desknet's NEO クラウド版
セキュアブラウザ（端末認証あり･端末認証なし）
利用ガイド
iOS 編

作成	株式会社ネオジャパン
バージョン	2022 年 5 月版

目　次

はじめに

セキュアブラウザは、デスクネッツを自宅や外出先などから安全に利用するためのツール（アプリ）です。セキュアブラウザというアプリを使用してデスクネッツを利用します。通常のブラウザアクセスと同じようにデスクネッツをご利用頂けます。端末の紛失・盗難による情報漏えいを防ぐため、皆さまの端末の中にはデスクネッツのデータは保存できないようになっています。

本書は、iOS 版 Soliton SecureBrowser サービスのセットアップ手順ついて説明したものです。
なお、表示されている証明書のファイル名はサンプルとなります。

- セットアップに必要な情報（共通）

  セキュアブラウザ起動時に必要なゲートウェイ接続用の証明書、及びパスワード
  ※セキュリティ仕様変更に伴い、2022 年 5 月 17 日より[ゲートウェイ接続用の証明書]が必要となりました。詳しくは管理者にご確認ください。

  - セキュアブラウザのログイン情報
    ※セキュリティ仕様変更に伴い、2022 年 5 月 17 日より[ssb2-neo.dn-cloud.com]となります。

- セットアップに必要な情報（セキュアブラウザ端末認証ありのお客様）
  - desknet's NEO にログインする時に必要な証明書、及びパスワード
    ※ゲートウェイ接続用の証明書とは別となります。
- Soliton SecureBrowser Ⅱ 動作環境
  - iOS 15.4～15.0 / 14.8～14.0 /13.7～13.1
    最新の情報については、以下の URL をご参照ください。

    https://www.soliton.co.jp/support/smartdevice.html

ご利用の機種によっては、本書で説明している設定箇所や操作方法が異なる場合があります。ご利用の機種に該当する、設定箇所および操作方法に置き換えてご確認ください。

① セキュアブラウザ端末認証ありをご契約の場合

クライアント証明書の配布が 2 つございます。

本書の [1.セットアップ（認証ありプラン）]から実施してください。

② セキュアブラウザ端末認証なしをご契約の場合

本書の[2.セットアップ（共通）]から実施してください。

[1.セットアップ（認証ありプラン）]は対象外となります。

1. セットアップ（認証ありプラン）

1.1 desknet's NEO 接続用の証明書をインストール

※desknet's NEO にアクセスする際に必要な証明書となります。
※こちらの証明書は、デバイス毎に異なる証明書となります。

証明書のインストールはご利用の端末により異なりますので、各端末の取扱説明書等をご参照いただき、ご不明点等は管理者にお問い合わせください。

1.1.1 iTunes からクライアント証明書をインストールする

ここでは iTunes にてクライアント証明書をインストールする方法を記載します。
メールからクライアント証明書をインストールする場合は、次項 1.1.2 を参照してください。

iTunes のファイル共有機能を使用して証明書のインストールを行うことができます。
iTunes からクライアント証明書をインストールする場合は拡張子が下記のクライアント証明書を利用してください。

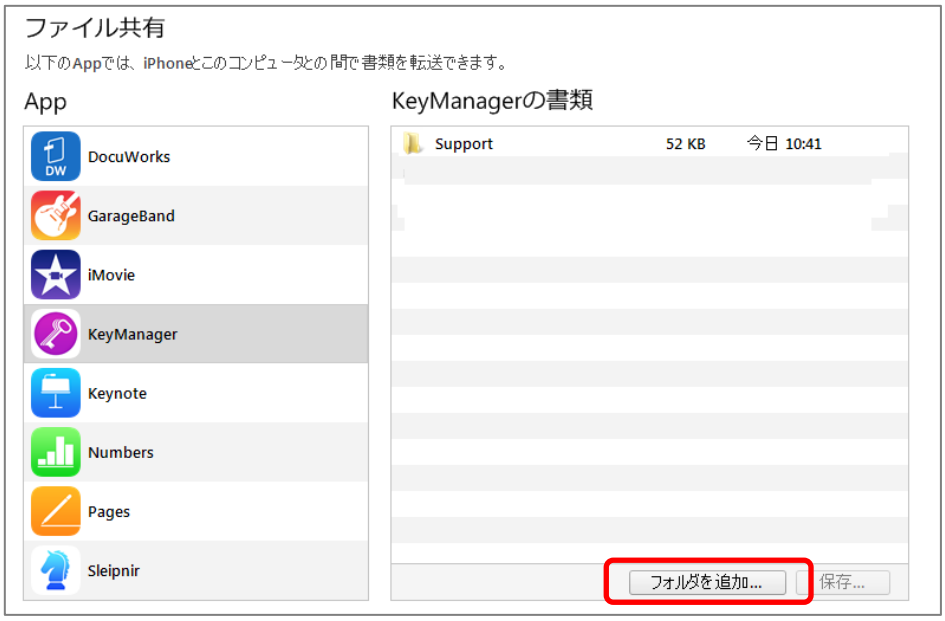
- .p12

クライアント証明書のインストールは、以下の手順で行ってください。

1. App Store から「Soliton KeyManager」をダウンロードし、インストールしてください。
   なお、Soliton KeyManager は、一般的なアプリケーションと同様の手順でアンインストールすることができます。
2. iOS をコンピューターに接続し、iTunes を起動してください。

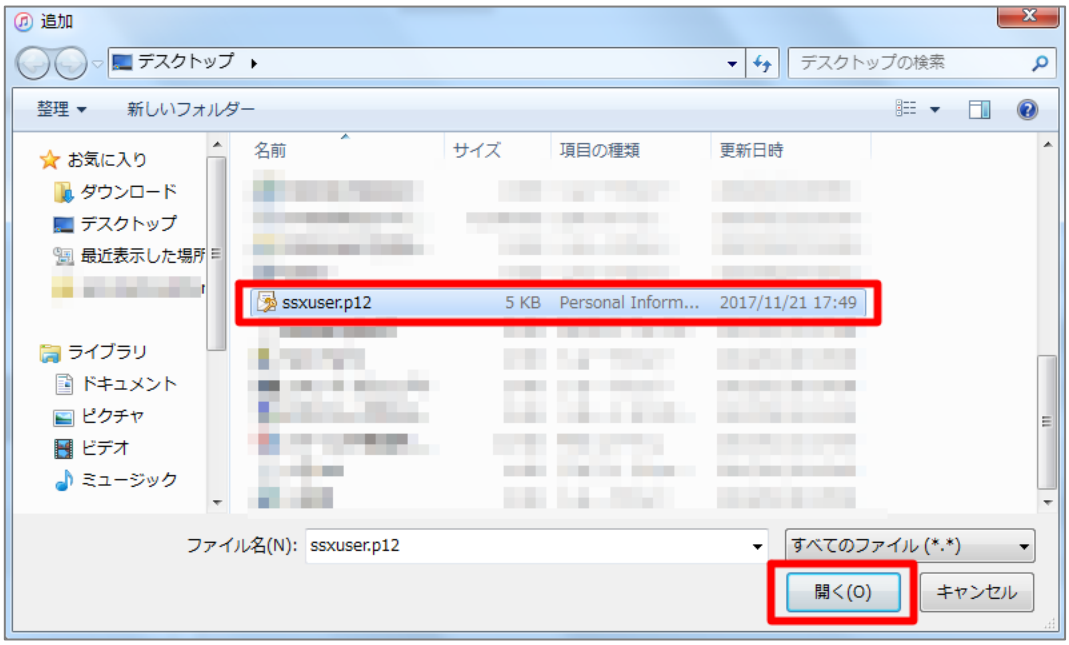
3. 接続している iOS デバイスの[ファイルの共有]タブを選択し、[ファイル共有]セクションの[App]で「Soliton KeyManager」を選択してください。

4. 「KeyManager の書類」で<ファイルを追加>をクリックしてください。



5. ファイル選択画面が表示されますので、クライアント証明書（.p12 形式）を選択し、<開く>をクリックしてください。

※クライアント証明書については管理者にお問い合わせください。



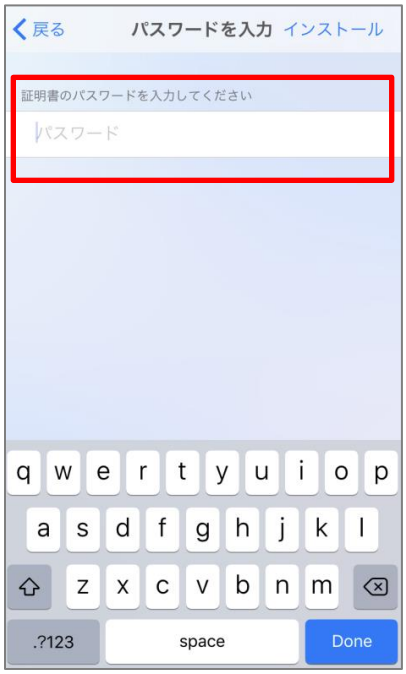
6. アップロードしたクライアント証明書が KeyManager のリストに表示されることを確認してください。アップロードが完了したら、ウィンドウ下部[同期]ボタン押し、iTune と端末の同期を実行してください。

7.　iOS 端末で Soliton KeyManager を起動し、画面右上の をタップしてください。

下図が表示されます。<iTunes から追加した証明書>をタップしてください。

8.　下図が表示されます。インストールするクライアント証明書をタップしてください。
なお、画面右上の<編集>をタップすると、iTunes からコピーしたクライアント証明書ファイルを手動で削除することができます。

9. 下図が表示されます。証明書に設定されているパスワードを入力し、画面右上の<インストール>をタップしてください。※パスワードは管理者にお問い合わせください。

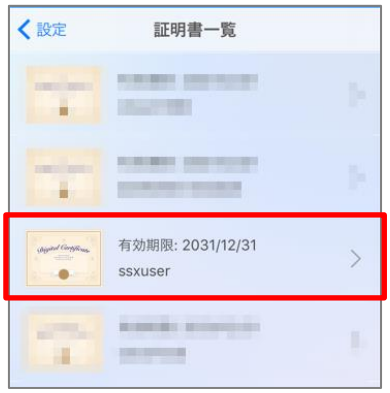


10. 下図が表示されます。<設定>をタップして 1 つ前の画面へ戻ります。

※インストールが完了すると、iTunes からコピーした証明書ファイルは端末から自動で削除されます。

11. 下図が表示されます。<証明書一覧>をタップしてください。

12. 下図が表示されます。インストールした証明書が表示されていることを確認してください。



インストールが完了したら、「2.セットアップ（共通）」へ進んでください。

1.1.2　メールからクライアント証明書をインストールする

ここではメールからクライアント証明書をインストールする方法を記載します。

iOS 端末ではメールに添付されたクライアント証明書を Soliton KeyManager にインストールすることができます。メールからクライアント証明書を Soliton KeyManager へインストールするには拡張子が下記の証明書を利用してください。

- .p12

1. 任意の PC から Soliton SecureBrowser を利用する端末のメールアドレス宛に、クライアント証明書(.p12 形式)を添付したメールを送信してください。
   ※クライアント証明書については、管理者にお問い合わせください。

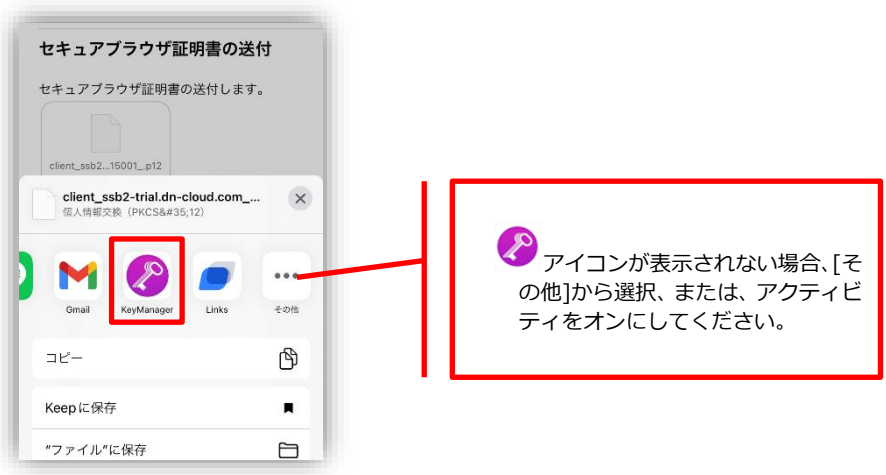
2. App Store から「Soliton KeyManager」をダウンロードし、インストールしてください。

なお、Soliton KeyManager は、一般的なアプリケーションと同様の手順でアンインストールすることができます。

3. iOS で標準メーラーを起動し、クライアント証明書(.p12 形式)が添付されたメールを開いてください。
   下図が表示されます。インストールするクライアント証明書ファイルをロングタップ（長押し）してください。

4. 下図が表示されますので、[共有]をタップしてください。

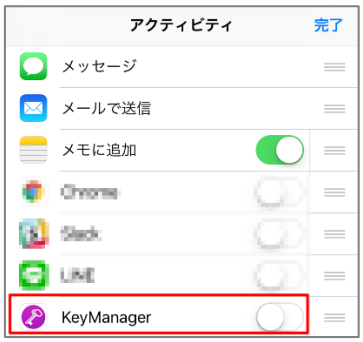
5.　[KeyManager]を選択してください。



6.　[KeyManager]をタップすると下図が表示されますので、[保存]をタップしてください。

アイコンが表示されない場合、下記の手順で、アクティビティをオンにしてください。

アクティビティに KeyManager があることを確認し、オフになっているボタンをオンにします。

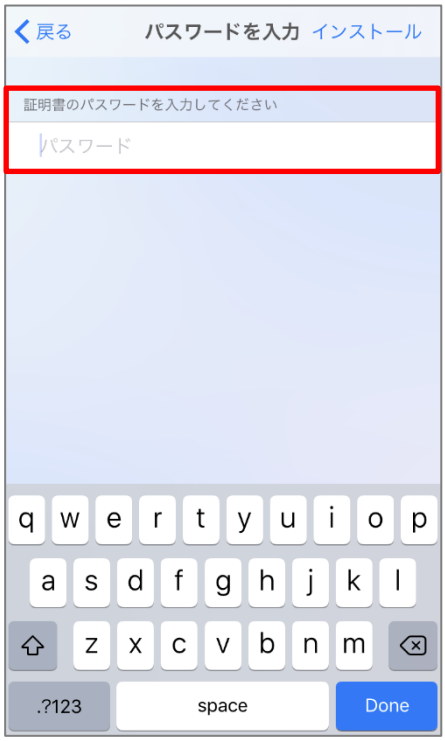


7. iOS で KeyManager を起動し、画面右上の  をタップしてください。

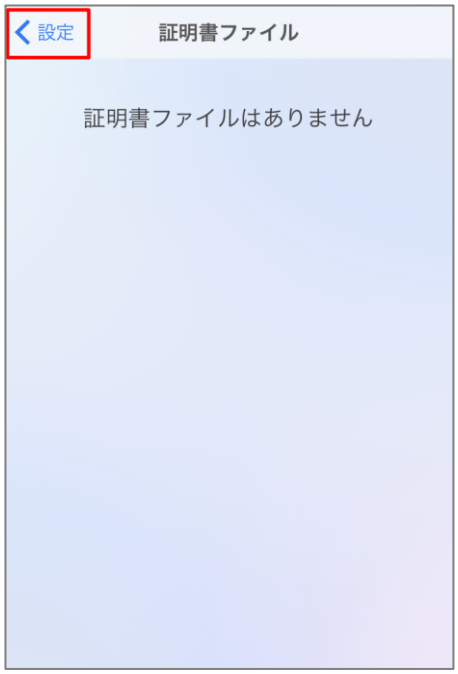
8. 下図が表示されます。<iTunes から追加した証明書>をタップしてください。

9. 下図が表示されます。インストールする証明書をタップしてください。画面右上の<編集>をタップすると、iTunes からコピーした証明書ファイルを手動で削除することができます。

10. 下図が表示されます。証明書に設定されているパスワードを入力し、画面右上の<インストール>をタップしてください。



11. 下図が表示されます。<設定>をタップして 1 つ前の画面へ戻ります。
※インストールが完了すると、iTunes からコピーした証明書ファイルは端末から自動で削除されます。



12. 下図が表示されます。<証明書一覧>をタップしてください。

13. 下図が表示されます。インストールした証明書が表示されていることを確認してください。

※[セキュアブラウザ端末認証あり]のお客様は、desknet's NEO 接続用の証明書が表示されます。

2. セットアップ（共通）

2.1 ゲートウェイ接続用の証明書をインストール

※セキュアブラウザ起動時に必要な証明書です。
※1 社 1 枚共通となります。

ゲートウェイ接続用のインストール手順は、上述の[1.1desknet's NEO 接続用の証明書をインストール]と同じ手順となります。
証明書のファイル名がそれぞれ異なりますので、ご留意ください。

2.2 iOS における証明書配布のご留意点

iOS については、証明書を KeyManager へ保存してから、インストールとなります。

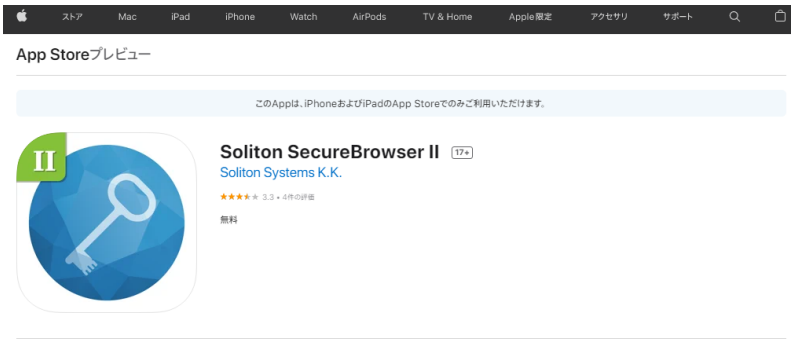
また、証明書のファイル名をシングルタップすると、構成プロファイルとして保存されてしまう場合がございますので、ロングタップ（長押し）をお願いします。

その他、証明書を正しくダウンロードできない場合や、KeyManager へ正しく保存できない場合がございましたら、下記のマニュアルをご参照ください。

https://www.desknets.com/sales/pdf/2204_sb_ios.pdf

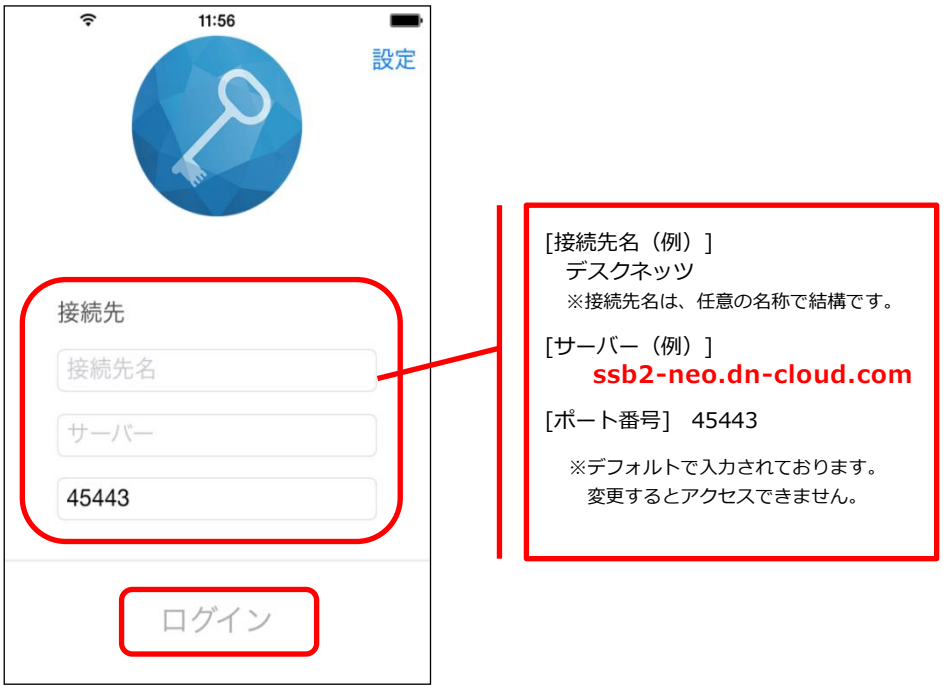
2.3 SecureBrowser Ⅱをインストールする

1. App Store から「Soliton SecureBrowser Ⅱ」をダウンロードし、インストールしてください。
   なお、SecureBrowser Ⅱは、一般的なアプリケーションと同様の手順でアンインストールすることができます。



2. SecureBrowser Ⅱを利用するためには、SecureGateway へログインする必要があります。
   SecureBrowser Ⅱのアイコンをタップし、SecureBrowser Ⅱを起動してください。

3. セキュアブラウザを起動したら、[接続先名]と[サーバー]に値を入力します。
   その後、[ログイン]ボタンをタップします。



4. 初回ログイン時には、ゲートウェイ接続用の[クライアント証明書の選択]が要求されます。
（2 回目以降のアクセスでは、証明書の選択画面は省略されます。）

※こでは、ゲートウェイ接続用の [クライアント証明書]を選択してください。
※お客様のクライアント環境に、既に登録されているクライアント証明書が複数表示される場合がございます。

5. ゲートウェイ接続用の証明書を選択後、下記画面が表示されましたら、OK を選択してください。

6. セキュアブラウザにログインが成功したら、下図が表示されますので、[desknet's NEO モバイルブラウザ版の URL]を入力します。

※入力する情報は、desknet's クラウド開通のご案内（メール）に記載されております。

※詳しくは、管理者にお問い合わせください。

7. **[セキュアブラウザ端末認証あり]**をご契約の場合には、[desknet's NEO モバイルブラウザ版の URL]を入力後に、クライアント証明書の選択画面が表示されます。
こちらでは、desknet's NEO 接続用の証明書を選択して、「許可」をタップしてください。

なお、[セキュアブラウザ端末認証なし]をご契約の場合は、クライアント証明書の選択は表示されませんので、次に進んでください。

8.　認証が成功した場合、desknet's NEO モバイルブラウザ版のログイン画面が表示されます。

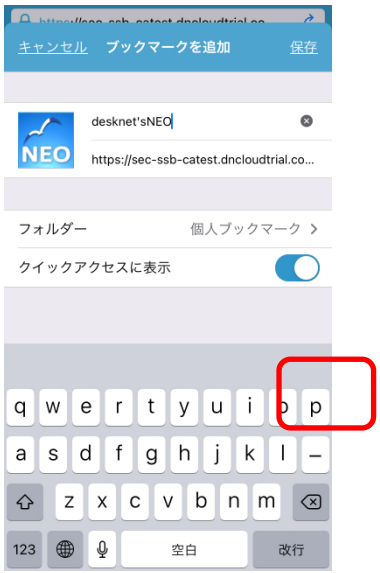
3. クイックアクセスの表示設定

desknet's NEO の URL を、個人ブックマークに登録いただければ、クイックアクセスの画面に表示されます。

1. 右下のメニューボタンをタップし、メニューを表示します。

2. [ブックマークを追加]をタップします。

3.　[クイックアクセスに表示設定]をＯＮにします。



4.　desknet's NEO のアイコンが追加され、次回以降 URL の入力は不要となります。

4. SecureBrowser Ⅱの使用方法

この章では、SecureBrowser Ⅱの使用方法について説明します。

ここでは、管理者によって SecureBrowser Ⅱの動作ポリシーが変更されていない、デフォルト設定の状態を前提として説明します。SecureBrowser Ⅱの動作ポリシーが変更されている場合、設定されている動作ポリシーによっては表示される項目の値や編集可能な項目などが変わります。

4.1 画面構成と機能

ここでは、SecureBrowser Ⅱの画面構成と機能について説明します。

画面構成と機能については、以下のとおりです。

項目	説明
http://www.soliton.co.jp/	アドレスバーです。現在表示している Web サイトの URL が表示されます。右端をタップすることで Web サイトのページの再表示を行います。
< >	ページの<戻る>、<進む>ボタンです。
3	タブ一覧ボタンです。表示される数字は、現在開いているタブの数です。タップするとタブ一覧を表示します。
	ブックマークボタンです。 タップするとブックマークを表示します。 ● 共通ブックマーク ※こちらはご利用頂けません。 ● 個人ブックマーク ● ダウンロード
	メニューボタンです。タップするとメニューを表示します。

<制約事項>

・デスクネッツのみアクセス可能です。検索・URL バーから他のサイトにはアクセスできません。

・セキュアブラウザ利用中は一時的にセキュアブラウザ内部にデータは保持しますが、
特定のタイミングでデータは消去されます。

[Windows / Mac]

アプリ終了時、ログアウト時

[iOS / Android]

ログアウト時、ホームボタン等でアプリ終了後 10 分以上経過してからアプリを再度立ち上げた時

4.2 ロックを設定する

ロックの設定を行う場合には、SecureGateway にログインしている状態で設定画面を開いてください。
なお、ログアウトすると、ロックの設定は削除されます。

❑ パスコードによるロックを設定する

パスコードによるロックを設定する手順は、以下のとおりです。

1. メニューボタンをタップし[設定]をタップしてください。

2. [ロック]をタップしてください。

3.　[ロック方法]をタップしてください。

4.　設定したいロック方法を選択し設定してください。

※ロック方法の種類は管理者設定により表示が下図と異なる場合があります。

4.3 ファイルを閲覧する

SecureBrowser Ⅱでファイルを閲覧する方法について説明します。

4.3.1　デスクネッツの添付ファイルを閲覧する

1.　添付ファイルをタップしてください。ダウンロードが完了すると、下図が表示されます。

ファイルを開く場合は、<開く>をタップしてください。

<キャンセル>をタップするとファイルは開かず、ダウンロードのみ行います。

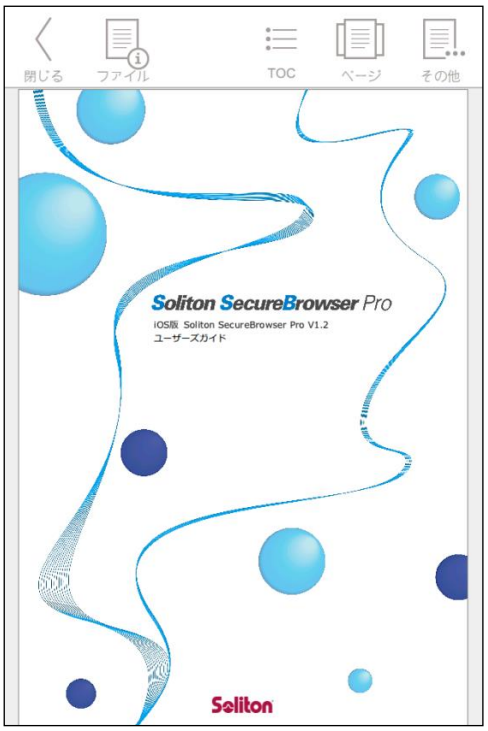
- ファイルが zip 形式の場合

ダウンロードしたファイルが zip 形式の場合、格納されているファイルを開くために展開を行います。

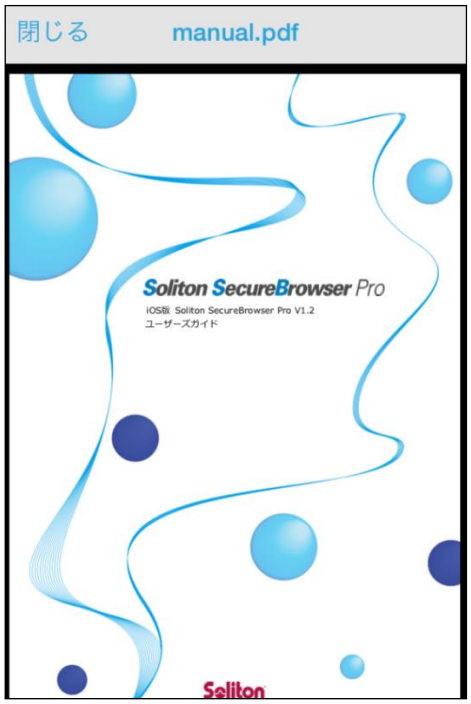
上図で<開く>をタップすると、zip 内に格納されているファイルが表示されます。展開するファイル名をタップし、展開先のフォルダー名の指定、パスワードが設定されている場合はパスワードの入力を行ってください。

スプラッシュスクリーンが表示された後に、ファイルが表示されます。閲覧しているファイルを閉じるには、ツールバーの<閉じる>をタップしてください。

※ツールバーが表示されない場合は画面をダブルタップしてください。



閲覧するファイルの種類によってはスプラッシュスクリーンが表示されず、下図のようにファイルが表示されます。閲覧しているファイルを閉じるには、<閉じる>をタップしてください。



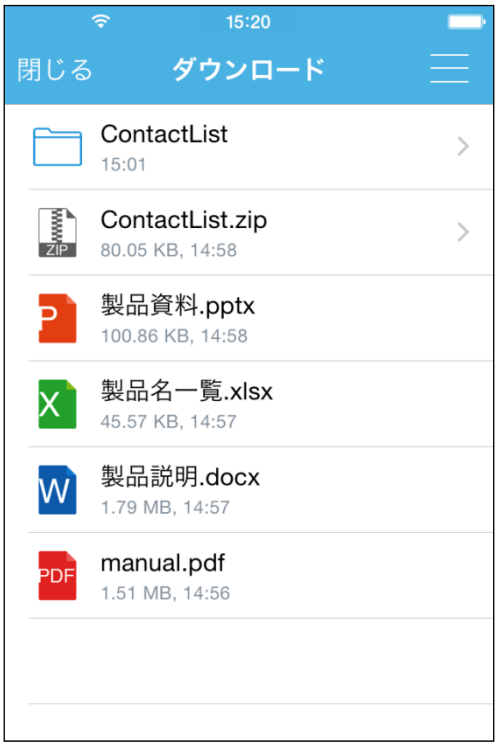
SecureBrowser Ⅱで閲覧することができるファイルの種類は、以下のとおりです。

- Microsoft Office Word ファイル（.doc、.docm、.docx）
- Microsoft Office Excel ファイル（.xls、.xlsm、.xlsx）
- Microsoft Office PowerPoint ファイル（.ppt、.pptm、.pptx）
- PDF ファイル（.pdf）
- TEXT ファイル（.txt、.csv、.rtf）
- Log ファイル（.log）
- 画像ファイル（.jpg、.jpeg、.jpe、.bmp、.png、.gif、.jps、.tif、.tiff）
- Keynote ファイル（.key）
- Numbers ファイル（.numbers）
- Pages ファイル（.pages）

4.3.2　ダウンロードしたファイルを閲覧する

SecureBrowser Ⅱがキャッシュとして保持している間は、過去にダウンロードしたファイルを閲覧することができます。

ブックマークの[ダウンロード]をタップすると、下図が表示されます。ファイル名をタップすることで、ファイルを閲覧できます。



5. サポート

この章では、本製品のサポートについて説明します。

5.1 診断情報

SecureBrowser Ⅱを使用中に障害が発生した場合などに、発生した障害を解析するために必要となる動作環境、動作状況などの情報収集を目的として、弊社より診断情報のご提供をお願いする場合があります。診断情報を提供していただくことで、お客様に環境を伺う、状況を調べていただくなどのお客様にかかる手間を軽減することができます。

通常は、診断情報を作成する必要はありません。診断情報の作成は、管理者より指示があった場合のみ行ってください。

5.1.1 診断情報を作成する

診断情報を作成する手順は、以下のとおりです。

1. 設定画面を表示し、[製品情報]をタップしてください。

2. 下図が表示されます。[診断情報の送信]をタップすると、診断情報ファイルが添付されたメール作成画面が表示されます。管理者から指定されたメールアドレス宛てに送信してください。診断情報ファイルは zip 形式で圧縮されています。

ご利用の環境によっては、[診断情報の送信]をタップするとアプリケーションの選択画面が表示されます。その場合は、使用するメールアプリケーションを選択すると、メール作成画面が表示されます。

個人情報の取り扱いについて

診断情報ファイルの送付にあたってご提供いただいた個人情報および自動収集した個人情報は、障害の解析と回答をお送りするためにのみ使用し、それ以外の目的には使用いたしません。また、その取り扱いには十分な注意を払います。

弊社の個人情報取り扱いポリシーについては、以下をご参照ください。

https://www.neo.co.jp/privacy/index.html

5.2 お問い合わせ

iOS 版 Soliton SecureBrowser Pro の使用方法についてご不明な点がございましたら、管理者にお問い合わせください。管理者様の場合は、クラウドお客様サポート窓口までお問い合わせください。

＜クラウドお客様サポート窓口＞

https://www.desknets.com/cloud/support/

＜障害・メンテナンス情報＞

https://www.desknets.com/cloud/support/mainte/

＜制限事項について＞

https://www.desknets.com/neo/faq/result/3944/

＜サービス利用約款について＞

https://www.desknets.com/neo/pdf/cloud_sb.pdf

セキュアブラウザ（端末認証あり・端末認証なし）　利用ガイド iOS 編

2016 年 2 月 23 日　第 1 版
2016 年 5 月 27 日　第 2 版
2016 年 7 月 20 日　第 3 版
2020 年 5 月　7 日　第 4 版
2022 年 5 月 13 日　第 5 版

NEOJAPAN
https://www.desknets.com/

本書に記載されている情報、事項、データは、予告なく変更されることがあります。