技術情報

サイバーセキュリティ　公式ガイドライン

太陽光発電システムにおける安全な通信に関するガイドライン

日本語

CyberSecurity-TI-ja-10 | バージョン 1.0

目次

1 本書について

1.1 適用範囲

本書は、太陽光発電システム通信ネットワーク内に相互接続されており、通信媒体機器を介してインターネットに直接的ないし間接的に接続可能な全製品を対象としています。

本文書は各製品に同梱されている文書を補足するものであり、製品の設置場所で適用される規則や規格に代わるものではありません。製品に同梱されているすべての説明書類を読み、その内容を遵守してください。

1.2 対象読者

本書は、SMAパワーコンディショナを装備した太陽光発電システムの施工者と運営者、および太陽光発電システムの設計者を対象にしています。

1.3 補足情報

詳細情報については、次に挙げるセキュリティ関連機関のウェブサイトをご覧ください。

安全性機関	文書	ハイパーリンク
連邦情報安全庁（ドイツ、BSI：Bundesamt für Sicherheit in der Informationstechnik）	Sichere Passwörter in Embedded Devices（埋め込みデバイスの安全なパスワード）	https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_069.pdf?__blob=publicationFile
連邦情報安全庁（ドイツ、BSI：Bundesamt für Sicherheit in der Informationstechnik）	Industrial Control System Security: Top 10 Threats and Countermeasures 2016（産業用生業システムのセキュリティ：10大脅威と対策、2016年）	https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005E.pdf?__blob=publicationFile&v=3
NIST (米国、National Institute of Standards and Technology)	10 Basic Cybersecurity Measures（サイバーセキュリティの基本10対策）	https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf

詳細情報は、次のリンクに掲載されています：www.SMA-Solar.com

表題	文書の種類
「Webconnect Systems in Sunny Portal」	使用説明書
「SMA SPEEDWIRE FIELDBUS」	技術情報
"System Monitoring - SMA Safety and Password Concept for Password-protected PV Plants with Bluetooth® Wireless Technology"	技術説明書

表題	文書の種類
「SMA Modbus® Interface」（SMA Modbus®インターフェース）	技術情報
「SunSpec® Modbus® Interface」（SunSpec® Modbus® インターフェース）	技術情報

2 はじめに

太陽光発電システムの監視や制御などほとんどの運用作業は、太陽光発電システムの運営者またはサービススタッフにより、外部のインターネットインフラに基づくデータ通信を介する必要なく、現場側の操作で実施できます。太陽光発電システムの運営者／サービススタッフとパワーコンディショナ／データロガー／その他装置との間のデータ通信を含む、これらの運用業務は現場のディスプレイ、キーパッドを使用して、または太陽光発電システムや建屋のLANに接続したデバイスのウェブサーバーにローカルにアクセスすることによって実施できます。

太陽光発電システムのその他アプリケーションでは、インターネットインフラに基づくグローバルな通信システムのなかに、太陽光発電システムが組み込まれていることもあります。

インターネットを介したデータ通信により、次のような最新のアプリケーションに容易にアクセスすることができます。お客様にとって使いやすく、かつ経済的な通信方法として、これは現在一般的に用いられています。

- クラウドプラットフォーム（Sunny Portalなど）
- スマートフォンまたはその他のモバイルデバイス（iOSまたはAndroidアプリ）
- SCADAシステム（リモート接続）
- 系統管理サービスのためのユーティリティインタフェース

あるいはインターネットの代わりに、限定されたセキュアな通信インタフェースを使用することもできます。しかし、これらのソリューションはもはや最新の技術水準を満たすものではなく、また使用に大きな費用がかかります（特殊な通信インタフェース、別途にWANが必要になるなど）。

インターネットインフラを使用する場合、インターネットに接続されるシステムは基本的に非セキュアな環境になります。潜在的な攻撃者は脆弱なシステムがないか常に探し続けています。通常、こうした攻撃者は犯罪に関わっており、背後にテロリストが潜んでいたり、事業妨害を目論んでいたりします。そうした悪用から太陽光発電システムやその他システムを保護する対策を講じない限り、データ通信システムをインターネットに接続すべきではありません。

正当な権限のないユーザー（犯罪者や秘密機関）による望ましくない攻撃から太陽光発電システムを効果的に保護するためには、ローカルネットワークをできるだけクリーンで閉じられたものに保つ必要があります。太陽光発電システムやその他同様のシステムがインターネットに接続されている場合、太陽光発電システムの運営者またはネットワーク管理者は次のことに責任を負います。

- ローカルネットワークでアクティブとなっているすべてのデバイスに関する知識をもつこと
- すべてのデバイスの通信要件および機能に関する知識をもつこと
- すべてのデバイスの潜在的な脆弱性に関する知識をもつこと
- システムにアクセスできるすべてのアカウントに関する知識をもつこと
- ローカルネットワークとデバイスに対するアクセスを制限するオプションに関する知識をもつこと（安全なパスワードの使用など）
- サイバーセキュリティ関連で必要とされるあらゆるセキュリティ対策（ルーター、ファイアウォール、プロキシサーバー）を導入し、設定すること
- セキュリティ対策が最新であり、適切に講じられていることを検証し、必要に応じて改善すること

以上の要件が満たされている場合、その太陽光発電システムは安全区域にあると考えられます。このようなシステムに外部から瞬時に直接アクセスすることは不可能です。

ほとんどの産業用通信システムでは主に標準フィールドバス・プロトコルが使用されています。以上のことから、大半のフィールドバスにはセキュリティ機構が組み込まれておらず、追加手段により保護する必要があるので、重要システムをセキュリティ防護策で守られた領域内に配置する戦略が必要不可欠です。これは、SMA Solar Technology AGの通信ソリューションで使用されているフィールドバス・プロトコルであるSMA Data2+とModbus TCPの両方に当てはまります。Data2+プロトコルのパスワード保護により、SMA製品のセキュリティ機能が確保されます。その例外となるのがWebconnectで、これにはエンドツーエンド暗号化によるセキュアな通信を可能にするWAN通信プロトコルが使用されます。ただし、Webconnectはローカルネットワークで使用するものではありません。太陽光発電パワーコンディショナとデータロガーの間、またはSunny Portalとモバイルソリューションの間のセキュアなインターネット通信のために設計されています。

i Modbus TCPによるセキュリティリスク

Modbus TCPは、ログインなしでアクセスできるカスタマーインタフェースとしてほとんどのSMA製品に組み込まれています。保護対策を講じることなしには、インターネットを介して安全にModbus TCPプロトコルパケットを転送することはできません。太陽光発電システム内でModbus TCPのログイン認証がないことが、セキュリティリスクになる可能性があります。このため、Modbus TCPはSMA製品でデフォルトでは無効に設定されています。必要に応じて、Modbus TCPを「施工者」のユーザーグループで有効にする必要があります。ただし、この有効化は慎重に行うべきで、システム全体を保護するために付加的な対策を必ず講じる必要があります。

3 リスク

個別に保護されていないシステムがインターネットに接続されていると、（ルーターを介してインターネットにつながっている）施工側ネットワークへのアクセスにそれが利用される可能性があります。それによって、ネットワーク内のほとんどすべてのデバイスが攻撃の危険にさらされます。潜在的な攻撃者がネットワークにアクセスする手段を得ると、次のようなリスクが発生します。

- ユーザー名、パスワード、その他の機密データを盗み出す
- ネットワークに接続しているデバイスにアクセスして、ボットネットエージェントを送り込む、またはクロスサイト・スクリプティング攻撃を仕掛ける
- ネットワークに接続されているデバイスにアクセスし、デバイスの動作を不正に操作する（中間者攻撃やリプレイアタックなどを使用）
- ネットワークに接続されているデバイスにアクセスして、送信データを不正に操作することにより、上位システムの誤った反応をトリガーする
- ネットワークに接続されているデバイスにアクセスして、（不法侵入や窃盗などを計画するために）ユーザーの行動を評価する
- ネットワークに接続されているデバイスにアクセスして、収集データに基づいて個別化した広告を行うためにユーザーの行動を評価する

こうした行為が次のような問題を招く可能性があります。

- 以下の理由による経済的損失
  - 発電量の喪失
  - 誤った売電料金や電気使用料金
  - デバイスの損傷
- ID盗難
- 電力系統の不安定化（被害を受けたシステムの数と規模が大きい場合）
  - 系統連系認可の喪失
  - 法的な問題

4 対策

セキュアなシステムのための基本要件を満たすために、SMA Solar Technology AG では最低限のラインをクリアするセキュリティ対策を推奨しています。SMA製品により提供されるセキュリティ機能と組み合わせれば、太陽光発電システムの安全な運用を実現できます。太陽光発電システムの安全な運用を確保するために、次のルールを守ってください。

- ファイアウォールとプロキシサーバーを正しく設定してください。
- 太陽光発電システムのネットワーク接続には、物理的に分離されたネットワークセグメントを使用してください（ホームネットワークや職場のネットワークと分離する）。
- 正式な権限のない者が、ネットワークに接続しているSMA製品やその他のデバイスに物理的または仮想的にアクセスするのを阻止してください。
  - ローカルネットワークからのシステムの物理的な操作を阻止してください。
  - ローカルネットワークでのスパイウェアデバイスの使用を避けてください（他者に属する、または身元不明なWLANアクセスポイントなど）。
  - Sunny Portal登録用の登録ID（RID）を不正に収集しようとする企てを阻止してください（登録IDは通常、製品に貼付されています）。登録IDはデバイス固有のランダムに割り当てられたIDで、製品への物理的なアクセスを証明します。
  - システムの詳細な情報（デバイスモデル、パスワード、RID）は、「必要最小限」の原則に従って保管してください。こうした情報はできるだけ厳重に機密管理してください。
  - すべてのパスワード、WebconnectのRID、SMA Grid Guardのコードは機密扱いにしてください。Grid Guardのコードは、系統関連のシステムパラメータを変更する際に使用され、その変更者が許可を受けた施工者であるかどうかを識別します。
  - ITセキュリティに関連するすべてのデバイスのシステム・ログファイルを定期的にチェックしてください。
  - 使用しているデバイスに不明なメモリ媒体（USBフラッシュドライブ、SDカード、CFカードなど）を接続しないでください。そうしたメディアは使用する前にマルウェアに感染していないか、チェックしてください。
  - 不明なデバイスや安全性の不確かなデバイスをネットワークで使用しないでください。
  - システムのバックアップを定期的に行ってください。
  - 関連システムを対象とするソリューションや手順を冗長化してください。重要なシステムエレメントごとに、設定調整済みの予備部品をバックアップとして準備しておくのも、手軽な対策です。
- LANとWANの間のポート通信などは避けてください。

  - 外部への接続はVPNまたはWebconnectを介して行います。遠隔接続（メンテナンス、サポート、卸電力市場へのアクセス、系統管理サービス）には、必ずこうした安全な通信手段を使用します。
- ファイアウォール内の未使用のIPポートがすべて閉じていることを確認してください。他のシステムの未使用のIPポートは無効になっている必要があります。開いているIPポートがあると、システム侵入を許す可能性があります。
- 安全ではない外部FTPサーバーは使用せず、必ずSFTPサーバー（安全なFTPサーバー）を使用するようにしてください。FTPサーバーはファイルを暗号化せずに送信します。SFTPサーバーを使用すれば、ファイルは送信中に暗号化されています。
- 電子メールには安全な外部メールサーバーを使用してください。今日、ほとんどの電子メールプロバイダーはTLS（または同等の）アクセスだけを許可しています。
- SMA Solar Technology AG製品以外の製品についても安全性を確認してください。安全性に欠けた製品は、攻撃者によるローカルネットワークへの望ましくないアクセスの危険にさらされます。
  - アンチウィルス/アンチマルウェアのソフトウェア、ルーターやファイアウォールのルールは常に更新し、最新に保ってください。
  - セキュリティ機能に例外規定を設ける場合は、絶対に必要なものだけに限ってください。
  - セキュリティのアップデートに関するOSの推奨事項に従ってください。
- 太陽光発電システムへのアクセス権限の割当てが、明確に整理されていることを確認します（どのユーザーにどのアクセス権限が認められているのかを確認）。
  - ほとんどの場合、「ユーザー」のユーザーグループ権限で太陽光発電システムを監視するに十分です。「施工者」のユーザーグループ権限は、製品の試運転調整およびパラメータ設定の際にだけ使用すべきものです。
- 遅くとも試運転時までに、すべてのデフォルトパスワードがユーザー固有のパスワードに変更されていることを確認してください。デフォルトパスワードは公知の情報です。
- パスワードは必ず一般的なガイドラインに従って使用するようにしてください。
  - パスワードは8文字以上で、文字、数字、特殊文字（!=?#+-:;*）を含んでいる必要があります。

  - パスワードは推察されにくいものである必要があります（「1?deFa-7」など）。
- どのパスワードも、単一の太陽光発電システムだけに使用されていることを確認してください。
- 太陽光発電システムにアクセスするときは、毎回、確実にログアウトしてください。アクティブなインターネットセッションは、中間者攻撃により乗っ取られる可能性があります。
- すべてのデバイスのWLANアクセスには、強度WPA以上の暗号化、できればWPA2暗号を使用するようにしてください。
  - WEPなどの古いタイプの暗号化方式は使用しないでください。
  - 暗号化の適用は絶対に省かないでください。
- サイバーセキュリティについて、全従業員の問題意識を高めてください。
  - 従業員は必ずサイバーセキュリティについての訓練を受けるようにしてください。
- お使いのシステムへの攻撃が発覚する、あるいは疑われる場合は、被害程度の査定を専門家に依頼し、影響がさらに拡大するのを防いでください。
- SMA製品への攻撃が発覚する、あるいは疑われる場合は、SMA Solar Technology AGに速やかに連絡してください。そのような事態の連絡には、次の電子メールアドレスをご使用ください。
  - Information-Security@SMA-Solar.com