泊発電所３号機
安全保護回路の不正アクセス等防止について

平成２５年１１月１９日
北海道電力株式会社

１．安全保護回路の不正アクセス行為防止のための措置について

「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」第二十四条（安全保護回路） 第１項第六号にて要求されている『不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができるものとすること。』に対してディジタル化している安全保護設備（原子炉安全保護盤、工学的安全施設作動盤、安全系現場制御監視盤）について下記の対策を実施している。

〇物理的な分離、機能的な分離対策
安全保護設備は、チャンネル毎及びトレン毎に盤筐体に収納し、他の各チャンネル間、トレン間及び計測制御系等とは物理的分離、機能的分離を行っている。また、他チャンネル等へのデータ伝送は、光信号を用いており、光変換カードによって、電気信号を光信号に変換して他チャンネル等へ送信することで、電気的分離も行っている。

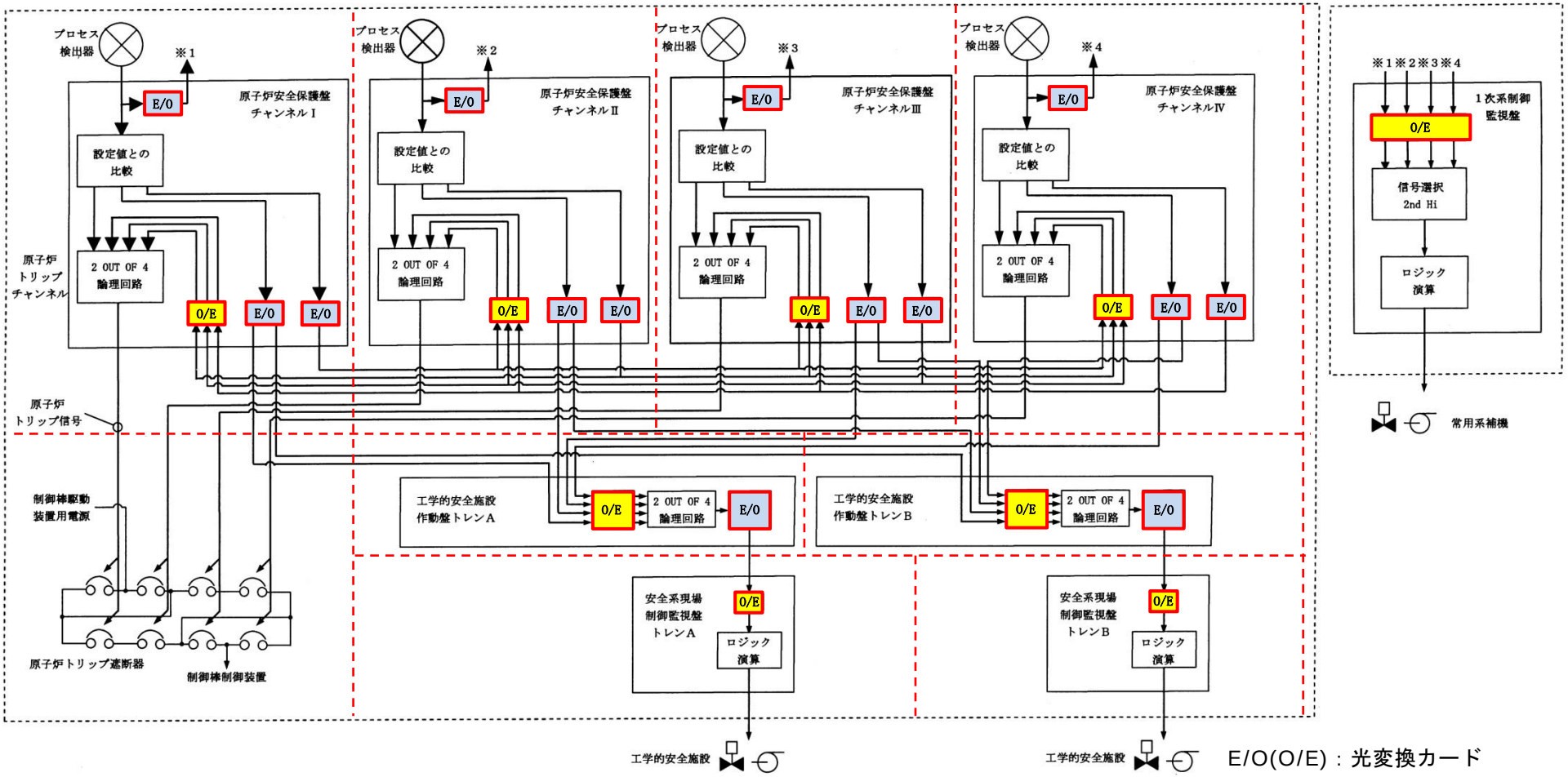
〇外部ネットワークからの不正アクセス及びコンピュータウイルス等の侵入防止対策
外部ネットワークとは、原則、直接接続させない。なお、外部ネットワークと接続させる場合には、外部ネットワークに対して外部からのデータ読み込み機能を設けないこと等により、外部からの不正なアクセス及びコンピュータウィルス等の侵入を防止している。

〇物理的及び電気的アクセスの制限対策
発電所への入域に対しては、出入管理等により入域を制限し、安全保護設備については、盤の施錠及びパスワード管理等によりソフトウェアの管理されない変更を防止している。

〇システムの導入段階、更新段階又は試験段階で承認されていない動作や変更を防ぐ対策
システムの設計、製作、試験、変更管理の各段階で、建設時は「安全保護系へのディジタル計算機の適用に関する指針」（JEAG4609-1999）に基づき検証及び妥当性確認（Ｖ＆Ｖ）を実施し、「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620-2008）及び「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609-2008）に改定されてからは、これらに基づき、安全保護上要求される機能が正しく確実に実現されていることを保証するため、検証及び妥当性確認（Ｖ＆Ｖ）がなされたソフトウェアを使用している。また、パスワード管理等によって関係者以外の不正な変更等を防止している。

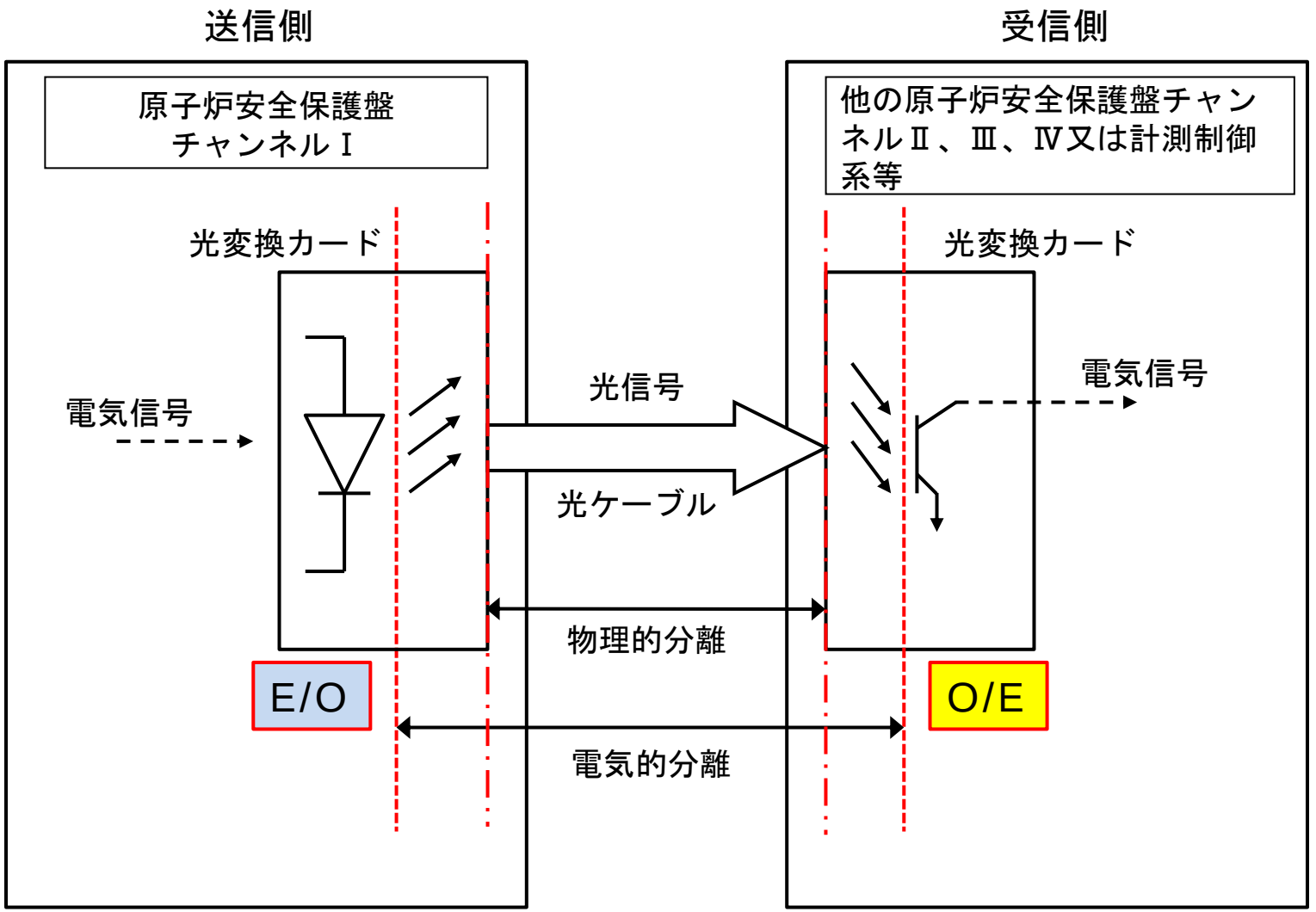
２．物理的分離、機能的分離について

安全保護設備は、チャンネル毎及びトレン毎に盤筐体に収納し、他の各チャンネル間、トレン間及び計測制御系等とは物理的分離、機能的分離を行っている。また、他チャンネル等へのデータ伝送は、光信号を用いており、光変換カードによって、電気信号を光信号に変換して他チャンネル等へ送信することで、電気的分離も行っている。



物理的、機能的分離概念図

２．物理的分離、機能的分離について

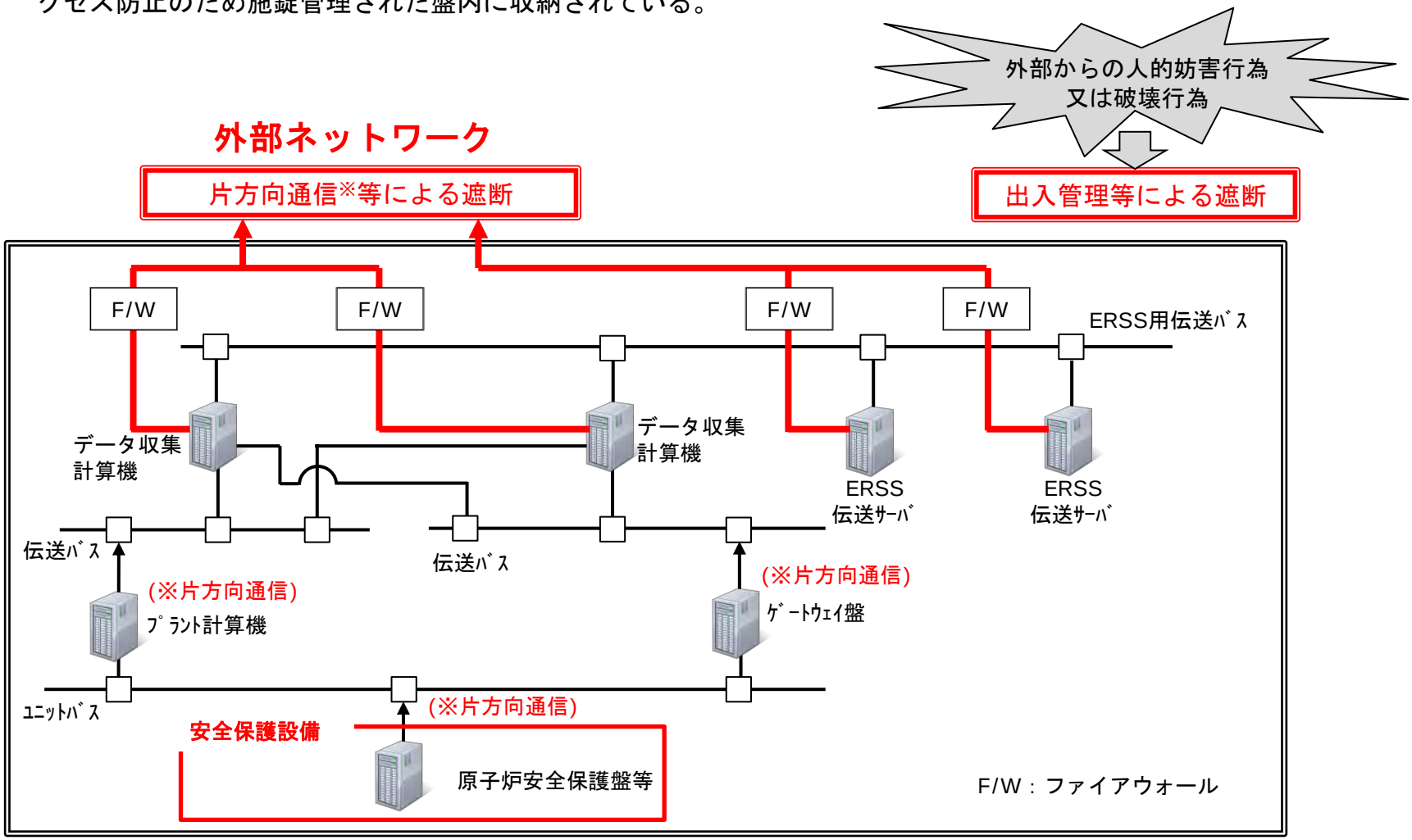


通信における分離概念図

３．外部からの不正アクセス行為防止について

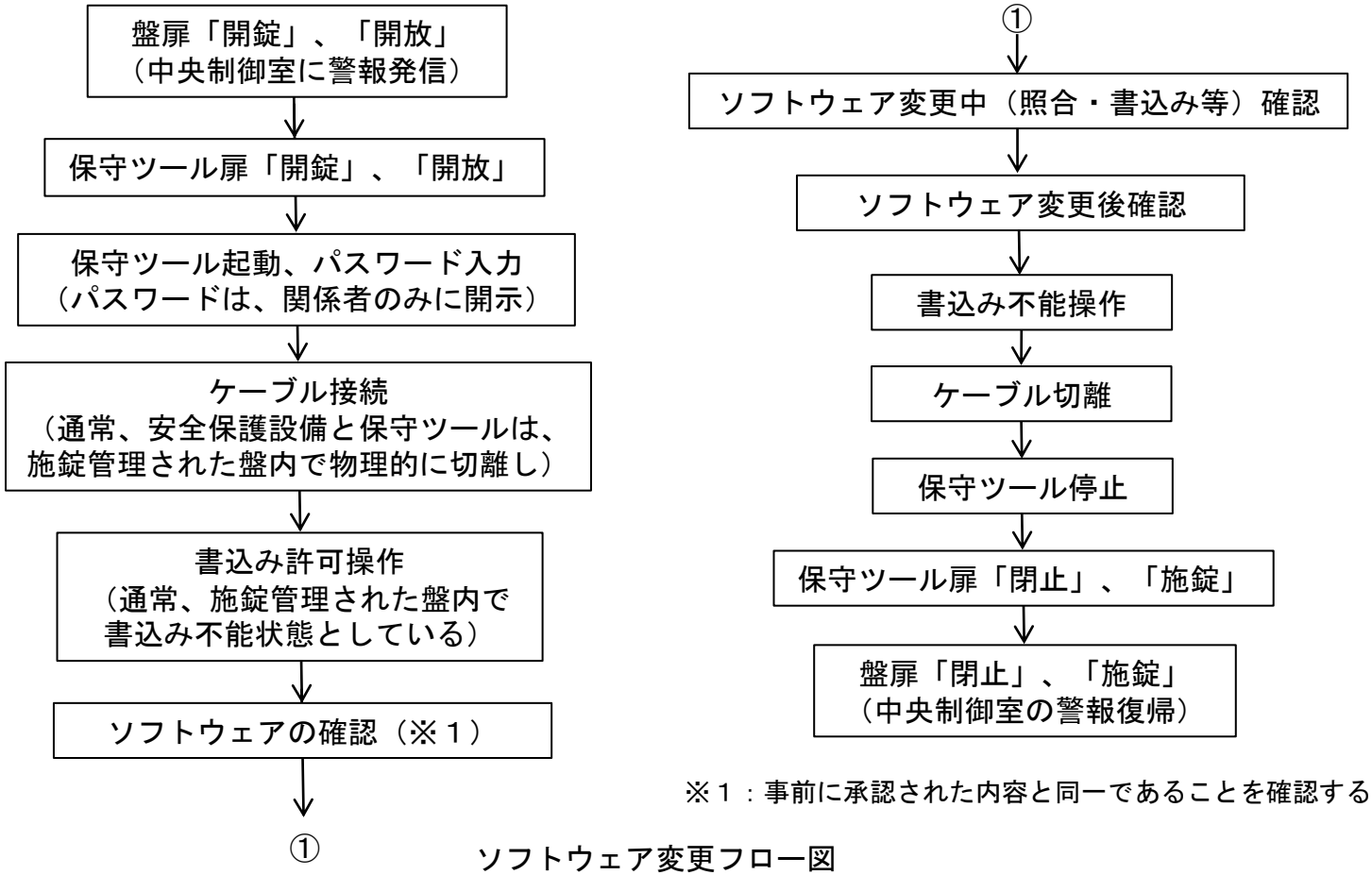
■ 安全保護設備は、以下により外部からの不正なアクセス及びコンピュータウィルス等の侵入を防止している。
- 安全保護設備は、汎用ではないプログラム及び言語を使用している。
- 安全保護設備、プラント計算機、ゲートウェイ盤は、外部ネットワーク側に対して片方向通信としている。
- 安全保護設備は、外部ネットワークと直接接続しない。すなわち、外部ネットワークへの伝送が必要なデータは、データ収集計算機等と外部ネットワーク間にファイアウォール（Ｆ／Ｗ）を設置して伝送している。

■ 外部からの人的妨害行為又は破壊行為について発電所への入域は、出入管理により制限し、盤に対して施錠、パスワード等による関係者以外の接近を防止している。なお、ネットワーク機器を構成しているＨＵＢについても、ポートへの不正アクセス防止のため施錠管理された盤内に収納されている。



４．安全保護設備へのアクセス制限の管理方法について

安全保護設備は、中央制御室と同等の入室管理を行っている安全系計装盤室に設置し、施錠管理している。安全保護設備のソフトウェアの変更にあたっては、安全系計装盤室に設置している施錠管理された保守ツールを使用すること、保守ツール起動時はパスワードを必要とすること等により、管理されないソフトウェアの変更を防止している。また、保守ツールのパスワードは開示を関係者に限定し、定期的に見直している。安全保護設備へソフトウェアをインストールする場合は、作業計画に基づき、当社立会のもと、当社が確認した複数の作業員で以下の手順にて実施する。

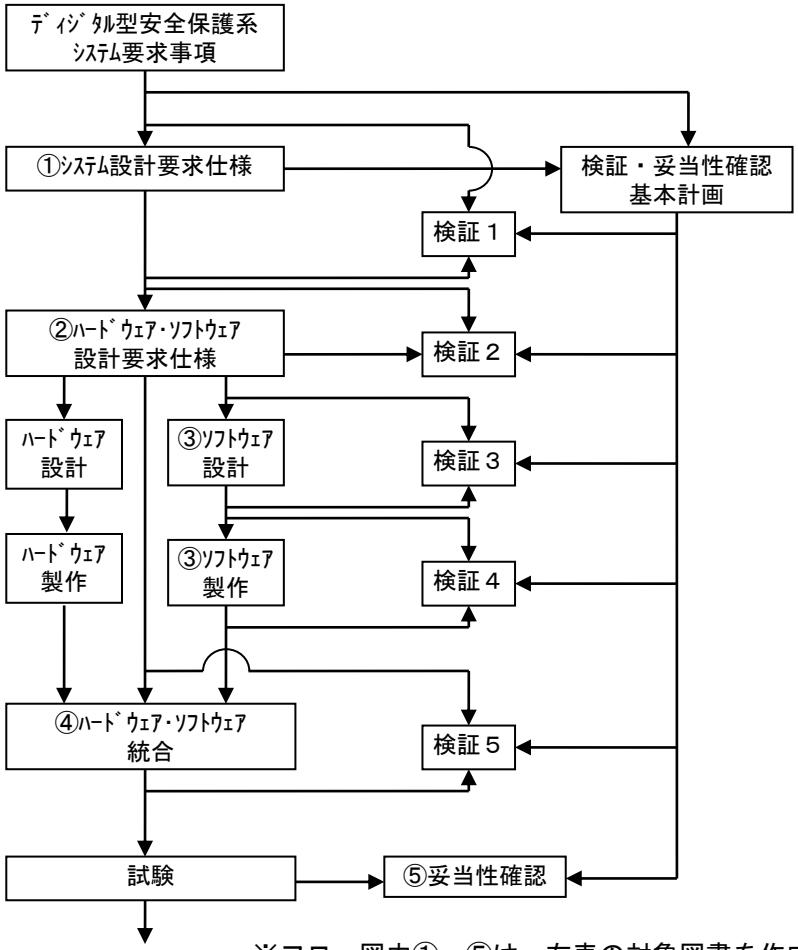


※１：事前に承認された内容と同一であることを確認する。

ソフトウェア変更フロー図

５．安全保護設備の検証及び妥当性確認について

安全保護設備の導入にあたり、設計、製作、試験、変更管理の各段階で、建設時は「安全保護系へのディジタル計算機の適用に関する指針」（JEAG4609-1999）に基づき検証及び妥当性確認（Ｖ＆Ｖ）を実施し、「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620-2008）及び「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609-2008）に改定されてからは、これらに基づき、安全保護上要求される機能が正しく確実に実現されていることを保証するため、検証及び妥当性確認（Ｖ＆Ｖ）がなされたソフトウェアを使用している。



検証項目	検証内容	対象図書
検証１	システム設計要求仕様検証 安全保護系システムへの要求事項が正しく設備の基本設計方針書に反映されていることを検証	①基本設計方針書
検証２	ハードウェア・ソフトウェア設計要求仕様検証 基本設計方針書の要求事項が正しくハードウェア・ソフトウェア設計要求図書に反映されていることを検証	②設備要求仕様書 ブロック図 他
検証３	ソフトウェア設計検証 ソフトウェアの設計要求図書が正しくソフトウェア設計に反映されていることを検証	③ソフトウェア図
検証４	ソフトウェア製作検証 ソフトウェア設計通りに正しくソフトウェアが製作されていることを検証	③ソフトウェア図
検証５	ハードウェア・ソフトウェア統合検証 ハードウェアとソフトウェアを統合してハードウェア・ソフトウェア設計要求仕様通りのシステムとなっていることを検証	④試験要領書 試験成績書
妥当性確認	ハードウェアとソフトウェアを統合して検証されたシステムが、ディジタル安全保護系システム要求事項を満足していることを確認	⑤試験要領書 試験成績書

※フロー図中①～⑤は、右表の対象図書を作成する段階を示すものである。

６．新規制基準への適合状況（１／１５）

「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」
第二十四条（安全保護回路）

新規制基準の項目	適合状況
発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。	
一　運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものとすること。	（規制要求変更なし） 安全保護回路は、運転時の異常な過渡変化時に、原子炉計装あるいは、安全保護系のプロセス計装からの信号により、原子炉停止系を含む適切な系統の作動を自動的に開始させ、燃料の許容限界を超えないようにできる。
二　設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させるものとすること。	（規制要求変更なし） 安全保護回路は、設計基準事故時に、その異常な状態を検知し、原子炉停止系の作動を自動的に開始させることができる。また、非常用炉心冷却設備の作動、原子炉格納容器隔離弁の閉止、原子炉格納容器スプレイ設備の作動等の工学的安全施設の作動を自動的に開始させることができる。
三　安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保するものとすること。	（規制要求変更なし） 原子炉保護設備は、原子炉トリップ演算処理装置、トリップチャンネル、原子炉トリップ遮断器等で構成されている。４つの原子炉トリップ演算処理装置は、安全保護回路のプロセス計装等からの信号を入力し、この信号が設定値に達した場合、チャンネルトリップ信号を発信する。４つのトリップチャンネルは、各々４つの原子炉トップ演算処理装置からの信号を入力し、２つ以上の入力により原子炉トリップ信号を

６．新規制基準への適合状況（２／１５）

新規制基準の項目	適合状況
	発信する。この原子炉トリップ信号は、対応するトリップチャンネルに属する原子炉トリップ遮断器に入力され、２つ以上の原子炉トリップ遮断器が動作すると、原子炉がトリップする。 工学的安全施設作動設備は、４つの工学的安全施設作動演算処理装置及び２つの工学的安全施設作動装置で構成されている。 工学的安全施設作動演算処理装置は、安全保護回路のプロセス計装からの信号を入力し、この信号が設定値に達すると、チャンネルトリップ信号を発信する。２つの工学的安全施設作動装置は、各々４つの工学的安全施設作動演算処理装置からの信号を入力し、２つ以上の入力により、工学的安全施設を作動させる。よって、単一故障又は使用状態からの単一の取外しを行った場合においても安全保護機能を喪失しないよう多重性が確保されている。
四　安全保護回路を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保するものとすること。	（規制要求変更なし） 安全保護回路を構成する計装配管は、実用上可能な限りチャンネルごとに分離及び独立させている。検出器からのケーブル及び電源ケーブルは、各チャンネルごとに専用のケーブルトレイ等を設け、独立に安全系計装盤室の各盤に導き、各原子炉トリップ演算処理装置等は、各々独立の盤に設けている。また、安全保護回路の電源は、相互に分離及び独立した計装用交流母線から、独立に供給されている。
五　駆動源の喪失、系統の遮断その他の不利な状況が発生した場合においても、発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できるものとすること。	（規制要求変更なし） 原子炉保護設備の原子炉トリップ遮断器の不足電圧コイル等は、駆動源の喪失、系統の遮断等に対して原子炉をトリップさせる方向に作動する。また、工学的安全施設作動設備は、駆動源の喪失、系統の遮断等に対してフェイル・セイフとなるか、又は故障と同時に現状維持（フェイル・アズ・イズ）となり、この現状維持の場合でも、多重化された他の回路によって工学的安全施設を作動させることができる設計である。

６．新規制基準への適合状況（３／１５）

新規制基準の項目	適合状況
＜新規要求事項＞ 六　不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができるものとすること。	物理的分離、機能的分離として、安全保護設備は、チャンネル毎及びトレン毎に盤筐体に収納し、他の各チャンネル間、トレン間及び計測制御系等とは物理的分離、機能的分離を行っている。また、他チャンネル等へのデータ伝送は、光信号を用いており、光変換カードによって、電気信号を光信号に変換して他チャンネル等へ送信することで、電気的分離も行っている。 外部ネットワークからの不正アクセス及びコンピュータウイルス等の侵入防止対策として、外部ネットワークとは、原則、直接接続させない。なお、外部ネットワークと接続させる場合には、外部ネットワークに対して外部からのデータ読み込み機能を設けないこと等により、外部からの不正なアクセス及びコンピュータウィルス等の侵入を防止している。 　物理的及び電気的アクセスの制限対策として、発電所への入域に対しては、出入管理等により入域を制限し、安全保護設備については、盤の施錠及びパスワード管理等によりソフトウェアの管理されない変更を防止している。 システムの導入段階、更新段階又は試験段階で承認されていない動作や変更を防ぐ対策として、設計、製作、試験、変更管理の各段階で、建設時は「安全保護系へのディジタル計算機の適用に関する指針」（JEAG4609-1999）に基づき検証及び妥当性確認（Ｖ＆Ｖ）を実施し、「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620-2008）及び「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609-2008）に改定されてからは、これらに基づき、安全保護上要求される機能が正しく確実に実現されていることを保証するため、検証及び妥当性確認（Ｖ＆Ｖ）がなされたソフトウェアを使用している。

６．新規制基準への適合状況（４／１５）

新規制基準の項目	適合状況
	また、パスワード管理等によって関係者以外の不正な変更等を防止している。 なお、システムの異常動作を検出させるウイルスチェック機能は、安全保護設備は汎用ではないプログラム及び言語を使用していることと通信方向を一方向に制限等の対策を行っていること、及び、安全保護設備の機能に悪影響を及ぼす恐れがあるため設けていない。
七　計測制御系統施設の一部を安全保護回路と共用する場合には、その安全保護機能を失わないよう、計測制御系統施設から機能的に分離されたものとすること。	（規制要求変更なし） 安全保護回路と計測制御系とは、電源、検出器及びケーブルルートを、原則として分離している。安全保護回路の一部から計測制御系へ信号を取り出す場合には、信号の分岐箇所に絶縁回路を設け、取り出し先の計測制御系での回路の短絡、開放等の故障が生じても安全保護回路へ影響を与えることが無いよう設計となっている。
【解釈】 １　第１号について、安全保護回路の運転時の異常な　過渡変化時の機能の具体例としては、原子炉の過出力状態や出力の急激な上昇を防止するために、異常な状態を検知し、原子炉停止系統を含む適切な系統を作動させ、緊急停止の動作を開始させること等をいう。	（規制要求変更なし） 第１項　第一号と同じ
２　第３号に規定する「チャンネル」とは、安全保護動作に必要な単一の信号を発生させるために必要な構成要素（抵抗器、コンデンサ、トランジスタ、スイッチ及び導線等）及びモール（内部連絡された構成要素の集合体）の配列であって、検出器から論理回路入口までをいう。	（規制要求変更なし） 第１項　第三号と同じ

６．新規制基準への適合状況（５／１５）

新規制基準の項目	適合状況
３ 第４号に規定する「それぞれ互いに分離し」とは、独立性を有するようなチャンネル間の物理的分離及び電気的分離等をいう。	（規制要求変更なし） 第１項 第四号と同じ
４ 第５号に規定する「駆動源の喪失、系統の遮断その他の不利な状況」とは、電力若しくは計装用空気の喪失又は何らかの原因により安全保護回路の論理回路が遮断される等の状況をいう。なお、不利な状況には、環境条件も含むが、どのような状況を考慮するかは、個々の設計に応じて判断する。	（規制要求変更なし） 第１項 第五号と同じ
５ 第５号に規定する「発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できるもの」とは、安全保護回路が単一故障した場合においても、発電用原子炉施設をより安全な状態に移行することにより、最終的に発電用原子炉施設が安全側の状態を維持するか、又は安全保護回路が単一故障してそのままの状態にとどまっても発電用原子炉施設の安全上支障がない状態を維持できることをいう。	（規制要求変更なし） 第１項 第五号と同じ

６．新規制基準への適合状況（６／１５）

新規制基準の項目	適合状況
＜新規要求事項＞ ６　第６号に規定する「不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止すること」とは、ハードウェアの物理的分離、機能的分離に加え、システムの導入段階、更新段階又は試験段階でコンピュータウイルスが混入することを防止する等、承認されていない動作や変更を防ぐ設計のことをいう。	「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」第二十四条第１項第六号と同じ。
７　第７号に規定する「安全保護機能を失わない」とは、接続された計測制御系統施設の機器又はチャンネルに単一故障、誤操作若しくは使用状態からの単一の取り外しが生じた場合においても、これにより悪影響を受けない部分の安全保護回路が第１号から第６号を満たすことをいう。	（規制要求変更なし（第６号を除く）） 第６号については、上記、解釈第６号に同じ。

６．新規制基準への適合状況（７／１５）

「実用発電用原子炉及びその附属施設の技術基準に関する規則」
第三十五条（安全保護装置）

新規制基準の項目	適合状況
（安全保護装置） 第三十五条　発電用原子炉施設には、安全保護装置を次に定めるところにより施設しなければならない。	
一　運転時の異常な過渡変化が発生する場合又は地震の発生により発電用原子炉の運転に支障が生ずる場合において、原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものであること。	（規制要求変更なし） 「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」 第二十四条　第１項第一号と同じ
二　系統を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保すること。	（規制要求変更なし） 「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」 第二十四条　第１項第三号と同じ
三　系統を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保すること。	（規制要求変更なし） 「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」 第二十四条　第１項第四号と同じ
四　駆動源の喪失、系統の遮断その他の不利な状況が生じた場合においても、発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できること。	（規制要求変更なし） 「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」 第二十四条　第１項第五号と同じ

６．新規制基準への適合状況（８／１５）

新規制基準の項目	適合状況
＜新規要求事項＞ 五　不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止するために必要な措置が講じられているものであること。	「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」 第二十四条　第１項第六号と同じ。
六　計測制御系の一部を安全保護装置と共用する場合には、その安全保護機能を失わないよう、計測制御系から機能的に分離されたものであること。	（規制要求変更なし） 「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」 第二十四条　第１項第七号と同じ。
七　発電用原子炉の運転中に、その能力を確認するための必要な試験ができるものであること。	（規制要求変更なし） 原子炉保護設備は、原子炉運転中でも模擬入力による原子炉トリップ演算処理装置の設定値確認及びトリップチャンネルの論理回路の作動確認を行うことができる。 原子炉トリップ遮断器は、４つのトリップチャンネルごとに設けているため、任意の１つのトリップチャンネルについてテストスイッチ操作により動作確認を行うことができる。
八　運転条件に応じて作動設定値を変更できるものであること。	（規制要求変更なし） 原子炉保護設備は、運転条件に応じて作動設定値を変更できるものである。

６．新規制基準への適合状況（９／１５）

新規制基準の項目	適合状況
【解釈】 １　第１号の安全保護装置の機能の確認については、設置許可申請書の添付書類八の設備仕様及び設置許可申請書において評価した運転時の異常な過渡変化の評価の条件に非保守的な変更がないことを確認すること。	（規制要求変更なし） 第１号の安全保護装置の機能の確認については、設置許可申請書の添付書類八の設備仕様及び設置許可申請書において評価した運転時の異常な過渡変化の評価の条件に非保守的な変更がないことを確認している。
２　第３号に規定する「独立性を確保すること」とは、チャンネル間の距離、バリア、電気的隔離装置等により、相互を分離することをいう。	（規制要求変更なし） 「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」 第二十四条　第１項第七号と同じ。

６．新規制基準への適合状況（１０／１５）

新規制基準の項目	適合状況
＜新規要求事項＞ ３　第５号に規定する「必要な措置が講じられているものであること」とは、外部ネットワークと物的な分離又は機能的な分離を行うこと、有線又無線による外部ネットワークからの遠隔操作及びウイルス等の侵入を防止すること、物理的及び電気的アクセスの制限を設けることにより、システムの据付、更新、試験、保守等で、承認されていない者の操作及びウイルス等の侵入を防止すること等の措置を講じることをいう。なお、ソフトウェアの内部管理を強化するために、ウイルス等によるシステムの異常動作を検出させる場合には以下の機能を有すること。 （１）ウイルス等によるシステムの異常動作を検出する機能を設ける場合には、ウイルス等を検知した場合に運転員等へ告知すること。 （２）ウイルス等によるシステムの異常動作を検出する機能は、安全保護装置の機能に悪影響を及ぼさないこと。	「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」 第二十四条　第１項第六号と同じ。 なお、ソフトウェア内部管理を強化するためのウィルス等によるシステムの異常動作を検出させるウイルスチェック機能は、安全保護設備は汎用ではないプログラム及び言語を使用していることと通信方向を一方向に制限等の対策を行っていること、及び、安全保護設備の機能に悪影響を及ぼす恐れがあるため設けていない。

６．新規制基準への適合状況（１１／１５）

新規制基準の項目	適合状況
４　デジタル安全保護系の適用に当たっては、日本電気協会「安全保護系へのディジタル計算機の適用に関する規程」（JEAC 4620-2008）（以下「JEAC4620」という。）５．留意事項を除く本文、解説－４から６まで、解説－８及び解説－１１から１８まで並びに「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609-2008）本文及び解説－９に以下の要件を付したものによること。ただし、「ディジタル」は「デジタル」と読み替えること。	（規制要求変更なし） デジタル安全保護系はJEAC4620、JEAG4609の要求事項を満足したものとなっている。
（１）JEAC4620の４．１の適用に当たっては、運転時の異常な過渡変化が生じる場合又は地震の発生等により原子炉の運転に支障が生じる場合において、原子炉停止系統及び工学的安全施設と併せて機能することにより、燃料許容損傷限界を超えないよう安全保護系の設定値を決定すること。	（規制要求変更なし） デジタル安全保護系は、プラントでの異常な状態を検知し、適切な系統を自動的に作動させ、燃料が許容設計限界を超えない設計としている。
（２）JEAC4620の４．１８．３において検証及び妥当性確認の実施に際して作成された文書は、４．１８．２の構成管理計画の中に文書の保存を定め、適切に管理すること。	（規制要求変更なし） 検証と妥当性確認の実施に際して作成された文書についても、ソフトウェア構成管理計画書の構成管理対象に含めている。

６．新規制基準への適合状況（１２／１５）

新規制基準の項目	適合状況
（３）JEAC4620の４．８における「想定される電源擾乱、電磁波等の外部からの外乱・ノイズの環境条件を考慮した設計とすること」を「想定される電源擾乱、サージ電圧、電磁波等の外部からの外乱・ノイズの環境条件を考慮して設計し、その設計による対策の妥当性が十分であることを確証すること」と読み替えること。	（規制要求変更なし） インバータと安全保護設備の電源装置との協調により、想定される電源擾乱が発生した場合においても安全保護設備に影響を与えない設計としている。また、サージ電圧(雷サージ)による擾乱に対しては、建屋内に設置するとともに、公的規格に基づいたサージに対する耐力を有する設計としている。 また、外部からの外乱・ノイズの環境条件を考慮した設計としており、その設計での対策の妥当性を確認している。
（４）JEAC4620の４．５及び解説－６の適用に当たっては、デジタル安全保護系は、試験時を除き、計測制御系からの情報を受けないこと。試験時に、計測制御系からの情報を受ける場合には、計測制御系の故障により、デジタル安全保護系が影響を受けないよう措置を講じること。デジタル安全保護系及び計測制御系の伝送ラインを共用する場合、通信をつかさどる制御装置は発信側システムの装置とすること。	（規制要求変更なし） 計測制御系とは機能的に分離した設計とする。 計測制御系へ信号を取り出す場合には、計測制御系に故障が生じても、デジタル安全保護系へ影響を与えない設計とする。
（５）JEAC4620の４．１６の「外部からの影響を防止し得る設計」を「外部影響の防止された設備」と読み替えること。	（規制要求変更なし） デジタル安全保護系は、外部のネットワークに直接接続しない設計とする。

６．新規制基準への適合状況（１３／１５）

新規制基準の項目	適合状況
（６）JEAC4620の４．における安全保護機能に相応した高い信頼性を有するとは、デジタル安全保護系のトリップ失敗確率及び誤トリップする頻度を評価し、従来型のものと比較して同等以下とすること。また、デジタル安全保護系の信頼性評価において、ハードウェア構成要素に異常の検出、検出信号の伝送、入出力信号の処理、演算処理、トリップ信号の伝送、トリップの作動等、評価に必要な構成要素を含むこと。	（規制要求変更なし） デジタル安全保護系のトリップが失敗する確率及び誤トリップする頻度は、必要なハードウェア構成要素について評価を行い、従来設備に比べて同等以下とする。
（７）安全保護系に用いられるデジタル計算機の健全性を実証できない場合、安全保護機能の遂行を担保するための原理の異なる手段を別途用意すること。（「日本電気協会「安全保護系へのディジタル計算機の適用に関する規程（JEAC 4620-2008）」及び「ディジタル安全保護系の検証及び妥当性確認に関する指針（JEAG 4609-2008）」に関する技術評価書」（平成２３年１月原子力安全・保安院、原子力安全基盤機構取りまとめ））	（規制要求変更なし） デジタル安全保護系はJEAC4620に基づき品質を確保しており、健全性は実証されている。

６．新規制基準への適合状況（１４／１５）

「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」
第六条（外部からの衝撃による損傷の防止）

新規制基準の項目 （安全保護回路関連項目のみ抜粋）	適合状況
＜規制要求の追加＞ ３　安全施設は、工場等内又はその周辺において想定される発電用原子炉施設の安全性を損なわせる原因となるおそれがある事象であって人為によるもの（故意によるものを除く。）に対して安全機能を損なわないものでなければならない。 【解釈】 ８　第３項に規定する「発電用原子炉施設の安全性を損なわせる原因となるおそれがある事象であって人為によるもの（故意によるものを除く。）」とは、敷地及び敷地周辺の状況をもとに選択されるものであり、飛来物（航空機落下等）、ダムの崩壊、爆発、近隣工場等の火災、有毒ガス、船舶の衝突又は電磁的障害等をいう。 　なお、上記の航空機落下については、「実用発電用原子炉施設への航空機落下確率の評価基準について」（平成14・07・29 原院第4号（平成１４年７月３０日原子力安全・保安院制定））等に基づき、防護設計の要否について確認する。	故意によるものを除く人為による事象としては、航空機落下、ダムの崩壊、爆発、近隣工場等の火災、有毒ガス、船舶の衝突及び電磁的障害を想定している。 ・航空機落下 航空機の落下を考慮する必要はない。（「外部火災の影響評価について」参照） ・ダムの崩壊 原子炉施設の近くには、ダムの崩壊により影響を及ぼすような河川はないことから、ダムの崩壊を考慮する必要はない。泊発電所の敷地境界から東約8kmに共和ダムが存在するが、発電所まで距離が離れており、発電所との間には丘陵地が分布している。 ・爆発、近隣工場等の火災、有毒ガス及び船舶の衝突 爆発、近隣工場等の火災、有毒ガス及び船舶の衝突により安全施設は安全機能を損なうおそれがない。（「外部火災の影響評価について」参照） ・電磁的障害 原子炉保護設備及び工学的安全施設作動設備は、日本工業規格（JIS）や電気規格調査会標準規格（JEC）等に基づき、安全施設に誤動作を生じないよう、ラインフィルタ、絶縁回路の設置によるサージ・ノイズの侵入防止及び鋼製筐体の適用により、電磁波の侵入等を防止する設計としている。従って、安全施設は安全機能を損なうおそれがない。

６．新規制基準への適合状況（１５／１５）

「実用発電用原子炉及びその附属施設の技術基準に関する規則」
第七条（外部からの衝撃による損傷の防止）

新規制基準の項目 （安全保護回路関連項目のみ抜粋）	適合状況
＜規制要求の追加＞ ２　周辺監視区域に隣接する地域に事業所、鉄道、道路その他の外部からの衝撃が発生するおそれがある要因がある場合には、事業所における火災又は爆発事故、危険物を搭載した車両、船舶又は航空機の事故その他の敷地及び敷地周辺の状況から想定される事象であって人為によるもの（故意によるものを除く。）により発電用原子炉施設の安全性が損なわれないよう、防護措置その他の適切な措置を講じなければならない。 【解釈】 ３　第２項に規定する「事故その他の敷地及び敷地周辺の状況から想定される事象であって人為によるもの（故意によるものを除く。）」には、ダムの崩壊、船舶の衝突、電磁的障害等の敷地及び敷地周辺の状況から生じうる事故を含む。	「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」第六条　第３項と同じ。