資料１別紙

次世代スマートメーターシステムの標準対策要件に新しく盛り込むべき事項

１．外部接続のセキュリティ

1.1　管理主体の異なる外部機器・システム接続

目的：管理主体の異なる外部機器・システムとスマートメーターシステムを接続する場合のセキュリティの運用・管理を確実にするため。

管理策：管理主体の異なる外部機器・システムに対して、スマートメーターシステムに接続して利用する場合に満たすべきセキュリティ要件を定めること。外部接続に起因した、管理主体の異なる外部機器・システムからの攻撃からスマートメーターシステムを守り、また、スマートメーターシステムから管理主体の異なる外部機器・システムへの攻撃を防ぐために、リスクアセスメントの実施や脆弱性管理、外部接続用ネットワークとの区別・分離、外部接続用ネットワークとの通信に関するログの取得・監視といった適切なセキュリティ対策を講ずること。

1.1.1　外部接続基準・ガイドラインの作成

対策：管理主体の異なる外部機器・システムをスマートメーターシステムに接続する場合の外部接続基準・ガイドラインを作成すること。

なお、国の行政機関や民間の業界団体が策定・公表している既存の基準・ガイドライン等のうち、スマートメーターシステムと外部接続する機器・システム等に関連する基準・ガイドライン等において、外部接続における必要なセキュリティ対策が求められている場合は、外部接続基準の作成において、それも十分に参照すること。

リスク例：セキュリティ確保が十分に行われず、接続を許可する機器へのなりすましや通信路上での盗聴や情報の改竄などが発生する可能性がある。

1.1.2 リスクアセスメントの実施

対策：管理主体の異なる外部機器・システムからの攻撃等の脅威を考慮したリスク評価を実施すること。

リスク例：外部機器・システムがマルウェアに感染したり、不正に侵入されたりすることにより、外部機器・システムから攻撃を受け、スマートメーターシステムへの不正アクセスや情報窃取などが発生する可能性がある。また、スマートメーターシステムから管理主体の異なる外部機器・システムに影響を与える可能性がある。

1.1.3 脆弱性管理

対策：システム構築時点において、攻撃者目線で、悪用される可能性のあるセキュリティ上の欠陥を発見・評価するため、管理主体の異なる外部機器・システムの接続に用いるネットワークやその接続点に設置される機器に対して、ペネトレーションテスト等を行うこと。システム運用時点において、管理主体の異なる外部機器・システムの接続に用いるネットワークとの接続点に設置される機器の脆弱性管理を行うこと。

リスク例：外部接続用ネットワークやその接続点に設置される機器に脆弱性が存在する場合、脆弱性が悪用されて、マルウェアに感染したり、不正に侵入されたりすることにより、スマートメーターシステムが当該機器から攻撃を受け、サービスの継続に影響を与える可能性がある。また、スマートメーターシステムから管理主体の異なる外部機器・システムに影響を与える可能性がある。

1.1.4 外部接続用ネットワークとの区別・分離

対策：管理主体の異なる外部機器・システムの接続に用いるネットワークと、スマートメーターシステムのネットワークを接続する場合は、相互を区別・分離可能なネットワーク構成を採用するとともに、中継される通信の極小化を行うこと。

リスク例：ネットワークへの不正なアクセスやマルウェアの侵入により、情報が保護できない可能性や、正常なネットワークアクセスが確立できない可能性がある。

1.1.5 外部接続用ネットワークとの通信に関するログの取得と監視

対策：管理主体の異なる外部機器・システムの接続に用いるネットワーク及び接続点に設置される機器の動作に関するログの取得と監視を行うこと。

リスク例：外部接続用ネットワークとの通信に関するログが適切に取得・監視されていないことにより、管理主体の異なる外部の機器・システムからの攻撃の検知が遅れ、停電が発生するなどサービスの継続に影響を与えたり、再発防止などの改善が適切に行われなかったりする可能性がある。

2. 外部接続事業者の管理

2.1 外部接続事業者との間の合意形成

目的：スマートメーターシステムの安全性・安定性の確保に関して、スマートメーターシステムの情報管理責任組織と外部接続事業者（スマートメーターシステムに接続される管理主体の異なる外部機器・システムの情報管理責任組織）間における義務と責任について明確化し、セキュリティの運用・管理や確保を確実に担保するため。

管理策：セキュリティ対策やサービスレベル、責任分担について、その内容が確実に実施されるように、スマートメーターシステムに接続する外部接続事業者との間で事前に合意すること。

2.1.1 通報義務

対策：外部機器・システムにおいて、スマートメーターシステムの安全性・安定性を損なうおそれがある事態が発生又は発覚した場合は、速やかにスマートメーターシステムの情報管理責任組織へその旨を通報するとともに、必要な対処を行い、その経過を連絡し、要因究明を行うことについて、外部接続事業者との間で事前に合意を形成すること。

リスク例：外部接続事業者において発生している事象等を把握しないことにより、スマートメーターシステムへの被害が拡大する可能性や初動・復旧が遅延する可能性がある。

2.1.2 システムの維持・運用

対策：セキュリティ確保に向けたシステムの維持・運用における協力事項に関して、事前に合意を形成すること。

リスク例：セキュリティ確保に向けて、双方で行うべき運用等を事前に定めておかないことにより、インシデント発生時にスマートメーターシステムへの被害が拡大する可能性や初動・復旧が遅延する可能性がある。

2.1.3 外部機器・システムのネットワーク接続の遮断と再接続

対策：スマートメーターシステムに接続している管理主体の異なる外部機器・システムについて、外部との通信ログの監視等により、セキュリティリスクが高いと判断された場合に、該当する特定通信を遮断するための仕組みや、遮断された機器・システムの管理主体による遮断解除の申告に基づいて、該当する特定通信を再接続するための仕組みを構築し、双方の仕組みの運用に関する実施基準や実施内容、実施体制・手順について、外部接続事業者との間で事前に合意を形成すること。

リスク例：スマートメーターシステムの安全性・安定性の確保に関して、スマートメーターシステムの情報管理責任組織、外部接続事業者の双方において義務と責任が果たされず、スマートメーターシステムへの被害が拡大する可能性や初動・復旧が遅延する可能性がある。また、スマートメーターシステムから管理主体の異なる外部機器・システムに影響を与える可能性がある。

2.1.4 責任分界点の設定

対策：事故やトラブルの発生時の対処を含め、外部接続事業者を中心とした関係者間の管理責任の分担について責任分界点を明確にし、外部接続事業者との間で事前に合意を形成した内容で対応すること。

リスク例：スマートメーターシステムの安全性・安定性の確保に関して、スマートメーターシステムの情報管理責任組織、外部接続事業者の双方において義務と責任が果たされず、スマートメーターシステムへの被害が拡大する可能性や初動・復旧が遅延する可能性がある。また、事故やトラブル発生時の作業分担が明確

でないため、契約者への通報業務、現地調査の派遣、機器・システムのログ調査などが漏れたり、重複したりすることによって、混乱が生じ、初動・復旧の対応を誤る可能性がある。

3. セキュリティ管理・対応の高度化

3.1 システムのライフサイクルを考慮したセキュリティ対策

目的：設計、調達、運用・保守、廃棄といったシステムのライフサイクルの各フェーズにおいて適切なセキュリティ対策を取り入れることにより、スマートメーターシステム全体における最適なセキュリティを確保するため。

管理策：システムのライフサイクルの各フェーズにおいて想定される脅威・リスクに対応して適切なセキュリティ対策を取り入れ、スマートメーターシステムにおけるセキュリティ対策の全体最適化を図ること。

3.1.1 設計フェーズのセキュリティ対策

対策：「スマートメーターシステムセキュリティガイドライン」の「第５章 機器のセキュリティ」に規定されているセキュリティ要件を遵守すること。

リスク例：「スマートメーターシステムセキュリティガイドライン」の「第５章 機器のセキュリティ」に記載されているリスク例を参照すること。

3.1.2 調達フェーズのセキュリティ対策

対策：スマートメーターシステムを構成する機器等を調達する際には、国の行政機関における情報システムに係る調達の動向等を踏まえつつ、意図せざる変更がなされないように、事前に確認すること。

リスク例：機器やネットワークに不正な侵入口を作り込むバックドアや、知らないうちにシステムから情報を盗み取るスパイウェア等の不正プログラム等が、調達された機器等に組み込まれることにより、スマートメーターシステムへの被害が拡大する可能性がある。

3.1.3 運用フェーズのセキュリティ対策

対策：「スマートメーターシステムセキュリティガイドライン」の「第８章 運用のセキュリティ」に規定されているセキュリティ要件を遵守すること。

リスク例：「スマートメーターシステムセキュリティガイドライン」の「第８章 運用のセキュリティ」に記載されているリスク例を参照すること。

3.1.4 廃棄フェーズのセキュリティ対策

対策：スマートメーターシステムの更改等の理由により、機器等を廃棄する場合には、新システムへの安全な移行を担保すべく、復元できない方法により当該データの消去・削除を行うなど、適切な処理を行うこと。

リスク例：機器等の廃棄を外部委託する委託先において機器等が不正に転売されたり、機器等に記録されている情報が流出・漏洩したりすることにより、スマートメーターシステムに対する攻撃に悪用される可能性がある。

4. 実効性のあるリスクアセスメント

目的 : スマートメーターシステムのセキュリティ対策を継続的に改善し、対策を計画に従って適切に行えるようにするため。

管理策 : セキュリティマネジメントシステムを構築すること。

対策 : 実績のあるセキュリティフレームワークなどを参考にしながら、検知・対応・復旧などを念頭に置いたリスクアセスメントを行うこと。また、異常を速やかに検知し、検知した際に速やかな対応を講じるための対応策を検討するとともに、異常を取り除き、通常状態に復旧するための復旧策を検討すること。

リスク例:インシデントレスポンスを実施できるかを検討しない場合、実際のインシデントが発生した際に、スマートメーターシステムへの被害が拡大する可能性がある。