SmartOn ID クラウド

サービス仕様書

2025 年 11 月 5 日

株式会社ソリトンシステムズ

目次

はじめに 3
1. サービスの概要 3
1-1. サービス提供条件 3
1-2. 通知 3
2. サービスのセキュリティ 3
2-1. 通信の暗号化 3
2-2. ユーザー認証 3
2-3. ユーザーID とパスワード 4
2-4. データの暗号化 4
3. サービス導入時の確認事項 4
3-1. サービス指定ソフトウェア 5
3-2. 使用する通信 6
3-3. レンタル VPN ルーターに関する特記事項 6

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 SmartOn ID クラウド（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、下記の機能を提供します。

- IC カードや生体情報などを利用した多要素認証により PC ログオン時の認証を強化する機能
- PC ログオン後のデスクトップ環境を制限する機能

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	SmartOn ID クラウド サービス実施要領別紙　「10.ライセンス」を参照

1-2. 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	メールおよびサービスポータル
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	メールおよびサービスポータル
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	メールおよびサービスポータル

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。

- SmartOn ID クライアント、SmartOn ID マネージャーおよび各種生体情報登録ツールから ACL サーバー、ログサーバーへの接続
- 各種生体情報登録ツール、インポート・エクスポートツールから ACL サーバーへの接続
- ドキュメントポータルへの接続

2-2. ユーザー認証

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

SmartOn ID マネージャー/各生体認証情報登録ツール

接続の種類	認証の方式
ツール起動時の管理者アカウント認証	ユーザーID/パスワード認証、IC カード認証、各生体認証

SmartOn ID クライアント

接続の種類	認証の方式
PC ログオン時認証	ユーザーID/パスワード認証、IC カード認証、各生体認証

ドキュメントポータル

接続の種類	認証の方式
ログオン時認証	パスワード認証

2-3. ユーザーID とパスワード

SmartOn ID マネージャー/各生体認証情報登録ツール　ログオンアカウント（管理者アカウント）

項目	内容
用途	ACL サーバーへの接続 SmartOn ID マネージャー/各生体認証情報登録ツールからは、管理者用メニューにアクセスできます。
発行方法	当社より管理者アカウントを発行します。 その他、管理者用メニューからアカウントの作成や管理者向けロール設定の追加が可能です。
パスワードポリシー	申し込み時にいただいたパスワードポリシーを当社にて設定します。

利用者アカウント

項目	内容
用途	クライアント PC のログオン認証に使用します。
発行方法	お客様管理者が管理画面からユーザーを追加して発行します。
パスワードポリシー	申し込み時にいただいたパスワードポリシーを当社にて設定します。

ドキュメントポータル

項目	内容
用途	ドキュメントポータルのログオン認証に使用します。
発行方法	当社よりパスワードを発行します。
パスワードポリシー	8 文字以上

2-4. データの暗号化

本サービスで ACL サーバーに暗号化して保存されるデータは以下の通りです。

- SmartOn パスワード
- Windows アカウント名/パスワード
- IC カード情報
- 生体認証情報
- その他、本サービスを利用するために必要な設定情報

またドキュメントポータルのパスワードも暗号化して保存されています。

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

本サービスのサービス指定ソフトウェアは下記の通りです。

サービス指定ソフトウェア名	機能
SmartOn ID マネージャー	本サービスに登録されている情報を操作するための管理ツールです。 ユーザー情報やディスク情報の 登録、SmartOn ID クライアントのインストールディスク発行などの操作を行います。
SmartOn ID クライアント	本サービスを利用する PC 等にインストールするクライアントソフトウェアです。SmartOn ID マネージャーでインストールディスクを発行して使用します。
SONY PaSoRi(パソリ) ドライバ	SONY 社製 IC カードリーダーPaSoRi を利用する際にインストールするドライバです。
AB Circle 各種デバイス(SO-SOL215A-D/SO-SOL215C-D) ドライバ	AB Circle 社製 IC カードリーダーを利用する際にインストールするドライバです。
生体認証ランタイム(指ハイブリッド/DigitalPersona/顔認証/指静脈認証)	各種生体認証を行う際にインストールするランタイムです。
SmartOn ID Pass Extension for Chrome/Edge	SmartOn Pass 機能のブラウザ認証を Google Chrome/Microsoft Edge で使用する場合に必要な拡張機能です。
SmartOn ID Pass Extension for Firefox	SmartOn Pass 機能のブラウザ認証を Mozilla Firefox で使用する場合に必要な拡張機能です。
SmartOn ID インポート・エクスポートツール	CSV ファイルに設定した情報を、ACL サーバーに設定、変更する、または ACL サーバーに設定されている情報を CSV ファイルに出力する際に使用するツールです。
SmartOn QR	顔認証と組み合わせ、PC ログオン時の強固な二要素認証を実現する iOS/Android アプリケーションです。
Authentication Redirector	SmartOn ID 環境でのリモートデスクトップ接続および、SmartOn ID for リモートアクセス環境で、生体認証を使用してリモートログオンを行う際に必要となるコンポーネントです。
SmartOn ID ログビューアー	SmartOn ID ログサーバーから出力される CSV 形式のクライアントログを GUI で閲覧できるツールです。
指ハイブリッド認証情報登録ツール	SmartOn ID クライアントのログオン/ロック解除認証時に使用する指ハイブリッド認証情報を取得し、ACL サーバーに登録するためのツールです。
指紋認証情報登録ツール(DigitalPersona Reader)	SmartOn ID クライアントのログオン/ロック解除認証時に使用する指紋認証情報を取得し、ACL サーバーに登録するためのツールです。
顔認証情報登録ツール	SmartOn ID クライアントのログオン/ロック解除認証時に使用する顔認証情報を取得し、ACL サーバーに登録するためのツールです。
指静脈認証情報登録ツール	SmartOn ID クライアントのログオン/ロック解除認証時に使用する指静脈認証情報を取得し、ACL サーバーに登録するためのツールです。

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。

SmartOn ID クラウド 動作環境
https://www.soliton.co.jp/products/smarton/specification.html

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	ポート、プロトコル
レンタルVPNルーター	アカウント通知書に記載の「VPNルーター接続先」	4500/udp、500/udp

3-3. レンタルVPNルーターに関する特記事項

SmartOn ID クラウド　サービス実施要領別紙内、レンタルVPNルーターに関する特記事項の項をご参照ください。