Dear Customer,

Laplace System Co., Ltd.
https://www.lapsys.co.jp/en/

About Security Measures for Solar Pro Network Authentication

Thank you for your continued patronage of our products.

We would like to inform you about the following security measures for the network authentication used in our product **Photovoltaic System Simulation Software Solar Pro**.
Please confirm the information below.

-Note-

◆ Subject product

Photovoltaic System Simulation Software Solar Pro Network Authentication Edition

◆ Overview of network authentication

Network authentication is a mechanism that enables the activation of Solar Pro by conducting license authentication on the Internet, instead of using the previously required hardware key.
A **Laplace ID** which is a service provided by Our Company, is used for network authentication.

◆ Authentication process

Authentication is conducted when Solar Pro is activated.
If authentication is successful, authentication will be automatically executed, at the times of the next and subsequent startups, by using the saved authentication information.
The details of the authentication process are as stated below.
Authentication is conducted with the Laplace ID server by using the authentication information (Laplace ID and password) that is entered into Solar Pro and the MachineGUID (the ID generated at the time of Windows installation).
The Laplace ID server manages Solar Pro licenses and allocates licenses. When there is a license that can be allocated, Solar Pro obtains the license information.

◆ Security measures

The Laplace ID server is encrypted (TLS 1.2) by HTTPS, it communicates by using a certificate, and it prevents eavesdropping and impersonation. HTTPS communication uses Port No. 443.
In addition, the Laplace ID server (using AWS, which has obtained ISO/IEC 27001 certification) has a firewall built in and it blocks unnecessary communication.
The only user information used for network authentication is the authentication information and the MachineGUID, and that information is encrypted when it is stored on the computer.

Communication between Solar Pro and the Laplace ID server starts with communication from Solar Pro, and therefore there is no direct communication with Solar Pro from the Laplace ID server or any other server or system.

◆ Security measures against potential threats

(1) Measures to prevent the Laplace ID from incurring unauthorized intrusion from external networks

Potential threats	Countermeasures
Unauthorized intrusion	Unnecessary services and ports are blocked
Detection of unauthorized access	Access logs are recorded and made available for checking

(2) Communication security

Potential threats	Countermeasures
Eavesdropping on communication and tampering of data	Communication between Solar Pro and the Laplace ID server is encrypted by TLS communication

◆ Proxy server support

Your environment may connect to the Internet through a proxy server.
If network authentication is conducted by using a proxy server, proxy settings are required in Solar Pro.
By default, Windows proxy settings will be used.
For proxies that require authentication, basic authentication and digest authentication are supported, and ID and password settings are required.
*For matters concerning proxy settings, please contact your system administrator.