Soliton SecureBrowser / WrappingBox サービス サービス仕様書

2023 年 2 月 14 日

株式会社ソリトンシステムズ

目次

はじめに

本書は、株式会社ソリトンシステムズ(以下、当社)が提供する Soliton SecureBrowser / WrappingBox サービス(以下、本サービス)の技術的な情報を記載したものです。本書の内容は、サービスの変更その他に伴い更新する場合があります。常に最新の版をご参照ください。

1. サービスの概要

本サービスは、VPN 機能内蔵のセキュアブラウザ「Soliton SecureBrowser Pro」（ソリトン セキュアブラウザ プロ、以下 SSB Pro)、「Soliton SecureBrowser II」(ソリトン セキュアブラウザ ツー、以下 SSB II) により、「社内へのリモートアクセス環境」、「クラウドアクセスのセキュリティ強化」、「端末からの情報漏えいの防止」の3つを同時に実現します。また、アプリケーションラッピングソフトウェア「WrappingBox」により、端末にデータを残さず保護領域内で Office などを用いたファイル編集を行うことができます。デジタル証明書による強固な端末認証、端末に Web アプリの閲覧ファイルやキャッシュなどのデータを残さない仕様により、社内やクラウドの Web アプリを安全に利用できます。

1-1. サービス提供条件

本サービスは下記の条件で提供します。

項目	内容
提供エリア	日本国内
データ保管先	日本国内のデータセンターにて保管・運用
サービス提供時間	24 時間 365 日、但しメンテナンスによる停止あり
稼働監視	24 時間 365 日、但しメンテナンス中は対象外
ライセンス	Soliton SecureBrowser / WrappingBox サービス実施要領別紙「10.ライセンス」を参照

1-2. アクセスログ

本サービスのアクセスログを下記の条件で提供します。

項目	内容
提供方法	サービスポータルからのダウンロード提供
ログの配置場所	サービスポータル上の「各種資料」の「マイフォルダ」の「Log」フォルダ内
保管期間	90 日
ログに記録される情報	SSB Pro /SSB II / WrappingBox からのアクセスに関するログ。

1-3. 通知

障害やメンテナンスに関する通知を下記の通り行います。

通知の種類	通知する条件	通知目標時間	通知方法
障害	サービス停止、性能低下などの影響が広範に生じた場合に通知	障害検知から 120 分以内	サービスポータルまたはメール
メンテナンス	サービスへの影響を伴うメンテナンスを行う場合に通知	原則 10 日前まで	サービスポータルまたはメール
緊急メンテナンス	緊急メンテナンスの実施時	なるべく早く	サービスポータルまたはメール

2. サービスのセキュリティ

2-1. 通信の暗号化

下記、本サービスに対する通信は、暗号化が行われます。

- SSB Pro / SSB II / WrappingBox から当社クラウドサービスへの接続
- Soliton KeyManager からの証明書取得・更新時のユーザーID、パスワード認証
- サービスポータルへの接続

2-2. ユーザー認証

各端末から本サービスへの接続では、すべて認証が必要です。認証の方式は下記の通りです。

接続の種類	認証の方式
SSB Pro / SSB II から SSG への接続	証明書によるクライアント認証※
WrappingBox から SSG への接続	証明書によるクライアント認証※
Soliton KeyManager からの証明書取得・更新	ユーザーID、パスワード認証
サービスポータルへの接続	ユーザーID、パスワード認証

※ イントラプランをご利用の場合、お客様環境の Active Directory や NetAttest EPS との連携によるユーザーID、パスワード認証を追加設定できます。

2-3. 証明書

本サービスに接続する SSB Pro、SSB II または WrappingBox を使用する端末（PC、スマートフォン等）には、本サービスで発行する証明書をインストールする必要があります。
本サービスで発行する証明書の仕様は下記の通りです。

（クラウドプラン / クラウド・イントラプラン）

項目	内容
証明書発行枚数	1 ユーザーアカウントあたり 4 枚まで
証明書の取得方法	サービスポータルから p12 ファイルをダウンロードして取得
証明書の有効期限	2030 年 12 月 31 日
証明書の失効	当社サポートページよりお申込みください。証明書番号を指定して失効可能です。失効作業には時間を要することがあります。 （目安： 1～3 営業日）。

（Plus クラウドプラン / Plus クラウド・イントラプラン）

項目	内容
証明書発行枚数	1 ユーザーアカウントあたり 4 枚まで
証明書の取得方法	Soliton KeyManager ソフトウェアにより取得
証明書の有効期限	2030 年 12 月 31 日
証明書の失効	サービスポータルの証明書管理より任意のタイミングで証明書を失効可能

2-4. ユーザーID とパスワード

Plus クラウドプラン / Plus クラウド・イントラプランの証明書取得時に使用するユーザーID と初期パスワードは当社で発行し、サポートポータルからのダウンロードにより提供します。ご利用に際してはサポートポータルからパスワード変更サイトに接続し、初期パスワードから変更して使用してください（ユーザーID は変更できま

せん)。
クラウドプラン / クラウド・イントラプランで提供する証明書のインポートパスワードは変更できません。

2-5. データの暗号化
本サービスシステム内のパスワードは暗号化されています。その他のデータは暗号化されていません。

3. サービス導入時の確認事項
本サービスの導入に際しては、下記の条件をご確認ください。

3-1. サービス指定ソフトウェア
本サービスを使用する PC、スマートフォンに、下記のソフトウェアをインストールする必要があります。

種別	サービス指定ソフトウェア名
Soliton SecureBrowser 端末	SSB Pro または SSB II
WrappingBox 端末	WrappingBox
Plus クラウドプラン または Plus クラウド・イントラプラン利用の場合	Soliton KeyManager（証明書配布ソフトウェア）

サービス指定ソフトウェアがサポートする OS、サポート対象バージョンに関して下記の情報をご確認ください。
マルチデバイス製品　サポート OS 一覧
https://www.soliton.co.jp/support/sms_supportos.html
クラウドサービスのサポートポリシー
https://www.soliton.co.jp/support/support_policy/support_policy_cloud.html

3-2. 使用する通信
本サービスの利用に必要な通信は下記の通りです。必要な通信が行えるようにファイアウォールの設定変更等を行って頂く必要があります。

通信元	通信先	プロトコル、ポート
SSB Pro (Windows / macOS / Android / iOS)	アカウント通知書に記載の「クライアント接続先」	45443/tcp
SSB II (Windows)	アカウント通知書に記載の「クライアント接続先」	45443/tcp
SSB II (iOS)	アカウント通知書に記載の「クライアント接続先」	45443/tcp 4500/udp 500/udp
WrappingBox (Windows)	アカウント通知書に記載の「クライアント接続先」	45443/tcp
※Plus クラウドプラン / Plus クラウド・イントラプランの場合 Soliton KeyManager (Windows / macOS / Android / iOS)	アカウント通知書に記載の 「証明書配布サイト」	80/tcp 443/tcp 5467/tcp
※クラウド・イントラプラン /	160.239.32.1	4500/udp

Plus クラウド・イントラプランの場合、またはファイルサーバーアクセスオプションを使用する場合 レンタルコネクタ	160.239.32.2	500/udp
※レンタルコネクタ+DR オプションを使用する場合 レンタルコネクタ	210.152.10.72 210.152.10.255	4500/udp 500/udp

3-3. プロキシ利用に関する注意

Plus クラウドプラン / Plus クラウド・イントラプランにおいて、Soliton KeyManager から本サービスへの通信がプロキシサーバーを経由する場合、プロキシサーバーによっては正しく動作しない場合があります。

3-4. 管理コンソールに関する特記事項

本サービスでは管理コンソールの設定のうち下記画面からの操作のみを許可しています。その他の画面へのリンクをクリックした場合、エラー画面が表示されます。

- トップページ - 信頼する認証局
- トップページ - 証明書失効リスト
- サービス - SecureGateway
- サービス -プロファイル
- サービス -ユーザー情報
- サービス -プロキシサーバー

3-5. SSB II に関する特記事項

iOS 版 SSB II で SecureGateway に接続する際の VPN 接続にて、172.30.0.0/16 のネットワークアドレスを使用します。このため、お客様ネットワークではこの範囲の IP アドレスを使用できません。

3-6. イントラプランに関する特記事項

1) クラウド・イントラプランおよび Plus クラウド・イントラプランにて接続する各種サーバーについて、以下の登録数を上限とします。

項目	登録数の上限
社内 Web サーバー	10
認証サーバー	2
プロキシサーバー	2

3-7. レンタルコネクタに関する特記事項

1) クラウド・イントラプラン、Plus クラウド・イントラプラン、ファイルサーバーアクセスオプションのいずれか、または組み合わせて契約する場合、お客様ネットワークに VPN 接続用機器（以下、レンタルコネクタ）を設置いただき、当社クラウドネットワークとお客様ネットワークを VPN 接続します。
2) サービス開始時、設定済みのレンタルコネクタを 2 台送付します。
   ※2 台のレンタルコネクタには、アクティブ-スタンバイ冗長化を設定しています。
   ※トライアル期間中は、レンタルコネクタは 1 台のみ送付します。トライアルから正式サービスに移行する際に 2 台目を追加送付します。
3) レンタルコネクタ設置環境と当社クラウドネットワークとの通信に使用するインターネット接続には、安定

した常時接続回線を使用する必要があります。特にファイルサーバーアクセスオプションを使用する場合、通信量に応じた十分な帯域を確保する必要があります。

3-8. ファイルサーバーアクセスオプションに関する特記事項

1) ファイルサーバーアクセスオプションでは、SSF へのログイン認証、ファイルサーバーへのアクセスについて ActiveDirectory と連携する構成を前提にしています。このため、連携先のファイルサーバーが ActiveDirectory ドメインに参加している必要があります。
2) SSF ではアップロード/ダウンロードのタイムアウトが 15 分に設定されています。このため、ファイルのアップロードやダウンロードに 15 分以上要する場合、そのアップロード/ダウンロードは失敗します。
3) SSF とファイルサーバー間にてインターネット回線と VPN 接続を経由するため、ローカル環境からファイルサーバーにアクセスする場合と比べてアップロード/ダウンロードに時間を要します。このため、ファイルのサイズやその時の回線速度によって、アップロード/ダウンロードに失敗することがあります。
4) 本オプションのライセンスは、1 ライセンスあたり SSF1 台となります。SSF1 台あたり、以下の登録数を上限とします。

項目	上限値
ファイルサーバー登録数	10
共有フォルダー登録数	2000
同時接続数	200

※上記の登録数で動作することを保証するものではありません。また、ソフトウェア的には登録数を制限していません。

5) SSF に iOS 版または Android 版 SSB Pro、SSB II を用いてアップロードする場合、1 ファイルずつアップロードする必要があります。Windows 版 SSB Pro、SSB II からアップロードする場合は、複数ファイルを同時にアップロードできます。
6) SSF の連携先ファイルサーバーは、Windows ファイルサーバーとします。Windows 以外のファイルサーバー、NAS (Windows Storage Server / Windows Server IoT 搭載製品含む) などは利用できません。
7) SMB のバージョンはデフォルトでは 2.1 に設定されています。1.0 または 3.0 への変更が可能ですが、同時に 2 つ以上のプロトコルを設定することはできません。また、SMB のオプション機能はサポートしていません。

3-9. DR オプションに関する特記事項

1) DR オプションを契約すると、ソリトンクラウド東日本 DC(以下、東日本 DC) に設置されているゲートウェイ（SSB Pro、SSB II または WrappingBox の接続先）のサービスを 300 秒間隔で監視し、6 回連続で応答がなかった場合に、接続先がソリトンクラウド西日本 DC（以下、西日本 DC）のゲートウェイに自動的に変更されます（お客様による変更作業等は必要ありません）。切り替え発生時は、メールおよびポータルサイトで通知を行います。
2) 西日本 DC にてサービス提供中、東日本 DC のゲートウェイが復旧した場合、当社作業により東日本 DC への切り戻しを行います（お客様による作業は必要ありません）。切り戻し時は、メールおよびポータルサイトで通知を行います。
3) 西日本 DC のゲートウェイの設定は、DR オプションお申込み時点で東日本 DC のゲートウェイに設定されている内容に基づいて構成します。それ以降にゲートウェイの設定変更を行う場合は、西日本 DC のゲートウェイにも同様の設定を行って頂く必要があります（変更内容は自動で反映されません）。西日本 DC のゲートウェイの設定変更は、ポータルサイトの「管理コンソール(DR オプション)」から行えます。
4) 管理ポータルの各設備は東日本 DC にて運用されているため、東日本 DC の障害中は管理ポータルを使用できません（ゲートウェイの設定変更もできません）。
5) Plus クラウドプランおよび Plus クラウド・イントラプランの証明書発行システムは東日本 DC で運用され

ているため、東日本 DC 障害中は、証明書の新規取得、証明書の失効はできません。配布済みの証明書を使用したアクセスは可能です。

6) 西日本 DC 内ネットワークにて 172.31.200.0/24-172.31.254.0/24 を使用しています。このため、各種イントラプラン、ファイルサーバーアクセスオプションで使用する VPN 装置（レンタルコネクタ）経由で通信する各機器では、この範囲の IP アドレスを使用できません。
7) 西日本 DC のゲートウェイは、東日本 DC の障害時にのみ接続できます。このため、本オプションを東日本 DC/西日本 DC のゲートウェイを同時に使用して負荷分散させるなどの目的には使用できません。