Arcserve Cloud Cyber Resilient Storage /Arcserve Cloud Storage スタートアップ ガイド

本資料は、Arcserve Cloud Cyber Resilient Storage および Arcserve Cloud Storage のサービス概要をご理解した方向けに、利用のための手順を記載したガイドです。
サービスの概要については、以下をご確認ください。

・Arcserve CRS シリーズのご紹介
https://www.arcserve.com/hubfs/243905555/jp-resources/crs-presentation.pdf

改訂履歴

2025 年 9 月　Rev1.0 リリース
2025 年 12 月 Rev1.1　Arcserve UDP 10.3 対応
2026 年 4 月　Rev1.2　Arcserve Cloud Storage ポータル日本語追加に伴う修正
2026 年 6 月　Rev1.3　前提条件に追記。Arcserve Storage Portal 一部の画面ショット差し替え

目次

1 はじめに

1-1. Arcserve Cloud Cyber Resilient Storage (クラウド CRS）とは

身代金要求型のマルウェアであるランサムウェアは、依然として企業/組織にとっての重大な脅威です。

攻撃の手口は巧妙化し、業務上の重要な本番データのみならず、それを復旧するためのバックアップ データも暗号化される事例が大半を占めています。攻撃から迅速に復旧するためには、バックアップ データが破壊・改ざんされても復旧可能な体制を整えることが不可欠です。

Arcserve の提供するイミュータブル（不変）ストレージ ソリューション、Arcserve Cyber Resilient Storage（以下、CRS と省略）シリーズは、Arcserve Unified Data Protection（以下、Arcserve UDP と省略）のバックアップ データを格納するクラウド / オンプレミスのストレージとしてご利用いただけます。不変なスナップショットにより、不正に破壊・改ざんされたバックアップ データを正常な時点の状態に復旧し、速やかに本番データの復旧に臨んでいただけるための仕組みを提供します。

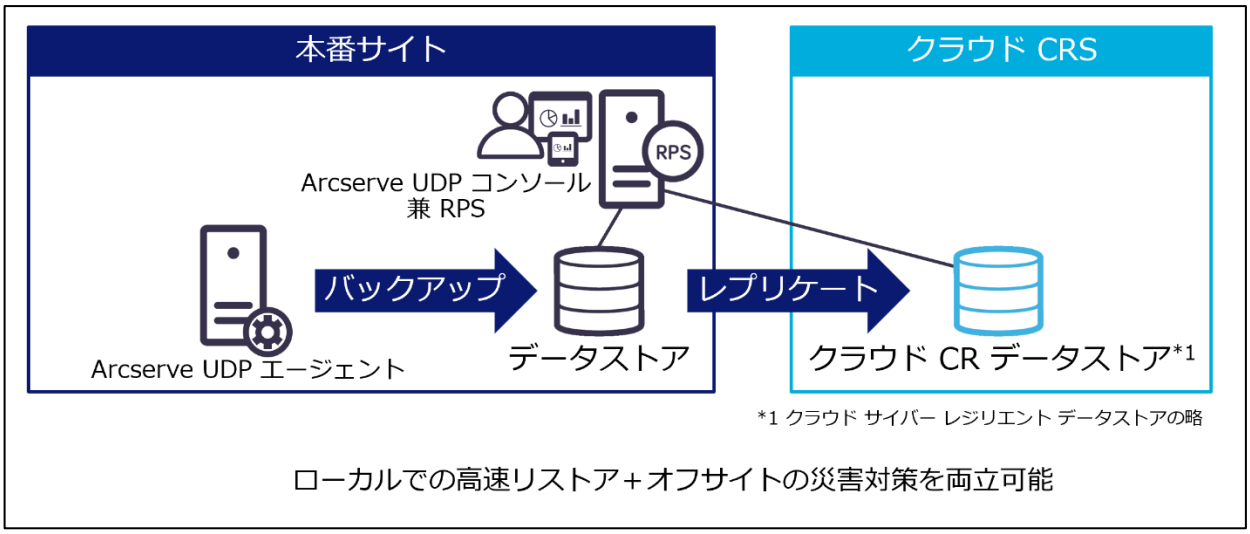
本書では、主にクラウド ベースのイミュータブル ストレージを提供する “Arcserve Cloud Cyber Resilient Storage（以下、クラウド CRS と省略）” を活用したデータ保護環境の構築と、復旧までの手順を解説します。

なお、イミュータブル機能のないクラウド ストレージである、”Arcserve Cloud Storage（以下、ACS と省略）” の環境構築方法についても、本書で解説します。

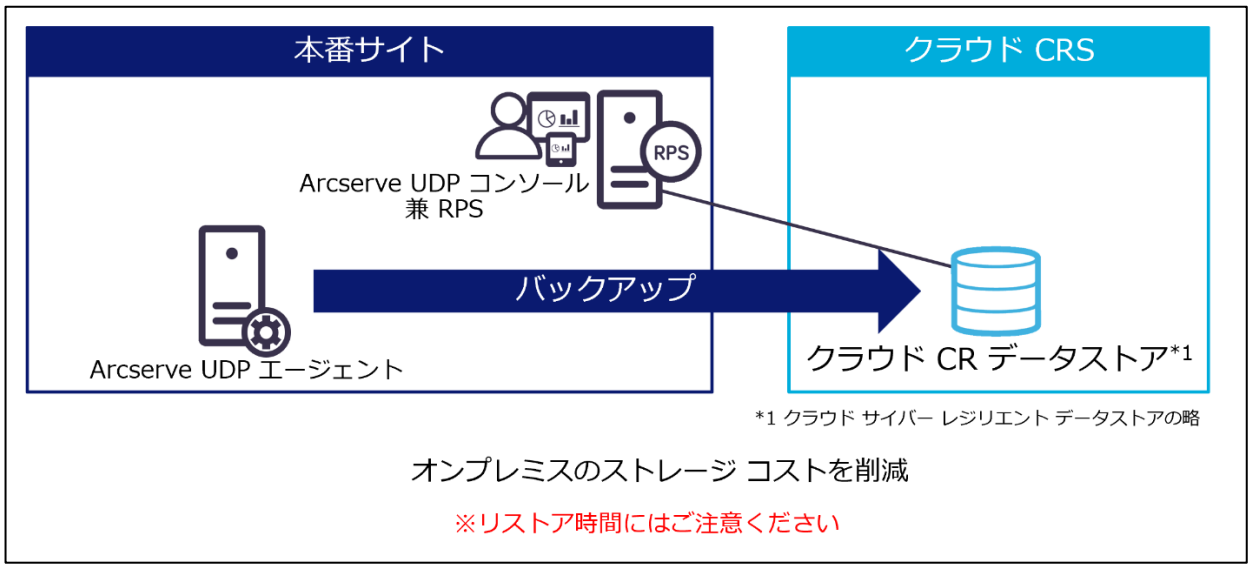
1-2. 構成

クラウド CRS / ACS は、Arcserve UDP の復旧ポイント サーバ（以下、RPS と省略）のデータ ストアとして利用します。バックアップ データの 2 次複製先（レプリケート先）や、1 次バックアップ先としてのご利用など、通常の RPS データ ストアと同様に利用いただけます。

構成例 1 （推奨） ： 2 次複製先（レプリケート先）としての利用



構成例 2 ： 1 次バックアップ先としての利用、



1-3. 前提条件

- Arcserve UDP コンソール / RPS がインターネットに接続できること
- Arcserve UDP コンソール / RPS から TCP/80 および TCP/443 (outbound) で通信できるようファイア ウォールを例外登録しておくこと
- 以下の URL への送信トラフィックを許可するファイアウォール ルールを追加。また、対応する公開 DNS の URL （例：*.cloudflare.net） をホワイトリストに追加
  - https://api.storagecraft.com/v1
  - s3.us-east-1.arcserve.com
  - s3.arcserve.com（汎用エンドポイント）もしくは
    s3.ap-northeast-1.arcserve.com（東京リージョン エンド ポイント）

※ Arcserve UDP 10.2 では、Web プロキシ経由でクラウド CRS に接続できません。
インターネット接続のために Web プロキシが必要な環境では、Arcserve UDP 10.3 以降をご利用ください。

◇その他の注意/制限事項は以下をご確認ください。

・Arcserve Cloud Cyber Resilient Storage / Arcserve Cloud Storage 注意/制限事項
https://support.arcserve.com/s/article/2025090304?language=ja

◇各サーバの動作要件や必要なリソースについては、以下をご参照ください。

・Arcserve UDP 10.x 動作要件
https://support.arcserve.com/s/article/Arcserve-UDP-10-X-Software-Compatibility-Matrix?language=ja

・Arcserve UDP 10.x サーバ構成とスペック見積もり方法
https://www.arcserve.com/hubfs/243905555/jp-resources/udp-10x-serverspec-guide.pdf?hsLang=ja

また、クラウド CRS のデータ ストアを追加する RPS には、その分のディスクやメモリが必要になります。詳しい考え方は、以下の資料中の参考情報をご確認ください。

・Arcserve CRS シリーズ紹介資料 – 参考情報
https://www.arcserve.com/hubfs/243905555/jp-resources/crs-presentation.pdf

1-4. 構築の流れ

以下はクラウド CRS を利用したバックアップ環境構築の流れです。

1. Arcserve UDP コンソール / RPS の構築
2. サービスのご購入 / 納品メール受信
3. アクセス キーの入手
4. クラウド アカウントの作成
5. クラウド サイバー レジリエント データ ストアの作成
6. バックアップ/レプリケート等での利用

本書では、「3. アクセス キーの入手」以降の手順について解説します。
「1. Arcserve UDP コンソール / RPS の構築」 については、以下のガイドの「1. インストール」を参考に、Arcserve UDP 10.2 以降の Arcserve UDP コンソール / RPS をインストールしたサーバを構築し、Arcserve UDP のライセンス登録までを行ってください。

・Arcserve Unified Data Protection 10.x 環境構築ガイド
コンソール+復旧ポイント サーバ (フル コンポーネント) インストール編
https://www.arcserve.com/hubfs/243905555/jp-resources/udp-10x-console-install-guide.pdf?hsLang=ja

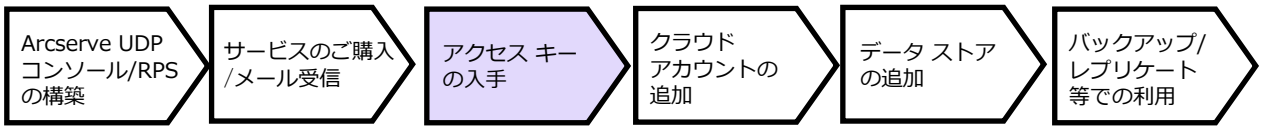
※無償トライアルをご利用いただく場合、 2．でサービスを購入する代わりに以下からトライアルにお申し込みください。その後の設定は購入時と同様です。
Arcserve UDP についてもトライアルを行えます。

・クラウド CRS トライアル
https://www.arcserve.com/ja/free-trials/arcserve-cloud-cyber-resilient-storage

・ACS トライアル
https://www.arcserve.com/ja/free-trials/arcserve-cloud-storage

・Arcserve UDP トライアル
https://www.arcserve.com/ja/free-trials/arcserve-udp

2 アクセス キーの入手

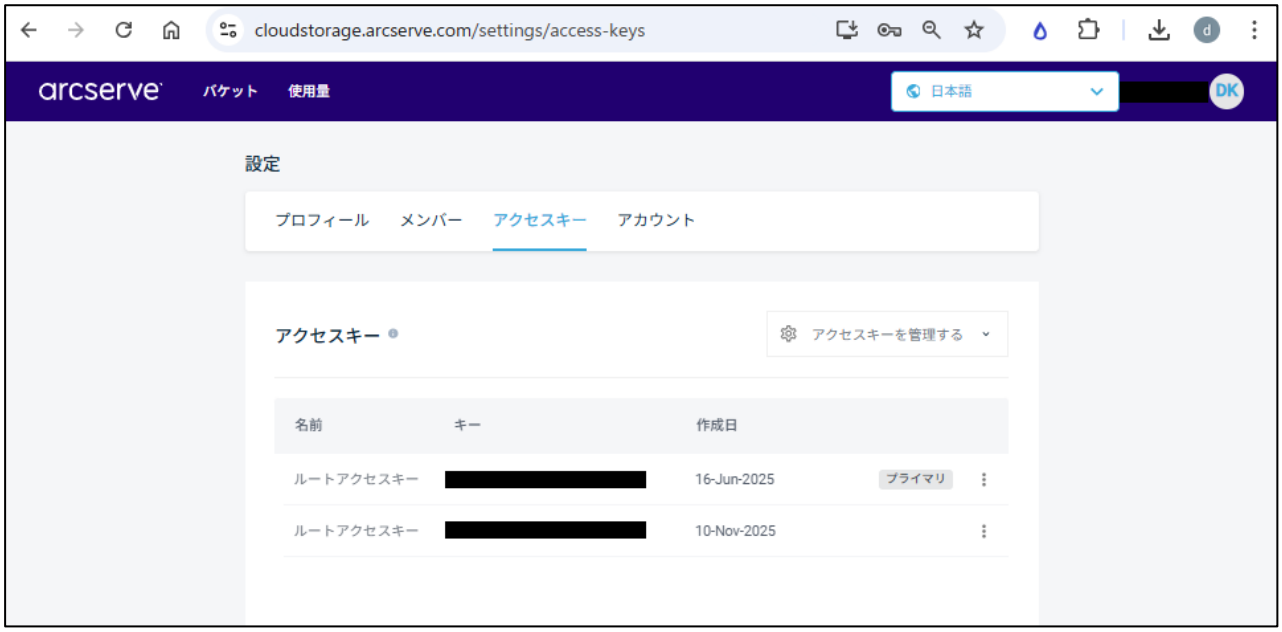


2-1. アクセス キー管理の概要

クラウド CRS / ACS を利用するためには、クラウドへのアクセス認証のために使用する「アクセス キー」 / 「シークレット アクセス キー」のペアが必要です。

アクセス キーの管理をするためには、以下の「Arcserve Cloud Storage ポータル」というクラウド ベースの管理画面を利用します。

Arcserve Cloud Storage ポータル では、アクセス キーのリセットや追加、アクセス キーの削除が可能です。



注意：

Arcserve Cloud Storage ポータルではバケットの操作は行わないでください。

バケットの作成やプロパティ設定（保持ポリシーの設定）は後述する Arcserve UDP コンソールでのデータ ストア作成時に行ってください。

2-2. Arcserve Cloud Storage ポータル へのアクセス

クラウド CRS / ACS を購入すると、申し込み時に記入したメール アドレスに Arcserve License-Program（ License-Program@arcserve.com ）からライセンス プログラム証書のメールが届きます。
※メールの件名は以下となります。

Arcserve - License Order Confirmation #xxxxxxx (xxxxxxx はオーダーID)

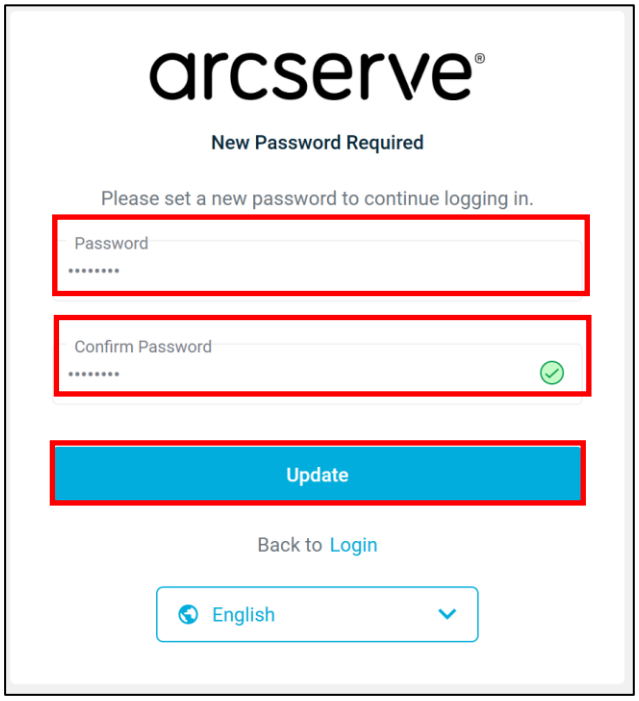
ライセンス プログラム証書のメールが迷惑メールとして扱われないように、あらかじめメールを受信できるように設定してください。

インターネットに接続できる端末から Web ブラウザ（JavaScript 有効のもの）を開き、以下の URL を入力して Arcserve Cloud Storage ポータルにアクセスしてください。
https://cloudstorage.arcserve.com

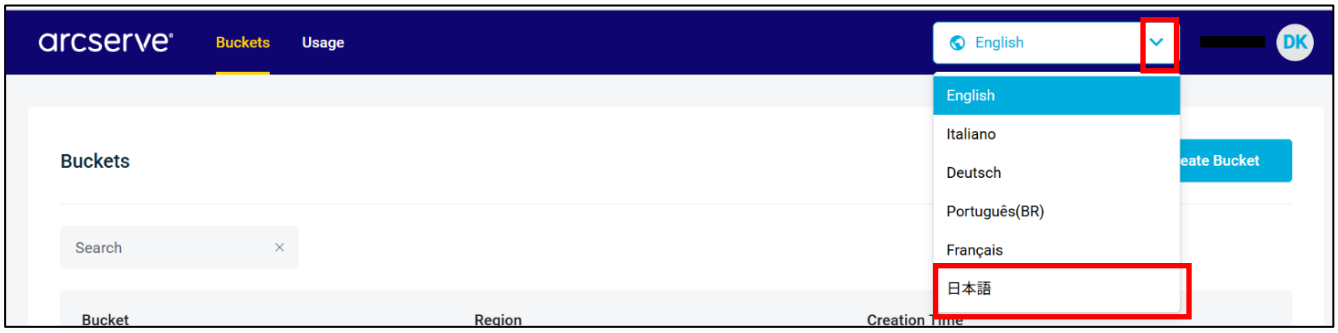
ログオン画面にて、[Email or Username] 、および [Password] に、ライセンス プログラム証書に記載されたメール アドレス、およびパスワードを入力して、[Sign in] をクリックします。

※画面下部で「日本語」を選択することで、この画面を日本語化することも可能です。

初回ログオン時には、画面の指示に従って新しいパスワードを設定します。新しいパスワード、および確認用に同じパスワードを入力し、[Update] をクリックします。



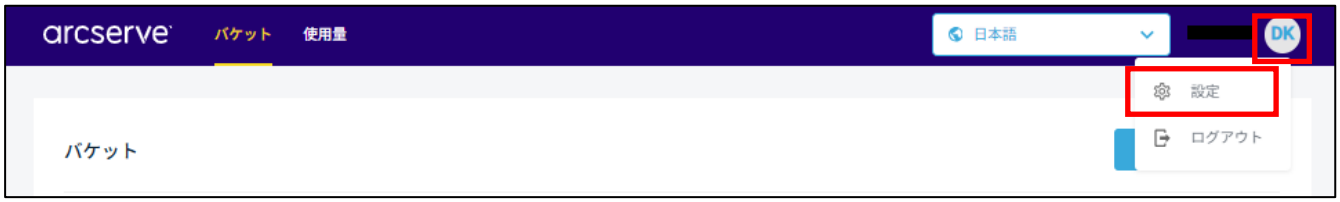
ログオン後、画面右上で「日本語」を選択することで、以降のユーザ インタフェースを日本語化できます。ここから先は日本語に設定した場合の手順を解説します。



2-3. アクセス キーのリセット

アクセス キーの管理をするためには、以下の操作を行ってください。

1. 画面右上のユーザを示すアイコンをクリックし、[設定] をクリックします。



2. [アクセスキー] タブをクリックします。

デフォルトでは 1 つのアクセス キーが発行されていますが、このアクセス キーとペアになるシークレット アクセス キーを確認する方法がないため、このアクセス キーは利用できません。
そのため、アクセス キーのリセット、もしくは追加が必要となります。

本書では、アクセス キーをリセットします。

3. [アクセスキーを管理する] をプルダウンし、[アクセスキーをリセットする] をクリックします。

4. 既存の全てのルート アクセス キー（管理者用のアクセス キー）が削除され、新しいルート アクセス キーが 1 つ発行される旨の警告が表示されます。警告の内容を確認した上で、日本語で“確認” と入力し、[確認] ボタンをクリックします。

アクセス キーはリセットされ、新しいアクセス キーが作成されます。
※既存のアクセス キーは使用できなくなります。

新しいアクセス キーおよびそれとペアになるシークレット アクセス キーは、[ダウンロード キー] からファイルとしてダウンロードしたり、[コピーキー] からクリップボードにコピーして、メモ帳などにテキスト形式で貼り付けたりすることができます。
これらのキーは、後の手順で Arcserve UDP 上で「クラウド アカウント」の設定をする際、クラウド ストレージにアクセスするための認証情報として利用します。

注意:

シークレット アクセス キーはこのタイミングでのみ、取得が可能です。

後から確認する方法はなく、紛失すると、アクセス キーのリセットや再作成が必要となります。

紛失や外部漏洩しないよう、大切に保管してください。

2-4. <参考> アクセス キーの追加

アクセス キーは追加が可能で、ご契約いただいたアカウントにつき最大 2 つまで利用できます。

追加したアクセス キーは、同一組織内において、 1 つめのキーのご利用環境とは異なるシステムでもご利用いただけます。

以下の手順でアクセス キーを追加できます。

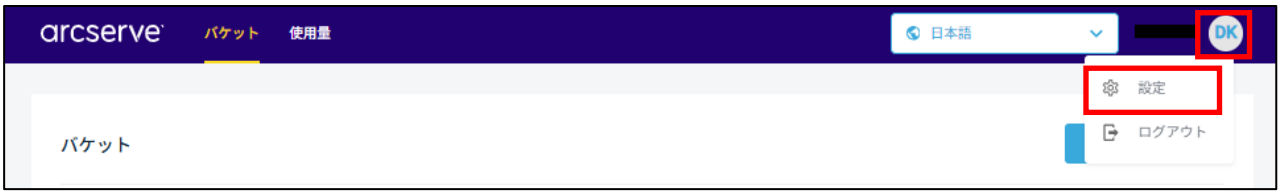
1. [アクセスキーを管理する] をプルダウンし、[アクセスキーを生成する] をクリックします。

新しいアクセス キーが発行されます

2-5. <参考> 多要素認証の設定

Arcserve Cloud Storage ポータルのセキュリティを向上させるために、サインイン時の多要素認証（MFA: Multi-Factor Authentication）を有効にすることができます。
これにより、サインイン時には電子メール/ユーザ名、パスワードに加えて、Google Authenticator 等の認証システム アプリケーションから取得したコード（ワンタイム パスワード）の入力も求められるようになり、攻撃者による Arcserve Cloud Storage ポータルへの不正アクセス リスクを低減できます。
以下は、多要素認証の設定手順です。

1. Arcserve Cloud Storage ポータルにサインインします。
2. 画面右上のユーザを示すアイコンをクリックし、[設定] をクリックします。



3. [プロフィール] タブを選択します（デフォルト）

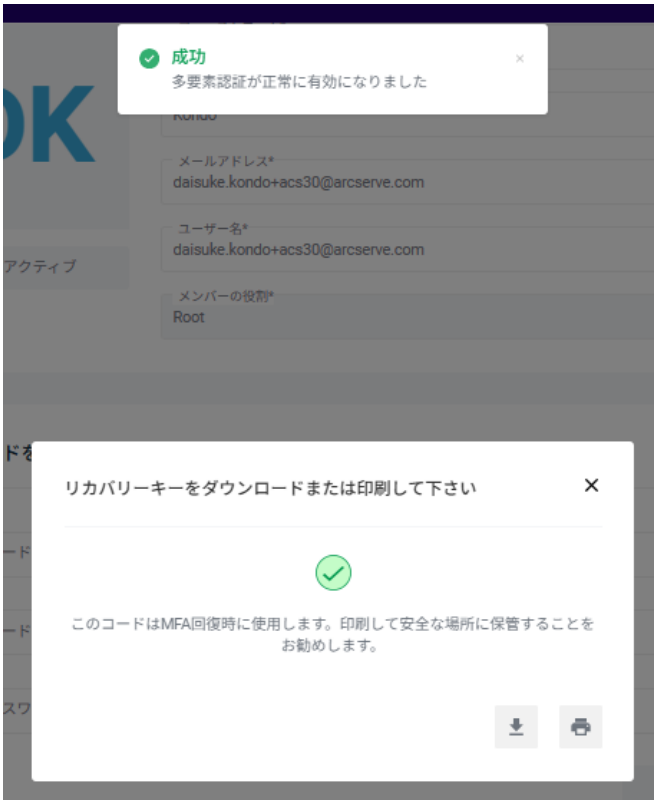
4. 画面下方にスクロールし、「多要素認証」のセクションを表示します。

5. [オンにする] をクリックします。

6. 認証アプリケーションに登録するためのキーと QR コードが表示されます。
   スマートフォン等のモバイル端末にインストールした Google Authenticator 等の認証アプリケーションで QR コードをスキャンしてアカウントを登録します。

7. [確認コード] に、認証アプリケーションに表示されるコードを入力し、[有効化] をクリックします。

これで多要素認証の設定は完了です。
リカバリ用のキーをダウンロードしたり印刷したりできるので、大切に保管してください。



モバイル端末には「Cloud Storage:（ユーザ名）」のアカウントが登録されます。

以後、Arcserve Cloud Storage ポータルへのサインイン時には認証情報の入力後に、「確認コードの入力」の画面が表示されるようになります。

モバイル端末の認証アプリケーションに表示されるコードを入力し、[確認] をクリックすることでサインインが完了します。

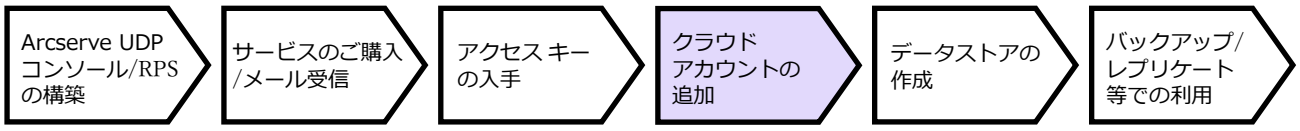
注意：

・Google Authenticator などモバイル端末上の、認証システム アプリケーション上のアカウントは、認証システム アプリケーションの解説を良くお読みになった上で必ずバックアップを行ってください。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。

・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 Arcserve Cloud Storage ポータルとモバイル端末、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失敗する場合があります。

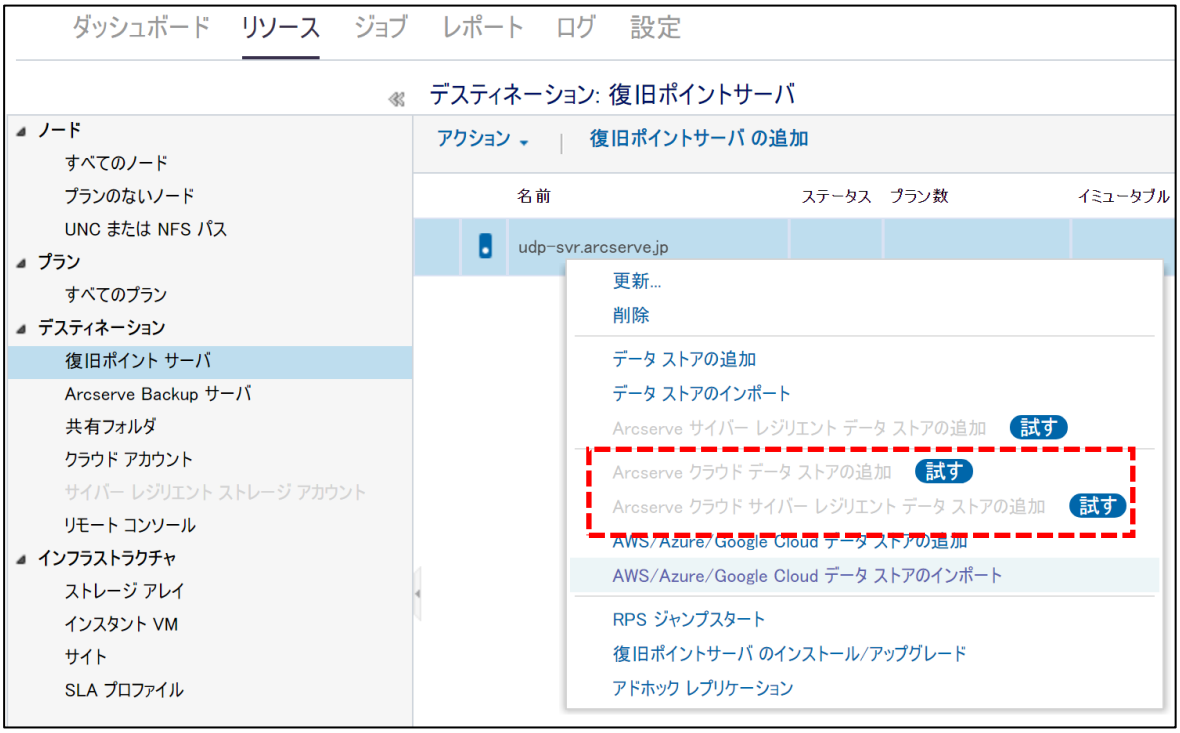
3 データストアの追加と利用

3-1. クラウド アカウントの追加



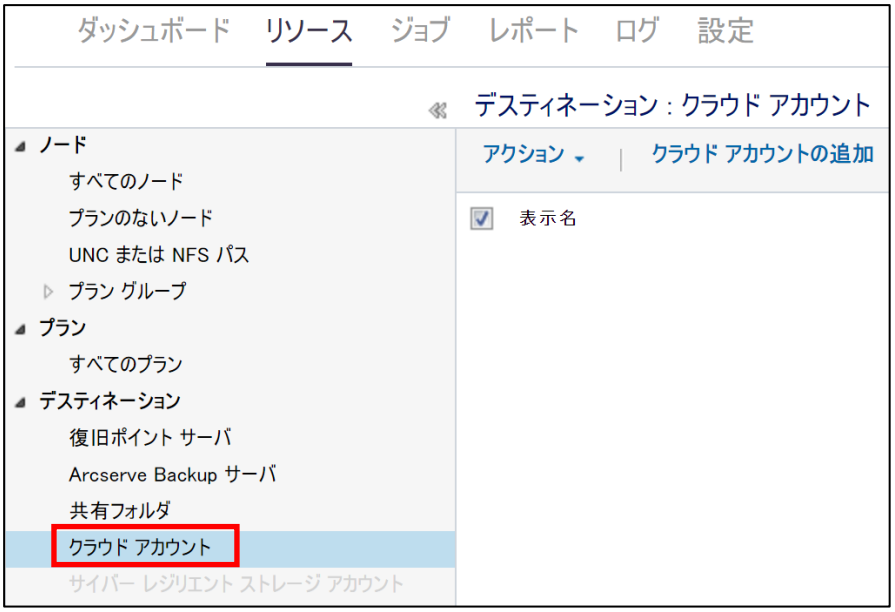
ここから先の設定は、Arcserve UDP コンソールで行います。

この時点では、[リソース] タブで復旧ポイント サーバを右クリックしても、まだ ACS のデータ ストア（Arcserve クラウド データ ストア）やクラウド CRS のデータ ストア（クラウド サイバー レジリエント データ ストア）は追加できません。



これらのデータ ストアを追加するには、以降の手順に従って、”クラウド アカウント” を作成します。

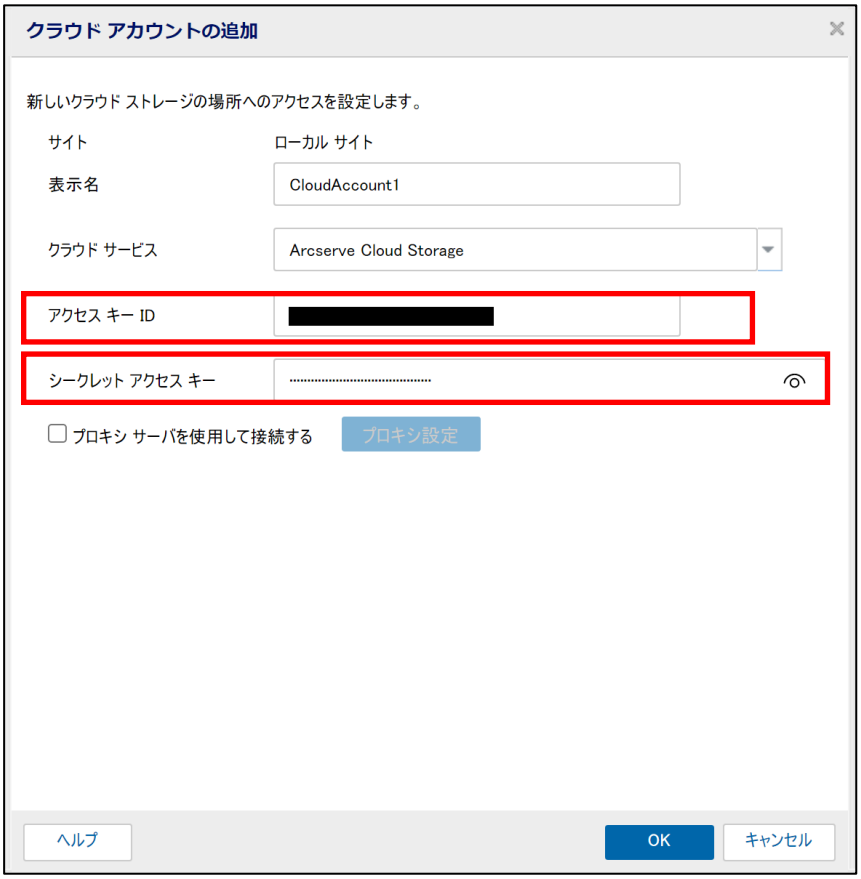
1. [クラウド アカウント] をクリックします。



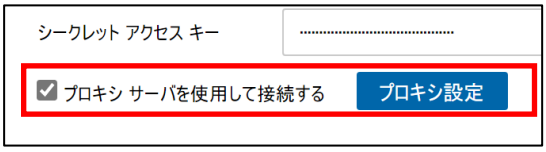
2. [クラウド アカウントの追加] をクリックします。

[表示名] に、クラウド アカウントを識別するための任意のアカウント名を入力します。また、[クラウド サービス] をプルダウンし、「Arcserve Cloud Storage」 を選択します。

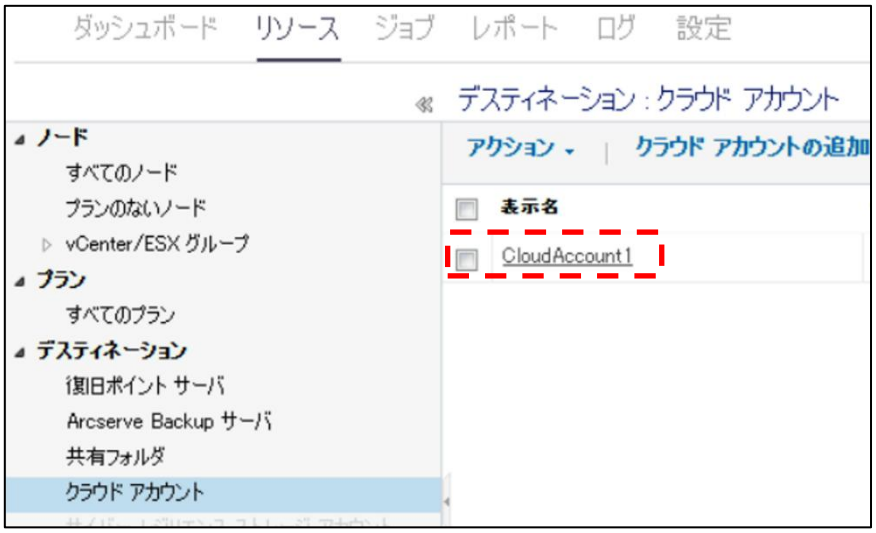
[アクセス キー ID]、[シークレット アクセスキー]に、Arcserve Cloud Storage ポータルで取得済みのアクセス キー、シークレット アクセス キーを入力します。



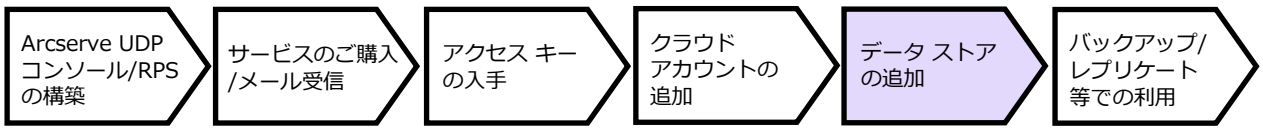
3. インターネット接続のために Web プロキシ サーバの設定が必要な環境では、[プロキシ サーバを使用して接続する] を必要な情報を入力します（Arcserve UDP 10.3 以降）。



4. 「クラウド アカウントの追加」画面で [OK] をクリックするとクラウド アカウントが作成され、データ ストアの追加が可能になります。



3-2. データ ストアの追加



クラウド CRS や ACS のデータ ストアは重複排除が有効なデータ ストアとして作成されます。その際、以下の 3 つの RPS 内のフォルダを指定します。

・データストア フォルダ

バックアップ データに関する情報、カタログの格納先

・インデックス デスティネーション

データに対するポインタ情報（インデックス）の格納先

・ハッシュ デスティネーション

重複を検知するためのハッシュ ファイルの格納先

注意：

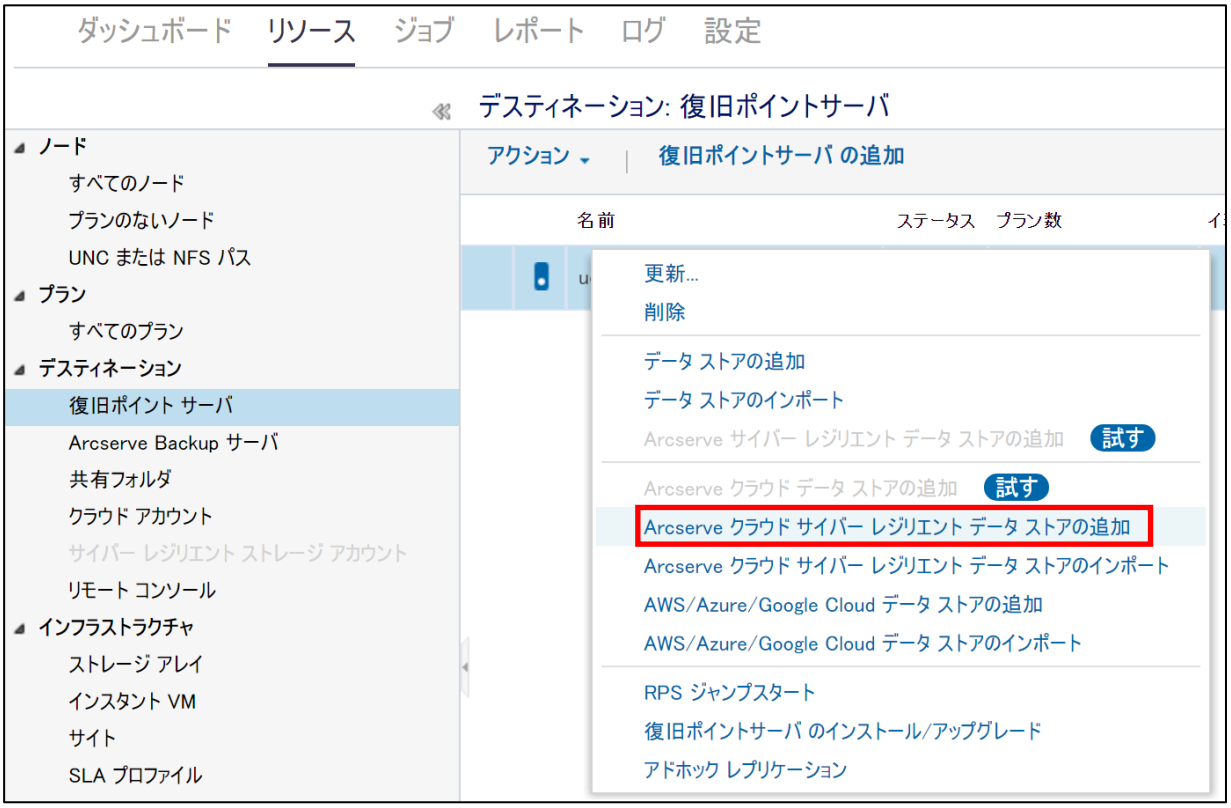
パフォーマンスの観点から、これらのフォルダはローカル ディスク上に設定してください。

また、データ デスティネーションとしてクラウド上のバケット（データ格納領域）を指定します。

なお、復旧時に必須となるデータストア フォルダやインデックス デスティネーションのフォルダは 15 分間隔でクラウドに同期されます。これにより、RPS が全損した場合でも、クラウド内のデータを元に復旧が可能となります。その際の復旧手順はバックアップ時と異なる RPS へのデータ ストア インポートをご覧ください。

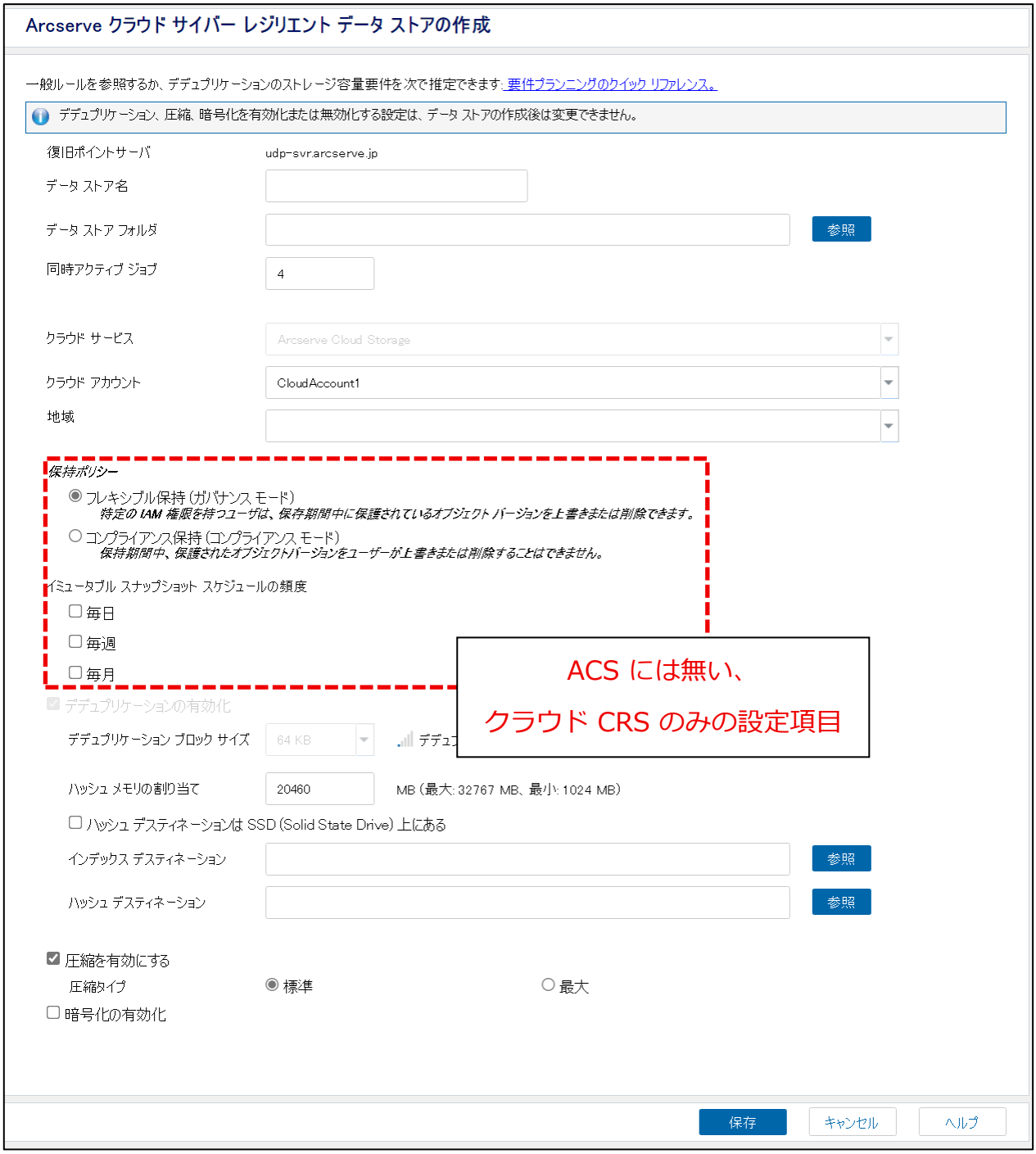
クラウド CRS のデータ ストアでは、イミュータブル スナップショットの取得のタイミングや保存期間も指定します。
次項からの手順に従って、データ ストアを作成します。

1. [リソース] – [復旧ポイント サーバ] にて 追加先の RPS を右クリックし、[Arcserve クラウド サイバー レジリエント データ ストアの追加] をクリックします。

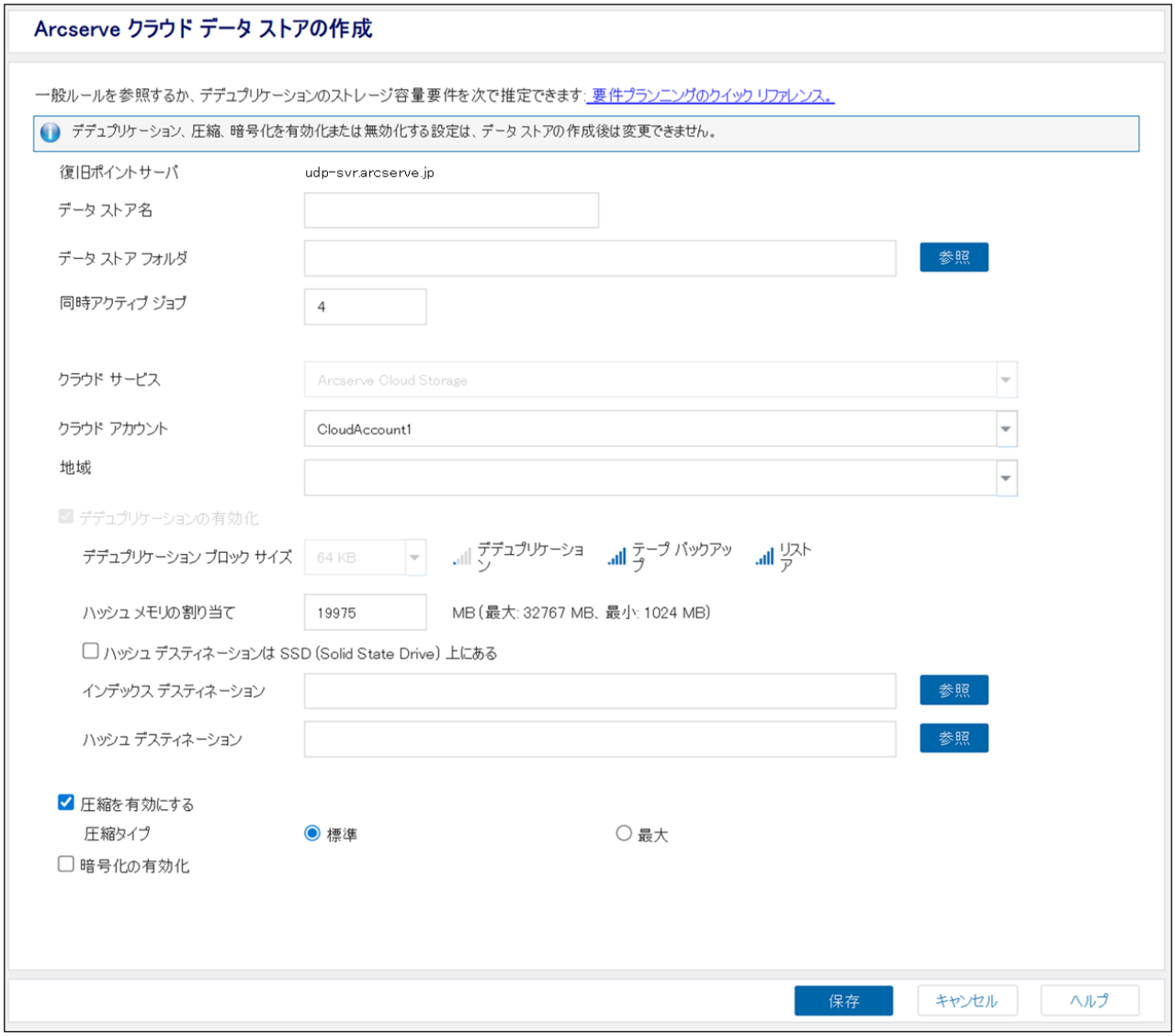


※以降の手順では、クラウド CRS のデータ ストア作成手順を解説します。ACS のデータ ストアを作成する場合は、この画面で [Arcserve クラウド データ ストアの追加] をクリックします。その際はスナップショットに関連する設定項目は表示されません。

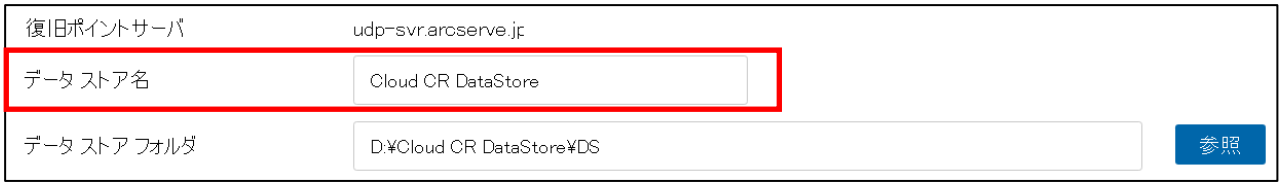
■クラウド CRS のデータ ストア設定画面



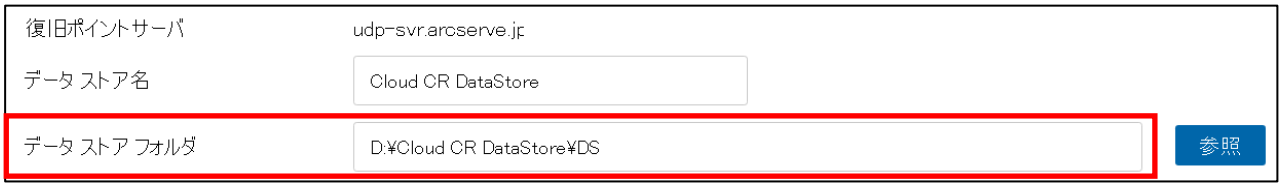
■ACS の設定画面


Arcserve クラウド データ ストアの作成
一般ルールを参照するか、デデュプリケーションのストレージ容量要件を次で推定できます: 要件プランニングのクイック リファレンス。
デデュプリケーション、圧縮、暗号化を有効化または無効化する設定は、データ ストアの作成後は変更できません。
復旧ポイント サーバ
udp-svr.arcserve.jp
データ ストア名
データ ストア フォルダ
参照
同時アクティブ ジョブ
4
クラウド サービス
Arcserve Cloud Storage
クラウド アカウント
CloudAccount1
地域
デデュプリケーションの有効化
デデュプリケーション ブロック サイズ
64 KB
デデュプリケーション
テープ バックアップ
リストア
ハッシュ メモリの割り当て
19975
MB (最大: 32767 MB、最小: 1024 MB)
ハッシュ デスティネーションは SSD (Solid State Drive) 上にある
インデックス デスティネーション
参照
ハッシュ デスティネーション
参照
圧縮を有効にする
圧縮タイプ
標準
最大
暗号化の有効化
保存
キャンセル
ヘルプ

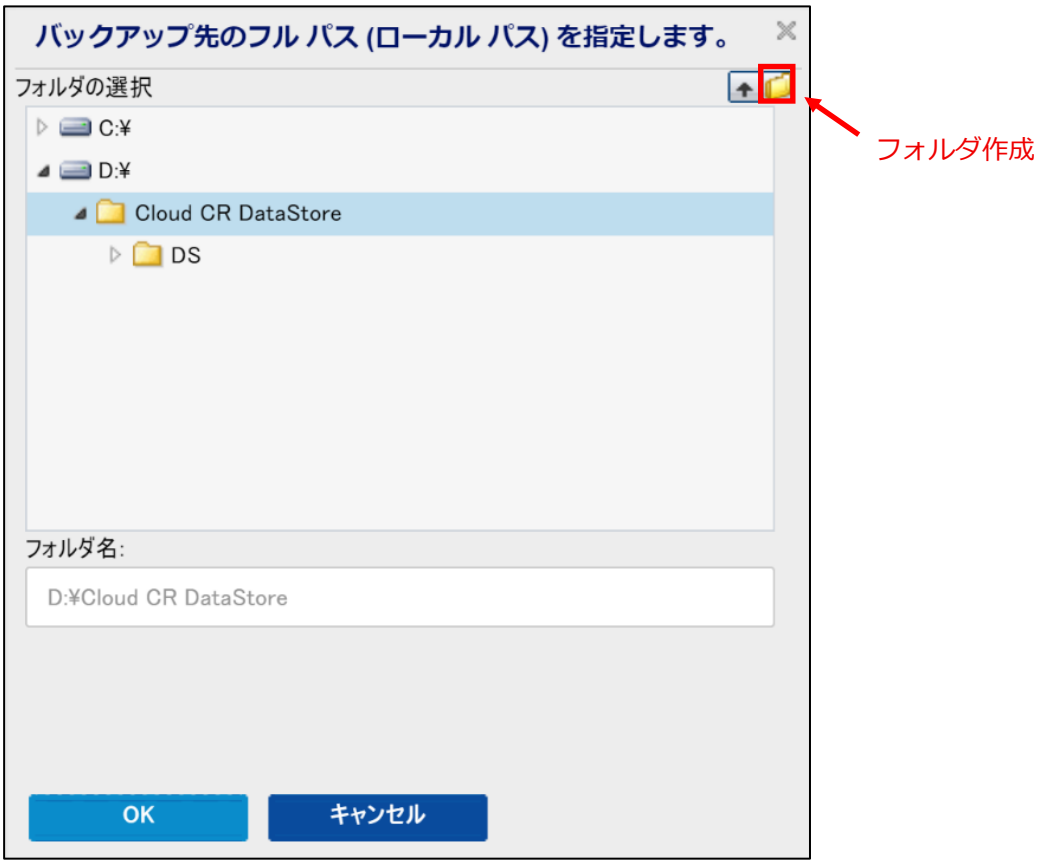
2. [データ ストア名] に任意のデータ ストア名を入力します。



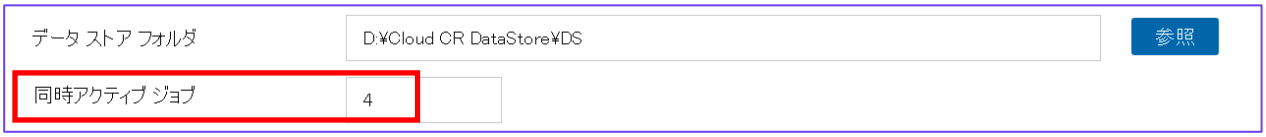
3. [データ ストア フォルダ] にパスを指定します。



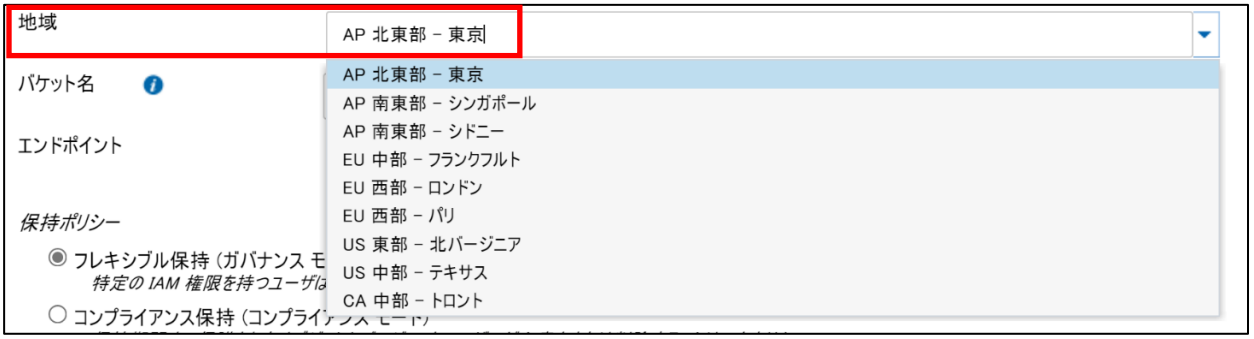
この際、右の [参照] ボタンからローカル ディスク上の場所を参照したり、選択している場所の配下にフォルダを作成したりすることも可能です。



4. [同時アクティブ ジョブ] により、データ ストアで許可される同時ジョブの最大数を指定できます。



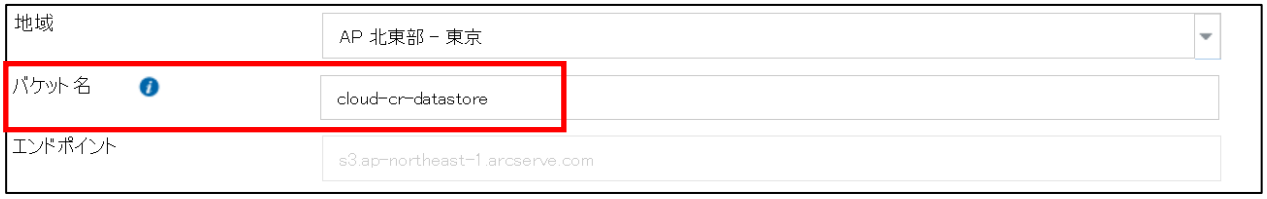
5. [地域] として「AP 北東部 – 東京」を選択します。



注意：

「AP 北東部 – 東京」以外は非サポートとなります。

6. [バケット名] に、任意のバケット名を指定します。



注意：バケット名の命名規則

バケット名は他のユーザと重複しない一意で、以下の要件を満たす必要があります。

- **ドメイン名の規則に従う有効な DNS 準拠名である必要があります**
- **小文字または数字にする必要があります**
- **3 ～ 63 文字である必要があります**
- **小文字、数字以外にピリオド（.）および/またはハイフン（-）が使用できます**

バケット名には、以下を使用できません。

- **アンダースコア（_）**
- **末尾にダッシュ**
- **連続するピリオド（…）**

- **ピリオドの前後にダッシュ**

  例： my-bucket-.name

- **IP アドレスのフォーマット**

  例： 123.45.678.90

7. （注：クラウド CRS のみの設定です）

[保持ポリシー] を設定します。デフォルトは「フレキシブル保持（ガバナンス モード）」となっていますが、「コンプライアンス保持（コンプライアンス モード）」に変更します。

参考：保持ポリシーの違い

	ガバナンス モード	コンプライアンス モード
クラウド内のデータ削除/変更	可能	不可能
スナップショット保存期間の変更	可能	不可能

ランサムウェア対策としては、バックアップ データの削除/改ざんを防ぐ必要があるため、コンプライアンス モードをご使用いただくことを推奨します。

8. **（注：クラウド CRS のみの設定です）**

イミュータブル スナップショット スケジュールの頻度を設定します。

デフォルトではイミュータブル スナップショットは取得されません。

[毎日]、[毎週]、[毎月] のチェック ボックスにチェックを入れて、[スナップショット時刻] や [保存期間] を設定できます。

スナップショットは設定した時刻に取得され、バックアップ データを保護します。

※詳細な設定については Arcserve UDP 10.x ソリューション ガイドの、

「Arcserve クラウド サイバー レジリエント データストアの変更」をご参照ください。

9. クラウド CRS / ACS のデータ ストアでは、デデュプリケーション（重複排除）は必ず有効になります。
   [ハッシュ メモリの割り当て] や [ハッシュ デスティネーションは SSD (Solid State Drive 上にある)] を適切に設定してください。

10. [インデックス デスティネーション] および [ハッシュ デスティネーション] を指定します。

11. [圧縮を有効にする] はデフォルト有効となっていて、標準レベルでの圧縮が行われます。

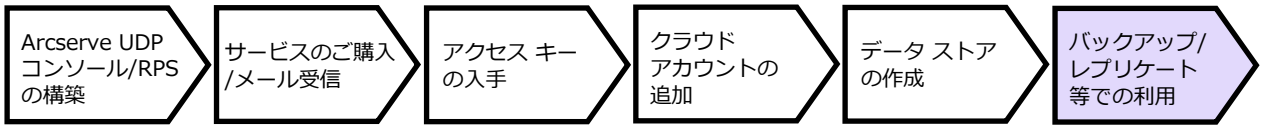
[暗号化の有効化] はデフォルトでは無効です。
必要に応じて設定してください。

暗号化を有効にする場合、[暗号化パスワード] および [暗号化パスワードの確認] も入力します。

12.設定を確認し、[保存] をクリックします

RPS にデータ ストアが追加されました。

3-3. バックアップ/レプリケート等での利用



作成したクラウド CRS / ACS のデータ ストアは、サーバを保護する「プラン内」で、バックアップ タスクやレプリケート タスクの保存先（デスティネーション）としてご利用いただけます。

プラン/タスクの設定方法については、Arcserve UDP のマニュアル「Arcserve UDP 10.x ソリューション ガイド」のデータを保護するプランの設定をご参照ください。

4 ランサムウェア攻撃からの復旧

4-1. 復旧の流れ

ランサムウェア攻撃などにより、本番データに加えて、バックアップ データも破壊・改ざんされた場合、以下の流れで復旧を行います。

1. クラウド CRS のデータ ストアにて、イミュータブル スナップショットの一覧から、健全な時点のスナップショットを選択する
2. 「読み取り専用データ ストア」として RPS にインポートする
3. インポートしたデータ ストアから、任意の復旧ポイントを使用して本番サーバをリストアする

注意：

読み取り専用データ ストアとしてインポートするには、インポート元のデータ ストアが RPS に追加済みである必要があります。RPS が全損して再構築などが必要な場合は、バックアップ時と異なる RPS へのデータ ストア インポートをご覧ください。

4-2. イミュータブル スナップショットのインポート

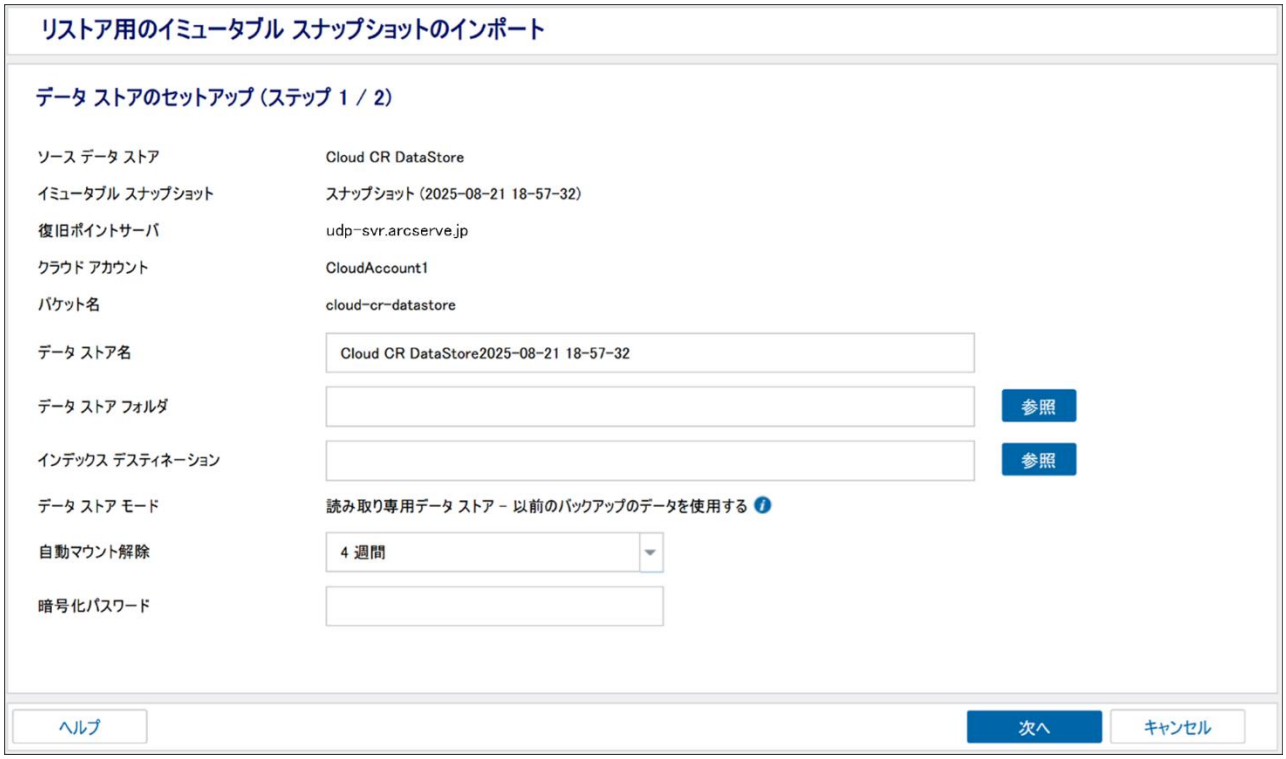
1. [リソース] タブをクリックし、[復旧ポイント サーバ] を選択します。

2. クラウド CRS のデータ ストアを管理している RPS を右クリックし、[イミュータブル スナップショットの表示] をクリックします。

作成済みのイミュータブル スナップショットが表示されます。

3. バックアップ データを破壊・改ざんされる前の健全な時点のスナップショットを選択し、[リストア用のイミュータブル スナップショットのインポート] をクリックします

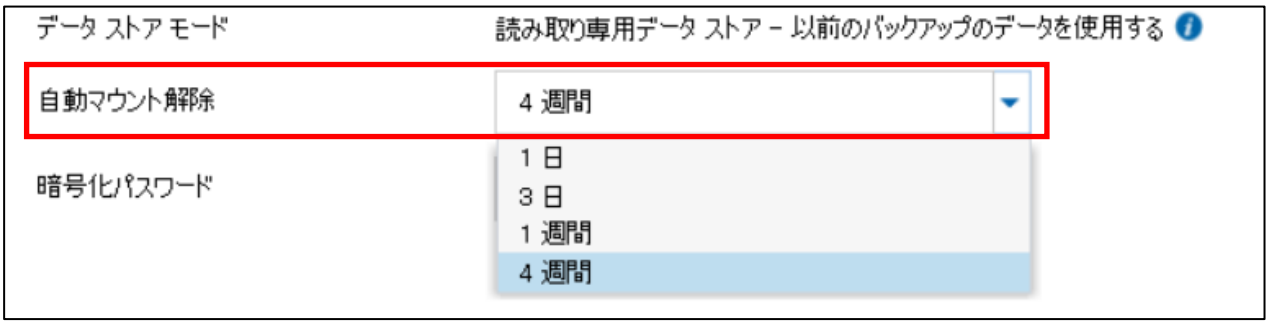
インポートのための設定画面が表示されます。



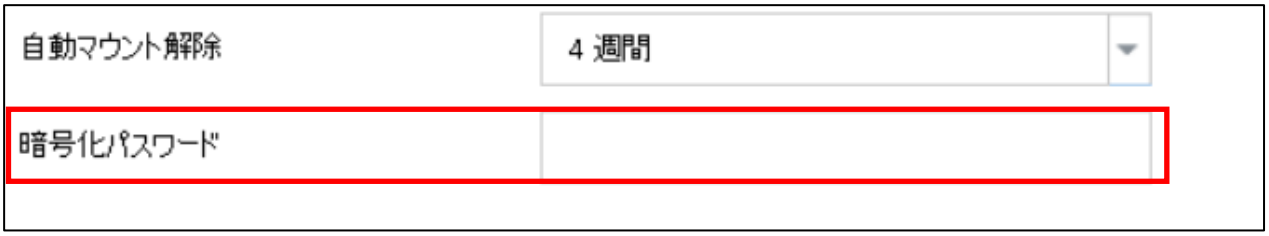
4. [データ ストア フォルダ] と、[インデックス デスティネーション] を指定します。

※ 読み取り専用データ ストアには、ハッシュ デスティネーションは不要です。

5. [自動マウント解除] では、読み取り専用データ ストアのマウントを自動解除するタイミングを設定します。デフォルトは 4 週間で解除されます。リストアに必要な時間を考慮して設定してください。

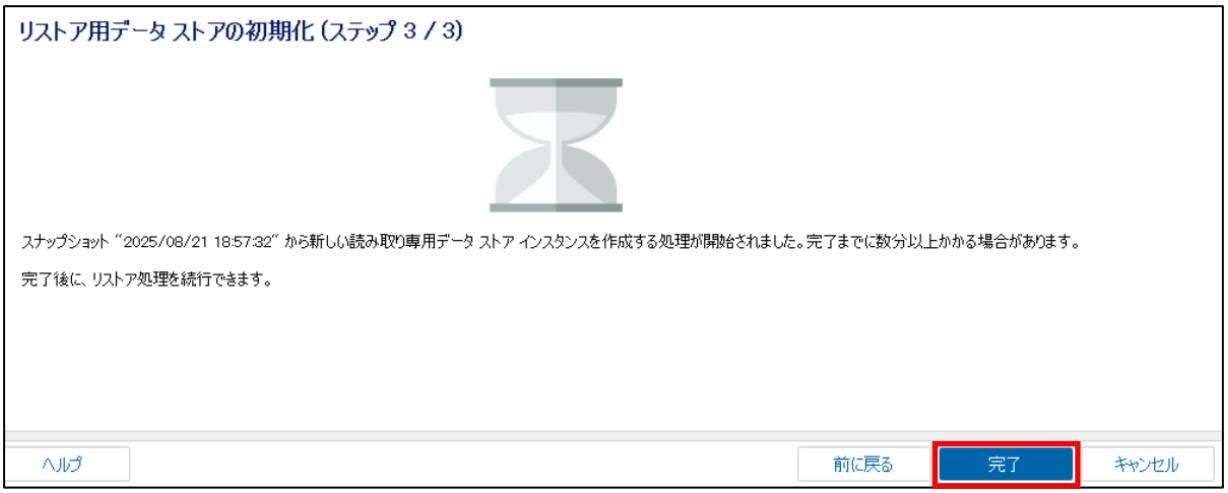


6. 暗号化を設定していた場合は、[暗号化パスワード] に設定時のパスワードを入力します。



7. 設定を確認し、[次へ] をクリックします。

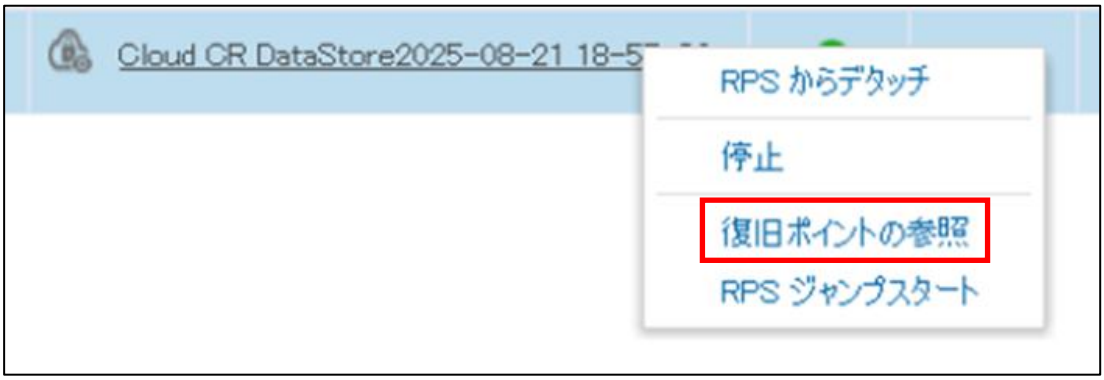
8. メッセージを確認し、[完了] をクリックします。



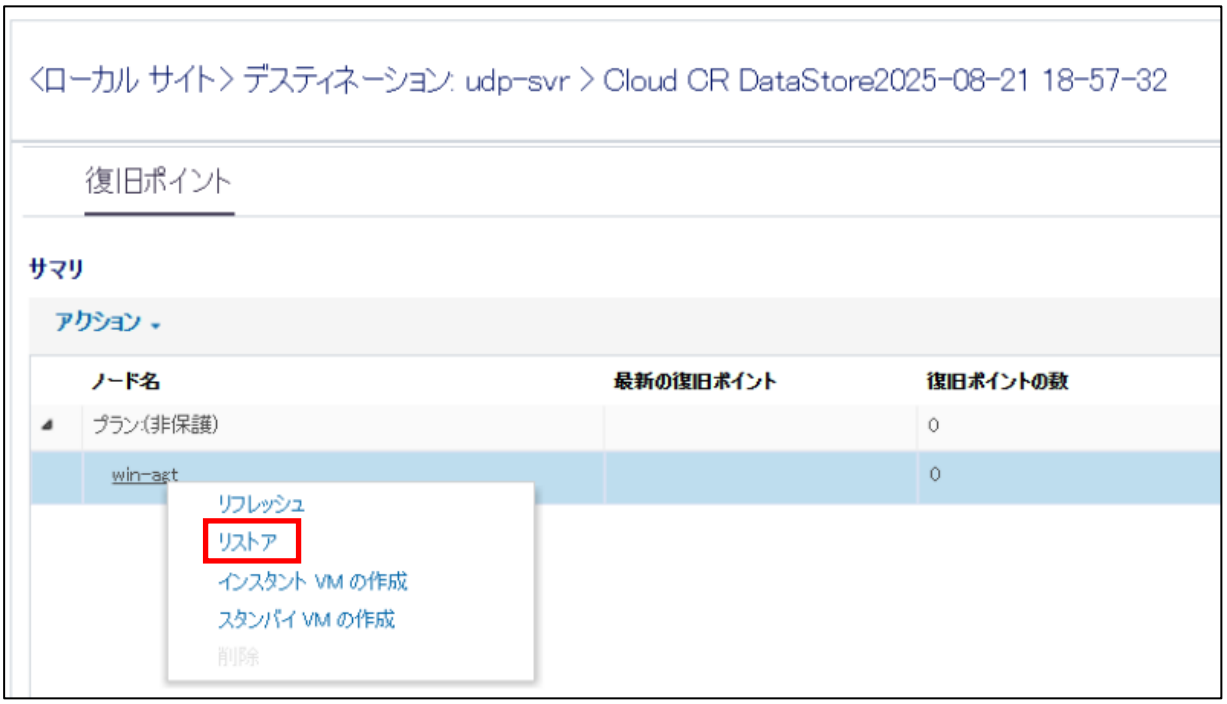
インポートが完了し、リストア用の読み取り専用データ ストアが追加されます。

4-3. リストアの実行

1. インポートしたデータ ストアを右クリックし、[復旧ポイントの参照] をクリックします。



2. リストアしたいノードを右クリックし、[リストア] を選択します。



3. 通常のデータ ストアと同様に、リストアを行うことができます。

詳細は「Arcserve UDP 10.x ソリューション ガイド」の保護データのリストアをご覧ください。

4-4. バックアップ時と異なる RPS へのデータ ストア インポート

サイバー攻撃などで UDP コンソールや RPS が全損してしまった場合、再構築するか、別な利用可能の UDP コンソール / RPS を使って復旧を行ってください。クラウド アカウントが UDP コンソールに登録されていない場合は、再作成も行ってください。
UDP コンソール、RPS、クラウド アカウントが利用可能になったら、クラウド CRS / ACS から RPS に元のデータ ストアをインポートします。クラウド CRS のデータストアがコンプライアンス モードで保護されていれば、スナップショット保持期間の間はクラウド内のバックアップ データは破壊されずにインポート可能な状態で保持されています。
クラウド CRS のデータ ストアでは、その後に必要に応じて、スナップショットを指定して読み取り専用データ ストアとしてインポートすることもできます。

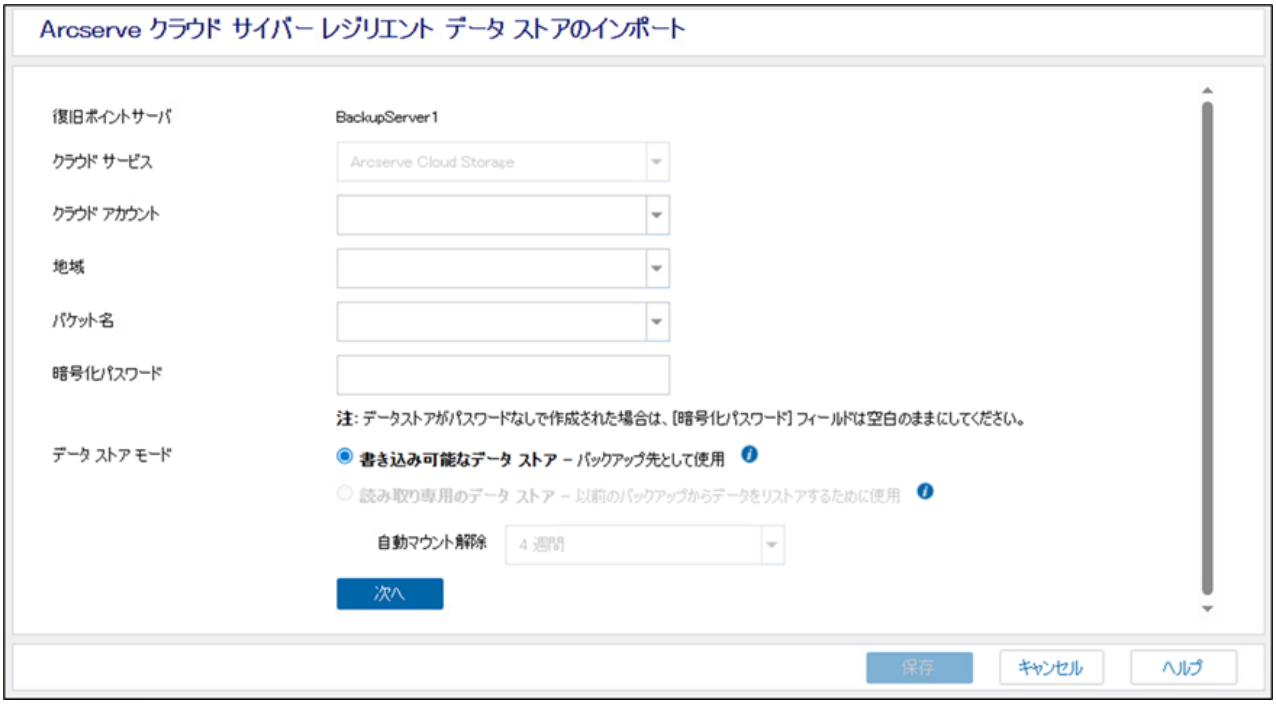
以下は、クラウドから RPS にクラウド CRS のデータ ストアをインポートする手順です。

1. クラウド アカウントが作成されていない場合は作成します。アクセス キー／シークレット アクセス キーの情報が無い場合は、新しくキーを発行して作成してください（キー発行に使用する Arcserve Cloud Storage ポータルのアカウントはデータストア作成時と同じアカウントである必要があります）。

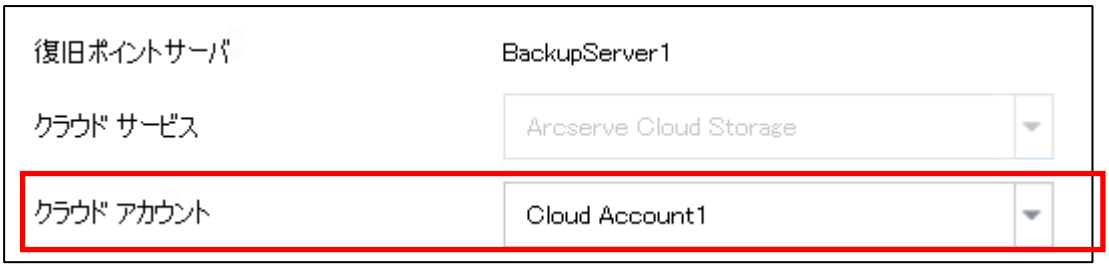
2. [リソース] – [復旧ポイント サーバ] をクリックします。

3. インポート先の RPS を右クリックし、[Arcserve クラウド サイバー レジリエント データ ストアのインポート] をクリックします。

Arcserve クラウド サイバー レジリエント データ ストアのインポート画面が開きます。

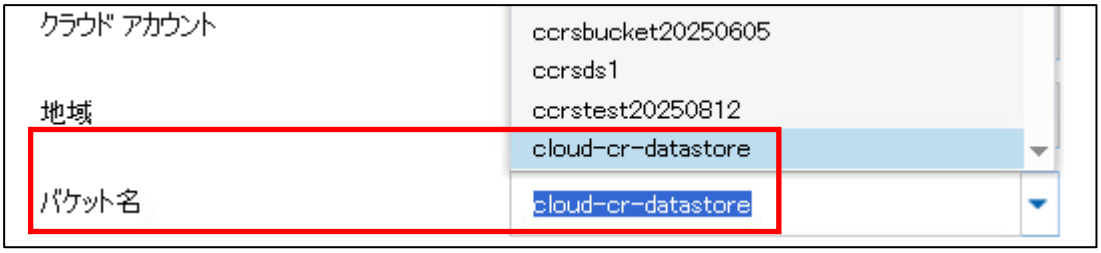


4. [クラウド アカウント] を選択します。データ ストアを作成したときのアカウントを選択してください。

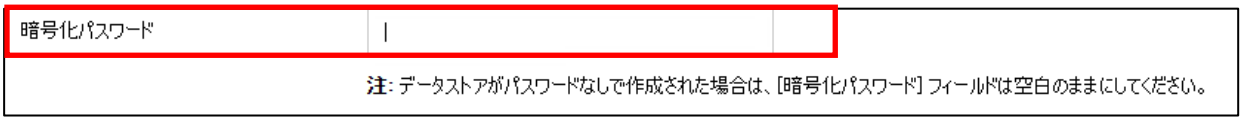


5. [地域] で「AP 北東部 – 東京」を選択します。

6. バケットのリストから、インポートするデータ ストアのバケットを選択します。

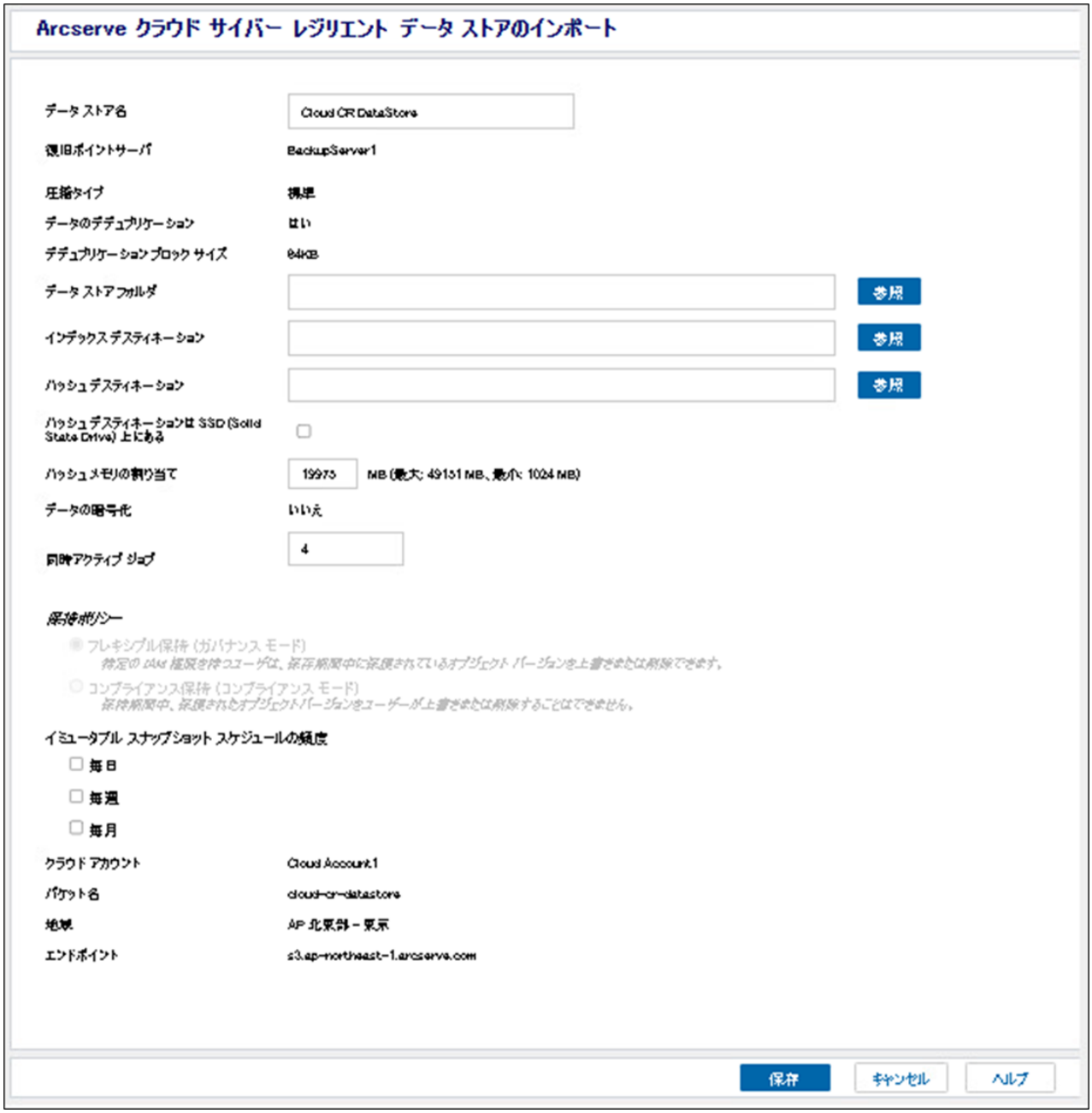


7. 暗号化していた場合は、[暗号化パスワード] を入力します。

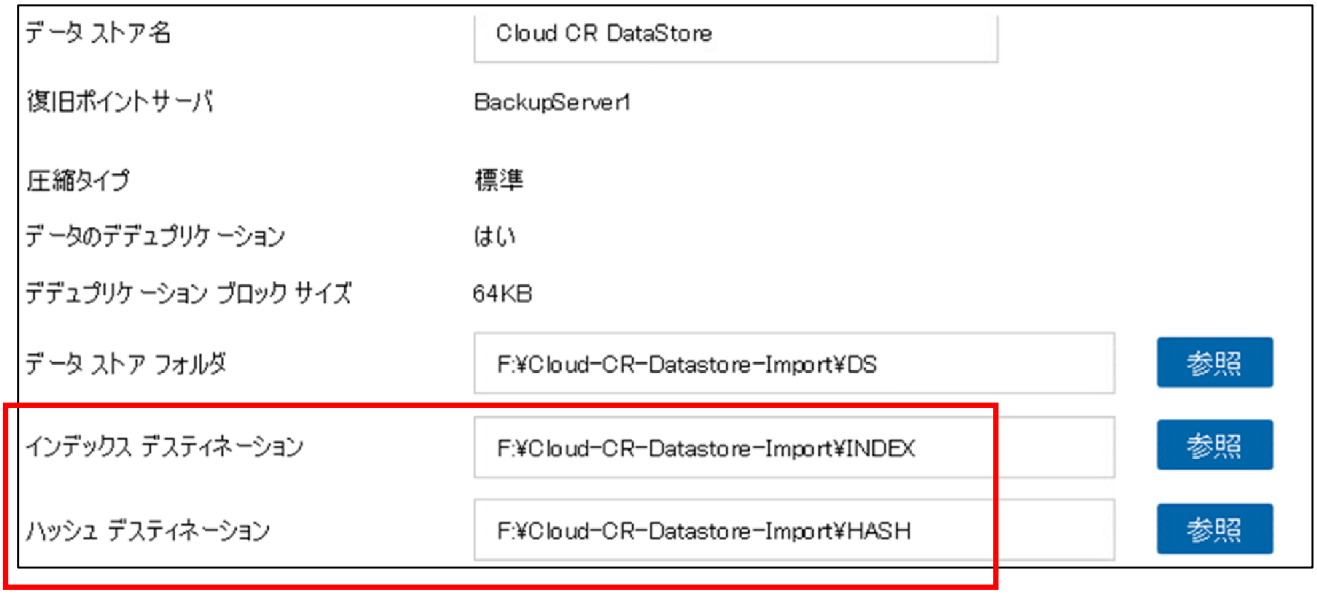


8. [次へ] をクリックします。

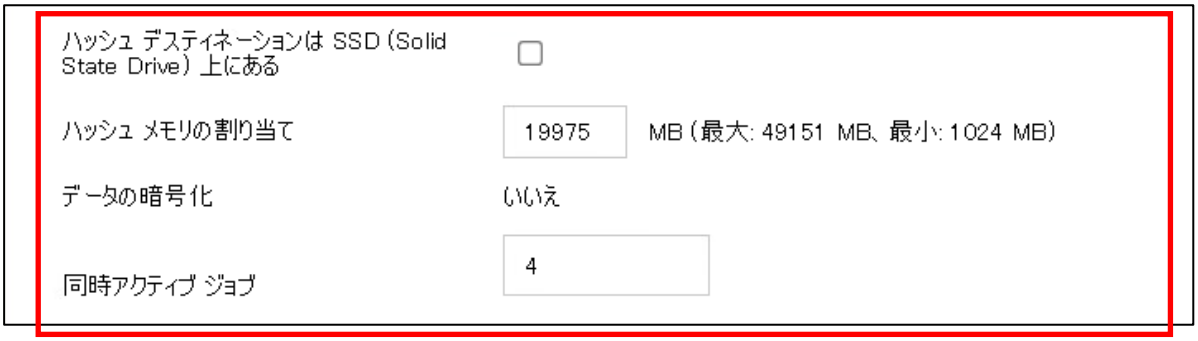
画面がリフレッシュし、追加の設定項目が表示されます。

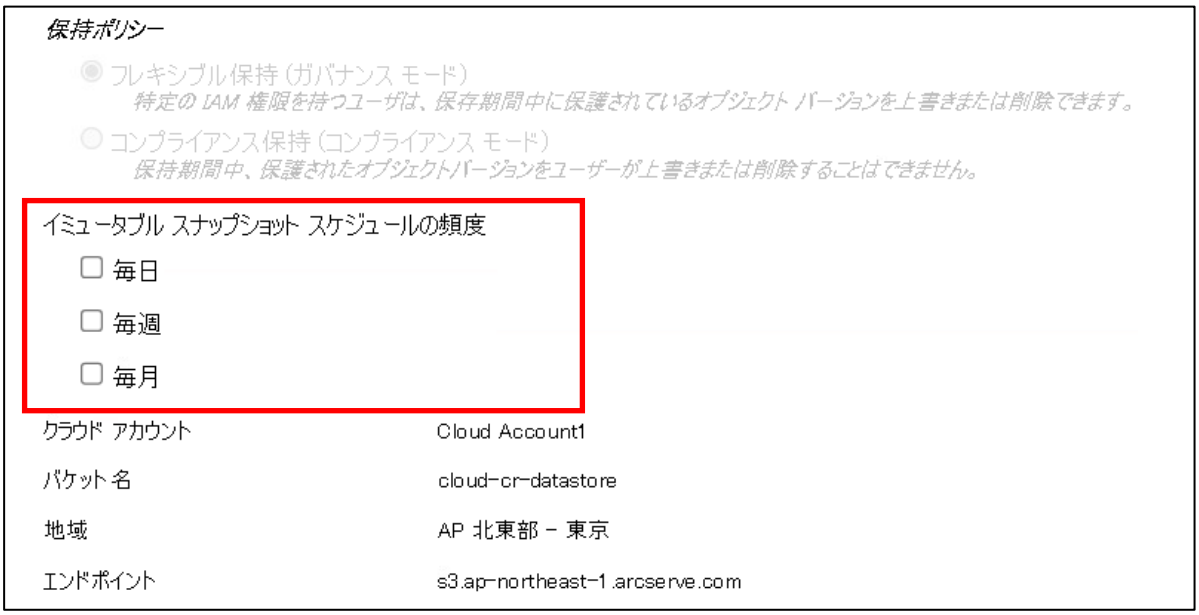


9. [データ ストア フォルダ]、[インデックス デスティネーション]、[ハッシュ デスティネーション] に、RPS 内の空フォルダを指定します。



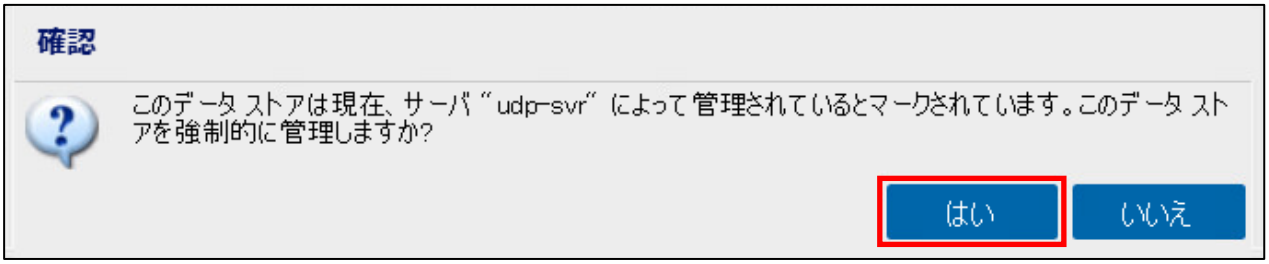
10. 必要に応じて、その他の設定可能な項目も設定します。手順としては、データ ストアの追加と同様です。





11.[保存] をクリックします。

12.他のサーバで管理されている旨のメッセージが出た場合、確認の上で[はい] をクリックします。



インポートが行われます。

この後は、イミュータブル スナップショットのインポートの手順で、スナップショットから読み取り専用データストアを作成してください。

5 参考情報

・Arcserve CRS シリーズ 紹介資料
https://www.arcserve.com/hubfs/243905555/jp-resources/crs-presentation.pdf

・よくあるご質問と回答
https://www.arcserve.com/hubfs/243905555/jp-resources/acs-ccrs-faq.pdf

・オンライン ヘルプ（Arcserve UDP 10.x ソリューションガイド内）
https://documentation.arcserve.com/Arcserve-UDP/Available/10.0/JPN/Bookshelf_Files/HTML/SolG/default.htm#UDPSolnGuide/add_crs_data_store.htm

・Arcserve UDP 10.x 動作要件
https://support.arcserve.com/s/article/Arcserve-UDP-10-X-Software-Compatibility-Matrix?language=ja

・注意/制限事項
https://support.arcserve.com/s/article/2025090304?language=ja

・購入方法と価格表
https://www.arcserve.com/ja/licensing-options

・Arcserve クラウド サービス規約
https://www.arcserve.com/ja/cloud-services

・Arcserve Japan Direct（購入前のお問い合わせ）
https://www.arcserve.com/ja/contact-us

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