**小出力太陽光発電設備に係る**

**サイバーセキュリティ対策実装例リスト**

令和4年3月

一般社団法人 太陽光発電協会

一般社団法人 日本電機工業会

小出力太陽光発電設備設置者における対策実装例リスト

小出力太陽光発電設備（一般用電気工作物に分類される出力10kW以上50kW未満の低圧事業用太陽光発電設備）の設置者[[1]](#footnote-2)は、以下の実装例を参考に、系統連系技術要件が求める3つのサイバーセキュリティ対策を実施する必要がある。サイバーセキュリティ対策の実施にあたっては、関連する小出力太陽光発電設備等（小出力太陽光発電設備及びそれに付随するPCS（パワーコンディショナー）、出力制御ユニット、通信装置等）のメーカーが説明書等に記載している実施すべき事項や注意事項を確認し、施工業者と連携しつつ対策を実施することが望まれる。

本リストで示す対策実装例は系統連系技術要件で求められる対策を実装するための例示的位置づけであり、小出力太陽光発電設備設置者は自組織の対策範囲についてリスクを評価した上で適切な実装例を選択することが求められる。また、記載の対策実装例以外にも、系統連系技術要件で求められる対策へ対応するための実装方法は存在することに留意する必要がある。

| **対策実装例** |
| --- |
| **対策①　ネットワーク接続点の保護** |
|  | (1) 小出力太陽光発電設備等に係る通信のうち、インターネットを介した通信については、防護装置（ルーター、ファイアウォール、VPN等）を必ず経由させる。 |
| (2) 防護装置（ルーター、ファイアウォール、VPN等）に対して、遮断する通信（小出力太陽光発電設備等の運転において不要な通信、事前に設定していない通信 等）に関する設定を行う。 |
| (3) 不正アクセス等のセキュリティ事象を適切に検知できるよう、インターネットを介した通信に関してネットワーク監視や通信のモニタリングを実施する。 |
| (4) 小出力太陽光発電設備等の制御に係るシステムにおいて、システムのネットワークを、情報システムのネットワークから論理的あるいは物理的にセグメントを分離する。 |
| (5) 小出力太陽光発電設備等の制御に係るシステムと他ネットワークとの接続点を最小化する。 |
| (6) 小出力太陽光発電設備等の運転設定に関する管理画面に対してアクセスする際の認証情報（パスワード等）を、適切に管理する。 |
| **対策②　データの保存・転送を行う機器・端末等のマルウェア対策** |
|  | (1) 利用する小出力太陽光発電設備等や防護装置（ルーター、ファイアウォール、VPN等）について、正規品を購入する。 |
| (2) 小出力太陽光発電設備等に接続する端末（PC等）に対して、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導⼊することで、攻撃コードの検知を実施する。 |
| (3) 小出力太陽光発電設備等に接続するUSBメモリ等の外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能なUSBメモリを⽤いる等の対策を行う。 |
| (4) 屋外に設置する小出力太陽光発電設備等や防護装置（ルーター、ファイアウォール、VPN等）において使⽤しないUSBポート、シリアルポートは栓をするなど物理的に閉塞する。 |
| (5) 小出力太陽光発電設備等や防護装置（ルーター、ファイアウォール、VPN等）に関する脆弱性、セキュリティパッチ、注意喚起等の情報を収集し、必要に応じた対応を行う。 |
| **対策③　連系先系統運用者に対するセキュリティ管理責任者の氏名及び緊急時連絡先の通知** |
|  | (1) 組織内で、小出力太陽光発電設備等に関するセキュリティ管理責任者を明確化し、組織内におけるセキュリティの役割と責任を明らかにする。 |
| (2) 明確化したセキュリティ管理責任者の氏名及び緊急連絡先を連系先系統運用者（系統連系協議を行った相手、契約先の一般送配電事業者等。）に通知し、変更があった場合には速やかに再通知を行う。 |

施工業者における対策実装例リスト

小出力太陽光発電設備（一般用電気工作物に分類される出力10kW以上50kW未満の低圧事業用太陽光発電設備）の設置に係る施工業者は、設備設置者が系統連系技術要件で求められるサイバーセキュリティ対策を実施できるよう、以下の実装例を参考に設備設置者の対策を支援することが望まれる。

本リストで示す対策実装例は系統連系技術要件で求められる対策を実装するための例示的位置づけであり、小出力太陽光発電設備の設置者が対策範囲についてリスクを評価した上で適切な実装例を選択できるよう、対策を支援することが望まれる。また、記載の対策実装例以外にも、系統連系技術要件で求められる対策へ対応するための実装方法は存在することに留意する必要がある。

| **対策実装例** |
| --- |
| **対策①　ネットワーク接続点の保護** |
|  | (1) 外部通信を行う小出力太陽光発電設備等を設置する際、小出力太陽光発電設備等に係る通信のうち、インターネットを介した通信については、防護装置（ルーター、ファイアウォール、VPN等）を必ず経由させる。 |
| (2) 防護装置（ルーター、ファイアウォール、VPN等）に対して、遮断する通信（小出力太陽光発電設備等の運転において不要な通信、事前に設定していない通信 等）に関する設定を行う。もしくは、設置者自身で設定ができるよう、設定方法に関して説明を行う。 |
| (3) インターネットを介した通信を行う小出力太陽光発電設備等を設置する際、小出力太陽光発電設備等の制御に係るシステムにおいて、システムのネットワークを、情報システムのネットワークから論理的あるいは物理的にセグメントを分離する。もしくは、設置者自身でセグメント分離の設定を行えるよう、設定方法に関して説明を行う。 |
| (4) インターネットを介した通信を行う小出力太陽光発電設備等を設置する際、小出力太陽光発電設備等の制御に係るシステムと他ネットワークとの接続点を最小化する。もしくは、設置者自身で接続点最小化の設定を行えるよう、設定方法に関して説明を行う。 |
| **対策②　データの保存・転送を行う機器・端末等のマルウェア対策** |
|  | (1) 施工業者が購入する小出力太陽光発電設備等や防護装置（ルーター、ファイアウォール、VPN等）について、正規品を購入する。 |
| (2) 設備設置工事において小出力太陽光発電設備等に対して端末（PC等）を接続する場合、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを当該端末に導⼊して攻撃コードの検知を実施する。 |
| (3) 設備設置工事において小出力太陽光発電設備等に対してUSBメモリ等の外部記憶媒体を接続する場合、ウイルス対策ソフトによるチェック、ウイルスチェックが可能なUSBメモリを⽤いる等の対策を行う。 |
| (4) 設置した小出力太陽光発電設備等において使⽤しないUSBポート、シリアルポートは栓をするなど物理的に閉塞する。もしくは、設置者自身で閉塞ができるよう、具体的な対策方法に関して説明を行う。 |

小出力太陽光発電設備等のメーカーにおける対策実装例リスト

小出力太陽光発電設備等（一般用電気工作物に分類される出力10kW以上50kW未満の低圧事業用太陽光発電設備及びそれに付随するPCS（パワーコンディショナー）、出力制御ユニット、通信装置等）のメーカーは、設備設置者が系統連系技術要件で求められるサイバーセキュリティ対策を実施できるよう、以下の実装例を参考に、小出力太陽光発電設備等に対して適切な対策を講じることが望まれる。

本リストで示す対策実装例は系統連系技術要件で求められる対策を実装するための例示的位置づけであり、小出力太陽光発電設備等のメーカーは、小出力太陽光発電設備等についてリスクを評価した上で適切な実装例を選択することが求められる。また、記載の対策実装例以外にも、系統連系技術要件で求められる対策へ対応するための実装方法は存在することに留意する必要がある。

|  |
| --- |
| **対策実装例** |
| **対策①　ネットワーク接続点の保護** |
|  | (1) 小出力太陽光発電設備等において、不要なネットワークサービスやネットワークポート等をあらかじめ無効化する。 |
| (2) 小出力太陽光発電設備等の運転設定に関する管理画面に対するアクセスにおいて、アカウント認証を実装する。 |
| (3) 小出力太陽光発電設備等に対する信頼できる接続先サーバー以外からのセッション開始を禁止する。 |
| (4) 設備設置者や施工業者が防護装置（ルーター、ファイアウォール、VPN等）に対して実施すべき設定やセキュリティ対策を、取扱説明書や施工説明書等に明記する。 |
| **対策②　データの保存・転送を行う機器・端末等のマルウェア対策** |
|  | (1) 小出力太陽光発電設備等において、実行可能なプログラムや機能をあらかじめ制限する。 |
| (2) 小出力太陽光発電設備等において、ソフトウェアやファームウェアをアップデートする機能を実装し、新たな脆弱性が検出された場合等に設置者が確実にアップデートを行える仕組みを実装する。 |
| (3) マルウェア対策やアップデートに関して設備設置者や施工業者が実施すべき設定やセキュリティ対策を、取扱説明書や施工説明書等に明記する。 |

監視サービスプロバイダー等における対策実装例リスト

小出力太陽光発電設備（一般用電気工作物に分類される出力10kW以上50kW未満の低圧事業用太陽光発電設備）の発電状況を監視するサービスのプロバイダー及び当該監視に必要な計測通信装置のメーカーは、設備設置者が系統連系技術要件で求められるサイバーセキュリティ対策を実施できるよう、以下の実装例を参考に、遠隔監視用装置に対して適切な対策を講じることが望まれる。

本リストで示す対策実装例は系統連系技術要件で求められる対策を実装するための例示的位置づけであり、小出力太陽光発電設備の発電状況を監視するサービスのプロバイダー及び当該監視に必要な計測通信装置のメーカーは、当該装置についてリスクを評価した上で適切な実装例を選択することが求められる。また、記載の対策実装例以外にも、系統連系技術要件で求められる対策へ対応するための実装方法は存在することに留意する必要がある。

|  |
| --- |
| **対策実装例** |
| **対策①　ネットワーク接続点の保護** |
|  | (1) 遠隔監視用装置において、不要なネットワークサービスやネットワークポート等をあらかじめ無効化する。 |
| (2) 遠隔監視用装置の運転設定に関する管理画面に対するアクセスにおいて、アカウント認証を実装する。 |
| (3) 遠隔監視用装置に対する信頼できる接続先サーバー以外からのセッション開始を禁止する。 |
| (4) 設備設置者や施工業者による対策や設定が必要な場合、その内容を取扱説明書や施工説明書等に明記する。 |
| (5) 遠隔監視用装置と監視サービスプロバイダーのサーバーとの接続は、適切なプロトコルを用いて認証・認可を行う。 |
| (6) 遠隔監視用装置と監視サービスプロバイダーのサーバーとの通信は、適切なプロトコルを用いて暗号化する。 |
| **対策②　データの保存・転送を行う機器・端末等のマルウェア対策** |
|  | (1) 遠隔監視用装置において、実行可能なプログラムや機能をあらかじめ制限する。 |
| (2) 遠隔監視用装置において、ソフトウェアやファームウェアをアップデートする機能を実装し、新たな脆弱性が検出された場合等に設置者が確実にアップデートを行える仕組みを実装する。 |
| (3) マルウェア対策やアップデートに関して設備設置者が実施すべき設定やセキュリティ対策を、取扱説明書や施工説明書等に明記する。 |

1. 仮に一般家庭が10kW以上の設備を有する場合、設置者の状況を考慮の上で、別途策定された「家庭用電気工作物に係るサイバーセキュリティ対策の実装例」の対策を実装することも検討される。 [↑](#footnote-ref-2)