

文書責任者	代表取締役 稲葉 博樹
正式版原本	data-retention-deletion-policy.md
SHA-256	37b59b5ffb4c6cbd3100764f88b88b2bfdc1ca79075c30230011d87f85e54145

NIDOME データ保持・出力・削除条件

版: 1.0 / 制定日: 2026-08-26 / 適用日: 2026-09-01

状態: 社内承認済み。初期3社限定試行で適用し、一般提供は外部法務レビューの再検討後に別途判断します。

1. 目的

本条件は、NIDOMEに保存する契約者データの保持、データ出力、契約終了、削除およびバックアップ上の取扱いを定めます。個別契約または法令に別の定めがある場合、その定めを優先します。

2. 基本原則

- 当社は、サービス提供、契約履行、セキュリティ、法令遵守、紛争対応に必要な期間を超えてデータを保持しません。
- 契約者は、自らに適用される法令・業界規則に基づく保存期間を判断し、必要な帳票・証明書・台帳を契約期間中または契約終了後30日のデータ出力期間内に出力します。当社は、契約者の法定保存義務を代わって履行する長期保管サービスを標準では提供しません。
- 「画面から非表示」「論理取消」「稼働中システムからの削除」「バックアップからの失効」「物理媒体廃棄」を区別します。
- 見積、請求、入出金、証明書、監査等の重要記録は、誤操作防止と証跡のため取消後も追記型または状態変更で保持する場合があります。
- 契約者の業務データと、当社自身の契約、請求、会計、セキュリティおよび紛争対応記録を分離し、それぞれ異なる保持期間とアクセス権限を適用します。

3. 契約期間中の保持

データ区分	保持方針	削除・取消
テナント、店舗、ユーザー、権限	契約中および終了後保持期間	ユーザーは利用停止を基本とし、関連監査との整合を維持
在庫、案件、回収、工程、販売	契約中および終了後保持期間	業務上の取消・廃棄は履歴を残す
契約者の見積、請求、支払、入出金	契約中および契約終了後30日のデータ出力期間	契約中は発行・取消・入出金イベントを追記型で保持し、期限後は例外保持を除き削除
契約者の消去記録・証明書原本	契約中および契約終了後30日のデータ出力期間	原本ファイルと表示用スナップショットは期限後に削除し、最小限の発行証跡は別管理
当社のNIDOME利用契約、利用料請求、会計記録	原則10年	テナント業務データから隔離し、法令・税務・紛争対応以外に利用しない
消去証明書の最小発行証跡	発行から7年	証明書番号、版、ハッシュ、発行・失効・再発行日時、監査イベント等に限定
在庫画像・添付ファイル	契約中および終了後保持期間	稼働中のオブジェクト削除後も旧版が保存周期の終了まで残る場合あり
業務監査ログ <code>audit_logs</code>	イベント発生から3年	全プラン共通。1年は検索可能な稼働領域、残り2年は暗号化・改ざん防止アーカイブで保持し、通常画面から編集・削除しない
サポートチケット本文・対応履歴・メタデータ	チケット終了から3年	テナント業務データから分離し、サポート、品質改善、紛争対応に必要な担当者だけが参照
通常のサポート添付ファイル	チケット終了から1年	インシデント証拠または法的保全対象へ指定したものを除き、本文・メタデータより早く削除
通常の運用インシデント内部記録	インシデント解決から3年	公開稼働状況の表示期間と分離し、原因分析、再発防止、SLA検証に限定して利用
重大なセキュリティ・個人データ・契約インシデント内部記録	インシデント解決から5年	影響、判断、通知、調査、証拠、再発防止に必要な最小限の記録に限定
公開稼働状況の履歴	インシデント解決から30日	公開期間終了後も、該当する内部インシデント記録は上記期間に従って保持
広告・宣伝メールの承諾・送信・配信停止記録	最後の送信日または配信停止日のいずれか遅い日から3年	対象アドレス、承諾・停止日時、取得経路、対象範囲および必要な送信履歴に限定。契約者から処理を委託された個人データを営業目的へ転用しない
ユーザー通知	システム既定180日	定期削除対象。契約条件化する値を要決定

業務監査ログ `audit_logs`には、操作主体、テナント、対象、操作、結果、日時、リクエストID等、業務上の追跡に必要な項目だけを記録します。パスワード、トークン、クッキー、認証ヘッダー、不要なリクエスト・レスポンス本文その他のシークレットは記録しません。大量のアクセスログ、アプリケーションログおよび通信ログは`audit_logs`と区別し、セキュリティ・運用上必要な最小期間を別の内部基準で管理します。

3.1 契約に至らなかった申込情報

状態	申込内容・添付ファイルの標準保持期限	期限の起算点
未提出の下書き	30日	最終更新日時
未使用または期限切れの招待	30日	招待期限
申込者による取下げ	90日	取下げ日時
当社による不承認	180日	不承認日時
契約成立	契約・テナントデータへ移行	契約成立日時

- 標準保持期限後は、申込の入力内容、提出時点の記録、添付ファイル、連絡先その他の申込本文を削除します。
- 申込番号、最終結果、作成・提出・取下げ・不承認・期限切れ日時、理由区分および申込者メールアドレスの不可逆ハッシュ等、再申込の判定、不正防止、説明責任および紛争対応に必要な最小限の監査証跡は、各申込みの終了から1年間保持します。

メールアドレス本文、自由記載、添付ファイルおよび審査担当者の不要な内部メモは監査証跡に残しません。

3. 未解決の紛争、不正利用、セキュリティインシデント、法令上の要請または法的保全がある場合、対象、理由、承認者および見直し期限を記録したうえで、関係する最小限のデータだけを解決まで隔離保持できます。
4. 状態別の削除処理、最小監査証跡への縮退、添付ファイル削除、法的保全の除外および削除結果監査の実装・受入が完了するまで、本項を公開版または契約上の削除保証として発効させません。

4. 契約者によるデータ出力

1. 契約者は、契約中または契約終了手続において、当社所定の方法でテナントデータのアーカイブ出力を申請できます。
2. データ出力処理は監査され、完了ファイルには件数、容量、SHA-256チェックサム等を記録します。
3. 完了したアーカイブは、現在のシステム既定で7日間ダウンロードできます。期限後はダウンロードできません。
4. ダウンロード用の一時URLは、現在のシステム既定で15分有効です。
5. 契約者は、ダウンロードしたファイルを安全な場所へ保存し、アクセス権限、暗号化、廃棄を管理します。
6. 標準データ出力は、当社が公開する版管理された出力対象一覧に定める契約者の業務データをUTF-8 BOM付きCSV、標準出力に対応済みの発行済み・取消済み・再発行済み帳票をPDF、契約者が登録した対象原本ファイルおよびmanifest.jsonとしてZIPまたは分割アーカイブで提供します。下書きは構造化データとして提供します。
7. パスワード、トークン、認証情報その他のシークレット、当社内部の運用・サポート内部メモ・セキュリティ情報および他テナントのデータは出力対象に含めません。出力対象は許可リストで管理し、テーブル・カラム・形式の変更履歴を保持します。
8. アーカイブはサービス提供者の暗号化ストレージへ非公開で保存し、TLSで送信します。AWS KMSその他の特定の暗号化方式は、実装と受入が完了してサービス仕様へ明記した場合に限り契約上の保証対象とします。
9. 提供期間中の一時URL再発行は無料です。契約終了後30日の標準保持期間内に行うアーカイブ再生成は、初回生成後1回まで無料とします。当社の障害、欠損または破損に起因する再生成は回数にかかわらず無料です。再発行または再生成によって契約終了後のデータ保持期限は延長されません。
10. 個別形式、標準上限を超える大容量、物理媒体、特別な復旧および契約者都合による追加再生成は、作業前に内容と費用を提示し、契約者が合意した場合に限り有料とします。標準データ出力そのものをデータ返還のために有料とはしません。
11. 標準容量、1アーカイブ当たりの上限および分割条件は、AWS検証環境での負荷・復元・ダウンロード受入後にサービス仕様へ定めます。受入前は特定の容量を契約上保証しません。
12. 対象原本の欠落が判明した場合、取得可能なデータの提供を不当に遅延させず、欠落対象をmanifest.jsonの警告へ記録します。重要な契約文書、帳票、証明書その他の証拠ファイルが欠落した場合は、完全なデータ出力であると表示せず、インシデントとして調査し、復旧または再生成の可否を通知します。

5. 契約終了後の保持

1. 契約終了が承認されるとテナントをcanceledとし、通常業務利用とデータ更新を停止したうえで、契約終了日から30日後をデータ保持期限に設定します。
2. 30日の標準保持期間中は、データ出力、請求・サポート対応等、当社が認めた必要な操作に限定します。契約者はこの期間内にテナントデータのアーカイブ出力を申請します。
3. 個別延長は、現在の保持期限前に契約者が申請し、当社が技術、セキュリティ、法令および運用上対応可能と判断して書面で承諾した場合に限り、標準保持期限から暦月単位で追加する前払いの有償条件とします。自動更新は行わず、契約終了日からの総保持期間は365日以内とします。延長は通常利用、データ更新または常時ポータルアクセスを再開するものではなく、保管、当社所定のデータ出力再生成およびサポート対応だけを対象とします。追加のデータ出力、個別形式、復旧その他の作業料金は保管料金と別に定めます。削除処理開始後または物理削除後の延長・復元は受け付けません。
4. 契約終了時、保持期限の14日前および3日前を目安に、登録されたテナント管理者と契約連絡先へ削除予定を通知します。契約者は有効な連絡先を維持し、契約終了日と保持期限を自ら管理します。宛先不備、受信拒否、迷惑メール判定その他当社の合理的支配外の理由による未達は保持期限を延長しません。当社システムの障害等により通知できなかった場合も保持期限は自動延長せず、当社が必要と判断した範囲で再通知または短期の削除保留を行えます。

5. 契約者から適法かつ明示的な即時削除依頼がある場合、当社は法定保存、未解決の請求・紛争、セキュリティインシデント、法的保全および未完了のデータ出力を確認したうえで、保持期限の前倒しを審査します。
6. 契約者の法定保存期間を満たす長期アーカイブは標準サービスに含めません。365日を超える原本保管を提供する場合は、保存方法、検索性、改ざん防止、アクセス、料金および削除を定めた別契約または将来の追加機能とします。
7. 当社自身の契約・請求・会計記録、最小限の発行証跡、業務監査ログおよびサポート・インシデント内部記録は、テナントの通常画面から参照できない隔離領域で、それぞれの保持期間に従って保存します。これらは、法令遵守、セキュリティ、サポート、品質改善、SLA検証または紛争対応以外の目的に利用しません。

6. 物理削除手順

1. 保持期限到来後、SaaS管理者が対象を事前検証し、データベース行、S3オブジェクト、関連データのスナップショットとチェックサムを確認します。
2. 物理削除は、異なるSaaS管理者による二者承認を必要とします。
3. 対象差異、未完了のデータ出力、法的保全、処理エラーがある場合は実行を停止します。
4. 削除はテナント範囲で行い、他テナントのデータを対象に含めません。
5. 実行結果、削除件数、オブジェクト数、失敗、再試行を監査し、削除証明書を生成します。
6. 削除証明書はシステムが記録した処理結果を示すものであり、クラウドサービス提供者の物理媒体廃棄証明を代替しません。
7. AWS検証環境で単発削除処理、部分失敗からの再試行、バックアップ復元後の削除状態再適用を受入するまで本番環境での実行を有効化しません。

7. バックアップと版管理

1. 本番環境のPostgreSQLにおける自動バックアップ保持は、現在のCDK設計で7日です。Point-in-Time Recoveryを有効にします。
2. メディア用バケットは版管理を有効にし、旧版を現在のCDK設計で30日後に削除します。
3. 稼働中システムから削除済みのデータが暗号化バックアップまたは旧版に残る場合、通常の保存周期で失効させます。
4. 削除後のバックアップを障害復旧に使用した場合、当社は削除記録を再適用し、削除済みデータが通常利用へ復帰しない手順を運用します。
5. バックアップは通常業務の検索・復元要求に使用せず、災害復旧、整合性確認、法令上必要な場合に限定してアクセスします。
6. スナップショット、ログ、生成物ごとの保持値はAWS検証環境の受入後に確定し、本条件とCDKを一致させます。

8. 例外保持

当社は、次の場合に必要最小限のデータを通常期間を超えて隔離保持できます。

1. 法令により保持が必要な場合。
2. 裁判所、行政機関その他権限ある機関から適法な要請を受けた場合。
3. 未解決の請求、紛争、不正利用またはセキュリティインシデントの証拠保全が必要な場合。
4. 契約者と書面で個別に合意した場合。

例外データは目的外利用せず、アクセスを限定し、理由が終了した後に削除します。

法的保全を設定する場合、対象、理由、承認者、開始日、見直し期限および解除条件を記録します。原則90日ごとに継続要否を確認し、保持理由が終了した場合は速やかに解除して、通常の削除手続へ戻します。

9. 外部サービス上のデータ

1. 契約者がSlack、Google Calendar、外部販路等へ送信したデータは、各サービス提供者の契約と保持・削除条件にも従います。

2. 接続解除時、当社は当社管理下の認証情報を無効化・削除し、可能な場合はサービス提供者へ取消を要求します。提供者側に既に保存されたメッセージ、カレンダー予定、出品情報等は契約者が提供者のサービス上で削除する必要がある場合があります。
3. OpenAIへ送信するAI分析リクエストは`store=false`を指定しますが、提供者による不正利用監視、法令対応その他の保持条件は契約時のDPAで確認します。
4. 電子契約サービス提供者へ送信する申込者情報、契約文書、署名・監査証明および通信情報は、当社の契約証跡保持に加え、当該提供者の契約と保持・削除条件にも従います。提供者、処理国および期間は利用開始前に再委託先一覧へ記載します。

10. 変更と問い合わせ

保持期間の短縮、標準データ出力範囲の縮小その他契約者へ重大な不利益を与える変更は、原則として適用日の30日前までに通知します。法令、セキュリティ、障害回避、外部サービス提供者の仕様変更その他事前通知が合理的に困難な場合は、通知期間を短縮し、または適用後速やかに通知できます。契約者へ重大な不利益を与えない運用・表示・技術上の変更は、事前通知の対象外とします。

- ・ データ出力窓口: support@nidome.jp (2026-08-25に開通・外部往復確認済み)
- ・ 契約終了・削除窓口: support@nidome.jp (2026-08-25に開通・外部往復確認済み)
- ・ プライバシー・法的保全窓口: privacy@nidome.jp (2026-08-25に開通・外部往復確認済み)

以上