を完了する]をクリックします。

ダウンロードが完了したら、フェイルバックは完了です。ダウンロードしたイメージは既存環境にマウントしてデータを参照できます。

9 参考情報

・動作要件

https://support.arcserve.com/s/article/115003836346?language=ja

・Arcserve クラウド サービス規約

https://www.arcserve.com/jp/cloud-services/

・購入方法と価格表

https://www.arcserve.com/jp/jp-resources/licensing-options/

・スタートアップ ガイド

【仮想エージェントレス 編】

https://www.arcserve.com/wp-content/uploads/2019/09/ucd-startup-guide-agentless.pdf

【Linux 編】

https://www.arcserve.com/wp-content/uploads/2019/09/ucd-startup-guide-linux.pdf

・オンライン ヘルプ

https://documentation.arcserve.com/Arcserve-Cloud/Available/JPN/Bookshelf_Files/HTML/olh/default.htm

・よくあるご質問と回答

https://www.arcserve.com/wp-content/uploads/2019/08/ucd-faq.pdf

・注意/制限事項

https://support.arcserve.com/s/article/2019081401?language=ja

・Arcserve Japan Direct（購入前のお問い合わせ）

フリーダイヤル： 0120-410-116（平日 9：00～17：30　※土曜・日曜・祝日・弊社定休日を除きます）

https://www.arcserve.com/jp/about/contact/call-me/

・サポート

https://support.arcserve.com/s/?language=ja