

一般競争入札（条件付）設計図書等に関する回答書

工 事 名	債務負担行為工事 発電施設監視制御システム更新工事
回 答 事 項	
質問 1	
・ 要求水準書 4. 2 (1) ⑩ について	
「山形県企業局電気事業における電力制御システムセキュリティマニュアル」の共有をお願いいたします。	
回答 1	
・ 別添のとおりです	
質問 2	
・ 要求水準書 別紙 1－3 について	
木川ダムコンのシステム構成図において、メディアコンバータ及びITV監視装置は工事範囲外となっていますが、それらを接続するLAN（拠点内）は工事範囲（水色）となっています。LANのみの布設工事と考えてよろしいでしょうか。	
回答 2	
・ お見込みのとおりです。	
質問 3	
・ 要求水準書 4. 2 (4) について	
木川ダム見張所にある既存衛星電話を活用した通信網を構築するとの記載について、既存衛星電話の仕様をご教授ください。	

回答 3

- ・既存衛星電話はNTTドコモビジネス㈱のワイドスターⅢ(可搬型)になります。

なお、既存衛星電話での通信が難しい場合は、協議のうえ発注者側で別途、衛星電話を整備します。

質問 4

- ・要求水準書 別紙 2 について

丹南発電所の各項目点数をご教授ください。

回答 4

- ・神室発電所と同程度の点数を想定しております。

質問 5

- ・要求水準書 別紙 1－2 について

丹南発電所は朝日制御所の監視・制御管轄と考えてよろしいでしょうか。

回答 5

- ・西川制御所の監視・制御管轄となります。

山形県企業局電気事業における 電力制御システムセキュリティマニュアル

山形県企業局電気事業課

令和6年3月

目 次

第 1 章 総則

第 1 条	目的	1
第 2 条	適用範囲	1
第 3 条	想定脅威	1
第 4 条	用語の定義	1
第 5 条	一般的責務	2

第 2 章 組織

第 6 条	セキュリティ管理責任組織	2
第 7 条	セキュリティ責任者	2
第 8 条	電気主任技術者	3
第 9 条	セキュリティ管理者	3
第 10 条	システム関係者	3
第 11 条	セキュリティ教育及び訓練	3
第 12 条	実施状況の報告	3
第 13 条	自己点検	3

第 3 章 設備・システムのセキュリティ

第 14 条	外部ネットワークとの分離	4
第 15 条	ネットワークとの接続	4
第 16 条	機器のマルウェア対策	4
第 17 条	不正処理防止策及びアクセス制限	4
第 18 条	機器・外部記録媒体及びデータの管理	4
第 19 条	外部記憶媒体等のマルウェア対策	4
第 20 条	管理者権限の適切な割当	4
第 21 条	セキュリティパッチの適用	5

第 4 章 セキュリティ事故の対応

第 22 条	情報の収集	5
第 23 条	セキュリティ事故の対応	5

第1章 総 則

(目的)

第1条 本マニュアルは、電気設備に関する技術基準を定める省令第15条の2及び電気設備技術基準の解釈第37条の2第2項に定める「電力制御システムセキュリティガイドライン」(以下、「ガイドライン」という。)に基づき、山形県企業局電気事業における電力制御システム等のサイバーセキュリティ確保を目的として、実施すべきセキュリティ対策に関して必要な事項を定める。

(適用範囲)

第2条 本マニュアルは、電力制御システム等及びそれに携わる者に適用するものとする。

(想定脅威)

第3条 本マニュアルにおいては、電力の安定供給、電気工作物の保安の確保の妨害等を目的としたサイバー攻撃を脅威として想定するものとする。

(用語の定義)

第4条 本マニュアルにおいて、次の各号に掲げる用語の定義はそれぞれ次に定めるものとする。

- (1)「電力制御システム」とは、山形県企業局が保有する遠方監視制御装置(水力、太陽光及び風力発電所のもの)及びダム情報通信装置をいう。
- (2)「電力制御用ネットワーク」とは、電力制御システム同士をつなぐネットワーク又は制御箇所と被制御箇所を結ぶネットワークをいう。
- (3)「電力制御システム等」とは、電力制御システム及び電力制御用ネットワークの全体をいう。
- (4)「機器」とは、システムを構成するサーバー、パソコンや可搬型の機器等の端末及びネットワークの構成機器をいう。
- (5)「外部ネットワーク」とは、不特定多数が接続できる回線で接続するネットワークをいう。
- (6)「他ネットワーク」とは、電力制御用ネットワーク以外のネットワークのうち、山形県企業局内の事務処理に用いられるネットワーク等をいう。
- (7)「外部記憶媒体」とは、機器に接続してそのデータを保存するための可搬型の装置をいう。
- (8)「サイバー攻撃」とは、システムに対する悪意のある電子的攻撃をいう。ネットワークを介した外部からの攻撃の他、施設内部への物理的な侵入による攻撃や内部不正

も含む。

- (9)「ぜい弱性」とは、ソフトウェアやアプリケーション等において、システムへの不正アクセスやマルウェア等の攻撃により、その機能や性能を損なう原因となり得るセキュリティ上の問題箇所をいう。
- (10)「セキュリティ事故」とは、意図的なサイバー攻撃により、電力の安定供給、電気工作物の保安の確保に支障を及ぼす、又はそのおそれのあるシステムの不具合が発生した事象をいう。
- (11)「セキュリティに関する情報」とは、セキュリティマネジメントに関する情報、セキュリティ対策の実施状況に関する情報をいう。

(一般的責務)

- 第5条 電力制御システム等に携わる者は、電力制御システム等に係るセキュリティ確保のため、ガイドライン及び本マニュアルに定める事項を遵守するものとする。
- 2 電力制御システム等に携わる者は、善良なる管理者の注意をもって電力制御システム等を取り扱うものとする。
 - 3 電力制御システム等に携わる者は、セキュリティに関する情報の収集及び知識の習得に努めるものとする。
 - 4 電力制御システム等に携わる者は、電力制御システム等のセキュリティに対する危険性の回避に努めるものとする。

第2章 組 織

(セキュリティ管理責任組織)

第6条 セキュリティ管理責任組織には次の責任者等を配置するものとする。

- (1) セキュリティ責任者
- (2) 電気主任技術者
- (3) セキュリティ管理者
- (4) システム関係者

(セキュリティ責任者)

第7条 セキュリティ責任者は電気事業課長とする。

- 2 セキュリティ責任者は、電力制御システム等における全てのセキュリティ対策に関する総括的な権限及び責任を有するものとする。
- 3 セキュリティ責任者は、セキュリティ管理責任組織を整備するものとする。
- 4 前項の組織は、セキュリティ責任者に直属するものとする。

(電気主任技術者)

第8条 電気主任技術者は、電力制御システム等におけるセキュリティ対策の技術的内容について、セキュリティ管理者へ指導及び助言を行うものとする。

(セキュリティ管理者)

第9条 セキュリティ管理者は各事務所長とする。

- 2 セキュリティ管理者は、その所管する施設におけるセキュリティ対策を実施する権限及び責任を有するものとする。
- 3 セキュリティ管理者は、その所管する施設に所属する職員に対して、セキュリティ対策に関する教育、訓練、指導及び助言を行うものとする。

(システム関係者)

第10条 システム関係者はセキュリティ管理者が選任するものとする。

- 2 システム関係者は、その所管する施設におけるセキュリティ対策の実施に関する権限及び責任を有するものとする。
- 3 システム関係者は、セキュリティ管理者の指示に従い、電力制御システム等のセキュリティ対策を実施するものとする。

(セキュリティ教育及び訓練)

第11条 セキュリティ責任者は、職員に対しサイバーセキュリティに関する研修を定期的に行うものとする。

- 2 セキュリティ責任者は、セキュリティ事故発生時の対応に関する訓練を定期的を実施するものとする。
- 3 セキュリティ責任者は、前1、2項を実施した際はその効果の確認を行うものとする。

(実施状況の報告)

第12条 セキュリティ管理者は、電力制御システム等に対するセキュリティに関する事項を変更した場合は、実施状況をセキュリティ責任者へ遅滞なく報告(様式1号)するものとする。

(自己点検)

第13条 システム関係者は、所管する電力制御システム等のサイバーセキュリティ対策の実施状況について、年1回、自己点検を実施するものとする。

- 2 システム関係者は、前項点検の結果をセキュリティ管理者へ報告(様式2号)するものとする。

- 3 セキュリティ管理者は、前項の報告があった時は点検結果に基づく改善策を取り纏め、セキュリティ責任者へ報告するものとする。
- 4 セキュリティ管理者は、前項報告があった時はサイバーセキュリティ対策の見直しに活用するものとする。

第3章 設備・システムのセキュリティ

(外部ネットワークとの分離)

第14条 電力制御用ネットワークと外部ネットワークは物理的に分離するものとする。

(ネットワークとの接続)

第15条 電力制御用ネットワークと他ネットワークとの接続点は最小化するものとする。

(機器のマルウェア対策)

第16条 外部ネットワーク及び他ネットワークとの接続においては、マルウェア対策としてファイアウォール及びウィルス対策ソフト等のハード又はソフト的な防護措置を講じるものとする。

(不正処理防止策及びアクセス制限)

第17条 電力制御システム等に接続する外部記憶媒体は、セキュリティ責任者が接続許可した者のみとする。

- 2 外部ネットワークに接続する機器は、セキュリティ責任者が接続許可した機器以外は接続しないものとする。

(機器・外部記録媒体及びデータの管理)

第18条 システム関係者は、機器・外部記録媒体について利用状況を把握し、適切に管理するものとする。

- 2 前項で使用するデータは適切に保護するものとする。

(外部記録媒体等のマルウェア対策)

第19条 システム関係者は、電力制御システム等に接続する外部記録媒体及び可搬型の機器について定期的にウイルスチェックを行うものとする。

(管理者権限の適切な割当)

第20条 電力制御システム等における管理者権限は、システムの根幹に関わる部分を除

きセキュリティ責任者にあるものとし、発電所監視制御に係るパラメータ設定及び変更等のメンテナンス装置へのアクセスは、システム関係者又はセキュリティ責任者が指定した職員のみが行えるものとする。

(セキュリティパッチの適用)

第 21 条 セキュリティ管理者は、外部ネットワークに接続する機器において、重大な脆弱性に対応するセキュリティパッチがリリースされた場合、遅滞無くそのパッチを適用するものとする。

第 4 章 セキュリティ事故の対応

(情報の収集)

第 22 条 セキュリティ責任者は、電力制御用ネットワークに係るセキュリティ事故の対応に必要な情報を随時収集するものとする。

(セキュリティ事故の対応)

第 23 条 職員は、第 3 条による脅威があった場合は、速やかにセキュリティ管理者へ報告するものとする。

2 報告を受けたセキュリティ管理者は、必要かつ十分な措置を行うようセキュリティ関係者に指示するものとする。

3 報告を受けたセキュリティ管理者は、電力制御システム等の不具合の緊急度及び深刻度を勘案し、必要によりセキュリティ責任者に報告（様式第 3 号）するものとする。

4 セキュリティ責任者は、セキュリティ事故及びその対応において得られた知見をサイバーセキュリティ対策の見直しに活用するものとする。