別添

2021 年 12 月●日

中部電力株式会社

情報管理計画書

1. 概要

（ア） 目的

本計画書は、中部電力株式会社（以下「当社」という。）が、特定重大事故等対処施設に関する秘密保持契約書（原規技発第 1410201 号）（以下「契約書」という。）に基づいて提供される秘密情報の漏えい、滅失、毀損の防止その他の秘密情報の適切な管理のために必要な措置を定めることを目的とする。

（イ） 本計画書で用いる用語定義

① 秘密情報

本計画書で管理の対象とする「秘密情報」とは、媒体の形式を問わず、甲が乙に対し秘密情報と明示して開示した情報及び当該情報を使用して作成された情報であって、甲が乙に対し秘密情報と明示し開示した情報の内容が推測できるもの並びにこれを複製・複写したものをいう。ただし、以下に該当する場合にはその限りではない。

- 原子力規制庁より開示を受ける前より既に保有していた情報
- 正当な手段により、第三者から受けた情報
- 既に公表されており、一般に入手可能な情報
- 書面により原子力規制庁が事前に公表を承認した情報
- 当社が独自の方法により発明又は開発した情報

② 書面

文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物をいう。

③ 電磁的記録

電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるものをいう。

2. 情報セキュリティに係る社内規程類

秘密情報は、当社が定める以下の情報セキュリティ関係規程類に従い情報セキュリティ対策を実施する。秘密情報に係る具体的な情報セキュリティ対策については、第 3 項以降に記載する。

	規程分類	文書名
1	情報セキュリティ対策に係る規程	情報管理規程 ＩＴシステムセキュリティ規程 特定重大事故等対処施設に係る秘密情報取扱手引（QMS）※
2	第三者提供に係る規程	特定重大事故等対処施設に係る秘密情報取扱手引（QMS）※

※原子力部門ＱＭＳ指針「文書管理指針」に基づき管理している個別文書

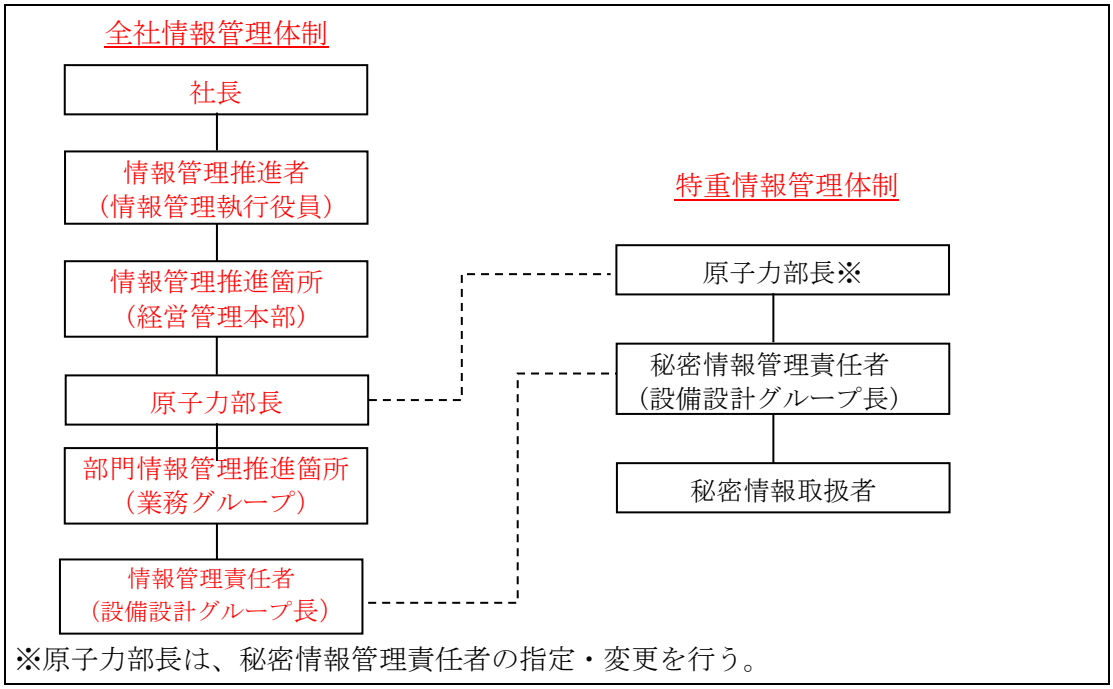
3. 秘密情報の取扱方法

（ア） 管理責任者、取扱者の役割と体制

秘密情報の取扱いに係る当社の情報セキュリティ管理体制は以下のとおりとする。

役割名称	役割
秘密情報管理責任者（管理責任者）	秘密情報に関する台帳管理および保管並びに受注者の適合性確認等、秘密情報を管理・保持するために必要な措置を講ずる者。
秘密情報取扱者（取扱者）	秘密情報を業務上取扱う必要がある者で、秘密情報について秘密保持義務が課せられる者。

体制図



※原子力部長は、秘密情報管理責任者の指定・変更を行う。

（イ） 秘密情報の取扱方法

秘密情報の取扱いは以下に従うものとする。

取得・入力時	秘密情報管理責任者は、秘密情報を取得・入力時に『秘密情報管理簿』に必要事項を記載し管理するとともに、秘密情報毎に『秘

	密情報利用管理簿』を作成する。 秘密情報はその旨表示し識別する。
利用・加工・複製	利用日時、用途、目的、持出先および持ち出す際の管理方法等の必要事項を『秘密情報利用管理簿』に記載し、秘密情報管理責任者の許可を得る。 複製・複写を行う場合は、秘密情報管理責任者の承認を受けるとともに、『秘密情報管理簿』に記載し管理する。
保存・保管	秘密情報管理責任者は、秘密情報取扱者以外の者が秘密情報にアクセスすることがないよう、書面の秘密情報の場合には施錠管理した金庫、キャビネット等で当該情報を保管する。 電磁的記録の秘密情報の場合には、秘密情報取扱者のみがアクセスできるフォルダ内に保存し管理するとともに、閲覧用パスワードを設定する。 秘密情報管理責任者は、秘密情報取扱者に秘密情報が適切に保管されていることを月１回確認させ、記録を作成させる。
移送・送信・運搬	・保管場所から持ち出さないことを原則とする。 ・やむを得ず持ち出す場合は、以下の通り対応する。 ①秘密情報取扱者間で、直接授受する。 ②電子メールで取扱う場合は、秘密情報取扱者間で連絡を取り合うとともに閲覧用のパスワード設定を行う。
消去・廃棄、その他	消去・廃棄等を行う場合、当該の秘密情報の指定を解除する。 秘密情報取扱者は秘密情報を返却した場合、『秘密情報管理簿』および『秘密情報利用管理簿』に返却した旨を記載し、秘密情報管理責任者の確認を受ける。 秘密情報を廃棄する際、書面の場合は焼却や裁断、電磁的記録の場合はファイルの完全削除等の復元不可能な方法で廃棄するとともに『秘密情報管理簿』および『秘密情報利用管理簿』に廃棄の処理結果を記載し、秘密情報管理責任者の確認を受ける。

（ウ）　第三者への提供の有無及び提供先における秘密情報の取扱い方法

提供の有無	無
提供先名称 （複数ある場合は全て記載すること）	―
秘密情報の授受	―
秘密情報の管理に係る措置	―

4. 情報管理に関する計画

当社は、以下に各号に掲げる場合にあっては、速やかに、それぞれに対応するものに記録する。

（１） 秘密情報取扱者を指定した場合　秘密情報取扱者名簿

（２） 秘密情報を指定、加工、複製・複写、返却、廃棄又は消去した場合　秘密情報管理簿

（３） 秘密情報を利用した場合、第三者へ提供を行った場合　秘密情報利用管理簿

5. 秘密情報の教育・研修・周知に関する計画

当社は、情報管理規程に定める情報管理に関する教育に加えて、秘密情報における情報セキュリティに関する教育を以下のとおり実施する。

教育内容	秘密情報管理に関する教育
対象者	秘密情報を業務上取扱う必要がある者
実施目的	秘密情報の漏えい防止のための管理方法等、秘密情報の保持に必要な知識の習得のため。
実施方法	秘密情報取扱者による対面（Web 会議含む）
実施頻度	秘密情報取扱者指定時

また、本計画書に定める事項について、秘密情報に関与する者に周知する。

教育内容	前述の教育に包含されるため、下記項目含め記載は省略。
対象者	―
実施目的	―
実施方法	―
実施時期	―

6. 情報セキュリティ確保に関する計画

（ア） 物理セキュリティ

秘密情報の保管場所及び保管場所における物理的な対策を以下のとおり定める。

保管場所	施錠管理している耐火キャビネット
入退室制御に係る設備（IC カードリーダ等）	執務室入室時の IC カードリーダによる認証
入室許可者	当社従業員
持込禁止物	特になし

入室許可者以外の管理	当社従業員の随行による行動の管理
その他対策内容詳細	特になし

（イ） 情報機器のセキュリティ

秘密情報を取り扱う情報機器及び情報機器に対する情報セキュリティ対策を以下のとおり定める。

情報機器	PC サーバ内特重専用共有フォルダ
セキュリティ機能 （ID 管理、ウイルス対策、アクセスブロック等）	PC: ・複雑なパスワード設定により第三者のアクセスをブロック ・内蔵ハードディスクの暗号化設定、外部記憶媒体接続データ保存時の自動暗号化により情報漏えいを防止 サーバ: ・秘密情報を保管する専用の共有フォルダを作成し、ID 管理を利用した共有フォルダへのアクセス制限 全般: ・ソフトウエア、ウィルス対策ソフトの導入、これらを随時アップデートすることにより脆弱性を排除 ・インターネットから社内のアドレスを隠蔽化することにより不正アクセスを防止
利用者 ID や情報機器の管理方法（管理簿等）	PC・サーバ ・原則、個人単位のPC配布、資産管理システムおよび定期的な現品実査による情報機器の設置箇所と利用者の管理。
モニタリング手法（稼働監視等）	・24 時間体制による社外からの不正アクセスを監視 ・セキュリティ事故発生時、システム利用ログの分析による原因調査
その他対策内容詳細	特になし

7. 情報セキュリティインシデント発生時の対応手順

（ア） 情報セキュリティインシデント発生時の対応体制

当社の秘密情報に係る情報セキュリティインシデント発生時の体制は以下のとおりとする。

名称	氏名	連絡先
インシデント対応責任者	[redacted]	メールアドレス：[redacted] 電話番号：[redacted]
インシデント対応者	[redacted]	メールアドレス：[redacted] 電話番号：[redacted]

（イ） 想定される主な事象

秘密情報の紛失、漏えい、もしくは秘密情報を電子データで取り扱うパソコンにウィルス等の感染もしくは秘密情報が保存されたパソコンが置かれたネットワークに接続された他のパソコン／サーバにウィルス等の感染があった場合等の紛失もしくは漏えいのおそれがあることを発見した場合

（ウ） 報告手順

① 秘密情報取扱者は、インシデント発生時において、その状態を発見した場合に、直ちに秘密情報管理責任者に連絡する。

② 秘密情報管理責任者は、秘密情報の漏えいがあった場合にはその事実を速やかに原子力規制庁へ報告する。

③ 秘密情報管理責任者は、①の事実について、原因の調査を行う等の対応を行う。