別添

2021 年　月　日
九州電力株式会社

案

情報管理計画書

1. 概要

（ア）　目的

本計画書は、九州電力株式会社（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（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

※甲・乙はそれぞれ契約書に定める原子力規制委員会、当社の契約者を指す。

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	・情報セキュリティ管理規程 ・特定重大事故等対処施設に関する情報管理要領（品質マネジメントシステムに係る社内規程）

#	規程分類	文書名
2	第三者提供に係る規程	・情報セキュリティ管理規程 ・特定重大事故等対処施設に関する情報管理要領（品質マネジメントシステムに係る社内規程）

3. 秘密情報の取扱方法

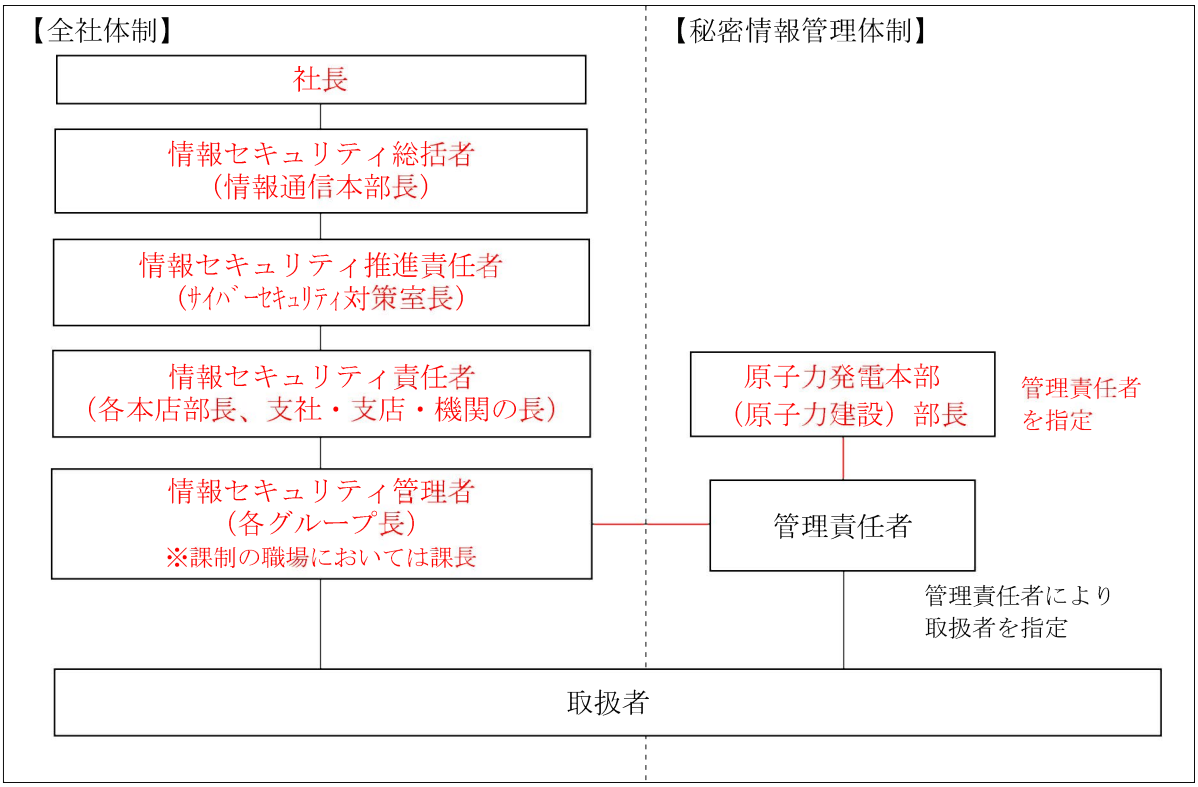
（ア） 管理責任者、取扱者の役割と体制

当社の情報セキュリティに関する全社体制は情報セキュリティ管理規程に基づく。

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
原子力発電本部 （原子力建設）部長	管理責任者の指定を行う者
管理責任者	【管理責任者】 契約書に基づき秘密情報の管理について責任を負う者
	【補助管理責任者】 管理責任者が任意に指定し、自らの責務の一部を負わせる者
	【補助管理責任者臨時代行者】 管理責任者が任意に指定し、補助管理責任者の職務を臨時に代行する者
取扱者	当社役員・従業員等で秘密情報を業務上知る必要があり、管理責任者により指定された者

体制図



（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	・秘密情報を受領しようとするときは、情報管理計画書を原子力規制庁に提出し、承認を得る。 ・秘密情報の提供を受けたときには、速やかに秘密情報の受領書を原子力規制庁に提出する。 ・秘密情報を適切に管理するため、秘密情報管理簿に記載する。
利用・加工・複製	・秘密情報の利用（秘密情報を第三者に提供した場合を含む。）の状況について秘密情報利用管理簿に記載する。 ・秘密情報の複製、複写は原則禁止する。ただし、秘密情報を複製、複写する必要が生じた場合、管理責任者の許可を得る。
保存・保管	・施錠管理ができるキャビネット等に秘密情報を保管する。 ・電子データについては、取扱者以外の者がアクセスできないよう、アクセス制限されたフォルダにて取扱う。
移送・送信・運搬	・手交は可。ただし、本人に直接手渡しする。 ・原則として、配達不可。ただし、やむを得ず送付する必要がある場合は、簡易書留（又はこれに類するもの）を利用し、封筒等に「親展」と朱記（又は押印）する。 ・電子メール等を用いた電子データの送付は不可。 ・ＦＡＸによる送信は不可。
消去・廃棄、その他	・契約書の契約が終了した場合又は原子力規制庁から要求を受けた場合には、原子力規制庁の指示に従って秘密情報を直ちに返却、廃棄又は消去するものとする。 ・返却、廃棄又は消去した場合は秘密情報管理簿に指定解除日又は廃棄日を記載する。廃棄する場合は、焼却、裁断その他復元不可能な方法を用いる。 ・秘密情報の取扱いに関する管理状況等の確認を１回／年以上行う。

（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	―
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。

（ア） 取扱者を指定した場合 秘密情報取扱者名簿

（イ） 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

（ウ） 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、全社での情報セキュリティに関する教育を情報セキュリティ管理規程に基づき、1回／年で実施する。また、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	特定重大事故等対処施設における秘密情報取扱いに関する教育
対象者	取扱者
実施目的	特定重大事故等対処施設における秘密情報取扱いの理解及び管理の徹底
実施方法	管理責任者等による教育（ＴＶ会議等を含む）
実施頻度	１回／年

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	上記教育に包絡される。
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	施錠管理ができるキャビネット等
入退室制御に係る設備 （IC カードリーダ等）	施錠管理
入室許可者	取扱者
持込禁止物	—
入室許可者以外の管理	—
その他対策内容詳細	—

（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	社内パソコン
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）	・取扱者の ID を登録することにより秘密情報へのアクセス管理を行い、取扱者以外のアクセスを制限 ・コンピュータウィルス等の不正ソフトウェアの侵入を防止し、検出 ・社内パソコンから外部へ電子データを持ち出す際に、当該電子データを自動的に暗号化
利用者 ID や情報機器の管理方法（管理簿等）	秘密情報取扱者名簿により ID を管理
モニタリング手法 （稼働監視等）	社外からの不正アクセスの監視
その他対策内容詳細	外部メディアへの書出し禁止

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	氏名、連絡先については別紙にて通知する。	
インシデント対応者	氏名、連絡先については別紙にて通知する。	

（イ） 想定される主な事象

秘密情報の紛失、盗難、情報漏えい及びサイバー攻撃

（ウ） 報告手順

① 取扱者はインシデントを発見した場合は、直ちにインシデント対応責任者に連絡する。

② インシデント対応責任者は、インシデントの発生を認めたとき及びそのおそれがある場合は、速やかに情報セキュリティ総括箇所と連携し、初動（緊急措置）を行い、その後直ちにその日時、場所、その他必要な事項を原子力規制庁に報告する。

③ ②項の場合において、インシデント対応責任者は、秘密保全上必要な措置を講じるとともに、秘密保全上講じた措置を原子力規制庁に報告する。

8. その他

本計画書に定める事項を変更する場合は、原子力規制庁に速やかに報告する。