2021年12月日（改訂2）
東京電力ホールディングス株式会社
原子力設備管理部安全施設建設センター

情報管理計画書

1. 概要

（ア） 目的

本計画書は、東京電力ホールディングス株式会社（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1410171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	・システムセキュリティ規程 ・情報事務取扱規程 ・特重設関連情報管理ガイド
2	第三者提供に係る規程	・特重設関連情報管理ガイド

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
安全施設建設センター所長	・安全施設建設センターの総括管理 ・原子力規制庁との秘密保持契約の締結 ・管理責任者の指定・変更及び原子力規制庁への通知
安全施設建設センター副所長	・安全施設建設センター所長の補佐 ・情報セキュリティインシデント発生時の対応責任者及び原子力規制庁への報告
管理責任者	・秘密情報の管理について責任を負う者 ・情報セキュリティインシデント発生時の対応者 ・秘密情報取扱者の指定及び解除
取扱者	・秘密情報を業務上知る必要があり、管理責任者に指定された者

体制図

[redacted]

(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	・秘密情報の提供を受けた場合は、速やかに「秘密情報の受領書」を原子力規制庁に提出する。また、「秘密情報管理簿」に必要事項を記載するとともに、その情報が秘密情報であることを明記して識別する。

	・秘密情報の提供を受けた場合は、「情報管理計画書」を原子力規制庁に提出し、承認を得る。
利用・加工・複製	・秘密情報を利用する場合は「秘密情報利用管理簿」に必要事項を記載する。 ・秘密情報を利用する場合は、情報保護区域内で行う。 ・複製・複写は原則禁止とする。やむを得ず行う場合は「秘密情報利用管理簿」に記載し、必要最小限にとどめる。また、目的を達したあとは速やかに廃棄する。
保存・保管	・紙媒体の秘密情報は、施錠管理された金庫、キャビネット等で保管する。 ・電子データの秘密情報は、アクセス制限が設定されたネットワーク上のフォルダ内に保存する。
移送・送信・運搬	・秘密情報の受渡しを行う場合は、取扱者間で直接授受する。 ・送付の場合は郵便書留等、配送状況が確認可能な措置を講じ、取扱者間で送受信の確認を行う。 ・電子データの秘密情報は、電子メールに添付しての送信は行わない。電子メールで送信する場合は、アクセス制限が設定されたネットワーク上のフォルダのリンクを貼り付け送信する。
消去・廃棄、その他	・秘密情報が業務上不要となった場合、契約が終了した場合または原子力規制庁から要求を受けた場合は、原子力規制庁の指示に従って秘密情報を直ちに返却、廃棄または消去する。また、「秘密情報管理簿」に返却、廃棄等の必要事項を記載する。 ・紙媒体及び電子データ等の廃棄の方法は、焼却、裁断その他復元不可能な方法で廃棄する。 ・秘密情報の管理状況等を定期的に確認する。

（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	・無し
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）　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、全社の情報セキュリティ教育（年１回）受講のうえ、秘密情報の取扱いに関する教育を以下のとおり実施する。

教育内容	・特重設関連情報管理ガイドの教育
対象者	・秘密情報取扱者
実施目的	・秘密情報の取扱い及び管理の徹底
実施方法	・ｅラーニング、メール等での周知
実施頻度	・定期（年１回） ・新規取扱者指定時 ・情報管理ガイドに変更があった場合

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	・上記教育に計画書内容の周知を含める。
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	・施錠管理された金庫、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）	・施錠管理が可能で入室制御された執務室
入室許可者	・安全施設建設センター所員
持込禁止物	―
入室許可者以外の管理	・原則入室許可者以外の入室は不可。やむを得ず入室させる場合は、入室許可者による監視
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	・業務用に貸与されたパソコン
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）	・ＩＤ、パスワード等によるアクセス制限 ・ウィルス対策 ・ファイアウォール等により保護されたネットワーク環境を構築
利用者 ID や情報機器の管理方法（管理簿等）	・盗難防止装置を講ずるとともに、社外への持ち出しを禁止 ・パソコン管理台帳による利用者の管理

モニタリング手法（稼働監視等）	・不正アクセス等の監視 ・不審メールの検知 ・ログの採取 ・ソフトウェア等の更新
その他対策内容詳細	・許可されていない外部記憶媒体の接続禁止及びソフトのインストール禁止

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	別途「情報セキュリティインシデント発生時の対応体制通知書」にて通知	
インシデント対応者		

（イ） 想定される主な事象

・秘密情報の紛失、漏えい等またはその可能性

・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または不正アクセスがあった場合またはそれらの可能性

（ウ） 報告手順

①秘密情報取扱者は、情報セキュリティインシデント発生時及びその可能性がある場合は、ⅰ）発生した内容、ⅱ）時期、ⅲ）場所、ⅳ）現状、ⅴ）対応経過、ⅵ）見通しのうち判明している事項を、直ちにインシデント対応責任者及びインシデント対応者へ連絡する。

②インシデント対応責任者は、①項の連絡に基づき、影響を最小限に抑えるために、迅速かつ適切な初動対応を講ずるとともに、直ちに原子力規制庁及び[redacted]へ報告する。

③報告を受けた[redacted]は、[redacted]及び[redacted]へ報告する。

④[redacted]とする[redacted]を開催し、対処方針等を審議し、必要な措置を講じる。

⑤インシデント対応責任者は、情報セキュリティインシデント発生時の原因を調査するとともに再発防止対策を検討し、[redacted]への報告、[redacted]での審議・検討を経て、原子力規制庁へ報告する。

8. その他

なし