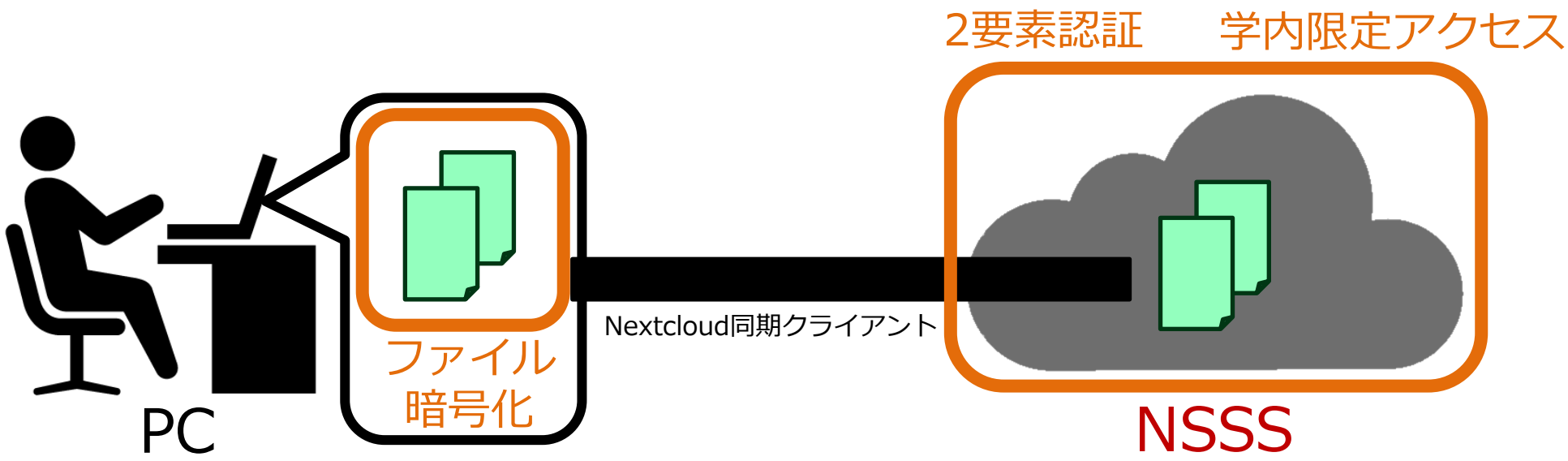
NSSS利用ガイド：ファイル同期と暗号化

名古屋大学情報連携推進本部

2021/9/13

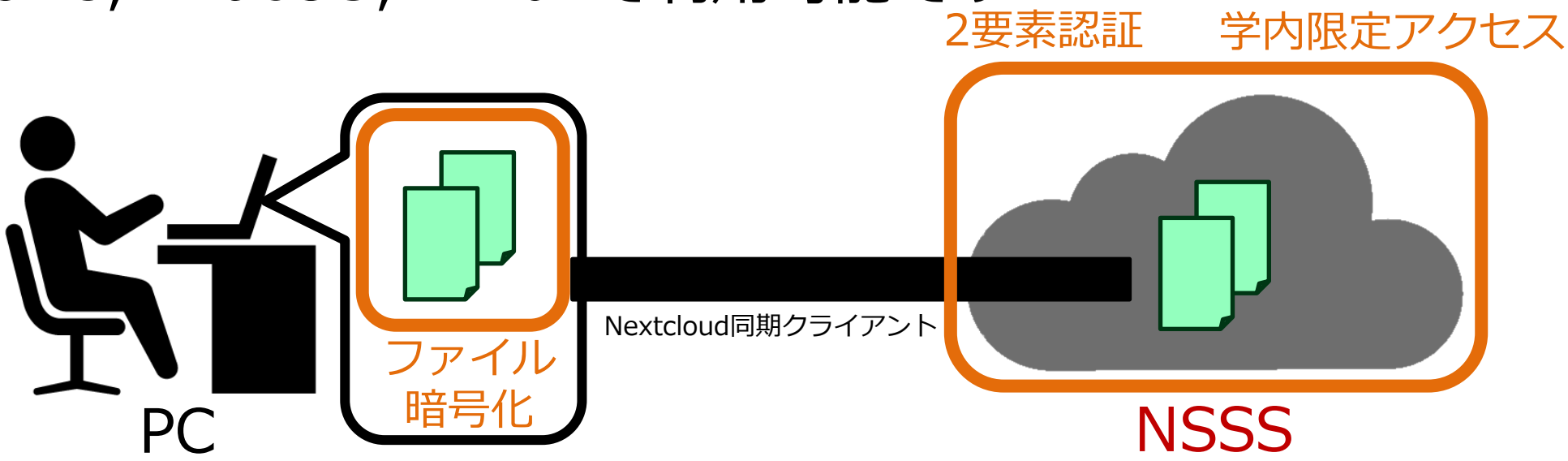
NSSSを使ったファイル管理

- NSSSでは，NUSSと同様にPCのファイルをNSSSを通じて自動的に同期させることが可能です
  - NSSSは2要素認証などで不正アクセスからファイルを守ります
  - PC上のファイルはファイル暗号化を行うことで安全性向上が可能です



NSSSとPCのファイル同期

- 同期クライアントを使用してNSSSとPCのファイルを自動的に同期させる方法を説明します
  - まずはPC上のファイルを暗号化しない場合を説明し，その後暗号化の方法を説明します
  - Windows，macOS，Linuxで利用可能です

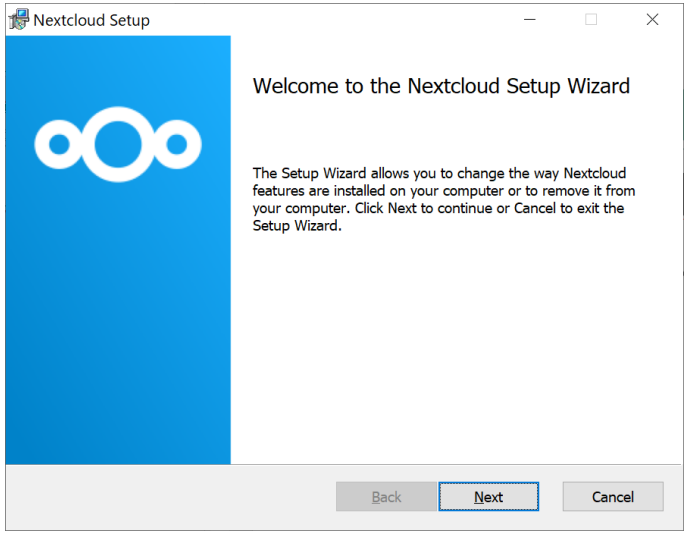


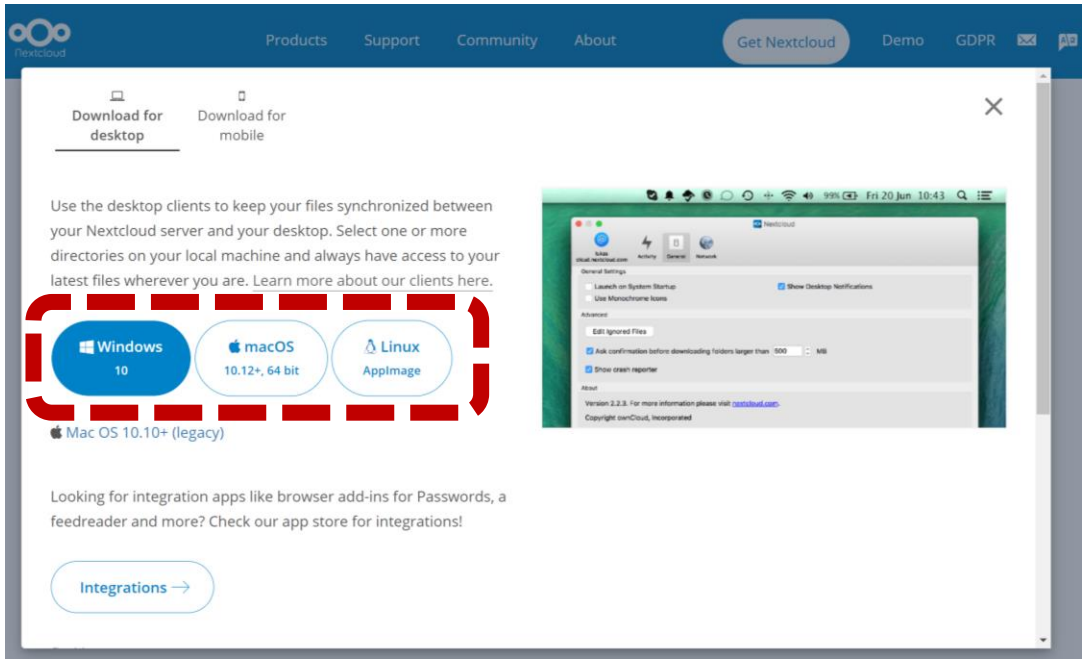
NSSSとPCのファイル同期

- NUSSと同様に，同期クライアントを使用してNSSSとPCのファイルを自動的に同期させることが可能です
- ファイル同期の方法を説明します

Nextcloudのインストール

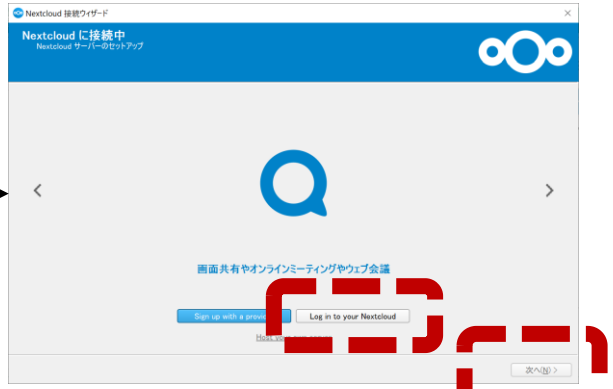
- クライアントソフトのインストール
  - https://nextcloud.com/ からダウンロード
  - インストーラを実行して インストールします

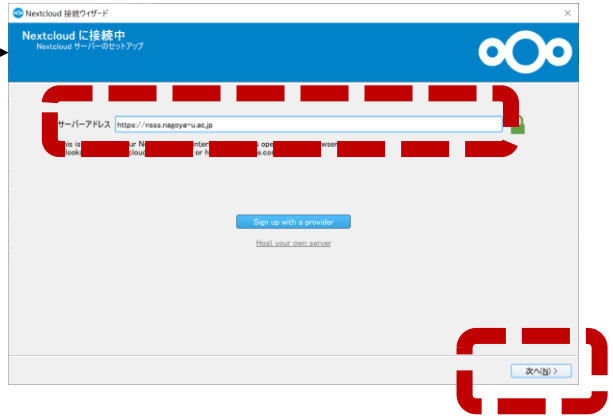




Nextcloudの設定①

- Nextcloudを起動し上部メニューから「アカウントを追加」を選択
- 接続ウィザード
  - 「Log in to your Nextcloud」を選択
  - サーバアドレスは「https://nsss.nagoya-u.ac.jp」
  - ブラウザが自動的に開くので表示に従って操作
    - 初回ログインの場合はスマホを使った認証が求められます．以下にある「NSSSの利用ガイド動画」を参考に認証を行ってください．
      https://icts.nagoya-u.ac.jp/ja/services/nuss/





ブラウザでの接続済み表示

ファイル同期について

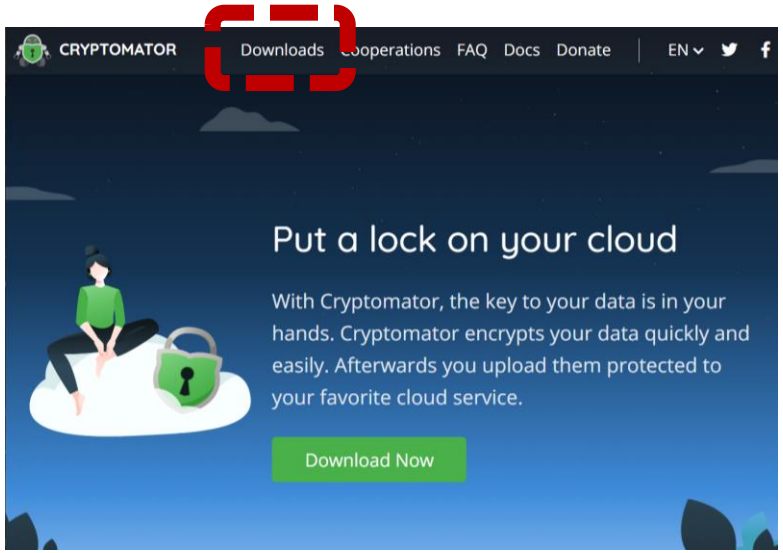
- ここまで行うとNUSSと類似したストレージサービスとしてNSSSが使用可能です
- NSSSがNUSSと異なる点
  - 学内のキャンパスネットワークからのみ接続可能です
  - 学外からはVPN接続を用いて接続可能です
    （私物PCから利用しないでください）
  - 学外からはURL共有機能は利用できません
- 扱うことができる情報機密性
  - 特別な指示がない限り暗号化すれば機密性4までの情報を保存できます

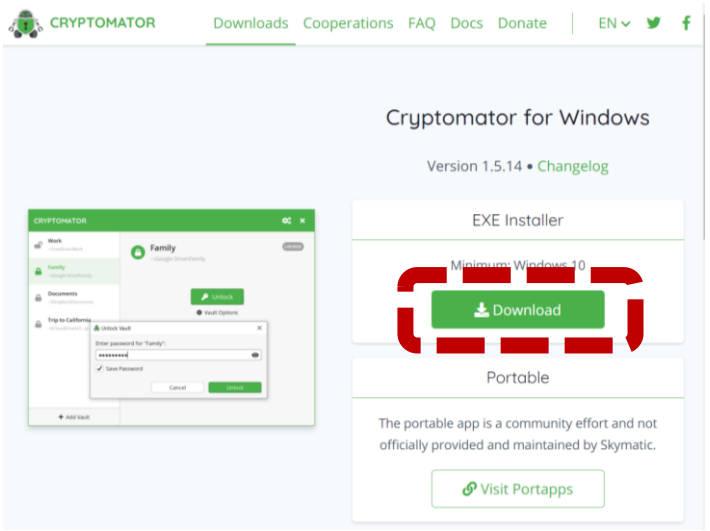
ファイル暗号化

- NSSS上のファイルは2段階認証でログインしない限り
  アクセスできないため安全です
- しかしNSSSと同期されたPC上のファイルは守られておらず,
  PCからファイルが流出すると危険です
- PC上のファイルも暗号化することでデータ流出の危険性を少なくすることができます
- PC上のファイルを暗号化するCryptomatorというソフトの
  使用法を説明します

Cryptomatorのダウンロード

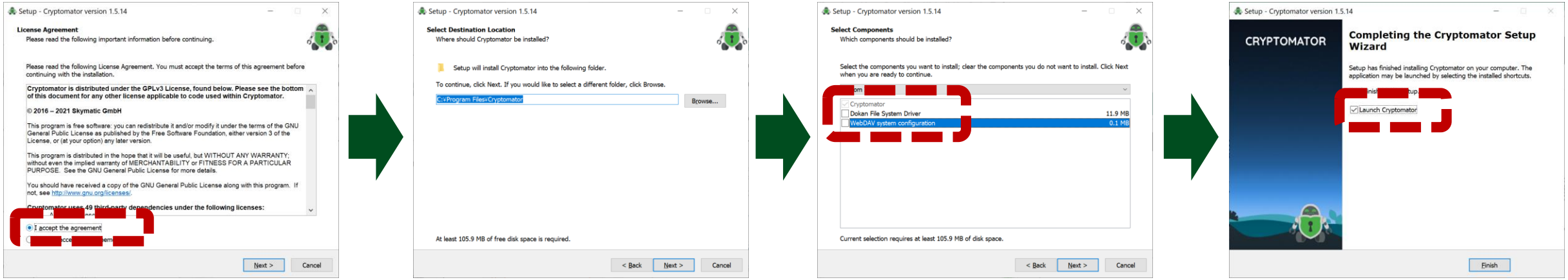
- ソフトのダウンロード
  - https://cryptomator.orgにアクセス
    - Donation（寄付）を勧める表示が出る場合がありますが寄付しなくても利用可能です
  - Downloadsをクリックしダウンロード実行





Cryptomatorのインストール

- インストール手順
  - ダウンロードしたファイルを実行
  - License Agreementでは記載を確認し「I accept...」を選択
  - Select Componentsでは「Cryptomator」以外はチェックを外す
  - 最後のCompleting...では「Launch Cryptomator」をチェックしてFinishボタンを押す

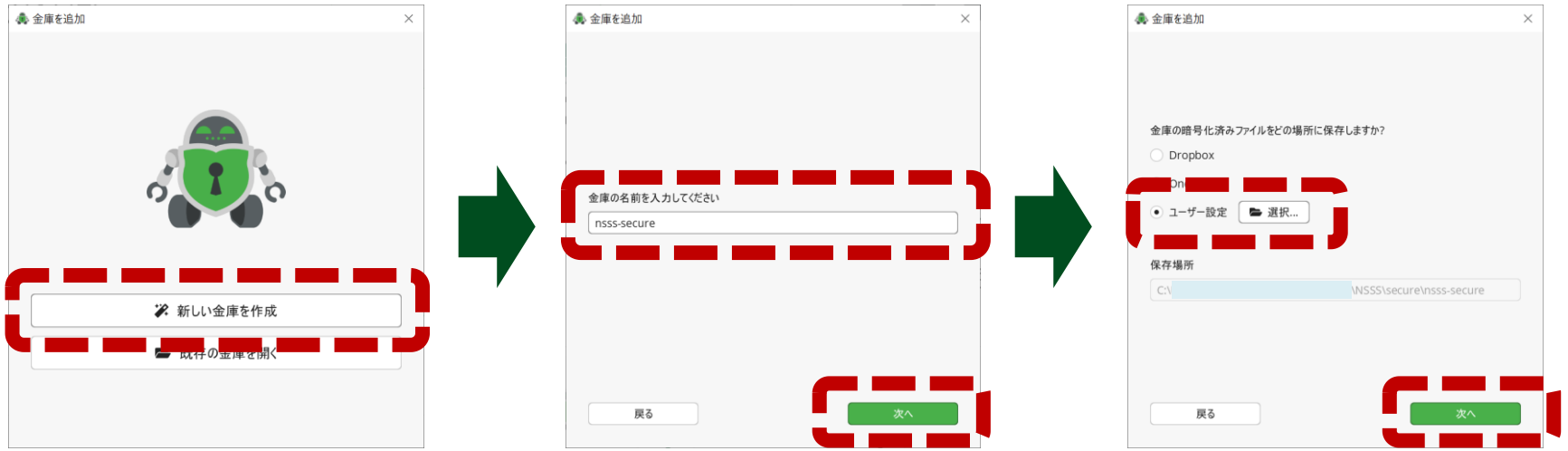


暗号化データの保存場所設定

- Cryptomatorを起動します
  - インストール終了時に起動，またはスタートメニューから起動
- 暗号化データの保存場所設定
  - 「＋金庫を追加」，「新しい金庫を作成」の順に選択

暗号化データの保存場所設定（続き）

- 「新しい金庫を作成」の次に金庫の名前を入力します
- 「金庫の暗号化済みファイルをどの場所に保存しますか？」では先ほどNextcloudでNSSSと同期させたフォルダ（またはその中のフォルダ）を指定します.
  ユーザー設定の「選択」を押し，暗号化ファイル保存用フォルダを指定してください.
  ここで日本語を含むフォルダ名は使用しないでください.



金庫の名前　　フォルダ指定

暗号化データの保存場所設定（続き）

- 以下を確認してパスワードを作成します

パスワード作成の注意点

- 8文字以上大文字，小文字，数字，記号のうち3種類以上使用
- 名大IDなど他で使用したものと異なるパスワードとする
- パスワードを忘れるとデータ取り出しが不可能になるので注意．NSSSサービス管理者でもデータ復旧できません．

パスワード作成

- リカバリーキーが必要なら「はい」を選びます

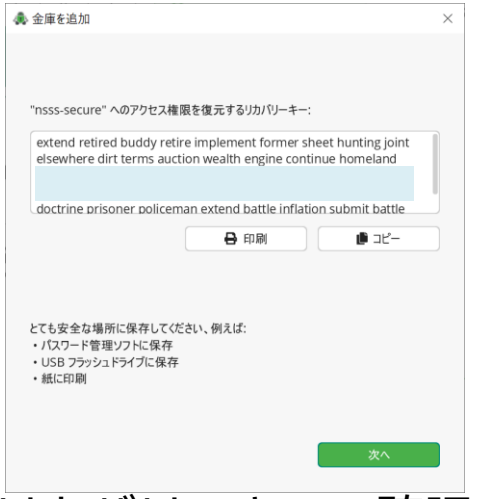
暗号化データの保存場所設定（続き）

- リカバリーキーを確認して記録します
  - 記録は「紙に印刷」「USBメモリに保存」のどちらかを勧めます

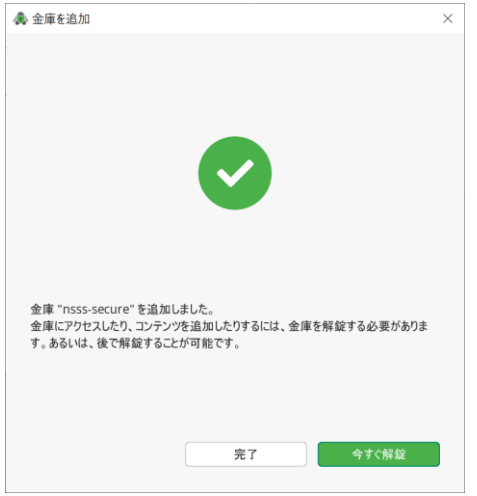
リカバリーキーの扱いの注意

- 他人に知られると暗号化が解除される可能性があります
- PC内に保存しないでください.
- PC内のデータが漏れる可能性を考慮し，キーは紙への印刷，PCから切り離されたUSBメモリへの保存を勧めます.

- 右の画面が表示されたら完了です



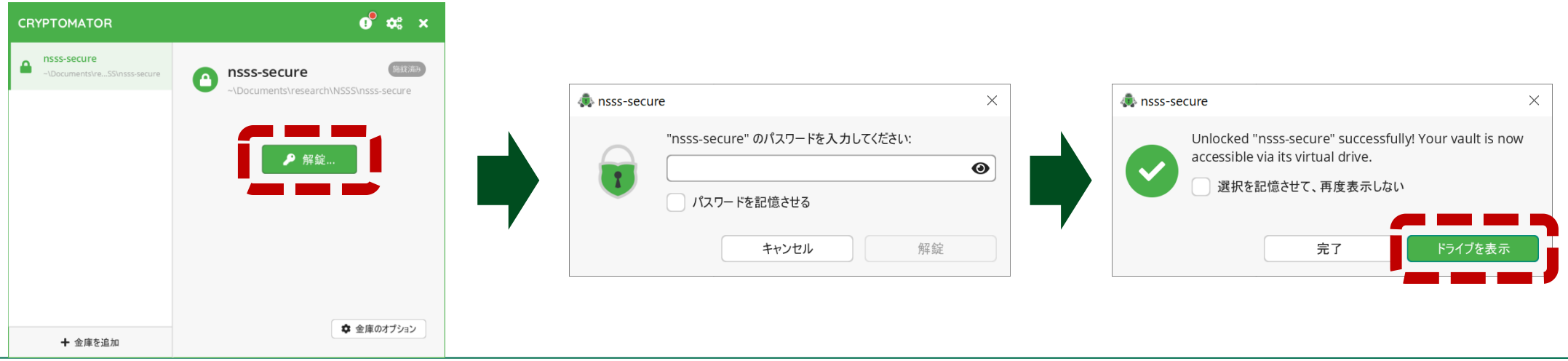
リカバリーキーの確認



完了画面

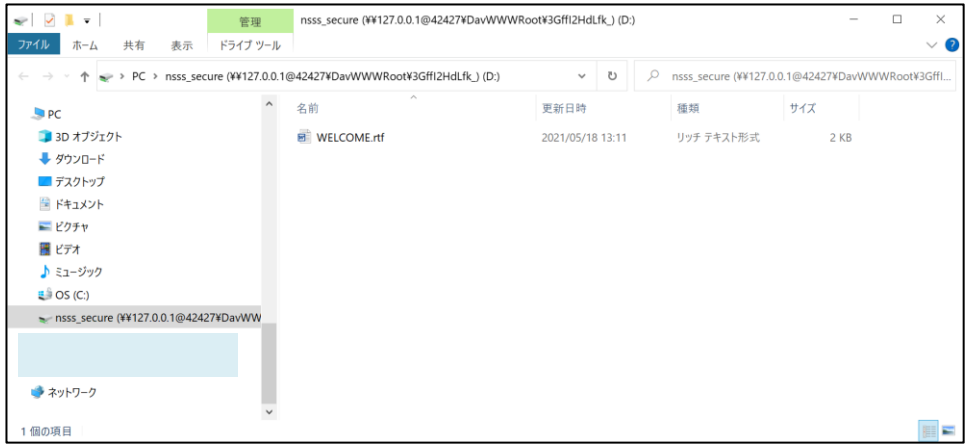
暗号化データにアクセス①

- 暗号化されたデータにアクセスする方法を説明します
- Nextcloudクライアントで「同期を一時停止」で同期を止めてください
- Cryptomatorでの操作
  - Cryptomatorの左リストで暗号化データを選択して「開錠」を押しパスワード入力
  - Unlockedと表示されたら「ドライブを表示」を押す



暗号化データにアクセス②

- データアクセス
  - 暗号化されたデータ領域は右図のように
    ネットワークドライブとして表示されます.
    例えばDやEドライブなど，開錠時だけ
    ドライブとして表示されます.
    このドライブ内に暗号化したいファイルや
    フォルダを保存してください.
- アクセスの終了
  - 暗号化データのアクセスが終わったら
    Cryptomatorで「施錠」を押してください
  - Nextcloudクライアントで「同期を再開」を
    選んでください



注意点

- 暗号化データ保存場所には暗号化に必要なファイルが自動生成されます．このファイルは絶対に手動での変更や削除をしないでください．暗号化データにアクセスできなくなります．