NetAttest EPS Cloud

サービス仕様書

第２版　2021 年２月１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 NetAttest EPS Cloud (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、無線 LAN など 802.1x 対応機器との連携によるクライアント証明書を用いた認証（EAP-TLS）機能、証明書の発行・配布・失効を含む管理機能を提供します。

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。

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	1 ライセンス契約につき、1 ユーザーが利用可能 最小ライセンス数は 100、最大ライセンス数は 2000 1 ユーザーID あたりの証明書発行枚数制限あり(申込み時に指定可能、最大 4 枚)

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。

提供方法	サービスポータルからダウンロード提供
ログの配置場所	サービスポータル上の「epsxxxxxx」-「Log」フォルダ内 (xxxxxx はサポート ID) ※サービスポータルの「ログ閲覧」からも閲覧可能
保管期間・容量等	30 日分
ログに記録される情報	認証成功・失敗、証明書取得に関するログ。詳細は NetAttest EPS Cloud ログ閲覧マニュアルを参照

1-3. 各種オプション

以下のオプションを追加できます。

オプション名称	サービス内容
社内冗長オプション	お客様環境に設置する NetAttest EPS(子機)を貸出するオプション 本オプションにより、ネットワーク障害などにより NetAttest EPS Cloud に通信できない状態でも認証が可能になります。

1-4. 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

本サービスに対する下記の通信は、暗号化が行われます。

- 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。

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

2-3. 証明書

本サービスに接続する Soliton KeyManager 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。

証明書発行枚数	申込み時に 1 ユーザーあたりの証明書発行枚数を選択可能（最大 4 枚）
証明書の取得方法	Windows / macOS /Android の場合、Soliton KeyManager ソフトウェアにより取得 iOS / iPadOS の場合、Safari（OS 標準ブラウザ）により取得
証明書の有効期限	2030 年 3 月 31 日
証明書の失効	サービスポータルの証明書管理画面から証明書を失効可能 ※失効は、翌日 0 時 0 分に反映します

2-4. ユーザーID とパスワード

管理者アカウント

用途	サービスポータルへの接続 ※サービスポータルから、各管理画面、ドキュメントダウンロード、問い合わせ等が行えます
発行方法	当社で ID、初期パスワードを発行し、申し込み時に指定いただいたメールアドレスにアカウント通知を送付 ※利用開始時に必ずパスワード変更をしてください。
パスワードポリシー	6 文字以上(英数字)

利用者アカウント

用途	サービス利用時のログイン
発行方法	当社で ID、初期パスワードを発行し、ドキュメントポータルから一覧をダウンロード提供 ※利用開始時に必ずパスワード変更をしてください。 ※ID は指定もできます。「NetAttest_EPSCloud ユーザーID 指定及び RADIUS_IP 制限_申請フォーマット」(サービスポータルよりダウンロード提供)によりお申込みください。
パスワードポリシー	6 文字以上(英数字)

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情報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。

2-6. RADIUS クライアントの IP アドレス制限

本サービスへアクセスする RADIUS クライアントの IP アドレス(グローバル IP アドレス)制限を行うことが可能です。

「NetAttest_EPSCloud ユーザーID 指定及び RADIUS_IP 制限_申請フォーマット」(サービスポータルよりダウンロード提供)によりお申込みください。

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。

サービス指定ソフトウェア名	機能
Soliton KeyManager （ Windows / macOS / Android の場合）	サービスシステムからの証明書取得・更新に使用します。サービスシステムを利用するすべての端末にインストールする必要があります。

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
PC (Soliton KeyManager または Safari)	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
RADIUS クライアント（無線アクセスポイントなど）	アカウント通知書に記載の 「RADIUS サーバー（メイン）」 「RADIUS サーバー（バックアップ）」	アカウント通知書に記載の 「認証用ポート」 「アカウンティングポート」
※社内冗長オプションを使用する場合 レンタルコネクタ	210.140.43.141	4500/udp 500/udp

3-3. プロキシ利用に関する注意

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。