2024 年 8 月 26 日

お客様各位

株式会社ラプラス・システム
商品部

弊社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。
ご確認の程、よろしくお願い申し上げます。

―記―

【対象製品】

遠隔監視システム＆サービス L・eye および 小型計測端末 Solar Link ZERO

【セキュリティ対策】

1. 発電所 ― 弊社クラウドサーバ間

便宜上、発電所 ― 弊社クラウドサーバ間を下記のブロックに分けて説明させて頂きます。

（1）発電所（パワーコンディショナ）― Solar Link ZERO 間
（2）Solar Link ZERO 内部
（3）Solar Link ZERO ― 弊社クラウドサーバ間

（1）発電所（パワーコンディショナ）― Solar Link ZERO 間

PCS メーカーより開示いただいた独自の通信プロトコルに則ってのみ通信しております。

（2）Solar Link ZERO 内部

Solar Link ZERO へのネットワーク接続時は、内部の Firewall により不要な通信は遮断しております。

（3）Solar Link ZERO ― 弊社クラウドサーバ間

① Solar Link ZERO のデータアップロード方式

HTTPS で暗号化（SSL/TLS）通信を行い、セキュリティで守られています。

② 通信回線（弊社提供の無線回線の場合）

データのアップロードに弊社提供の無線回線を使用する場合、Solar Link ZERO にグローバル IP アドレスは割り当てられていません。

また、インターネット側から直接 Solar Link ZERO にアクセスする方法は提供していないため、IP アドレスを特定しての攻撃は非常に困難です。

③通信回線（お客様先でご用意いただく有線回線の場合）

この場合のセキュリティ対策は、お客様と回線業者との契約に依存したものとなりますので、弊社の責任範囲外とさせて頂いております。

上記より、計測データの改ざんや破壊行為（パワーコンディショナなどに異常をきたすような操作）などを特定の発電所に行うのは極めて難しいレベルのセキュリティを維持しています。

2. 弊社クラウドサーバ側

遠隔視画面へのアクセスには HTTPS で暗号化（SSL/TLS）通信を行い、セキュリティで守られています。また、遠隔監視画面の閲覧にあたっては発電所毎に異なる URL・ID・パスワード、または利用者毎に異なる ID・パスワードが必要となっております。

また、弊社クラウドサーバ（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おります。

上記より、弊社クラウドサーバにおいても高いセキュリティレベルを維持しています。

【電力会社に出力制御を申し込む場合のセキュリティ対策への回答】

下記いずれも対応しております。

☑ 外部ネットワークや他ネットワークを通じた発電設備の制御に係るシステムへの影響を最小化するための対策を講じています。

☑ 発電設備の制御に係るシステムには、マルウェアの侵入防止対策を講じています。

【想定される脅威への計測・制御システムのセキュリティ対策】

①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。
不正侵入 DoS 攻撃	外部からの侵入を禁止し、不正アクセスを遮断している。
	不要なポートを閉じて、端末側から必要な通信以外は遮断している。
遠隔監視サーバのなりすまし	遠隔監視サーバがなりすまされていないことを確認するために証明書を検証している。
	アクセス先の URL は発電所ごとに設けられた遠隔監視サーバを設定しており、外部からの追加・削除・編集を不可としている。

電力サーバのなりすまし	出力制御情報を扱うアクセス先の対象サーバがなりすまされていないことを確認するために証明書を検証している。
	アクセス先の URL は発電所ごとに決められた電力会社のサーバを設定しており、外部からの追加・削除・編集を不可としている。
固定スケジュールの書換え/読み出し	外部ネットワークから端末側へのアクセスによる固定スケジュールの書換え/読み出しができないように、不要なポートを閉じ、外部からスケジュールへのアクセスを禁止している（通信しているポートに対する防御） 。

②機器のマルウエア侵入防止対策

想定される脅威	対策内容
マルウエア侵入	Firewall を設定することで、外部からのセッション開始を不可としている。
マルウエア対策	Firewall を設定することで、不要なサービス、ポートを遮断している。

③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	遠隔監視サーバとの計測・制御データの通信は SSL 通信によって、暗号化して行っている。
	電力会社の通信仕様書に従い、出力制御情報を扱うアクセス先の対象サーバとの通信は SSL 通信によって、暗号化して行っている。

④セキュリティパッチの適用

対策内容
OS やミドルウェアの不具合情報、パッチリリースに関する情報を収集し、必要に応じてアップデートしている。

以上