NetAttest LAP Managed by cloud

サービス仕様書

第 3 版　2022 年 1 月 24 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 LAP Managed by cloud 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 IPv4 ネットワーク接続端末の可視化と不正端末の接続防止を実現します。お客様環境に設置する機器（LAP Sensor）が ARP や DHCP のパケットを監視し、端末の IP や MAC アドレスなどを一覧化します。また、クラウド提供の管理サービス(LAP Manager Cloud)にて LAP Sensor の検知端末情報、接続を許可する端末のホワイトリストの集中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	本サービスは、下記 2 種類のライセンスの組み合わせにより提供します。 ・LAP Manager cloud 期間ライセンス 契約した期間、LAP Manager cloud を使用できます。 ・LAP Sensor 期間ライセンス 契約した期間、契約した台数の LAP Sensor を LAP Manager cloud に接続して使用できます。

1-2. 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
LAP Sensor 予備機	LAP Sensor の予備機を購入できます。 ※予備機は、通常時は LAP Manager Cloud に接続できません。LAP Sensor 故障時の交換用として、電源を入れない状態で保管してください。 ※予備機の購入数は、契約中の LAP Sensor 年間ライセンスの数を上限とします。

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

本サービスに対する下記の通信は、暗号化が行われます。

・LAP Sensor から当社クラウドサービスへの接続
・ブラウザから LAP Manager cloud サービスページへの接続
・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には認証が必要です。認証の方式は下記の通りです。

ブラウザからLAP Manager cloud サービスページへの接続	・ユーザーID、パスワード認証 ・メール認証トークンによる 2 段階認証 (オプション)
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. ユーザーID とパスワード

スーパーユーザーアカウント

用途	LAP Manager cloud サービスページにログインし、管理者アカウントの作成、カテゴリの作成を行うアカウントです。
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します。 ※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	8 文字以上 64 文字以下で半角英小文字、半角英大文字、数字、記号のうち 3 種類以上を含める必要があります。また、ユーザーID に含まれるフレーズは使用できません。

管理者アカウント

用途	MAC アドレスのリストの管理及び割り当てられたカテゴリ内に限り、LAP Sensor の設定、管理を行うアカウントです。
発行方法	スーパーユーザーアカウントにて LAP Manager cloud サービスページにログインして発行します。
パスワードポリシー	8 文字以上 64 文字以下で半角英小文字、半角英大文字、数字、記号のうち 3 種類以上を含める必要があります。また、ユーザーID に含まれるフレーズは使用できません。 ※アカウント作成時にパスワードが自動生成されます。

閲覧のみアカウント

用途	割り当てられたカテゴリ内に限り、検知情報の確認を行うアカウントです。
発行方法	スーパーユーザーアカウントにて LAP Manager cloud サービスページにログインして発行します。

パスワードポリシー	8 文字以上 64 文字以下で半角英小文字、半角英大文字、数字、記号のうち 3 種類以上を含める必要があります。また、ユーザーID に含まれるフレーズは使用できません。 ※アカウント作成時にパスワードが自動生成されます。

3. サービス導入時の確認事項

3-1. 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	アカウント通知書に記載の 「LAP Manager cloud サービスページ」	443/tcp
PC	LAP Sensor	80/tcp (システム管理ページ)
PC	LAP Sensor	8080/tcp (拒否端末用通知ページ)
LAP Sensor	アカウント通知書に記載の 「LAP Manager cloud サービスページ」	443/tcp
LAP Sensor	Syslog サーバー ※	514/udp
LAP Sensor	DNS サーバー ※	53/udp
LAP Sensor	メールサーバー ※	25/tcp (SMTP) 465/tcp (SMTP over SSL) 587/tcp (STARTTLS)

※ Syslog サーバー、DNS サーバー、メールサーバーについてはお客様にてご用意ください。

3-2.端末検知と通信制御に関する制限事項

本サービスでは、LAP Sensor が設置されているネットワークセグメント上の ARP 通信を解析し、ブロック対象の端末からの ARP に対して偽装応答を行うことで通信制御します。このため、下記は制限事項となります。

1) 通信パケットは LAP Sensor を通過しません。LAP Sensor は直接通信をフィルタリングする製品ではありません。
2) LAP Sensor による通信制御は、ユニキャスト通信に効力を発揮します。マルチキャスト、ブロードキャスト通信には影響しません。
3) LAP Sensor による通信制御は、MAC アドレスベースで動作します。外付け LAN アダプタ等の MAC アドレスを正規端末として登録してしまうと、その LAN アダプタを別の端末に搭載しても通信が可能になります。したがって、不正端末接続防止のために本サービスを使用する場合、外付け LAN アダプタの使用を禁止することが前提となります。
4) 端末の仕様によっては、本サービスでの可視化および通信制御の機能が動作しない場合があります。また、現在本サービスでの可視化および通信制御が機能している環境でも、通信デバイスまたは OS のアップデート等に伴う仕様変更によって、動作が変わる可能性があります。当社は、端末環境の変化に伴う問題が生じた場合、調査および対策検討につとめますが、すべての端末環境に対して本サービスが有効に機能することを保証するものではありません。