お客様各位

株式会社ラプラス・システム
https://www.lapsys.co.jp

Solar Pro ネットワーク認証のセキュリティ対策について

平素は弊社製品をご愛顧賜り誠にありがとうございます。

弊社製品「太陽光発電システム シミュレーションソフトウェア Solar Pro」で使用するネットワーク認証のセキュリティ対策につきまして、下記の通りお知らせいたします。

ご確認のほどよろしくお願い申し上げます。

―記―

【対象製品】

太陽光発電システム シミュレーションソフトウェア Solar Pro ネットワーク認証版

【ネットワーク認証の概要】

ネットワーク認証は、これまで必須だったハードウェアキーの代わりに、インターネットでライセンスの認証を行い Solar Pro を起動できる仕組みです。

ネットワーク認証には、弊社提供サービスの「ラプラス ID」を使用します。

【認証プロセス】

認証は Solar Pro の起動時に行われます。

認証に成功すると、次回以降の起動時には保存された認証情報を使用して自動で認証を実行します。

認証のプロセスの内容は以下の通りです。

Solar Pro に入力された認証情報（ラプラス ID、パスワード）と MachineGUID（Windows インストール時に生成される ID）を使ってラプラス ID サーバとの間で認証を行います。

ラプラス ID サーバで Solar Pro のライセンスを管理しており、ライセンスの割り当てを行います。

割り当て可能なライセンスがある場合に、Solar Pro はライセンス情報を取得します。

【セキュリティ対策】

ラプラス ID サーバとは HTTPS で暗号化（TLS 1.2）し、証明書を用いた通信を行い盗聴やなりすましを防止します。HTTPS 通信はポート番号 443 を使用します。

また、ラプラス ID サーバ（ISO/IEC 27001 認証を取得している AWS を利用）には Firewall が組み込まれており、不要な通信は遮断しています。
ネットワーク認証で利用するユーザに関する情報は認証情報と MachineGUID のみで、PC に情報を保存する際は暗号化します。

Solar Pro－ラプラス ID サーバ間の通信は、Solar Pro からの通信を起点とするため、ラプラス ID サーバやその他のサーバやシステムから直接 Solar Pro と通信することはありません。

＜想定される脅威へのセキュリティ対策＞

①ラプラス ID サーバが外部ネットワークから不正侵入されない対策

想定される脅威	対策内容
不正侵入	不要なサービス、ポートを遮断している。
不正アクセス検知	アクセスログを記録して確認できるようにしている。

②通信のセキュリティ

想定される脅威	対策内容
通信の盗聴・データ改ざん	Solar Pro－ラプラス ID サーバ間の通信は TLS 通信によって暗号化している。

【プロキシサーバ対応】

お客様の環境ではプロキシサーバを介してインターネットと接続する場合があります。
プロキシサーバを使用してネットワーク認証を行う場合、Solar Pro でプロキシの設定が必要です。
デフォルトでは Windows のプロキシ設定を使用するよう設定されています。
認証が必要なプロキシについては、Basic 認証と Digest 認証に対応しており、ID とパスワードの設定が必要です。
※プロキシの設定についてはシステム管理者様にお問い合わせください。

以上