JESCZ003(2016)

スマートメーター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，スマートメーターシステムのセキュリティ確保を目的として，一般送配電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，一般送配電事業者が施設するスマートメーターシステム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，スマートメーターシステムの運用に影響を与えること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)「**スマートメーターシステム**」とは，スマートメーター（電力量をデジタル計測し，通信機能を持たせた電力量計）と，それに係るシステムをいう。（第 1-2-1 図）

(2)「**機器**」とは，スマートメーターシステムを構成するサーバー，スマートメーター，ハンディターミナル等の端末及びネットワーク機器をいう。

(3)「**経営層**」とは，一般送配電事業者における経営責任を持つ者をいう。

(4)「**委託先等**」とは，委託先，再委託先及び発注先をいう。

(5)「**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。

(6)「**文書化**」とは，情報や手順を可視化することをいう。

(7)「**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。

(8)「**ログ**」とは，システム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。

(9)「**ライフサイクル**」とは，スマートメーターシステムの計画・開発・調達・運用・保守・廃止をいう。

(10)「**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。

(11)「**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。

(12)「**セキュリティ事故**」とは，意図的なサイバー攻撃を要因としたリスクの顕在化により事業損失を与える損害の発生する事象をいう。

(13)「**セキュリティ事象**」とは，直接損害は発生しないがセキュリティ事故につながる可能性のある事象をいう。

(14)「**セキュリティ仕様**」とは，スマートメーターシステム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)「**外部ネットワーク**」とは，スマートメーターシステムを構成するネットワーク以外のネットワークをいう。

(16)「**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。

(17)「**サービス継続**」とは，スマートメーターシステムが提供するサービスの継続性をいう。

(18)「**コマンド**」とは，スマートメーター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。

第２章　組織

第２−１条　体制

１．経営層の責任

　経営層はスマートメーターシステムにおけるセキュリティの確保について責任を負うこと。（勧告）

２．管理組織の設置

　スマートメーターシステムのセキュリティ管理責任組織を設置すること。また，スマートメーターシステムのセキュリティ管理責任組織と全社のセキュリティ管理責任組織との関係を明確化し，一般送配電事業者においてスマートメーターシステムに関するセキュリティガバナンスの構築を行うこと。（勧告）

３．目的の明確化

　スマートメーターシステムのセキュリティの実施目的を明確にすること。（勧告）

第２-２条　役割

１．責任者の設置

スマートメーターシステムのセキュリティ管理責任者を任命すること。（勧告）

２．役割の定義

スマートメーターシステムに関連する者の役割を明確にすること。（勧告）

３．委託先等の対応

スマートメーターシステムに関連する委託先等のセキュリティに関する役割を明確にすること。（勧告）

第２-３条　セキュリティ教育

１．教育の計画・実施

スマートメーターシステムに関するセキュリティ教育を計画し，実施すること。（勧告）

２．教育効果の確認

スマートメーターシステムに関するセキュリティ教育が効果的に実施されていることを確認すること。（勧告）

第３章　文書化

第３-１条　文書管理

１．文書化

スマートメーターシステムのセキュリティに関する情報を文書化すること。（勧告）

２．文書の管理

スマートメーターシステムのセキュリティに関する文書を適切に管理すること。（勧告）

第３ - ２条　実施状況の報告

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。（勧告）

第４章　セキュリティ管理

第４－１条　セキュリティ管理

セキュリティマネジメントシステムを構築すること。（勧告）

第５章　機器のセキュリティ

第５－１条　セキュリティ仕様

１．機器のセキュリティ仕様

機器の調達時にセキュリティ仕様を明確にすること。（推奨）

２．準拠性の確認

機器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。（推奨）

３．セキュリティ仕様の変更

機器のセキュリティ仕様を変更できる仕組みを構築すること。（推奨）

第５－２条　機器の取扱い

機器のライフサイクルにおいて，継続的な管理が可能な手順を明確にすること。（推奨）

第５－３条　ファームウェアアップデート

ファームウェアアップデートを適切かつ確実に実施することができる仕組みを構築すること。（勧告）

第５－４条　認証

予め許可された機器と通信するための認証を行い，スマートメーターシステムを保護すること。（勧告）

第６章　通信のセキュリティ

第６－１条　通信プロトコル

機器間の通信において，通信路上のセキュリティ確保が可能な通信プロトコルを選択すること。（勧告）

第６－２条　暗号

１．暗号の利用

機器間の通信や機器が保有する重要なデータは暗号化すること。（勧告）

２．暗号鍵の管理

暗号鍵は適切に配布し，管理すること。（勧告）

第６－３条　ネットワークの管理

１．ネットワークへのアクセス制御

スマートメーターシステムのネットワークに対する適切なアクセス制御を行うこと。（勧告）

２．ネットワークの分離

スマートメーターシステムのネットワークは，原則として外部ネットワークと分離し，外部ネットワークと接続する場合は接続点を最小化すること。（勧告）

第７章　システムのセキュリティ

第７－１条　システム設計

１．プログラムの実行制限

予め定められたプログラムのみが実行されるようにすること。（勧告）

２．コマンド管理

コマンドが不正に発行されないようにすること。（推奨）

３．外部記憶媒体の利用制限

原則として外部記憶媒体の利用を制限すること。（推奨）

第８章　運用のセキュリティ

第８－１条　システムの管理

１．管理者権限の管理

管理者権限の割当を適切に行い，不正行為が行われない仕組みを構築すること。（推奨）

２．マルウェア対策

マルウェア対策を実施すること。（勧告）

３．変更管理

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。（勧告）

４．ログの取得

ログを取得，保持し，定期的に確認すること。（勧告）

第８－２条　機器の管理

機器を管理し，状態を監視すること。（推奨）

第８－３条　データの管理

スマートメーターシステムに関連するデータを管理し，保護すること。（推奨）

第８－４条　ぜい弱性の管理

ぜい弱性に関する情報を継続的に管理すること。（推奨）

第９章　物理セキュリティ

第９－１条　施設及び機器の管理

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。（推奨）

２．アクセス管理

セキュリティ区画には認可された者だけにアクセスを許可し，そのアクセス記録を保持すること。（推奨）

第１０章　セキュリティ事故の対応

第１０－１条　セキュリティ事故とセキュリティ事象

セキュリティ事故とセキュリティ事象を定義し，判断に必要な証拠を収集すること。（勧告）

第１０－２条　セキュリティ事故の対応

セキュリティ事故やセキュリティ事象の対応体制と手順を明確にすること。（勧告）

第１０－３条　セキュリティ事故の報告と情報共有

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は，一般送配電事業者内だけではなく関係機関への報告及び対応を行うこと。（勧告）

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。（勧告）

第１０－４条　周知と訓練

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。（勧告）

第１１章　サービス継続管理

第１１－１条　サービス継続管理

１．サービス継続計画

スマートメーターシステムで提供する機能を定義し，それぞれの関連性を考慮してサービス継続のための計画を構築すること。（勧告）

２．事故対応

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。（勧告）

３．改善の検討

サービス継続のための計画が計画通りに実施されているかを定期的に確認し，改善の要否を検討すること。（勧告）