小出力コージェネレーション設備に係る

サイバーセキュリティ対策実装例リスト

令和４年３月

一般財団法人 コージェネレーション・エネルギー高度利用センター

一般社団法人 日本ガス協会

小出力コージェネレーション設備設置者における対策実装例リスト

小出力コージェネレーション設備（一般用電気工作物に分類される出力 10kW 未満のコージェネレーション設備）の設置者は、以下の実装例を参考に、系統連系技術要件が求める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、関連する小出力コージェネレーション設備等（小出力コージェネレーション設備及び設備に付属するコントローラー、遠隔監視端末）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、小出力コージェネレーション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) 小出力コージェネレーション設備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、それらに準じた接続・確認を行う。
	(2) 小出力コージェネレーション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。
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) 利用する小出力コージェネレーション設備等や防護装置（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) 利用する小出力コージェネレーション設備等や防護装置（ルーター、ファイアウォール、VPN 等）に関して、小出力コージェネレーション設備等のメーカーが説明書等に記載しているマルウェア対策やアップデートに関する注意事項を確認し、それらに準じた使用を行う。
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) 小出力コージェネレーション設備等の設定を主に担当する人物をセキュリティ管理責任者として連系先系統運用者（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

小出力コージェネレーション設備（一般用電気工作物に分類される出力 10kW 未満のコージェネレーション設備）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、小出力コージェネレーション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) 小出力コージェネレーション設備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、それらに準じた接続を行う。設置工事後に、工事責任者等により設備設置者に対して、説明書等に準じた接続・設定を行った旨の説明を行う。
	(2) 小出力コージェネレーション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。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。
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コージェネレーション設備等や防護装置（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) 利用する小出力コージェネレーション設備等や防護装置（ルーター、ファイアウォール、VPN 等）に関して、メーカーが説明書等に記載しているマルウェア対策やアップデートに関する注意事項を確認し、それらに準じた接続・設定を行う。設置工事後に、工事責任者等により設備設置者に対して、説明書等に準じた接続・設定を行った旨の説明を行う。

小出力コージェネレーション設備等のメーカーにおける対策実装例リスト

小出力コージェネレーション設備等（一般用電気工作物に分類される出力 10kW 未満のコージェネレーション設備及びそれらに付随するコントローラー、遠隔監視端末）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、小出力コージェネレーション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、小出力コージェネレーション設備等のメーカーは、小出力コージェネレーション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) 小出力コージェネレーション設備等において、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) 小出力コージェネレーション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) 小出力コージェネレーション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小出力コージェネレーション設備等・接続される防護装置（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) 小出力コージェネレーション設備等において、実行可能なプログラムや機能をあらかじめ制限する。
	(2) 小出力コージェネレーション設備等において、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アップデートする。
	(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。

監視・制御等のサービスプロバイダーにおける対策実装例リスト

小出力コージェネレーション設備（一般用電気工作物に分類される出力 10kW 未満のコージェネレーション設備）の発電状況を監視・制御等を実施するサービスのプロバイダー及び当該サービスに必要な設備のメーカー、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、小出力コージェネレーション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、小出力コージェネレーション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) 防護装置（ルーター、ファイアウォール、VPN 等）・遠隔監視端末・コントローラーにおいて、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。汎用品の装置・端末を用いる場合、不要なネットワークサービスやネットワークポート等が無効化されている装置・端末を用いる。
	(2) 防護装置（ルーター、ファイアウォール、VPN 等）・遠隔監視端末・コントローラー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。汎用品の装置・端末を用いる場合、アカウント認証が実装されている装置・端末を用いる。
	(3) 防護装置（ルーター、ファイアウォール、VPN 等）・遠隔監視端末・コントローラー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。汎用品の装置・端末を用いる場合、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できる装置・端末を用いる。
	(4) 設備設置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) 遠隔監視端末・コントローラーと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) 遠隔監視端末・コントローラーと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) 防護装置（ルーター、ファイアウォール、VPN 等）・遠隔監視端末・コントローラーにおいて、実行可能なプログラムや機能をあらかじめ制限する。汎用品の装置・端末を用いる場合、不要なプログラムや機能があらかじめ制限されている装置・端末を用いる。

対策実装例	
	(2) 防護装置（ルーター、ファイアウォール、VPN 等）・遠隔監視端末・コントローラーにおいて、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アップデートする。汎用品の装置・端末を用いる場合、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有している装置・端末を用いる。
	(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。