電力制御システムセキュリティガイドライン

第1章　総　　則

第1-1条　目的

本ガイドラインは，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，電気事業者が実施すべきセキュリティ対策の要求事項について規定したものである。

第1-2条　適用範囲

本ガイドラインは，電気事業者が施設する電力制御システム等及びそれに携わる者に適用する。

第1-3条　想定脅威

本ガイドラインにおいては，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。

第1-4条　用語の定義

本ガイドラインにおいて，次の各号に掲げる用語の定義は，それぞれ次に定めるところによる。

(1) 「**委託先等**」とは，委託先，再委託先及び発注先をいう。

(2) 「**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。

(3) 「**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。

(4) 「**監査**」とは，セキュリティに関する取り組みを客観的に評価することをいう。

(5) 「**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。

(6) 「**経営層**」とは，電気事業者における経営責任を持つ者をいう。

(7) 「**コマンド**」とは，システムにおける命令をいう。その中でも特に発行に慎重を要するものを「重要なコマンド」という。

(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) 「**システム関係者**」とは，委託先等を含む電力制御システム等の利用，管理，開発，保守に従事する者の総称をいう。

(10) 「**システムの不具合**」とは，システムの障害，作業ミス及びサイバー攻撃等により，システムが設計時の期待通りの機能を発揮しない又は発揮できない状態をいう。

(11) 「**セキュリティガバナンス**」とは，経営層が主体的かつ適切に情報リスクを管理する仕組みを構築・運用することをいう。

(12) 「**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。

(13) 「**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（公衆安全を含む）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。

(14) 「**セキュリティ仕様**」とは，電力制御システム等の機能要件に応じて策定されたセキュリティ要件をいう。

(15) 「**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。

(16)「**セキュリティマネジメントシステム**」とは，組織（企業，部，課等）におけるセキュリティを管理するための仕組みをいう。

(17)「**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，「外部ネットワーク」以外のものを指す。具体的には，自社内の事務処理に用いられるネットワーク等をいう。

(18)「**電気事業者**」とは，発電事業者，送配電事業者，小売電気事業者の総称をいう。

(19)「**電力制御システム**」とは，電力の安定供給，電気工作物の保安（公衆安全を含む）の確保に資するために，電気事業の用に供する電気工作物を監視・制御する機能等を具備したシステムをいう。

(20)「**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。

(21)「**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。

(22)「**文書化**」とは，情報や手順を可視化することをいう。

(23)「**報告**」とは，予め設定された報告経路及び手順に従って，文書化された情報を伝達することをいう。

(24)「**防護装置**」とは，他ネットワークからの攻撃や不正アクセスから電力制御用ネットワークを防御するためのファイアウォール等の装置をいう。

(25)「**ライフサイクル**」とは，電力制御システム等の計画・開発・調達・運用・保守・廃止をいう。

(26)「**リスク**」とは，脅威とぜい弱性の合致により損失が発生する可能性，また，その損失をいう。

(27)「**ログ**」とは，電力制御システム等に対して行われた操作状況や動作状況を記録したものをいう。

第1-5条　システム重要度

本ガイドラインにおいて，システム重要度の定義は，それぞれ次に定めるところによる。

(1)　「**重要度Ｓ**」とは，電力の安定供給等に与える影響が大きく，重要なシステムをいう。

(2)　「**重要度Ａ**」とは，電力の安定供給等に与える影響が比較的大きいと考えられるシステムをいう。

(3)　「**重要度Ｂ**」とは，電力の安定供給等に与える影響が限定的なシステムをいう。

(4)　「**重要度Ｃ**」とは，電力の安定供給等に与える影響が軽微なシステムをいう。

【重要度ごとの対象システム】

重要度	対象システム	
	送配電に関するシステム	発電に関するシステム
S	・一般送配電事業者が所管し，電気の使用量と発電量をバランスさせる需給制御システム ・発電所，変電所及び送電線を監視し，電気の流れを制御する系統制御システム	－
A	・17 万 V 以上の変電所における変電所等システム ・制御対象の需要規模が 50 万 kW 以上の配電自動化システム	・火力の発電所監視制御システム及びこれらにアクセス可能な電力制御ネットワークに属する端末・制御装置。ただし，出力合計 300 万 kW 以上の複数発電設備が一度に発電停止するおそれのある場合に限る。
B	・重要度がＳ，Ａ，Ｃ以外の電力制御システム等	
C	－	・制御する水力発電所の出力合計が 3 万 kW 未満の発電所監視制御システム ・ダムの高さが 15m 未満のダム管理システム ・太陽光の発電所監視制御システム

第2章　組　　織

第2-1条　体制

（勧告的事項）

１．経営層の責任

経営層は電力制御システム等におけるセキュリティの確保について責任を負うこと。

２．管理組織の設置

目的実現のためのセキュリティ管理責任組織を設置し，セキュリティガバナンスの構築を行うこと。

３．目的の明確化

電力制御システム等のセキュリティの実施目的を明確にすること。

第2-2条　役割

（勧告的事項）

１．責任者の設置

電力制御システム等のセキュリティ管理責任者を任命すること。

２．役割の定義

電力制御システム等のシステム関係者の役割を明確にすること。

３．委託先等の対応

電力制御システム等に関連する委託先等の役割を明確にすること。

第2-3条　セキュリティ教育

（勧告的事項）

１．教育の計画・実施

セキュリティ教育を計画し，実施すること。

２．教育効果の確認

セキュリティ教育の効果を確認すること。

第3章　文書化

第3-1条　文書管理

（勧告的事項）

１．文書化

電力制御システム等のセキュリティに関する情報を文書化すること。

２．文書の管理

電力制御システム等のセキュリティに関する文書を適切に管理すること。

第3-2条　実施状況の報告

（勧告的事項）

セキュリティ対策の実施状況に関する報告事項を定め，適切に報告を行うことができる仕組みを構築すること。

第4章　セキュリティ管理

第4-1条　セキュリティ管理

（勧告的事項）

セキュリティマネジメントシステムを構築すること。

第5章　設備・システムのセキュリティ

第5-1条　外部ネットワークとの分離

（勧告的事項）

電力制御システム等と外部ネットワークとは，原則分離すること。

第5-2条　他ネットワークとの接続

（勧告的事項）

１．接続点の最小化

他ネットワークとの接続点は最小化すること。

２．接続点の防御

他ネットワークとの接続点に防御措置を講じること。

第5-3条　通信のセキュリティ

（推奨的事項）

機器間の通信における傍受や，機器が保有する重要データの漏えい，改ざんの危険が高い区画においては，通信データの保護を行うことが望ましい。

第5-4条　機器のマルウェア対策

（推奨的事項）

電力制御システム等の機器に対してマルウェアの侵入防止対策を実施することが望ましい。

第5-5条　不正処理防止策

（推奨的事項）

１．不正プログラム防止

不正なプログラムの実行を阻止する仕組みを講じることが望ましい。

２．不正処理防止

本来の操作によらない処理が発行されないようにすることが望ましい。

第5-6条　アクセス制御

（推奨的事項）

１．接続制御

予め許可された機器以外の接続を許可しない仕組みを講じることが望ましい。

２．認証

通信相手が予め許可された機器であることを確認する仕組みを講じることが望ましい。

３．ネットワーク分割

電力制御用ネットワーク内において，利用目的等に応じてネットワークを分割することが望ましい。

第5-7条　ログの取得（重要度がＳの電力制御システム等が対象）

（勧告的事項）

ログを取得し，保管すること。

第5-8条　ログの取得（重要度がＡ，Ｂ，Ｃの電力制御システム等が対象）

（推奨的事項）

ログを取得し，保管することが望ましい。

第6章　運用・管理のセキュリティ

第6-1条　セキュリティ仕様の確認

（推奨的事項）

１．セキュリティ仕様

電力制御システム等の調達時にセキュリティ仕様を明確にすることが望ましい。

２．準拠性の確認

電力制御システム等がセキュリティ仕様通りに設計，製造されていることを確認することが望ましい。

３．仕様変更

セキュリティに影響を与える可能性がある変更を適切に管理することが望ましい。

第6-2条　機器・外部記憶媒体及びデータの管理

（推奨的事項）

１．機器・外部記憶媒体の管理

機器・外部記憶媒体を管理し，保護することが望ましい。

２．データの管理

電力制御システム等の制御に関連するデータを管理し，保護することが望ましい。

第6-3条　外部記憶媒体等のマルウェア対策

（勧告的事項）

電力制御システム等に接続する外部記憶媒体及び可搬型の機器はウイルスチェックを行うこと。

第6-4条　管理者権限の適切な割当

（推奨的事項）

電力制御システム等における管理者権限の割当を適切に行い，不正な行為が行われない仕組みを構築することが望ましい。

第6-5条　セキュリティパッチの適用

（推奨的事項）

重大なぜい弱性に対応するセキュリティパッチがリリースされ，電力制御システム等への

リスクがあると判断された場合には，影響度を踏まえて可能な範囲でセキュリティパッチを適用するか，代替策を適用することが望ましい。

第6-6条　入退管理（重要度がＳ，Ａの電力制御システム等が対象）

（勧告的事項）

１．セキュリティ区画

セキュリティ区画を明確にし，保護対象となる施設及び区画について適切に保護すること。

２．アクセス管理

セキュリティ区画には許可された者だけがアクセスできるようにすること。

第6-7条　入退管理（重要度がＢ，Ｃの電力制御システム等が対象）

（推奨的事項）

１．セキュリティ区画

セキュリティ区画を明確にし，保護対象となる施設及び区画について適切に保護することが望ましい。

２．アクセス管理

セキュリティ区画には許可された者だけがアクセスできるようにすることが望ましい。

第7章　セキュリティ事故の対応

第7-1条　情報の収集

（勧告的事項）

セキュリティ事故の対応に必要な情報を収集すること。

第7-2条　セキュリティ事故の対応

（勧告的事項）

セキュリティ事故の対応体制と手順を明確にすること。

第7-3条　セキュリティ事故の報告と情報共有

（勧告的事項）

１．セキュリティ事故の報告

セキュリティ事故が発生した場合には，対応手順に従い報告を行うこと。

２．情報の共有

セキュリティ事故から得られた知見を，セキュリティ事故の予防及び再発防止に活用する仕組みを構築すること。

第7-4条　周知と訓練

（勧告的事項）

セキュリティ事故発生時の対応に関する周知や訓練を定期的に行うこと。