Soliton OneGate

サービス仕様書

2026 年 10 月 26 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. アクセスログ 3
1-3. 通知 3
2. サービスのセキュリティ 4
2-1. 通信の暗号化 4
2-2. ユーザー認証 4
2-3. 証明書 4
2-4. ユーザーID とパスワード 4
2-5. データの暗号化 5
2-6. バックアップ 5
3. サービス導入時の確認事項 6
3-1. サービス指定ソフトウェア 6
3-2. 使用する通信 7
3-3. WebSocket に関する注意 8
3-4. IPv6 対応に関する情報 8
3-5. 顔認証オプションに関する留意事項 8

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 OneGate 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、デジタル証明書による多要素認証（MFA）でクラウドに点在する企業の情報資産を不正アクセスから守る、ID 認証サービスを提供します。機能の詳細は、当社 Web サイト 製品紹介ページの機能一覧をご参照ください。

Soliton OneGate　製品紹介ページ

https://www.soliton.co.jp/lp/onegate/

顔認証機能は、パナソニック コネクト株式会社が提供する KPAS クラウドとの連携により実現しています。顔認証オプションの利用に際しては、KPAS クラウド サービス仕様書を併せて参照してください。

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 OneGate サービス実施要領別紙「10.ライセンス」を参照 ※Soliton OneGate for LE、Soliton OneGate for Education の場合、Soliton OneGate for LE 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	サービス管理画面より閲覧・ダウンロード可能
ログの配置場所	「Soliton OneGate 管理者マニュアル」を参照
保管期間・容量等	90 日間（184 日に延長可能、申し込みが必要）
ログに記録される情報	「Soliton OneGate 管理者マニュアル」を参照
ログのタイムゾーン	日本標準時 (JST)
参照する NTP サーバー	time.google.com

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	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。

- Web ブラウザ、サービス指定ソフトウェアから本サービスへの接続
- NetAttest EPS-edge、NetAttest EPS、NetAttest D3（SX06 モデル）から本サービスへの接続
- Soliton KeyManager からの証明書取得・更新

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。

接続の種類	認証の方式
Web ブラウザからサービス管理ページへの接続（管理者からのアクセス）	ユーザーID/パスワード認証、サービスポータルからのシングルサインオン ※ 設定により証明書によるクライアント認証を追加可能
Web ブラウザや連携サービスアプリからログインサービスへの接続（利用者からのアクセス）	ユーザーID/パスワード認証 ※ 設定により証明書によるクライアント認証、統合 Windows 認証、FIDO2 認証、Soliton Authenticator 認証、IC カード認証、顔認証、外部 IdP 認証を追加可能
Soliton KeyManager からの証明書取得・更新	ユーザーID/パスワード認証
Web ブラウザからサービスポータルページへの接続（管理者からのアクセス）	ユーザーID/パスワード認証（2 ステップ認証必須）、Soliton Authenticator 認証

2-3. 証明書

本サービスに接続する Web ブラウザ（証明書認証利用時のみ）、およびサービス指定ソフトウェアを使用する端末には、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。

証明書の種類	発行枚数	取得方法
ユーザー証明書	1 ユーザーアカウントあたり 10 枚まで	Soliton KeyManager ソフトウェアにより取得 サービス管理ページからダウンロード Web ブラウザによる取得（iOS/iPadOS）
連携クライアント用証明書	無制限	サービス管理ページからダウンロード

本サービスで発行した証明書の失効は、証明書管理画面から任意のタイミングで行えます。

2-4. ユーザーID とパスワード

サービスポータルログインアカウント（管理者アカウント）

項目	内容
用途	サービスポータルページへの接続 サービスポータルからは、サービス管理ページ、ドキュメントダウンロード等にアクセスできます。
発行方法	当社で申し込み時に指定いただいたメールアドレスをもとに ID を発行します。 利用開始時にパスワードの設定が必要です。
パスワードポリシー	8～64 文字、大文字/小文字/数字/記号から 3 種類以上

サービス管理ページログインアカウント（管理者アカウント）

項目	内容
用途	サービス管理ページへの接続
発行方法	申し込み時に指定いただいたメールアドレスをもとに ID を発行します。 パスワード認証を使用する場合は、利用開始時に必ずパスワード変更をしてください。 サービス管理ページのログインアカウントは、サービス管理ページから管理者権限で登録や変更が行えます。
パスワードポリシー	10～256 文字

利用者アカウント

項目	内容
用途	クラウドサービス、Wi-Fi/VPN などのログイ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登録して発行します。 AD 連携機能を利用して、Active Directory との同期により発行します。
パスワードポリシー	8～64 文字、大文字/小文字/数字/記号から 3 種類以上

2-5. データの暗号化

本サービスシステムのデータを保存しているストレージは、Google Cloud の機能により暗号化されます。暗号の仕様は、Google 社が提供する Google Cloud セキュリティ ホワイトペーパーを参照してください。
クラウドサービス利用者のデータは、テナント毎に固有の鍵を使用して暗号化します。テナントデータの暗号化に際しては、テナント作成時に自動的に生成した暗号鍵を使用します。また、テナント削除時はそのテナントの暗号化に使用した暗号鍵も削除し、データを復号できないようにします。
本サービスシステム内のパスワード情報はすべてハッシュ化または暗号化して保存します。

2-6. バックアップ

本サービスシステムでは、下記の仕様によりバックアップを実施しています。

対象データ	バックアップの実施タイミング	データ保管先
テナントのデータ（ユーザーデータを含む）	毎日 4:00	Google Cloud ※東京・大阪リージョンの冗長化されたディスク

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
Soliton KeyManager	本サービスからの証明書取得・更新に使用します。
Soliton PasswordManager	本サービスに保存された ID/パスワード情報を取得し、Web アプリやネイティブアプリのログイン時に自動入力を行います。
Soliton Authenticator	ユーザーの指紋、顔、PIN などスマートフォンのセキュリティを利用して本サービスへのログインを行うスマートフォンアプリです。
Soliton CardReader	IC カード認証を利用して本サービスへのログインを行うスマートフォンアプリです。
Soliton OneGate Updater	新しいモジュールの有無を定期的に本サービスに確認するアプリです。
Soliton SecureBrowser for OneGate	セキュアブラウザー機能を持つ Web ブラウザーアプリケーションです。
Soliton ADConnector	AD 連携機能利用時、本サービスと Active Directory とを同期させるためのソフトウェアです。複数台にインストールすることで冗長構成とすることができます。
CRL Uploader	NetAttest EPS などの外部認証局との連携時に、認証局の登録と失効リストの同期を行うためのソフトウェアです。
OneGate SSO Manager	PasswordManager による代理入力を利用するアプリケーションを登録・設定する際に使用します。
カード情報登録ツール	IC カードリーダーから IC カード情報を読み取って、本サービスの IC カード管理画面でインポートする CSV ファイルを作成します。

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。

Soliton OneGate 動作環境
https://www.soliton.co.jp/products/onegate/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
PC (利用者端末)	OneGate サービス ※	80/tcp 443/tcp
	Soliton OneGate Updater 用モジュール配信サーバー	443/tcp
	OneGate 共通システム (common-system.ids-s.soliton-ods.jp)	443/tcp
	https://cdn.felica-support.sony.biz ※ICカード認証を利用する場合に必要	443/tcp
サーバー（Soliton ADConnector）	OneGate サービス ※	443/tcp
	OneGate 共通システム (common-system.ids-s.soliton-ods.jp) ※V1.13.x 以降	443/tcp
	ドメインコントローラー	88/tcp 88/udp 389/tcp 389/udp 445/tcp 636/tcp
EPS-edge	OneGate サービス ※	80/tcp 443/tcp 636/tcp（PAP を使用する場合）
	OneGate 共通システム (common-system.ids-s.soliton-ods.jp)	443/tcp
	NTP サーバー (time1.google.com / time2.google.com)	123/udp
	任意の DNS サーバー	53/udp
	（外部 CA を使用する場合） 失効リスト公開サーバー	80/tcp
	ファームウェア配信サーバー	443/tcp
RADIUS クライアント（無線アクセスポイントなど）	EPS-edge	1812/udp
PC（管理者端末）	サービスポータルページ (service-portal.soliton-ods.jp) ポータル IDP (service-portal.ids.soliton-ods.jp)	443/tcp

	サービスポータル API (service-portal-api.soliton-ods.jp)	
OneGate サービス （ログ転送オプション） 34.84.192.13 34.85.96.138 34.146.150.58 34.146.231.113 34.146.242.62 34.97.195.240 34.97.72.232 34.97.246.135 34.97.243.163 34.97.92.18	外部 syslog サーバー	任意ポート/tcp
NetAttest EPS NetAttest D3	OneGate サービス ※	443/tcp

※ OneGate サービスは、テナントごとに異なる下記 2 つのホストにより提供します。
（テナントコード）.ids.soliton-ods.jp　管理サービス、ログインサービスおよび利用者ポータルを提供します。
（テナントコード）.ids-s.soliton-ods.jp　証明書認証利用時の管理サービス、ログインサービスおよび利用者ポータルを提供します。

テナントコード確認方法：
Soliton Cloud Service Portal（https://service-portal.soliton-ods.jp）にログインし、「サービス管理」タブにて Soliton OneGate の管理ページへのリンクをクリックしてください。
管理ページの URL は下記の形式です。（テナントコード）の箇所でテナントコードを確認できます。
https://（テナントコード）.ids.soliton-ods.jp

3-3. WebSocket に関する注意

Soliton ADConnector や NetAttest EPS-edge、NetAttest EPS、NetAttest D3 は、「WebSocket」の仕組みを利用して Soliton OneGate と相互通信を行っています。
インターネットへの接続にプロキシサーバーが必要な環境では、WebSocket をサポートしていることを確認した上で、プロキシ設定を行ってください。プロキシサーバーが WebSocket をサポートしていない場合、プロキシの除外となるように構成してください。

3-4. IPv6 対応に関する情報

Soliton OneGate は IPv6 に対応していません。

3-5. 顔認証オプションに関する留意事項

顔認証機能は、パナソニック コネクト株式会社が提供する KPAS クラウドとの連携により実現しています。顔認証に使用する顔画像、顔特徴量などの KPAS クラウド上のデータに関して、当社が KPAS クラウド上から取得したり、当社にて保管したりすることはありません。万一 KPAS クラウド上のデータが破損、消失した場合、利用者自身で顔認証情報を再登録する必要が生じます。顔認証情報は登録後も保管することを推奨します。
オフラインログインを有効にしている場合、顔認証成功時に顔特徴量データを端末内に暗号化して保存します。