

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	2020年5月版

目次

はじめに.....	3
1. セットアップ	4
1.1 クライアント証明書をインストールする	4
1.1.1 iTunes からクライアント証明書をインストールする.....	4
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	10
1.2 SecureBrowser Pro をインストールする	18
2. SecureBrowser Pro の使用方法	21
2.1 画面構成と機能	21
2.2 ロックを設定する.....	22
2.3 ファイルを閲覧する	24
2.3.1 デスクネットの添付ファイルを閲覧する	24
2.3.2 ダウンロードしたファイルを閲覧する	26
3. サポート	27
3.1 診断情報	27
3.1.1 診断情報を作成する	27
3.2 お問い合わせ	29



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必要となります。本書の「1.1.1 iTunes からクライアント証明書をインストールする」または、「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」に従ってインストールをしてください。

② セキュアブラウザ端末認証なしをご契約の場合

クライアント証明書のインストールは不要です。「1.2 Soliton SecureBrowser Pro をインストールする」へ進んでください。

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について説明したものです。

- 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用のクライアント証明書
 - クライアント証明書に設定されているパスワード
 - セキュアブラウザのログイン情報

※詳しくは管理者にご確認ください。

- Soliton SecureBrowser 動作環境
 - iOS 10.0/10.1/10.2/10.3/11.0/11.1/11.2/11.3/11.4
 - 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. セットアップ



1.1 クライアント証明書をインストールする

証明書のインストール方法は、ご契約のプランによって異なります。管理者の指示に従ってインストールしてください。



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。



図 1.1.1 ファイル共有タブ

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

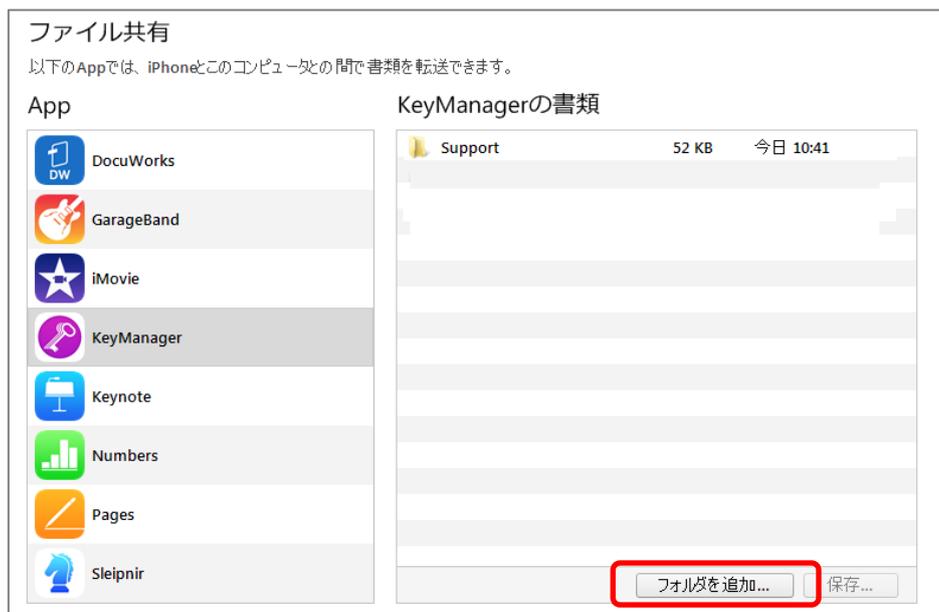


図 1.1.2 ファイル共有

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。

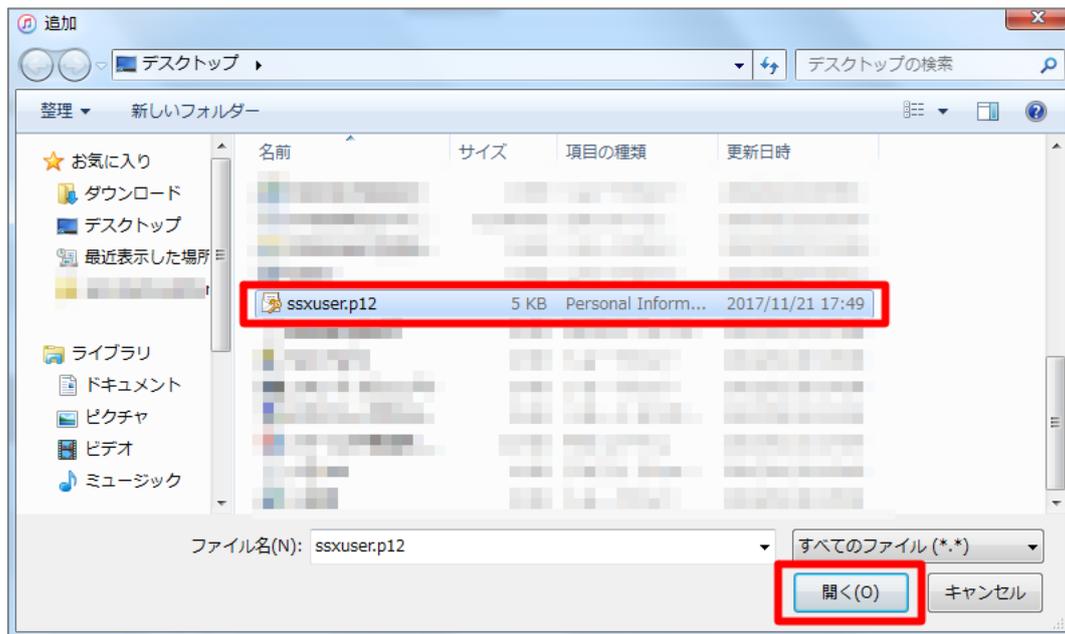


図 1.1.3 ファイル選択画面

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。



図 1.1.4 クライアント証明書アップロード完了

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。



図 1.1.5 メニュー

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。

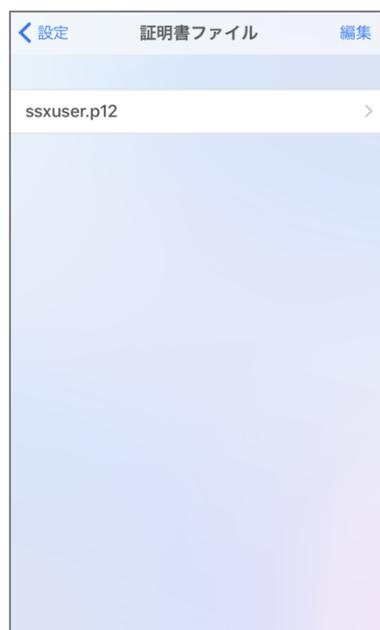


図 1.1.6 証明書ファイル

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。



図 1.1.7 パスワードの入力

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。

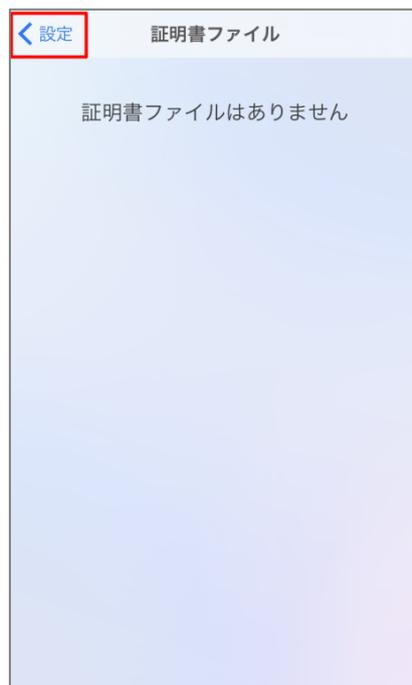


図 1.1.8 証明書ファイル

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。



図 1.1.9 メニュー

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。

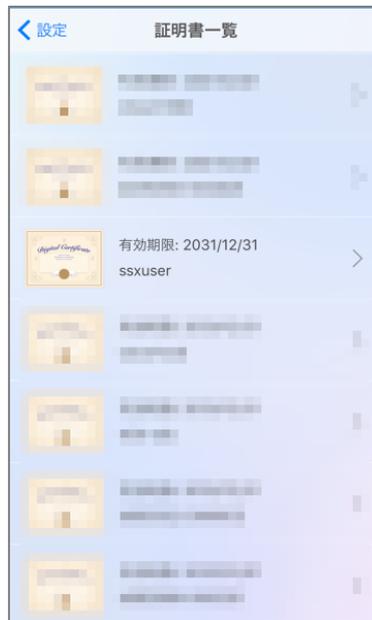


図 1.1.10 証明書一覧

インストールが完了したら、2 項「SecureBrowser Pro の使用方法」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。**

- .pkcs12

※拡張子が[.p12 形式]では、インストールできませんので、拡張子を[.pkcs12 形式]に変更してください。

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 (.pkcs12 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(.pkcs12 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。

※  アイコンが表示されないこともあります。



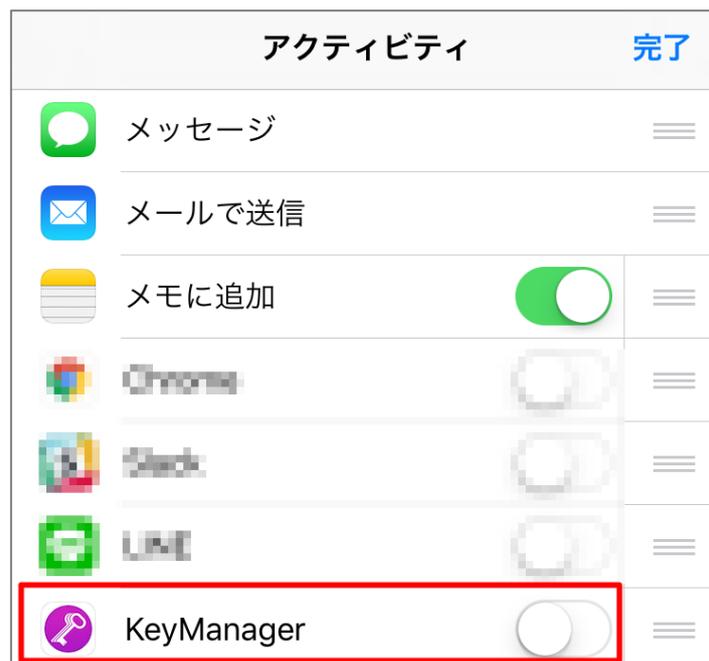
図 1.1.12 メール添付ファイル

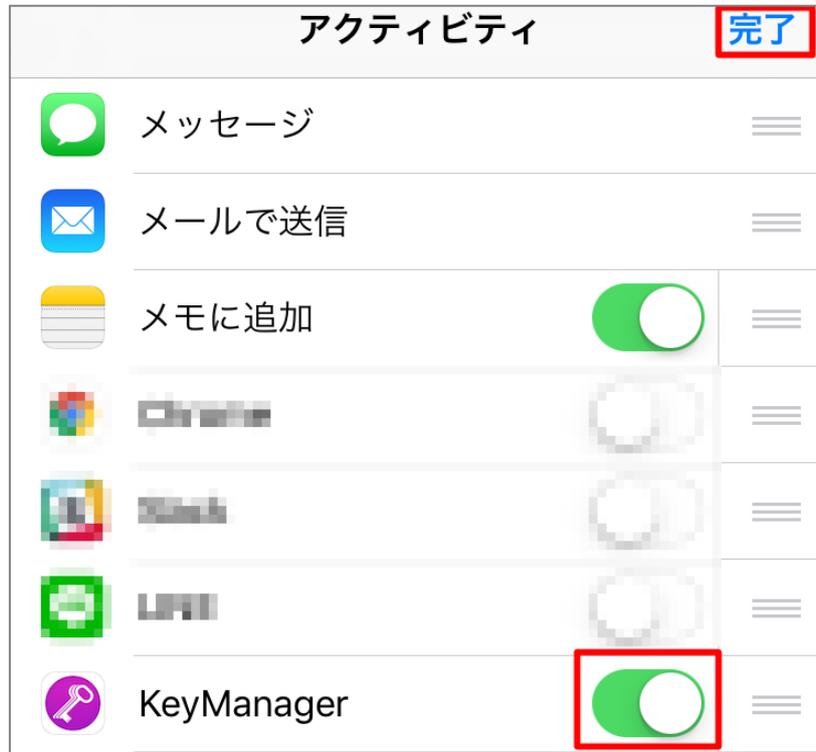
※  アイコンが表示されない場合、下記の手順で、アクティビティをオンにしてください。

証明書をタップ後、その他を選択します。

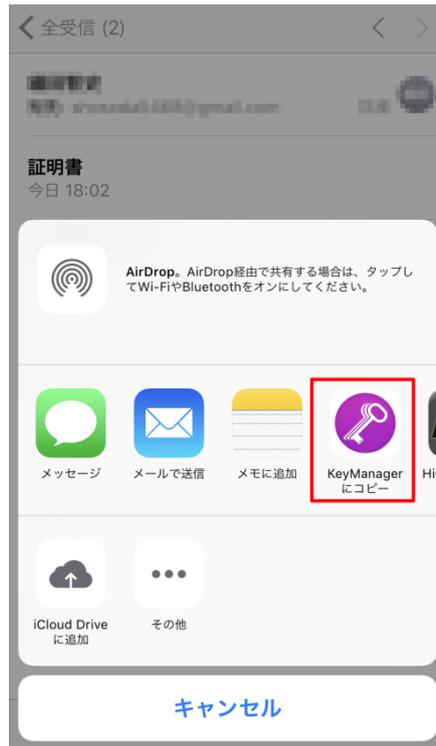


アクティビティに KeyManager があることを確認し、オフになっているボタンをオンにします。





 アイコンが表示されるようになることを確認してください。



4. 下図が表示されます。[KeyManager にコピー]をタップしてください。

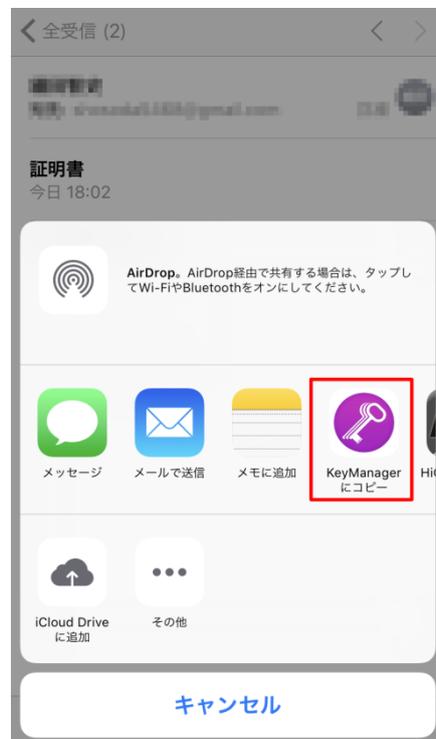


図 1.1.13 操作の選択

5. 下図が表示されます。[保存]をタップしてください。

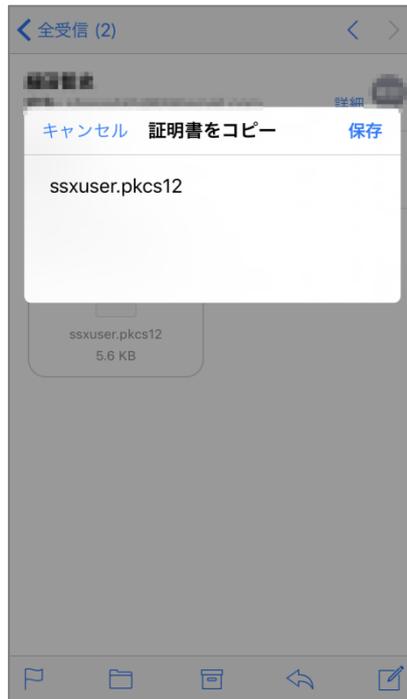


図 1.1.14 保存をタップ

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

7. 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。



図 1.1.15 メニュー

8. 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。

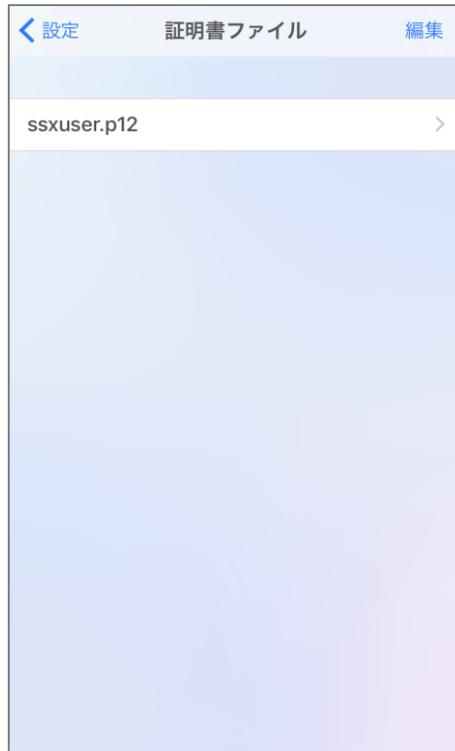


図 1.1.16 証明書ファイル

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。

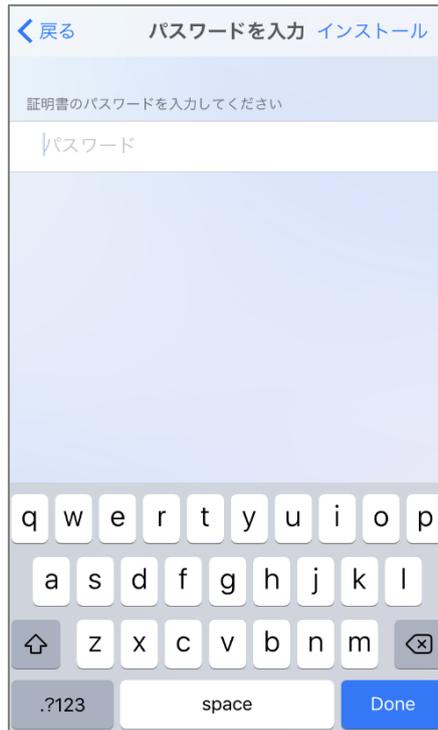


図 1.1.17 パスワードの入力

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。

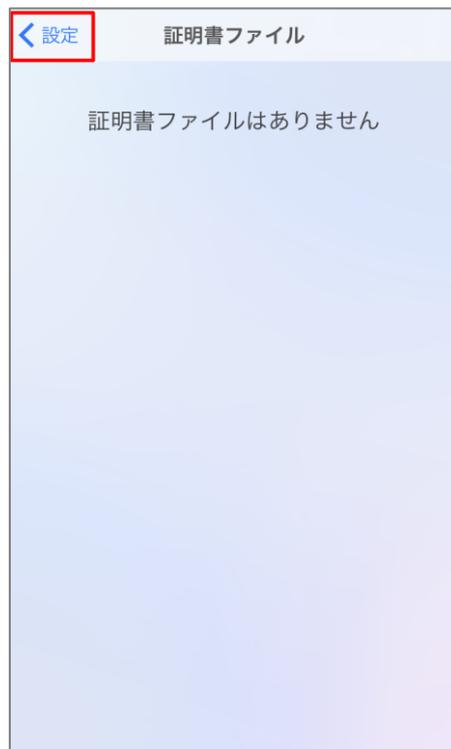


図 1.1.18 証明書ファイル

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。



図 1.1.19 メニュー

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。

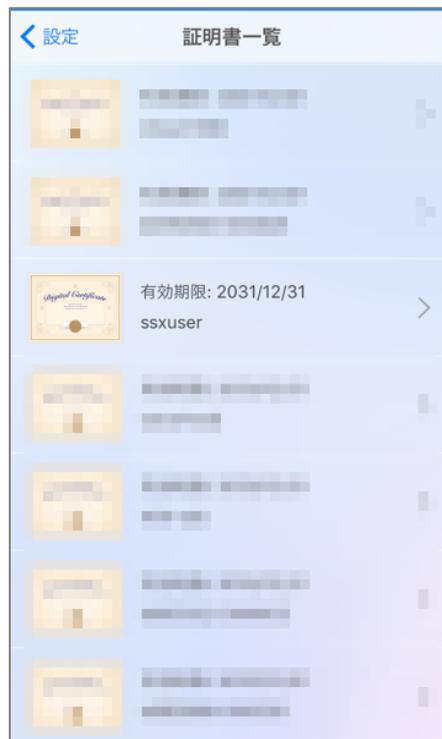


図 1.1.20 証明書一覧

1.2 SecureBrowser Pro をインストールする

1. App Store から「Soliton SecureBrowser Pro」をダウンロードし、インストールしてください。
なお、SecureBrowser および SecureBrowser Pro 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 Pro 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 Pro のアイコンをタップし、SecureBrowser Pro を起動してください。



図 1.2.1 SecureBrowser Pro アイコン

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。

図 1.2.2 セキュアブラウザのログイン画面

[接続先名 (例)]
デスクネッツ
※接続先名は、任意の名称で結構です。

[サーバー (例)]
xxxx.sb.dn-cloud.com
※セキュアブラウザに接続するための情報をご入力ください。
※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、デスクネッツの管理者にお問い合わせください。

[ポート番号] 45443
※デフォルトで入力されております。変更するとアクセスできません。

4. 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。

その後、[desknet's クラウドのスマートフォン版 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。

5. [desknet's クラウドのスマートフォン版 URL]を入力後、下図が表示されます。

クライアント証明書を選択し、<OK>をタップしてください。



図 1.2.3 クライアント証明書の選択

6. 認証が成功した場合、desknet's NEO スマートフォン版のログイン画面が表示されます。



図 1.2.4 desknet's NEO ログイン画面（スマートフォン版）

2. SecureBrowser Pro の使用方法

この章では、SecureBrowser Pro 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 Pro 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 Pro 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。

2.1 画面構成と機能

ここでは、SecureBrowser Pro 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
	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。
	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。 <ul style="list-style-type: none"> ● 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>

- ・デスクネット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

2.2 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。



図 2.2.1 メニュー

2. [ロック]をタップしてください。



図 2.2.2 接続先情報

3. [ロック方法]をタップしてください。



図 2.2.3 ロック

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。

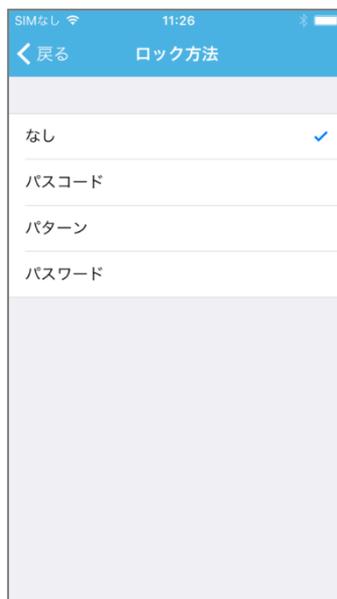


図 2.2.4 ロック方法

2.3 ファイルを閲覧する

SecureBrowser Pro でファイルを閲覧する方法について説明します。

2.3.1 デスクネット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。



図 2.3.1 ダウンロード

- 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。

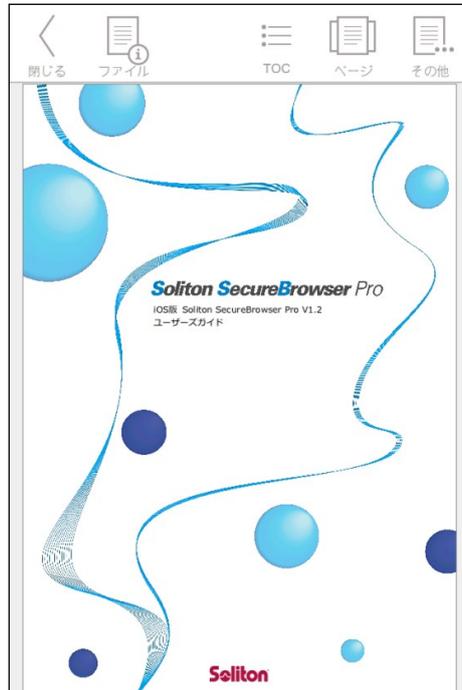


図 2.3.2 ファイルの閲覧

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。

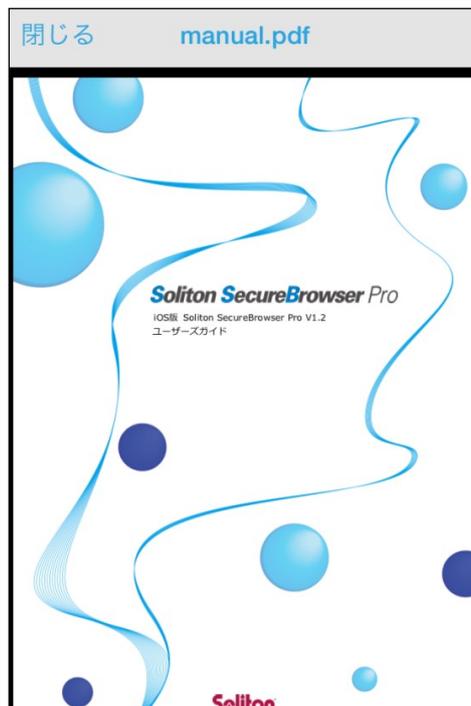


図 2.3.3 ファイルの閲覧

SecureBrowser Pro 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）
- 画像ファイル（.jpg、.bmp、.png、.gif、.emf、.wmf、.jps、.tif、.tiff）
- Keynote ファイル（.key、.key.zip）
- Numbers ファイル（.numbers、.numbers.zip）
- Pages ファイル（.pages、.pages.zip）

2.3.2 ダウンロードしたファイルを開覧する

SecureBrowser Pro 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開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、ファイルを開覧できます。

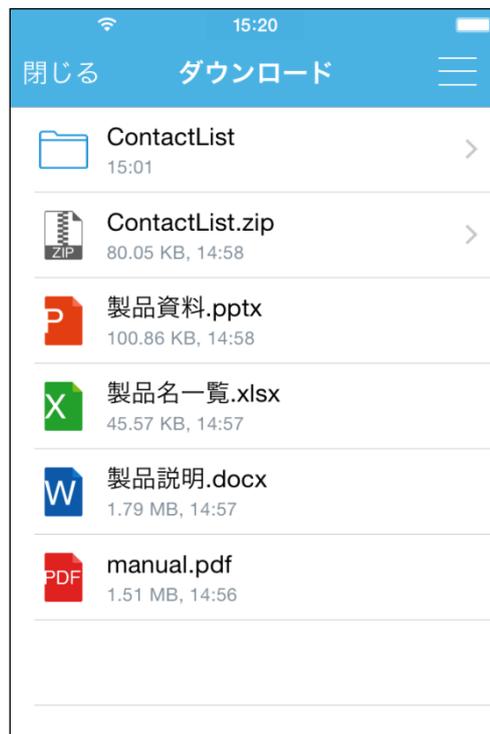


図 2.3.4 ダウンロード

3. 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。

3.1 診断情報

SecureBrowser Pro 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。

3.1.1 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。



図 3.1.1 設定画面

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。



図 3.1.2 製品情報画面

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>

3.2 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>

<http://www.desknets.com/cloud/support/>

<障害・メンテナンス情報>

<http://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

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。