DATA SEALED SAFER

サーバ運用マニュアル

2025 年 4 月 1 日

1.0 版

本書の目的

内容

本書は、DATA SEALED SAFER サーバの操作や運用方法内容について説明しています。

前提と対象者

本書は、DATA SEALED SAFER サーバの管理を行う方を対象としております。
また、Windows サーバの基本的な操作方法を習得していることが前提です。

目次

1. 概要

DATA SEALED SAFER は、機密性の高い電子資産を情報セキュリティポリシーに基づき、ファイル単位で保護・管理できる暗号技術を用いた情報セキュリティソリューションです。
DATA SEALED SAFER サーバ、DATA SEALED SAFER マネージャクライアント、DATA SEALED SAFER ユーザクライアントから構成されます。

2. 動作環境

DATA SEALED SAFER の動作環境につきましては、別紙「DATA SEALED SAFER 動作環境.pdf」をご参照ください。

3. サーバサービス

DATA SEALED SAFER サーバは Windows サービスとして登録されているため、OS の起動／停止と連動してサーバの開始／停止が行われます。各サービスを個別に開始／停止する場合を除き、通常の OS メンテナンス操作時に特別な操作は必要ありません。

手動でサーバサービスの操作を行う場合は、以下の手順を参考に実施してください。

3.1 サーバサービスの開始

スタートメニューより「DATA SEALED SAFER」-「開始」をクリックします。

※なお DATA SEALED SAFER サーバを利用する際は PostgreSQL サーバが動作している必要があります。
Windows サービス一覧にて、表示名が「postgresql-x64-16 - PostgreSQL Server 16」となっているサービスの状態が「実行中」となっている事を確認し、停止していた場合は開始してから作業を行ってください。

3.2 サーバサービスの停止

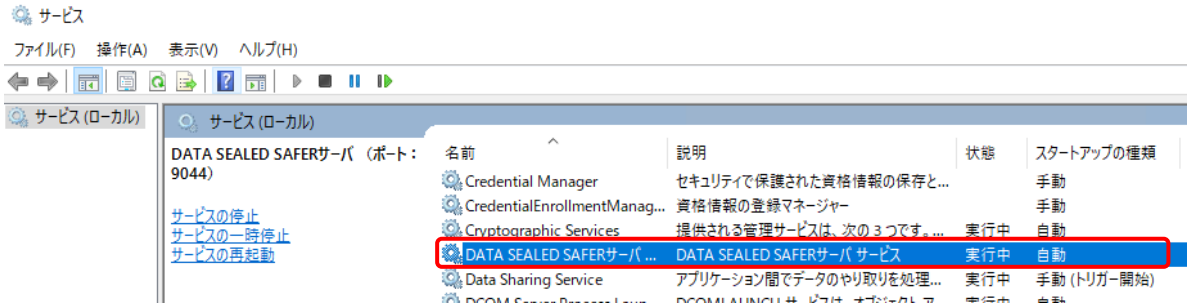
スタートメニューより「DATA SEALED SAFER」-「停止」をクリックします。

3.3 サーバサービスの再起動

スタートメニューより「DATA SEALED SAFER」-「再起動」をクリックします。

3.4 Windows サービスからの操作

Windows のサービス一覧より直接、サービスの操作を行う事も可能です。
その場合、サービス一覧より表示名が「DATA SEALED SAFER サーバ （ポート：9044)」となっているサービスに対して操作を行ってください。



4. ライセンス

DATA SEALED SAFER サーバにご契約のライセンス情報を登録します。

※DATA SEALED SAFER サーバインストール後 30 日以内に以下の作業を完了してください。

4.1 ライセンス入手準備

【C:¥DATA SEALED SAFER¥管理】フォルダ内にあるライセンス発行用ファイル「Register.dat」を santec Japan 株式会社よりインストール URL のご案内として送られているメール「表題；【DATA SEALD SAFER】　インストール URL のご案内 （〇〇〇株式会社 様)」へファイル名を編集せずメールに添付してご返送ください。

4.2 ライセンス登録準備

santec Japan 株式会社よりライセンス登録用ファイル「License.dat」を送付いたします。

C:¥Program Files¥DATA SEALED SAFER¥Server 内に「License.dat」を保存します。

※6.1 ライセンス入手準備の際の「Register.dat」があるフォルダと異なります。

※License.dat の発行には数営業日かかります。

4.3 ライセンス登録の実施

Windows のスタートメニューより「DATA SEALED SAFER」-「ライセンス登録」をクリックします。

コマンドプロンプトが起動し、キー入力を求められますので、「Enter」キーなどを押して処理を続行させます。

4.4 ライセンス確認

Windows のスタートメニューより「DATA SEALED SAFER」-「ライセンス確認」をクリックします。

コマンドプロンプトが起動し、以下のライセンス情報が表示されますので、正しくライセンス情報が反映されている事を確認し、「Enter」キーなどを押して処理を終了します。

・License count　　：ライセンス保有数
・License count in use　　：使用ライセンス数
・License period　　：ライセンス有効期間
・License registration　　：ライセンス認証の状態

5. マネージャクライアント起動

DATA SEALED SAFER マネージャクライアントの起動時には、「C:¥DATA SEALED SAFER¥管理」内の DATA SEALED SAFER 管理者 ID ファイル「Admin.cid」が必要となります。

① **マネージャクライアント起動**

スタートメニューより、「DATA SEALED SAFER」-「マネージャクライアント起動」をクリックします。

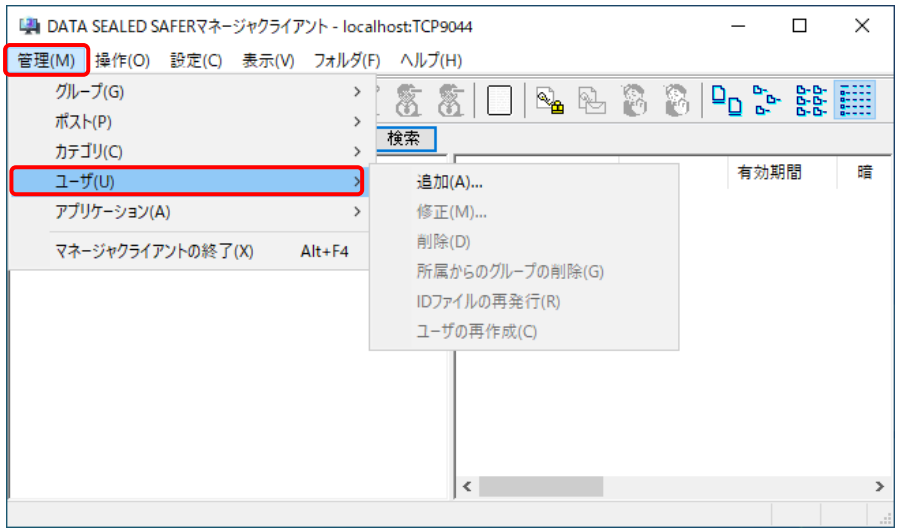
② **「Admin.cid」の指定**

ID ファイルの選択画面が表示されますので、「参照」をクリックし、「C:¥DATA SEALED SAFER¥管理¥Admin.cid」を指定後、インストール時に設定した DATA SEALED SAFER サーバ管理者（Admin.cid）パスワードを入力し、「OK」をクリックします。

(サーバセットアップ手順書 P6～8 参照)

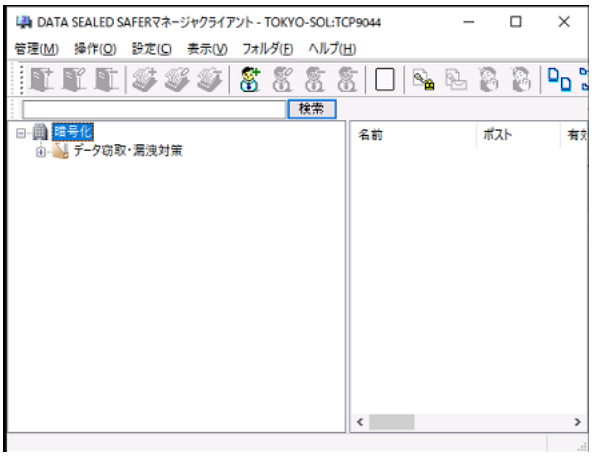
6. ユーザ設定

ユーザに関連する各操作は、「管理」-「ユーザ」をクリックして表示されるメニューより行います。



メニュー	内容
追加	予め新規ユーザを所属させたいグループを選択してからメニュー操作を行う事により、新規ユーザの追加画面を表示します。
修正	予め修正対象のユーザを選択してからメニュー操作を行う事により、対象ユーザの修正画面を表示します。
ID ファイルの再発行	予め ID ファイル再発行対象のユーザを選択してからメニュー操作を行う事により、対象ユーザの ID ファイルを再発行します。
ユーザの再作成	予め再作成対象のユーザを選択してからメニュー操作を行う事により、対象ユーザを再作成します。

「暗号化」グループが選択され青くなっていることをご確認ください。
なお、グループの追加は出来ません。



6.1 ユーザの追加

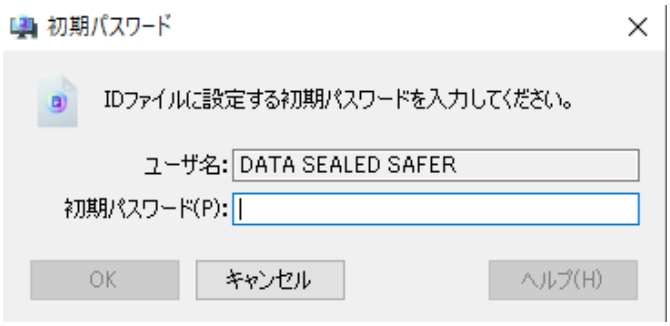
暗号化ファイルを扱う利用者を登録します。

ユーザの追加は、「管理」-「ユーザ」-「追加」のメニュー操作の他、「暗号化」グループを右クリックして表示される「新規ユーザを追加」、あるいは「ユーザの追加」アイコンからも行う事が出来ます。

新規ユーザ追加時は、以下の画面が表示されますので、以下の項目を任意の設定し、「OK」 をクリックします。

項目名	設定内容
ユーザ名	必須設定項目です。 任意のユーザ名を指定します。
ユーザ ID	ユーザの追加後、DATA SEALED SAFER が固有に採番するユーザのコードが自動登録されます。入力を行う必要はなく、表示された内容を変更する事もできません。
有効期間	対象ユーザに有効期間を設けたい場合に設定します。 デフォルトでは期間の制限なく利用可能である「無期限」が設定されています。 操作の詳細については、「6.6 有効期間の予約機能」をご参照ください。

なお、ユーザ追加時にパスワードの設定を行いたい場合は、ユーザ追加作業の前に「6.7 ID ファイルの初期パスワードの設定」を参照し設定を行ってください。新規ユーザ追加の際に以下の画面が表示されますので、パスワードポリシーに準じた任意のパスワードを設定して「OK」をクリックします。



パスワードポリシーについては、「10.5 パスワードポリシー」をご参照ください。
パスワードポリシーから外れるパスワードを設定した場合は、以下のメッセージが表示され、ユーザは作成されますが、ID ファイルは生成されません。

この場合「OK」をクリックして処理を終了し、別途「6.4 ID ファイルの再発行」の操作を行い、ID ファイルを発行してください。

ID ファイルの初期パスワード設定を行っていない場合は、パスワードが何も設定されていない状態で ID ファイルが生成されます。

6.2 ユーザの修正

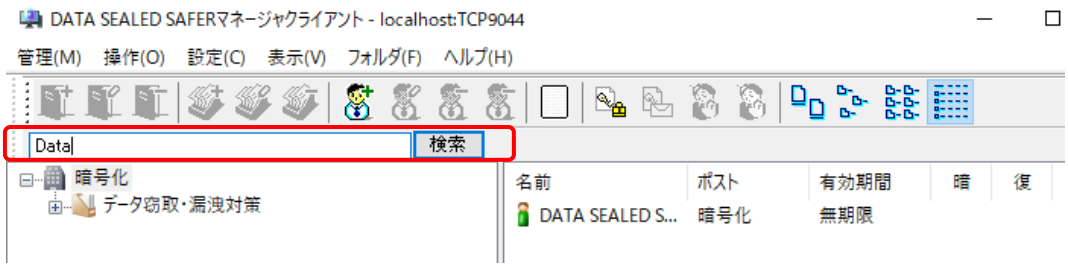
作成したユーザの設定内容を変更したい場合、ユーザの修正を行う事が可能です。

ユーザの修正は、対象のユーザを選択した上で「管理」-「ユーザ」-「修正」のメニュー操作の他、対象ユーザを選択して右クリックで表示される「このユーザを修正」からも行う事が可能です。

ユーザ修正時は、修正対象として選択したユーザの修正画面が表示されます。
修正したい項目を追加時と同様に任意の修正し、「OK」をクリックします。

6.3 ユーザの検索

マネージャクライアントのツールバーの検索窓より、登録済みのユーザを検索することができます。検索したい文字をフィールドに入力し「検索」ボタンをクリックするか「Enter」キーを押すと、検索条件にヒットしたユーザが表示されます。



検索結果をクリアするには、フィールドを空にして「検索」ボタンをクリックするか「Enter」キーを押します。

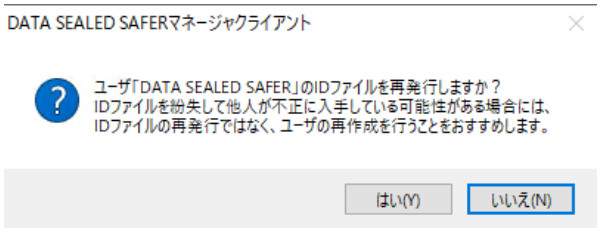
6.4 ID ファイルの再発行

配布した ID ファイルをユーザが紛失、或いは破損やパスワードを忘れた場合など、ユーザの ID ファイルを再発行する事が可能です。

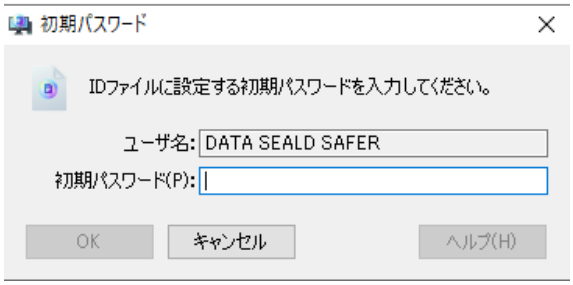
ID ファイルの再発行は、対象のユーザを選択した上で「管理」-「ユーザ」-「ID ファイルの再発行」のメニュー操作の他、対象ユーザを選択して右クリックで表示される「ID ファイルを再発行」からも行う事が可能です。

なお、ID ファイルの紛失時に他者が ID ファイルを取得して利用されるおそれがある場合は、状況に応じて「6.5 ユーザの再作成」を参考にユーザを再作成してご利用になる事をお勧め致します。

ID ファイル再発行操作時は以下の画面が表示されますので、対象のユーザ名が表示されている事を確認し、問題無ければ「はい」をクリックします。



なお、ID ファイル再発行操作の前に予め ID ファイルの初期パスワードの設定を行っていた場合、以下の画面が表示されますので、パスワードポリシーに準じた任意のパスワードを設定して「OK」をクリックします。



パスワードポリシーについては、「10.5 パスワードポリシー」をご参照ください。

パスワードポリシーから外れるパスワードを設定した場合は、以下のメッセージが表示され、ユーザは作成されますが、ID ファイルは生成されません。

この場合「OK」をクリックして処理を終了し、再度 ID ファイルの再発行操作を行い、パスワードポリシーに則ったパスワードを付与してください。

ID ファイルの初期パスワード設定を行っていない場合は、パスワードが何も設定されていない状態で ID ファイルが生成されます。

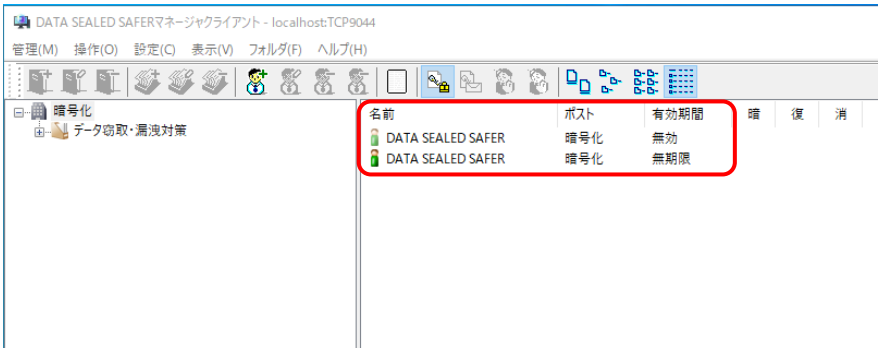
6.5 ユーザの再作成

配布した ID ファイルをユーザが紛失したなど、他者が ID ファイルを取得して利用されるおそれがある場合は、状況に応じてユーザの再作成を行います。

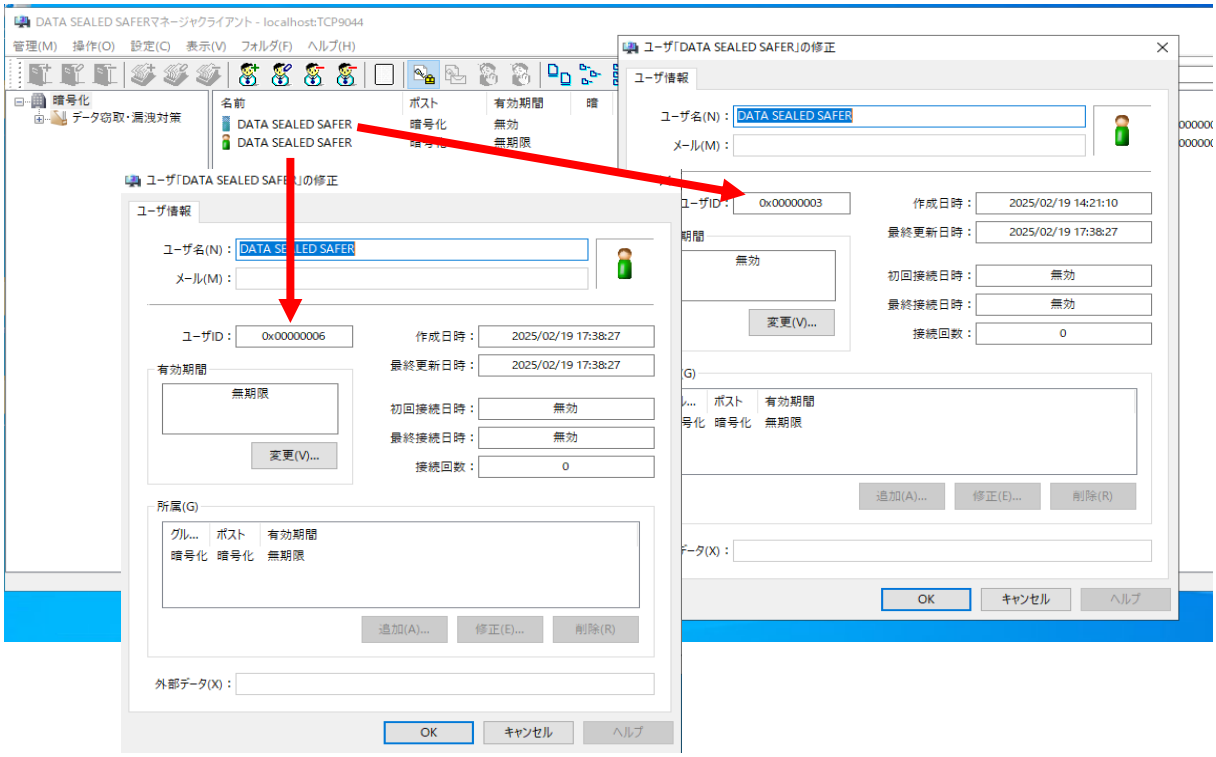
ユーザの再作成は、対象のユーザを選択した上で「管理」-「ユーザ」-「ユーザの再作成」のメニュー操作の他、対象ユーザを選択して右クリックで表示される「ユーザの再作成」からも行う事が可能です。
なお、ユーザの再作成では元のユーザが無効化され、同名のユーザが新しく作成されます。
無効化された元のユーザは削除できませんが、ライセンス数のカウント対象外となります。
また、ユーザが無効化前に暗号化したファイルは、無効化後も他ユーザは復号化が可能です。

ユーザの再作成操作時は以下の画面が表示されますので、対象のユーザ名が表示されている事を確認し、問題無ければ「はい」をクリックし、続けて表示される画面も内容を確認し、「OK」をクリックします。

元のユーザは無効化されグレーアウトして表示され、新たに作成した同名のユーザが有効なユーザとして作成されます。

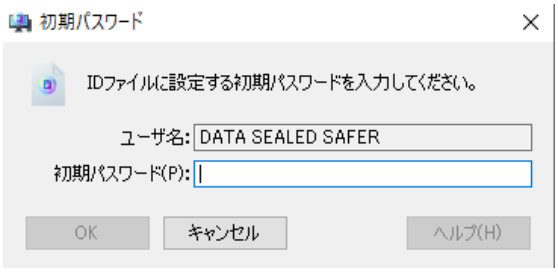


無効化されたユーザと新規作成されたユーザは、ユーザ名は同じとなりますが、DATA SEALED SAFER 固有のユーザ ID が異なります。



なお、ユーザの再作成時に同時に ID ファイルも生成されますが、無効化された元のユーザの発行済み ID ファイルは自動で削除されません。
ID ファイル名の先頭 8 桁に、上図例「ユーザ ID」欄の 3～10 桁と同じコードが付与されますので、配布時に混乱しないよう、無効化して不要となった ID ファイルは、必ず手動で削除してください。

また、ユーザ再作成操作の前に予め ID ファイルの初期パスワードの設定を行っていた場合、以下の画面が表示されますので、DATA SEALED SAFER サーバにて設定したパスワードポリシーに準じたパスワードを設定し、「OK」をクリックします。



パスワードポリシーについては、「10.5 パスワードポリシー」をご参照ください。
パスワードポリシーから外れるパスワードを設定した場合は、以下のメッセージが表示され、ユーザは作成されますが、ID ファイルは生成されません。

この場合「OK」をクリックして処理を終了し、別途「6.4 ID ファイルの再発行」の操作を行い、ID ファイルを発行してください。

ID ファイルの初期パスワード設定を行っていない場合は、パスワードが何も設定されていない状態で ID ファイルが生成されます。

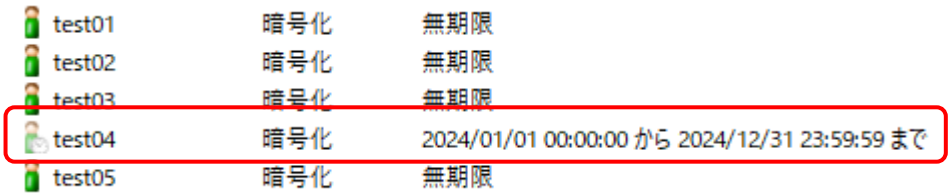
6.6 有効期間の予約機能

ユーザ権限は、ユーザ設定画面にてその有効期間を設ける事ができます。

具体例として、以下のケースで有効期間を設定する事により、対象期間外の DATA SEALED SAFER ユーザクライアントの利用制限を行う事ができます。

ケース	設定内容	動作
入社予定	ユーザ有効期間の「開始日時」を指定。	指定日まで DATA SEALED SAFER ユーザクライアントは使用不可。
退職予定	ユーザ有効期間の「終了日時」を指定。	指定日以降、DATA SEALED SAFER ユーザクライアントは使用不可。

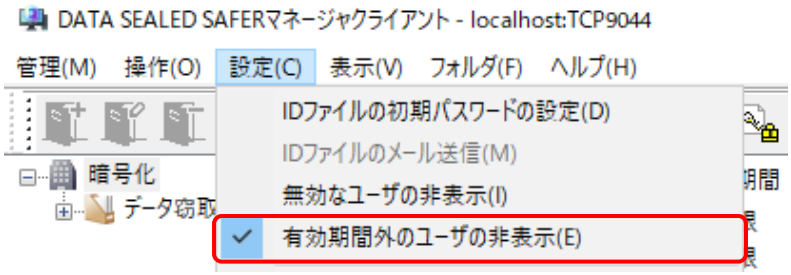
有効期間が設定されたユーザは設定した有効期間の範囲外の場合、時計のマーク付きでグレーアウトして表示されます。



該当ユーザは ID ファイルを使って DATA SEALED SAFER ユーザクライアントを起動する事はできますが、暗号化ファイルの閲覧や更新、削除といった操作や、平文ファイルの暗号化や暗号化ファイルの復号といった、暗号化ファイルの操作が全て拒否されます。

なお対象期間外としてグレーアウトされたユーザも有効なユーザと同列で、ユーザリストに表示され、ライセンスを消費します。
不要となったユーザは無効にしていただくことでライセンスのカウント対象外となります。
ユーザの無効化については「6.9 ユーザの無効化」を参照してください。

有効なユーザだけを表示させたい場合は、「設定」-「有効期間外のユーザの非表示」にチェックを入れ、表示設定を変更してください。



ユーザの有効期間の設定方法は、以下の通りです。

■ ユーザの有効期間

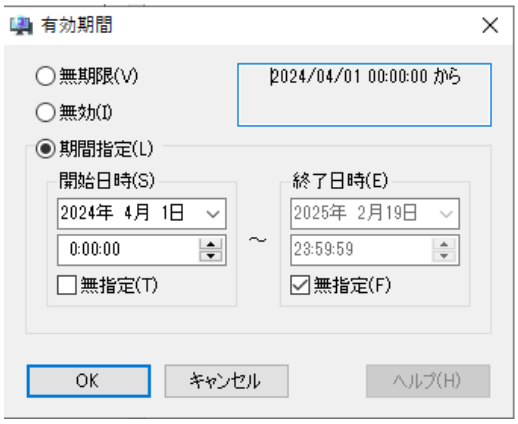
対象ユーザの利用に有効期間を設けたい場合、ユーザ設定画面中、「有効期間」欄の「変更」をクリックします。

有効期間設定画面が表示されますので、ラジオボタンにて「期間指定」を選択し、開始日時と終了日時を指定して「OK」をクリックして有効期間を設定します。

開始日時及び終了日時の下部にある「無指定」チェックボックスにチェックを入れると、該当日時の指定が外れます。

開始日時だけを指定したい場合は、「開始日時」欄のみ日時を指定し、終了日時では「無指定」をチェックします。なお開始日時と終了日時の両方で「無指定」を設定した場合は、「無期限」と同等の設定となります。

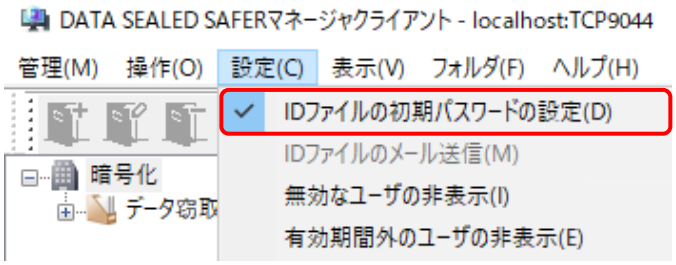
(例) 2024 年 4 月 1 日から利用を開始させる場合



6.7 ID ファイルの初期パスワードの設定

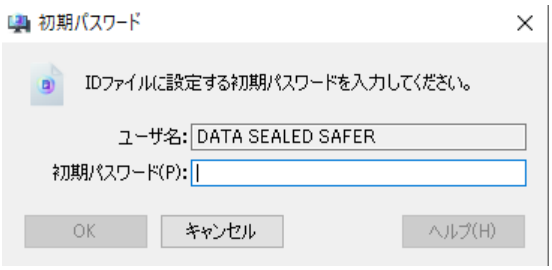
ユーザの作成や再作成、ID ファイルの再発行時など、デフォルトでは ID ファイルの初期パスワードは空の状態で発行されますが、予め DATA SEALED SAFER マネージャクライアントの設定を有効化しておく事で、初期パスワードを設定した状態で ID ファイルを発行する事ができます。

ID ファイルの初期パスワード設定は、「設定」-「ID ファイルの初期パスワードの設定」にチェックを入れる事で有効化されます。



「ID ファイルの初期パスワードの設定」文字部分をクリックするとメニュー表示が消えますが、チェックがされていなかった場合はチェックされ、チェックされていた場合はチェックが外れる動作をします。

ID ファイルの初期パスワード設定が有効となっている場合、ユーザの追加や ID ファイルの再発行時など ID ファイルが発行されるタイミングで、下例の初期パスワード入力画面が表示されます。パスワードポリシーに準拠するパスワードを任意の入力し、「OK」をクリックして ID ファイルを発行してください。

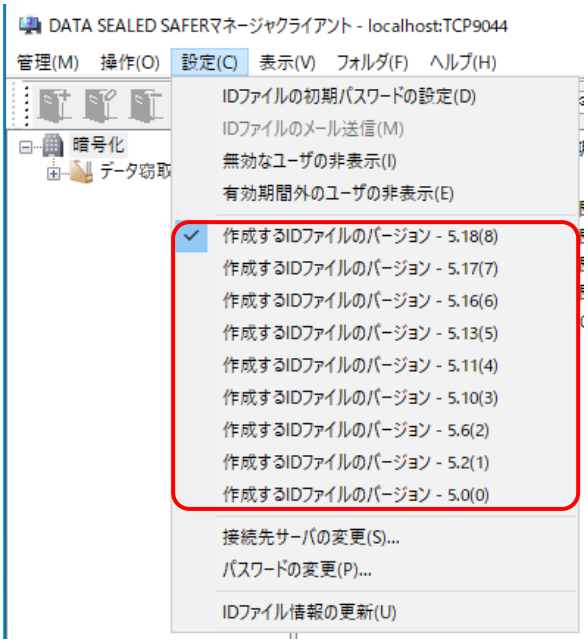


パスワードポリシーについては、「10.5 パスワードポリシー」をご参照ください。

6.8 ID ファイルのバージョン設定

発行する ID ファイルのバージョン設定は、DATA SEALED SAFER マネージャクライアント画面のメニュー「設定」で表示される、作成可能な ID ファイルバージョンのリストより、作成対象のバージョンにチェックを入れる事で有効化されます。

ID ファイルのバージョンは 5.18 を指定してください。



6.9 ユーザの無効化

DATA SEALED SAFER ではユーザの削除は行えません、そのため、退職者など一度でも ID ファイルを配布または使用した事のあるユーザを失効させる場合は、ユーザの無効化を行います。

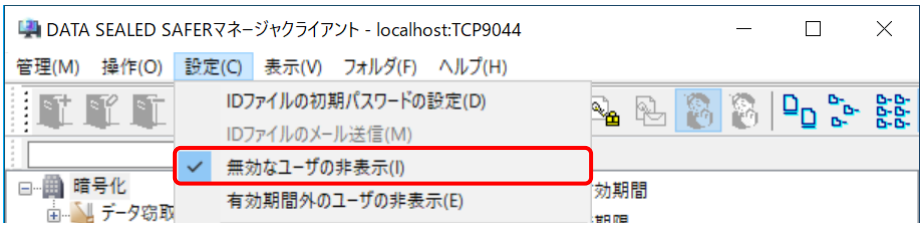
無効化されたユーザは、ID ファイルを使って DATA SEALED SAFER ユーザクライアントの起動は行えますが、暗号化ファイルの閲覧や更新、削除といった操作や、平文ファイルの暗号化や暗号化ファイルの復号といった、暗号化ファイルの操作が全て拒否されます。

ユーザの無効化設定は、ユーザの修正時に表示される画面の「ユーザ情報」タブ内、「有効期間」欄の「変更」をクリックして表示される有効期間設定画面より行うか、ユーザを右クリックし「この宇 yー座を無効化(I)」をクリックします。

対象のユーザは無効化され、ユーザアイコンもグレーアウトした状態で表示されます。

有効期間が「無効」と設定されたユーザは、ライセンス数のカウント対象外です。

また、グレーアウトされた「無効なユーザ」も有効なユーザと同列で、ユーザリストに表示されます。
有効なユーザだけを表示させたい場合は、「設定」-「無効なユーザの非表示」にチェックを入れ、表示設定を変更してください。



「無効なユーザの非表示」文字部分をクリックするとメニュー表示が消えますが、チェックがされていなかった場合はチェックされ、チェックされていた場合はチェックが外れる動作をします。

6.10 無効化したユーザの再有効化

無効化したユーザを有効にする場合は、ユーザの修正時に表示される画面の「ユーザ情報」タブ内、「有効期間」欄の「変更」をクリックして表示される有効期間設定画面より行います。

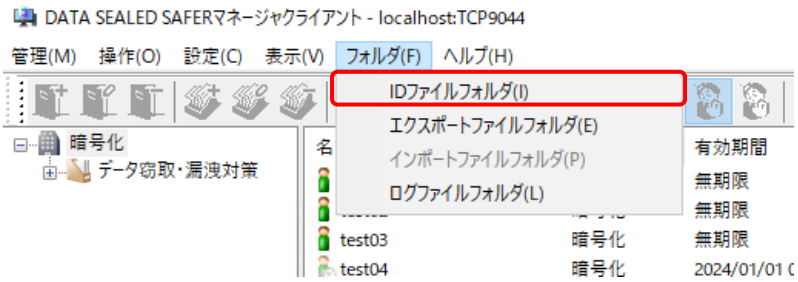
有効期間を「無期限」または有効な日付を指定して「OK」をクリックする事で、対象のユーザは有効化され、ユーザアイコンもグレーアウトから通常の表示に戻ります。

6.11 生成した ID ファイルの格納場所

ユーザ追加や再作成、また ID ファイルの再発行時に生成された ID ファイルは、以下のフォルダに格納されます。

C:¥Users¥<ログオンユーザ名>¥AppData¥Local¥DATA SEALED SAFER¥ManagerClient¥Idfile

上記の ID ファイル格納フォルダはエクスプローラより開く他、DATA SEALED SAFER マネージャクライアントの「フォルダ」-「ID ファイルフォルダ」から直接開く事も可能です。



生成された ID ファイルを各ユーザへ配布してください。

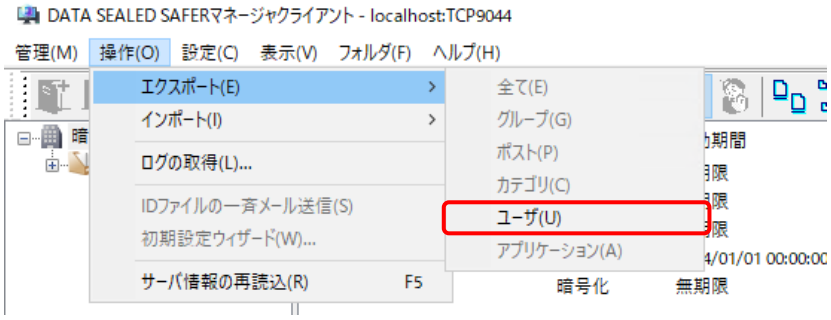
7. ユーザ情報のエクスポート

ユーザ情報は CSV ファイルでのエクスポートを行う事ができます。
なお、エクスポートした設定ファイルは UTF-8 の文字コードで作成されていますので、Microsoft Excel などで参照する場合は、一旦メモ帳などのテキストエディタより開き、Shift-JIS などの文字コードに変換して保存し直してから参照して下さい。

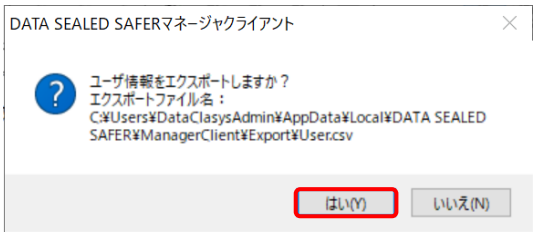
エクスポートされるファイル名は、以下となります。

設定対象の名称	ファイル名
ユーザ	User.csv

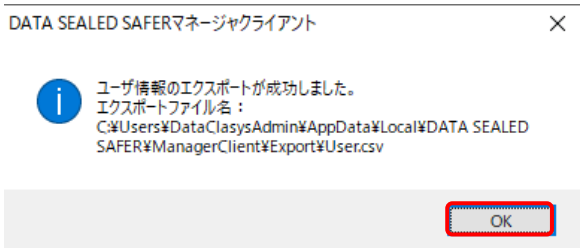
エクスポートする際は、「操作」-「エクスポート」をクリックし、「ユーザ」をクリックします。



エクスポートする設定の確認画面が表示されますので、「はい」をクリックし処理を開始します。



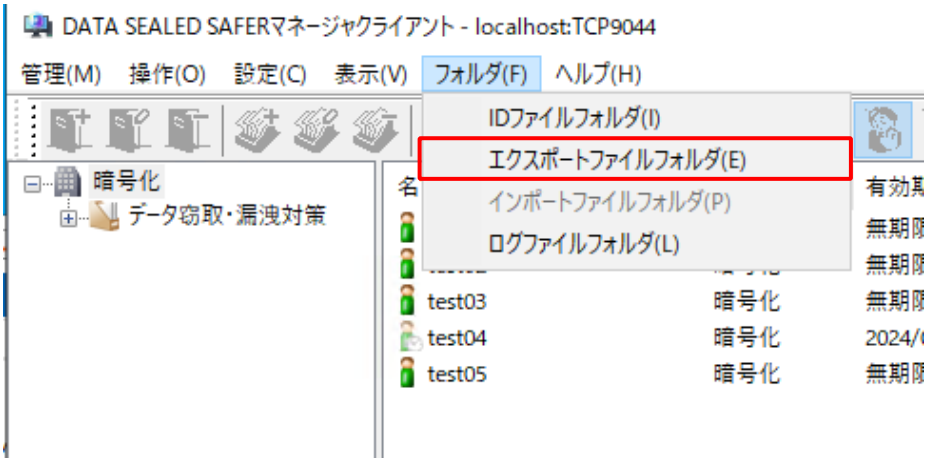
エクスポート処理は、書き出す情報の件数によっては完了までに時間がかかる場合がありますので、その場合は次のメッセージが表示されるまでしばらく待機してください。
エクスポート処理が完了すると、下例の画面が表示されますので、「OK」をクリックして処理を終了します。



エクスポートされた CSV ファイルは、DATA SEALED SAFER マネージャクライアントを実行中のユーザプロファイルの以下フォルダに出力されます。

C:¥Users¥<ログオンユーザ名>¥AppData¥Local¥DATA SEALED SAFER¥ManagerClient¥Export

上記フォルダは DATA SEALED SAFER マネージャクライアントの「フォルダ」-「エクスポートファイルフォルダ」から開く事が可能です。



フォルダ内には、エクスポートした設定名で以下拡張子のファイルが出力されます。

拡張子	説明
.csv	設定ファイル本体です。
.csv.err	エクスポート処理でエラーが発生した際に、内容が記録されるファイルです。 何もエラーが無くても処理時に必ず出力されるファイルとなり、エラーの無い場合は 0KB、エラーがあった場合はそれ以上のサイズでファイルが作成されます。
.csv.old	「.csv」が既に存在する状態でエクスポート処理を行った場合、予め出力されていた「.csv」の拡張子のファイルは本拡張子に変更され、新たに出力された設定ファイルが「.csv」として保存されます。

出力された csv ファイルでは、各ユーザ名と有効期限を確認することができます。

M,0x00000003,"DATA SEALED SAFER","","",INVALID|INFINITE,".....

ID　　ユーザ名　　有効期限（※）

※有効期限は「開始日時 | 終了日時」が記載され以下の意味となります。

有効期限	開始日時|終了日時
無期限	INVALID|INFINITE
無効	INFINITE|INVALID
期間指定	YYYY/MM/DD hh:mm:ss|YYYY/MM/DD hh:mm:ss

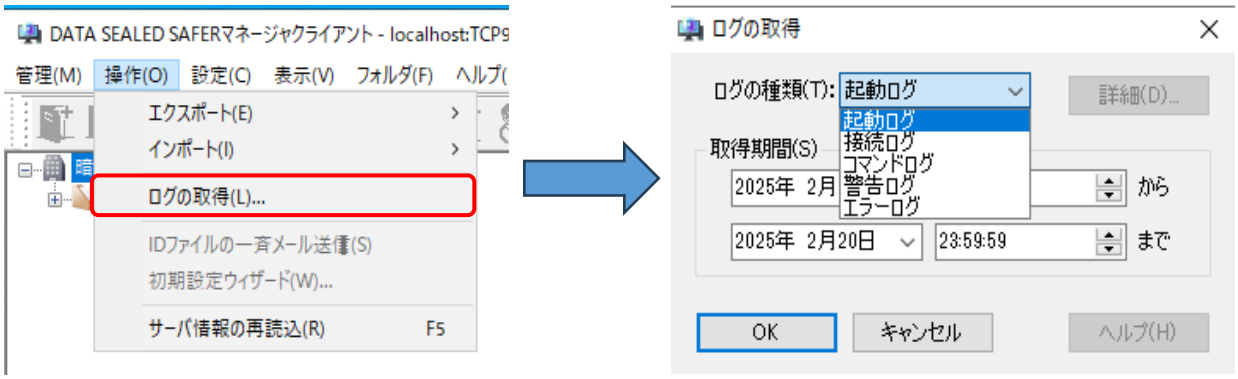
8. ログの取得

DATA SEALED SAFER サーバは以下のログを収集し過去 1 年分をログデータベースに保存しています。
月次のメンテナンス処理により、1 年以上前のログは削除されます。
メンテナンス処理については「9 定期処理」を参照してください。

ログ名称	内容
起動ログ (Administration)	DATA SEALED SAFER サーバの起動及び終了のログ
接続ログ (Connection)	DATA SEALED SAFER ユーザクライアント、DATA SEALED SAFER マネージャクライアントの DATA SEALED SAFER サーバへの接続のログ
コマンドログ (Command)	DATA SEALED SAFER ユーザクライアント、DATA SEALED SAFER マネージャクライアントの操作のログ
警告ログ (Warning)	DATA SEALED SAFER の運用中に生じた、ID ファイルの複製使用や端末固定情報の変更など、セキュリティ上注意が必要な事象のログ
エラーログ (Error)	DATA SEALED SAFER サーバで発生したエラーのログ

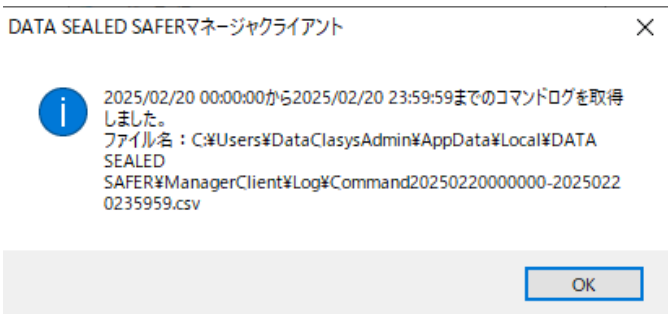
(カッコ内の名称は、ログ取得時に出力されるファイル名称です。)

これらのログを参照する際は一旦ファイルとしてログを取得する必要があります。
ログの取得を行う際は、「操作」-「ログの取得」をクリックし、表示されるログの取得画面より、以下を指定して「OK」をクリックします。

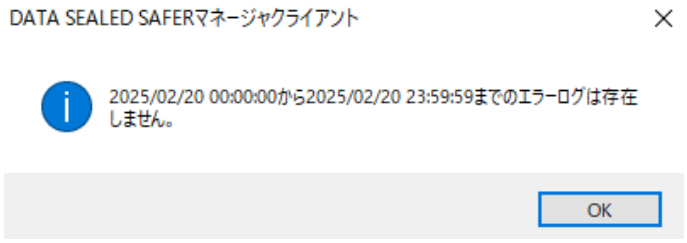


項目	操作内容
ログの種類	リストより、取得対象のログの種類を指定します。
取得期間	取得するログファイルに含める、ログの期間を指定します。 ご利用の設定や暗号化ファイルの利用頻度などで、ログファイルのサイズが大きくなる場合がありますので、あまり長い期間を指定しないようご注意ください。

ログの取得が完了すると、下例のメッセージが表示されますので、「OK」をクリックします。
取得するログの量が多い場合は、完了するまで時間がかかる場合がありますので、その際は下例のメッセージが表示されるまで待機してください。



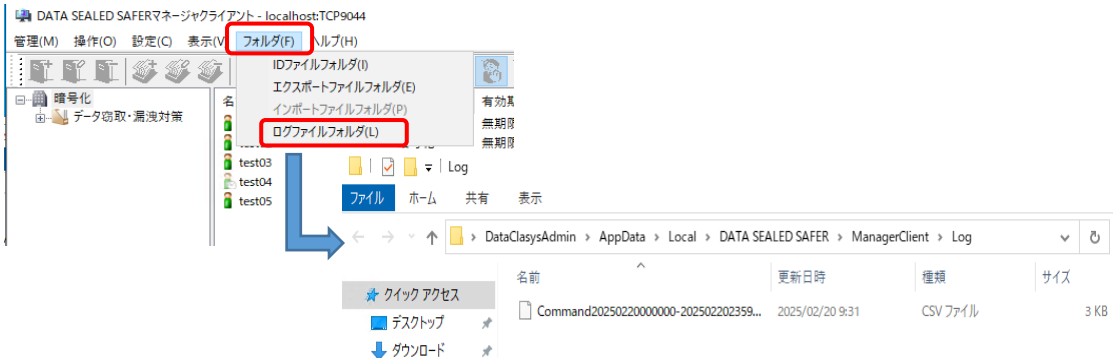
指定した取得期間に該当のログが存在しない場合は下例のメッセージが表示され、ログの取得はできません。



取得したログファイルは、DATA SEALED SAFER マネージャクライアントを実行中のユーザプロファイルに存在する、以下フォルダに出力されます。

C:¥Users¥<ログオンユーザ名>¥AppData¥Local¥DATA SEALED SAFER¥ManagerClient¥Log

上記フォルダは DATA SEALED SAFER マネージャクライアントのメニューより「フォルダ」-「ログファイルフォルダ」をクリックする事で簡単に開く事が可能です。



フォルダ内にはログ名称と取得期間を組み合わせたファイル名で、取得したログが出力されます。
上図の例では、「Command20250220000000-20250220235959.csv」となっており、「2025 年 2 月 20 日 0 時 0 分 0 秒から同日 23 時 59 分 59 秒までのコマンドログ」が出力されています。

なおログファイルは、UTF-8 の文字コードで作成されていますので、Microsoft Excel などで参照する場合は、一旦メモ帳などのテキストエディタより開き、Shift-JIS などの文字コードに変換して保存し直してから参照してください。

各ログの書式詳細については、別紙「DATA SEALED SAFER LogFormat.html」をご参照ください。

9. 定期処理

9.1 データベース運用保守の概要

(1) データベース構成

DATA SEALED SAFER サーバは PostgreSQL 上の以下の 2 つのデータベースにて情報管理をしています。

■ 鍵データベース（データベース名：clasyskey）

DATA SEALED SAFER の暗号化鍵や登録したユーザ情報を管理しています。

■ ログデータベース（データベース名：clasyslog）

DATA SEALED SAFER サーバの動作ログが蓄積されています。ログの種類は、以下の 5 つです。

種類	説明
起動ログ	DATA SEALED SAFER サーバの起動、終了ログ
接続ログ	DATA SEALED SAFER ユーザクライアント、マネージャクライアントの DATA SEALED SAFER サーバへの接続ログ
コマンドログ	DATA SEALED SAFER ユーザクライアント、マネージャクライアントの操作ログ
警告ログ	DATA SEALED SAFER の運用中に発生したセキュリティ上のエラーログ
エラーログ	DATA SEALED SAFER サーバのエラーログ

(2) データベース運用保守

DATA SEALED SAFER を安全に運用するには以下の定期処理を行う必要があります。

・鍵データベースのバックアップ

・ログデータベースの古い情報の削除処理

DATA SEALED SAFER の運用において、サーバ故障などによる再構築を行う際や設定を誤った際などでロールバックする必要がある場合、データベースのバックアップを使用します。DATA SEALED SAFER の設定をバックアップ時点に戻す場合は、過去の鍵データベースのバックアップファイルから手動でリストアを行い、データベースを元に戻します。

そのため、DATA SEALED SAFER サーバのセットアップ時や DATA SEALED SAFER サーバへユーザ追加を行った際は鍵データベースのバックアップを実施し、バックアップファイルは必ず外部媒体に退避してください。

9.2 定期処理によるデータベース自動メンテナンス

別紙「DATA SEALED SAFER サーバ構築手順書.pdf」-「2.3 定期処理登録」の実施によって、「タスクスケジューラ」の「DATA SEALED SAFER」フォルダに「MainServerTask」タスクと「LogRotateTask」タスクの二つが設定されます。

(1) 鍵データベースダンプ定期出力タスク

DATA SEALED SAFER サーバの鍵データベースのダンプ出力は「MainServerTask」タスクによって以下の内容で定期実行されます。

項目	内容
実行日時	毎日 1 時
出力フォルダ	C:¥DATA SEALED SAFER¥key-dump
出力ファイル名	key-dumpYYYYMMDD.sql （YYYYMMDD は年月日の 8 桁の数字）
保持する世代数	5 世代

エクスポートされたファイルは外部媒体にバックアップとして必ず退避してください。

(2) ログデータベース定期ローテーションタスク

DATA SEALED SAFER サーバのログデータベースの削除処理は「LogRotateTask」タスクによって以下の内容で定期実行されます。

項目	内容
実行日時	毎月 1 日 1 時 30 分
削除対象ログ	直近 12 ヶ月より古いログ

9.3 手動操作でのメンテナンス作業

(1) 定期処理の手動実行

メインサーバのバックアップなど、通常は定期的に行っている処理を即時に行う場合は、タスクスケジューラより手動実行をします。
出力されたファイルは外部媒体にバックアップとして必ず退避してください。

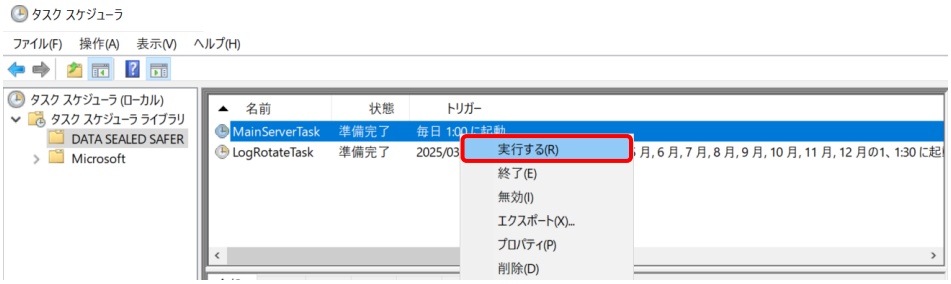
※それぞれの処理実行時、実行サーバの DATA SEALED SAFER サーバサービスが一時的に停止しますので、実行タイミングにご注意ください。

例として「MainServerTask」を手動実行する手順を以下に記載します。

■MainServerTask の手動実行手順

① タスクの手動実行

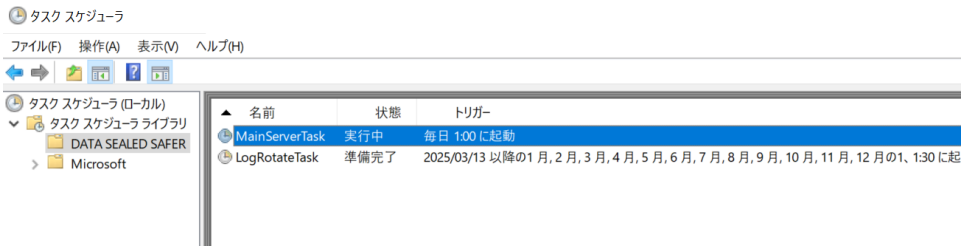
タスクスケジューラを開き「MainServerTask」を選択し、「実行する」をクリックします。



② タスクの実行確認

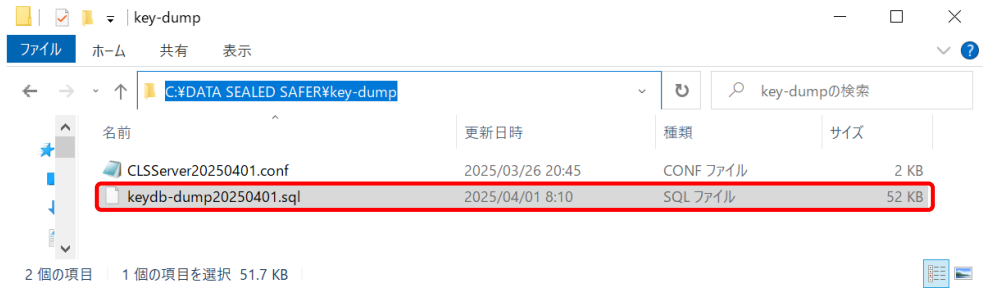
タスク処理中はタスクスケジューラの「状態」が「実行中」となりますので
タスク処理が完了し、「状態」が「準備完了」に更新される事を確認します。

※処理完了後もタスクスケジューラの表示に反映されるまで時間がかかる場合がありますので、その際は一度タスクスケジューラを再起動いただき、再度ご確認ください。



③ バックアップファイルの出力確認

タスク処理が完了後、バックアップファイルの出力先フォルダの“C:¥DATA SEALED SAFER¥key-dump”フォルダを開き、ファイル名末尾がタスク実行日の拡張子「.sql」ファイルが出力されていることを確認します。



※バックアップファイルが出力されていない場合は、再度①から手順を実施いただきそれでもファイルが出力されていない場合はサポート窓口にお問い合わせください。

(2) データベースの手動リストア

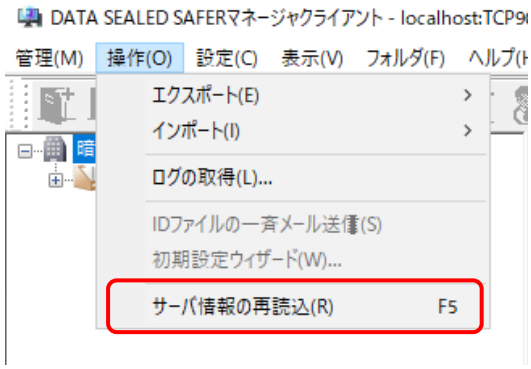
ハードウェアや OS、PostgreSQL の障害により DATA SEALED SAFER が起動できなくなった場合や、誤設定の復旧を行いたい場合などに、過去の DATA SEALED SAFER サーバのバックアップファイルをリストアすることで、現在のデータベースやテーブル内容を破棄し、バックアップ時の状態に戻すことができます。

詳細は別紙「DATA SEALED SAFER サーバ復旧手順書.pdf」をご参照ください。

10. その他

10.1 サーバ情報の再読み込み

DATA SEALED SAFER マネージャクライアントの画面表示は、リアルタイムでの更新は行われません。
ユーザに対して行った設定の画面表示に時間を要している場合は、「操作」-「サーバ情報の再読込」をクリックし、DATA SEALED SAFER サーバの最新情報へ更新してから、DATA SEALED SAFER マネージャクライアントでの操作を行ってください。

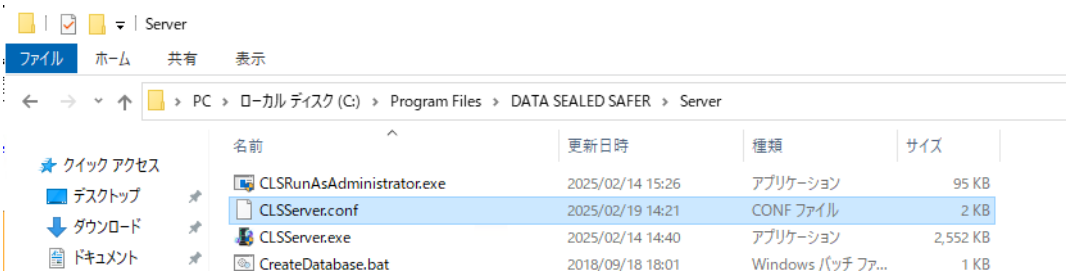


10.2 接続先サーバの変更

DATA SEALED SAFER サーバの IP アドレスの変更により接続先情報が変更された場合、サーバ設定情報、マネージャクライアントを起動するアドミニストレータ用 ID ファイル「Admin.cid」の接続先サーバ設定、ユーザの ID ファイルの接続先サーバ設定をそれぞれ変更する必要があります。

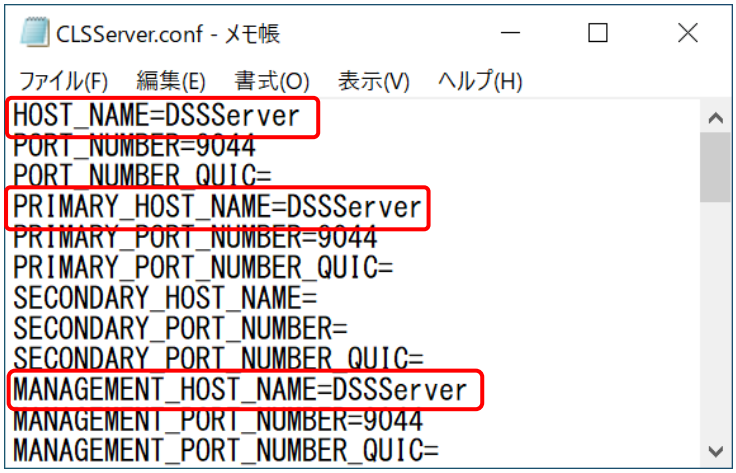
① サーバ設定情報変更

“C:¥Program Files¥DATA SEALED SAFER¥Server”フォルダ内の「CLSServer.conf」をデスクトップなど、任意の場所にコピーします。



「CLSServer.conf」をメモ帳で開き、以下のパラメータを修正します。

・「HOST_NAME」
・「PRIMARY_HOST_NAME」
・「MANAGEMENT_HOST_NAME」



各パラメータは IP アドレスを指定します。

修正が完了しましたら、「CLSServer.conf」を”C:¥Program Files¥DATA SEALED SAFER¥Server”フォルダに配置してください。

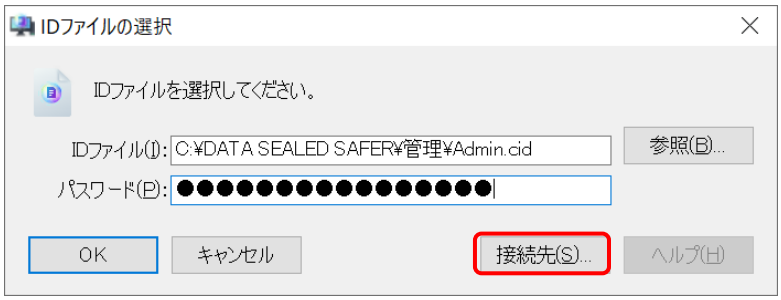
② サーバサービスの再起動

設定を反映させるため、スタートメニューより「DATA SEALED SAFER」-「再起動」を実行ください。

以上でサーバ側の設定は完了です。

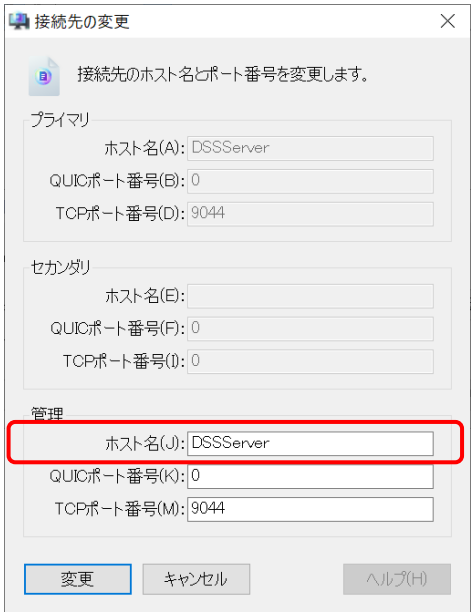
③ 「Admin.cid」の接続先サーバ設定変更

接続先サーバの変更操作は、DATA SEALED SAFER マネージャクライアントを起動し、ID ファイルの選択画面にてログオンする ID ファイルの指定及び、その ID ファイルのパスワードを入力した上で、「接続先」をクリックして表示される接続先の変更画面より行います。



接続先の変更画面では、「管理」欄に指定されている「ホスト名」を新しい接続先 DATA SEALED SAFER サーバの IP アドレスへと変更し、「変更」をクリックします。

特に確認のメッセージなどは表示されませんので、ID ファイル選択画面に戻った後、そのまま「OK」をクリックし、接続先変更した DATA SEALED SAFER サーバに接続できる事をご確認ください。

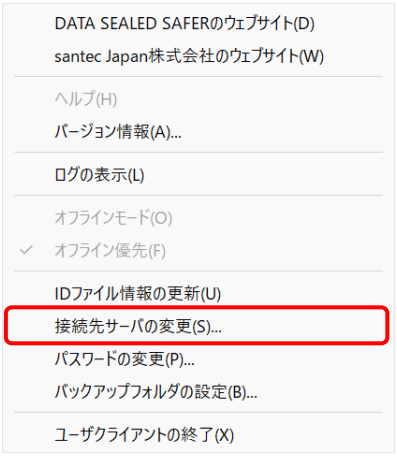


④ ユーザの ID ファイルの接続先変更

DATA SEALED SAFER ID ファイルには、DATA SEALED SAFER サーバへの接続情報が格納されています。

DATA SEALED SAFER サーバの IP アドレスに変更があった場合などは、接続設定の変更が必要になります。

接続先サーバの変更は、DATA SEALED SAFER ユーザクライアントのタスクトレイアイコメニューより表示される画面で行います。



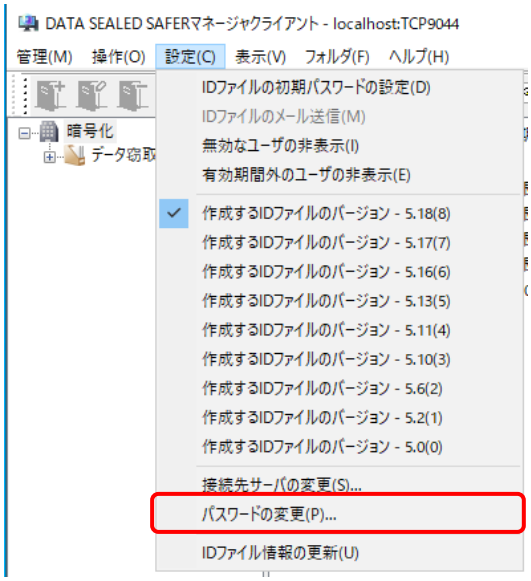
この画面では、プライマリ DATA SEALED SAFER サーバへ接続時に使用する IP アドレスの指定ができます。

それぞれ適切な情報を指定し、「変更」をクリックして操作を終了してください。

「管理」欄の情報は、「プライマリ」欄で指定した DATA SEALED SAFER サーバに接続時、接続先 DATA SEALED SAFER サーバで設定されている内容を自動で取得します。

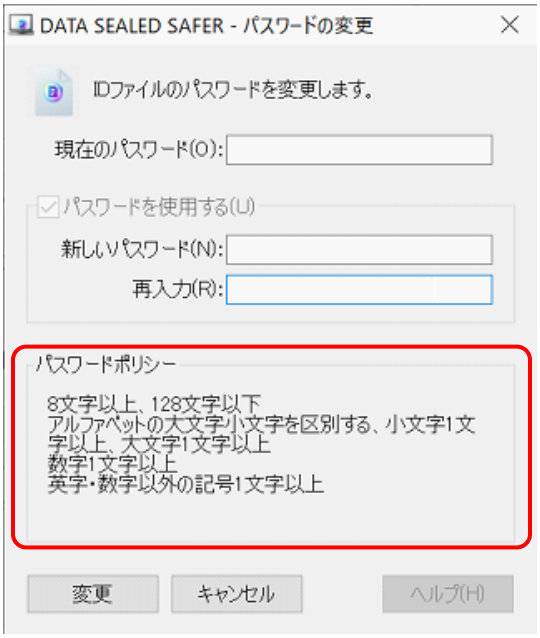
10.3 管理者 ID ファイルのパスワード変更

DATA SEALED SAFER マネージャクライアントを起動している管理者 ID ファイルのパスワード変更は、「設定」-「パスワードの変更」より行います。



パスワードの変更画面が表示されますので、現在のパスワード及び、新しいパスワードを入力して「変更」をクリックします。

パスワードポリシーに準じた任意のパスワードを設定して「OK」をクリックします。



10.4 管理者 ID ファイルの再発行

紛失や不正利用の可能性があるなど、DATA SEALED SAFER 管理者 ID ファイル(Admin.cid)を再発行する必要がある場合は、再発行用ファイル(Reissue1.dat、Reissue2.dat、Reissue3.dat)を使用して以下の手順で操作を行ってください。
ファイルの保存先は「C:¥DATA SEALED SAFER¥管理」フォルダです。

再発行用ファイルは、3 つのうち 2 つ以上存在すれば処理が可能です。
(例：Reissue2.dat と Reissue3.dat)

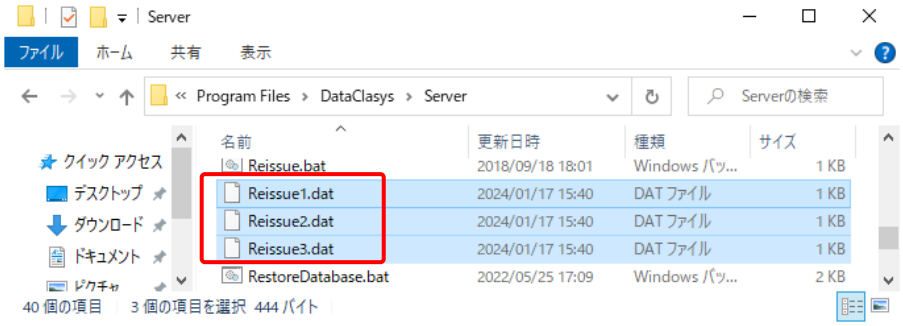
なお、DATA SEALED SAFER 管理者 ID ファイルを再発行すると、再発行前の DATA SEALED SAFER 管理者 ID ファイル(Admin.cid)及び、再発行用ファイル(Reissue1.dat、Reissue2.dat、Reissue3.dat)は使用できなくなります。

① **再発行用ファイルの配置**

DATA SEALED SAFER サーバのインストールフォルダ（デフォルトでは「C:¥Program Files¥DATA SEALED SAFER¥Server」）内に、DATA SEALED SAFER 管理者 ID ファイル再発行用の以下の 3 つのファイルを移動します。
※3 つのファイルのうち、2 つ以上で処理は可能です。

■DATA SEALED SAFER 管理者 ID ファイル再発行用ファイル

・Reissue1.dat
・Reissue2.dat
・Reissue3.dat



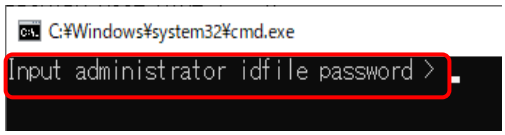
② **管理者 ID ファイル再発行処理の起動**

アプリケーション一覧より、「DATA SEALED SAFER」-「管理者 ID ファイル再発行」をクリックします。

③ **管理者 ID ファイル再発行**

コマンドプロンプト画面が立ち上がり、「Input administrator idfile password >」と表示されますので、DATA SEALED SAFER のアドミニストレータ ID「Admin.cid」で使用したいパスワードを入力し、「Enter キー」を押します。

※パスワードポリシーに準じた任意のパスワードを設定する必要があります。



処理が終了すると、「続行するには何かキーを押して下さい...」のメッセージが表示されますので、「Enter」キーなどを押して処理を完了してください。

なお処理により DATA SEALED SAFER の管理者 ID「Admin.cid」が、DATA SEALED SAFER サーバのインストールフォルダ「C:¥Program Files¥DATA SEALED SAFER¥Server」に作成されます。

※管理者 ID ファイル再発行前の管理者 ID「Admin.cid」と混同しないよう、古い管理者 ID「Admin.cid」は削除し、再発行した管理者 ID「Admin.cid」を「C:¥DATA SEALED SAFER¥管理」に保管してください。誤って古い管理者 ID「Admin.cid」で DATA SEALED SAFER マネージャクライアントにログインしようとすると以下のメッセージが表示されログインできません。

10.5 パスワードポリシー

DATA SEALED SAFER は以下のパスワードポリシーが設定されています。
そのため、DATA SEALED SAFER の ID ファイルパスワードを設定する際は、ポリシーに準拠したパスワードを設定ください。

パスワード要件	許容範囲
最小文字数	8 文字以上
最大文字数	128 文字以下
アルファベットの大文字と小文字の区別	区別する
アルファベットの小文字の文字数	1 文字以上
アルファベットの大文字の文字数	1 文字以上
数字の文字数	1 文字以上
アルファベット、数字以外の特殊文字の文字数	1 文字以上