資料１－２－３

島根原子力発電所２号炉

安全保護回路

令和元年11月

中国電力株式会社

本資料のうち，枠囲みの内容は機密に係る事項のため公開できません。

第 24 条：安全保護回路

＜目　　次＞

1.　基本方針

1.1　要求事項の整理

安全保護回路について，設置許可基準規則第 24 条及び技術基準規則第 35 条において，追加要求事項を明確化する（第 1.1 - 1 表）。

第 1.1 - 1 表　設置許可基準規則第 24 条及び技術基準規則第 35 条要求事項

設置許可基準規則 第 24 条（安全保護回路）	技術基準規則 第 35 条（安全保護装置）	備考
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。	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。	変更なし
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。	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。	変更なし
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。	－	変更なし
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。	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。	変更なし
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。	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。	変更なし

設置許可基準規則 第 24 条（安全保護回路）	技術基準規則 第 35 条（安全保護装置）	備考
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。	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。	変更なし
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。	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。	追加要求事項
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。	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。	変更なし
－	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。 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。	変更なし

2.　追加要求事項に対する適合方針

2.1　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，安全保護回路（原子炉保護系作動回路，工学的安全施設作動回路）のうちデジタル化している部分については，下記の対策を実施している。

(1)　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，出入管理により物理的アクセスを制限し，電気的アクセスについては，安全保護回路を有する制御盤を施錠管理とし，デジタル処理部と接続する保守ツールは施錠管理された場所に保管し，パスワード管理することで管理されない変更を防止している。

(2)　ハードウェアの物理的な分離又は機能的な分離対策

安全保護回路の信号は，安全保護回路→ＳＰＤＳデータ収集サーバ→防護装置→ＳＰＤＳ伝送サーバ→防護装置を介して外部に伝送している。この信号の流れにおいて，安全保護回路からは発信されるのみであり，外部からの信号を受信しないこと，及びハードウェアを直接接続しないことで物理的及び機能的分離を行っている。

(3)　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防止対策

安全保護回路の信号で外部ネットワークへデータ伝送の必要がある場合は，防護装置（通信状態を監視し，送信元，送信先及び送信内容を制限することにより，目的外の通信を遮断）を介して安全保護回路の信号を一方向（送信機能のみ）通信に制限し外部からのデータ書き込み機能を設けないことでウイルスの侵入及び外部からの不正アクセスを防止している。

(4)　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

安全保護回路のうちデジタル処理部を持つ機器は，固有のプログラム言語を使用（一般的なコンピュータウイルスが動作しない環境）するとともに，保守以外の不要な演算回路へのアクセス制限対策として入域制限や設定値変更作業での施錠管理及びパスワード管理を行い，関係者以外の不正な変更等を防止している。

(5)　耐ノイズ・サージ対策

安全保護回路は，雷，サージ・ノイズ，電磁波障害等による擾乱に対して，制御盤へ入線する電源受電部や外部からの信号入出力部にラインフィルタや絶縁回路を設置している。

ケーブルは金属シールド付ケーブルを適用し，金属シールドは接地して電磁波の侵入を防止する設計としている。安全保護回路は，鋼製の筐体に格納し，筐体を接地することで電磁波の侵入を防止する設計としている。

(6) ウイルス侵入防止について，供給者への要求事項及び供給者で実施している対策

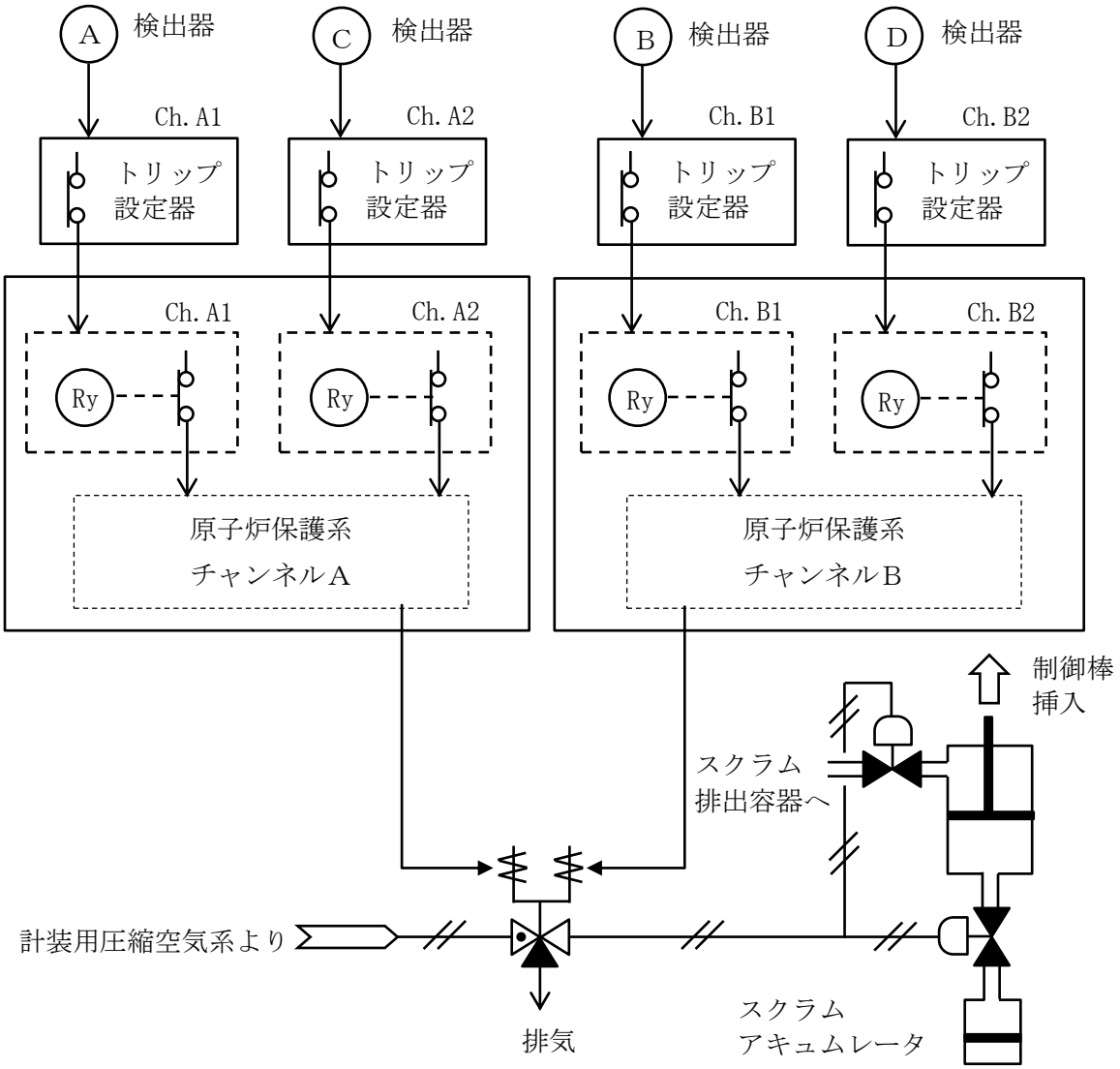
供給者は，制御システムへ保守ツールや小型記憶媒体の機器接続が必要な場合，当社所有の保守ツール及び小型記憶媒体（ＭＯディスク，ＣＤを含む）については，作業前に当社によりウイルスチェックが実施され，ウイルス感染がないことを確認して供給者が使用する。また，供給者所有のパソコン，小型記憶媒体を使用する場合は，供給者は，ウイルスチェックを行いウイルス感染がないことを確認し，その結果を当社に提出する。

2.2　安全保護回路の概要

安全保護回路は，検出信号処理において一部デジタル演算処理を行う機器がある他は，アナログ回路で構成している。また安全保護回路とそれ以外の設備との間で用いる信号はアナログ信号であり，ネットワークを介した不正アクセス等による被害を受けることはない。

例として，原子炉保護系の構成例を第 2.2-1 図に示す。

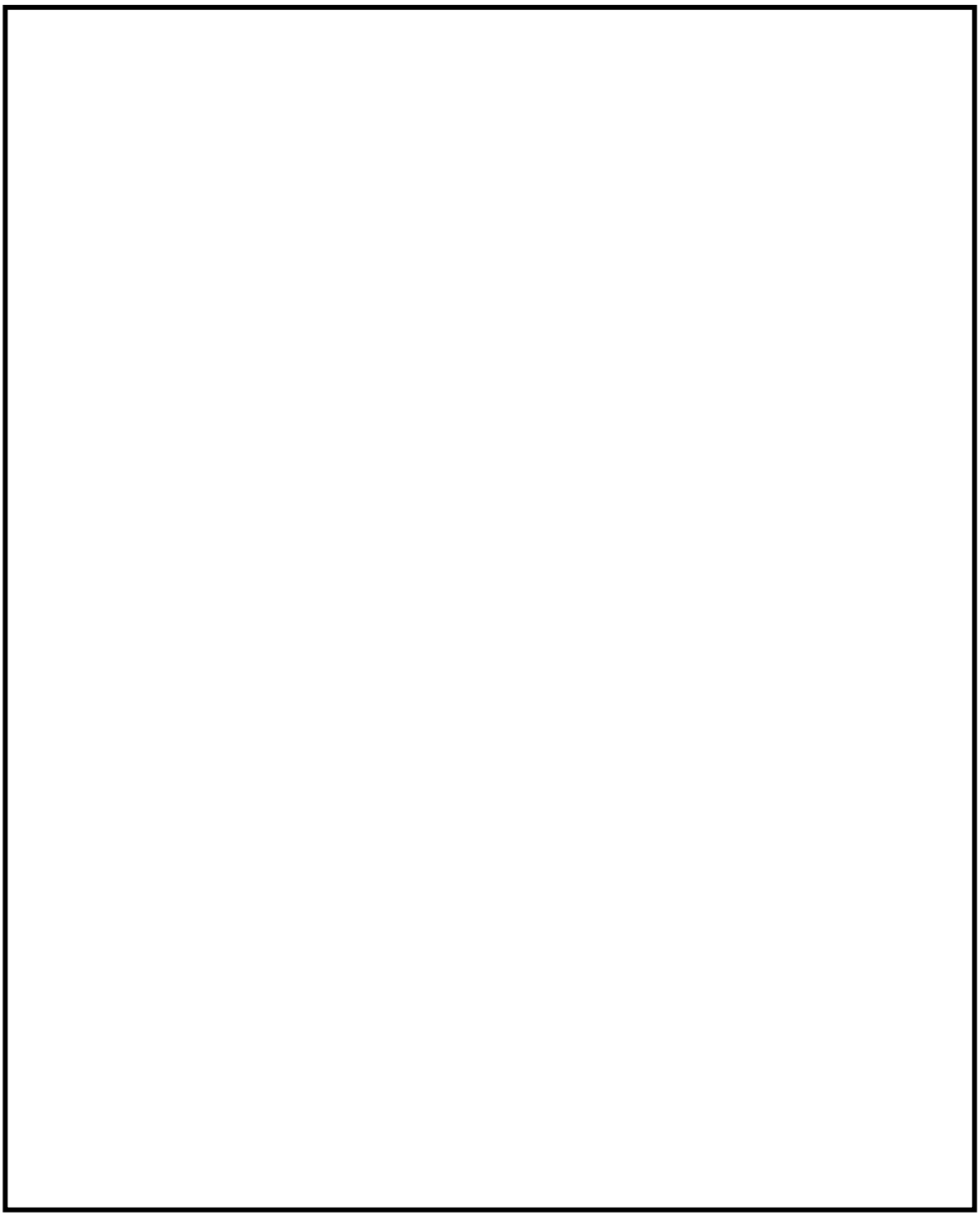
安全保護回路は，安全保護系のプロセス計装からの信号を受信し，原子炉停止系統を自動的に作動させる信号を発生する原子炉保護系と，安全保護系のプロセス計装からの信号を受信し，工学的安全施設を作動させる信号を発する工学的安全施設作動回路で構成しており，多重性及び電気的・物理的な独立性を持たせている。



第 2.2 - 1 図　原子炉保護系の構成例

2.3　安全保護回路の物理的分離対策

安全保護回路は，不正アクセスを防止するため，安全保護系盤の扉については施錠を行うこととし，保守ツールは施錠管理された保管ラック内に保管しており，許可された者以外はハードウェアへ直接接続できない対策を実施している。



第 2.3 - 1 図　安全保護系盤及び保守ツール

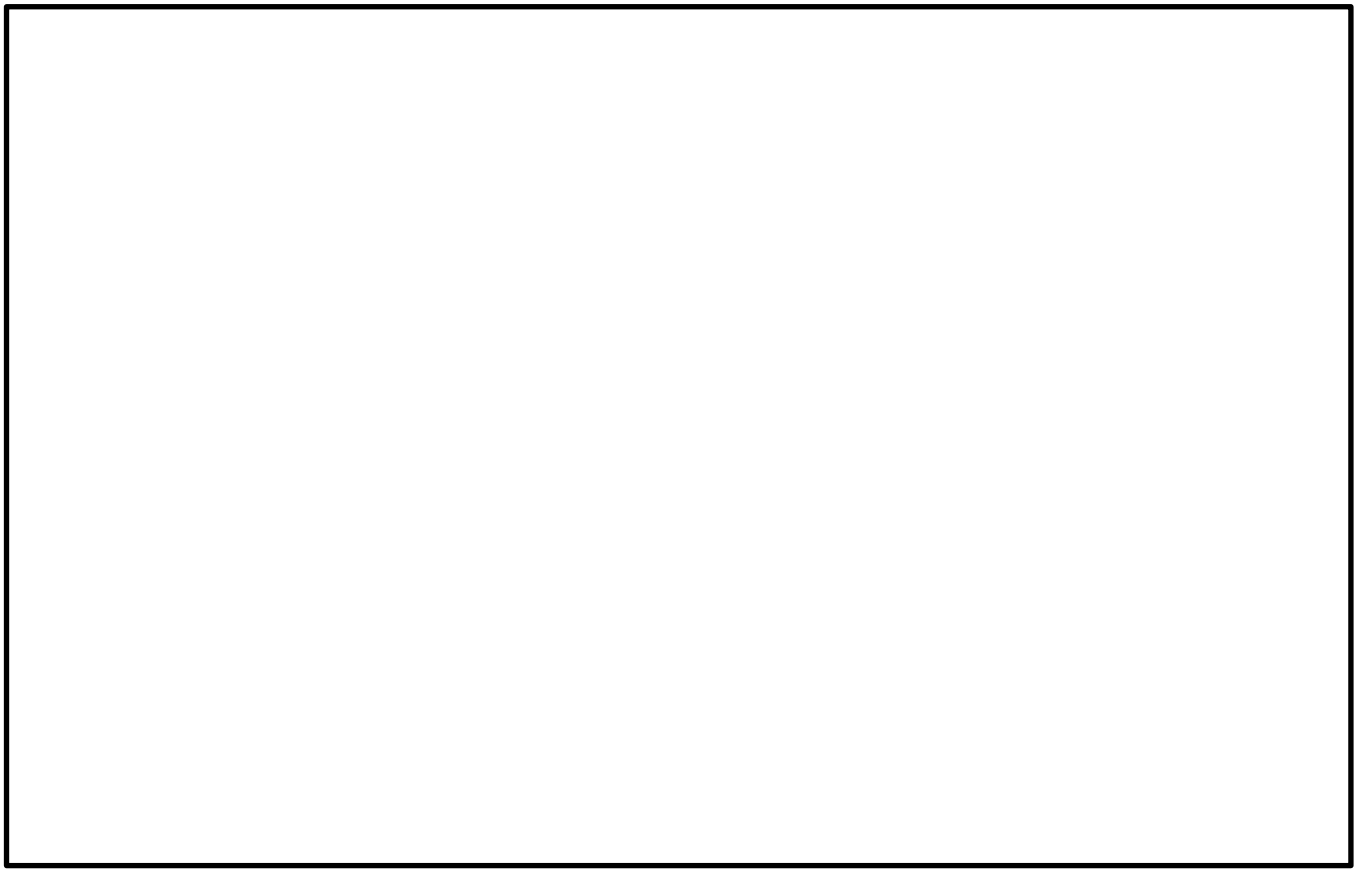
本資料のうち，枠囲みの内容は機密に係る事項のため公開できません。

2.4　外部からの不正アクセス行為防止について

安全保護回路は，外部ネットワークと直接接続は行っていない。外部システムと接続する必要のあるデータ等については，防護装置を介して接続している。安全保護回路のうちデジタル処理部を持つ機器は，固有のプログラム言語を使用するとともに，外部からのデータ書き込み機能を設けないことでウイルスの侵入等を防止している。

外部からの妨害行為または破壊行為については，出入管理により関係者以外の接近を防止している。また，安全保護系盤については施錠を行い，関係者以外のアクセスを防止している。

外部ネットワークとの接続構成概要を第 2.4 - 1 図に示す。



第 2.4 - 1 図　外部ネットワークとの接続構成概要

本資料のうち，枠囲みの内容は機密に係る事項のため公開できません。

2.5　想定脅威に対する対策について

安全保護回路のデジタル処理を行っている機器については，工場製作段階から第 2.5 - 1 表に示す想定脅威に対する対策を行っている。

第 2.5 - 1 表　想定脅威に対する対策（工場製作及び出荷）

想定脅威		対策

2.6　物理的分離及び電気的分離について

(1)　物理的分離について

安全保護回路と計測制御系とは，電源，検出器，ケーブルルート及び格納容器を貫通する計装配管を原則として分離する設計とする。

安全保護回路と計測制御系で計装配管を共用する場合は，安全保護回路の計装配管として設計する。

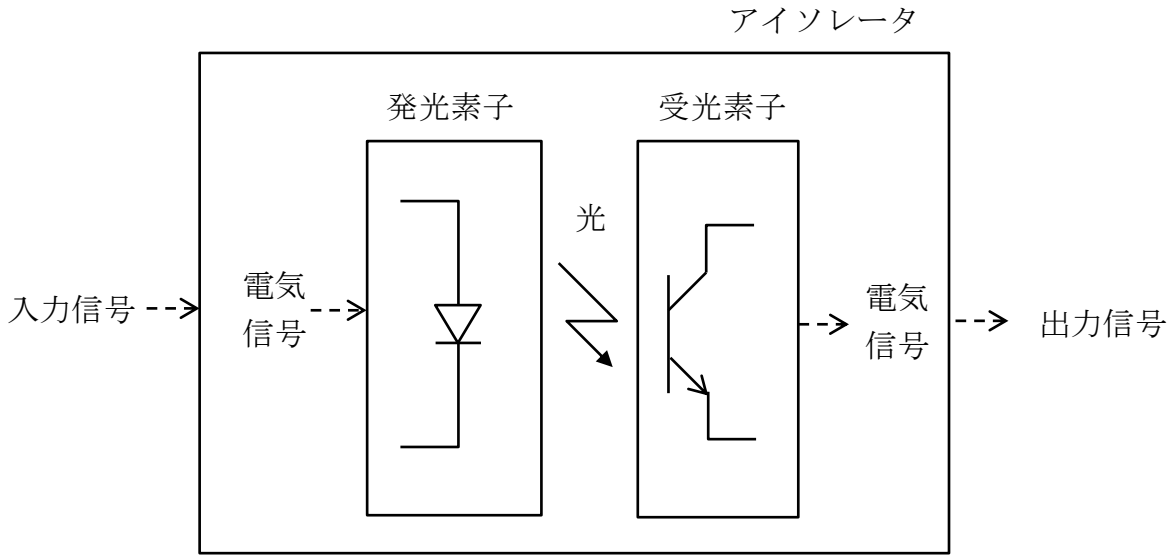
(2)　電気的分離について

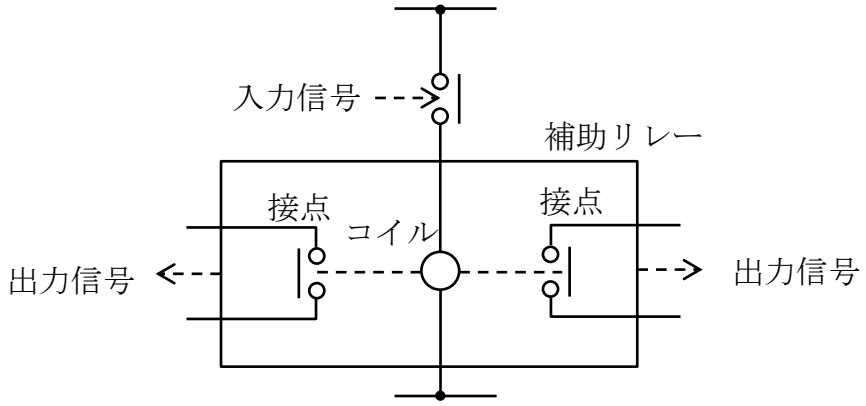
安全保護回路からインターフェース部（計測制御系）の分離は，アイソレータや補助リレー等の隔離装置を用いて，電気的に分離（計測制御系で短絡等の故障が生じても安全保護回路に影響を与えない）を行っている。

原子炉中性子計装系等の検出部が表示，記録計用検出部と共用しているが，計測制御系の短絡，地絡又は断線によって安全保護回路に影響を与えない設計とする。

隔離装置（アイソレータ及び補助リレー）を第 2.6 - 1 図に示す。

本資料のうち，枠囲みの内容は機密に係る事項のため公開できません。



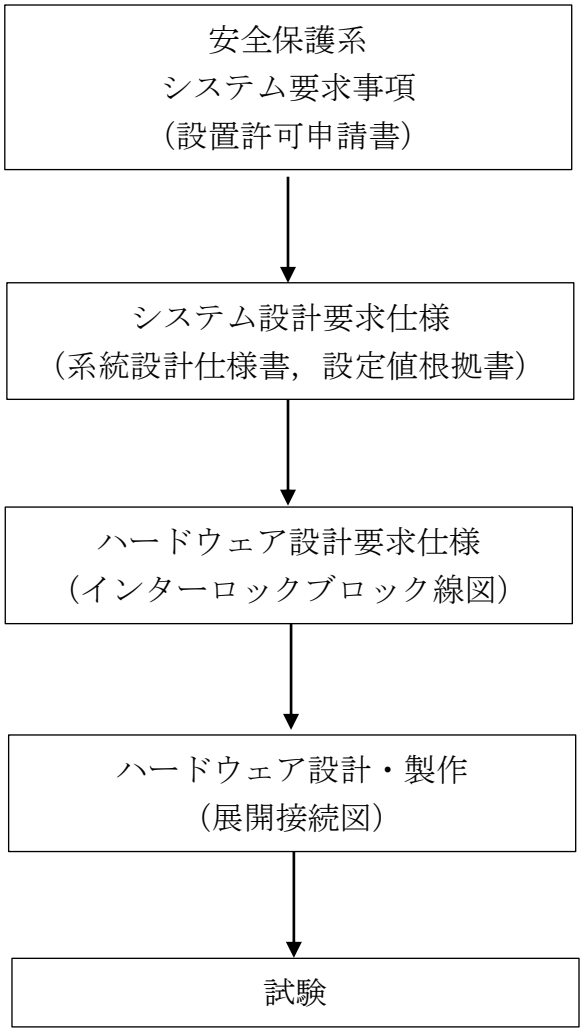


第 2.6 - 1 図　隔離装置（アイソレータ及び補助リレー）

別紙１　アナログ型安全保護回路について，承認されていない動作や変更を防ぐ設計方針

アナログ型の安全保護回路は，論理回路がハードワイヤーロジック（リレーや配線によるアナログ回路）で構成されており，これらの回路に対し，承認されていない動作や変更を防ぐ措置として，以下を実施している。

・安全保護回路の変更が生じる場合は，上流文書から下流文書（第１図参照）へ変更内容が反映されていることを設備図書で承認する。
・改造後はインターロック試験や定期事業者検査等にて，安全保護回路が正しく動作することを複数の人間でチェックしている。
・なお，中央制御室への入域に対しては，出入管理により関係者以外のアクセスを防止している。



第１図　安全保護回路の設計・製作・試験の流れ（例）

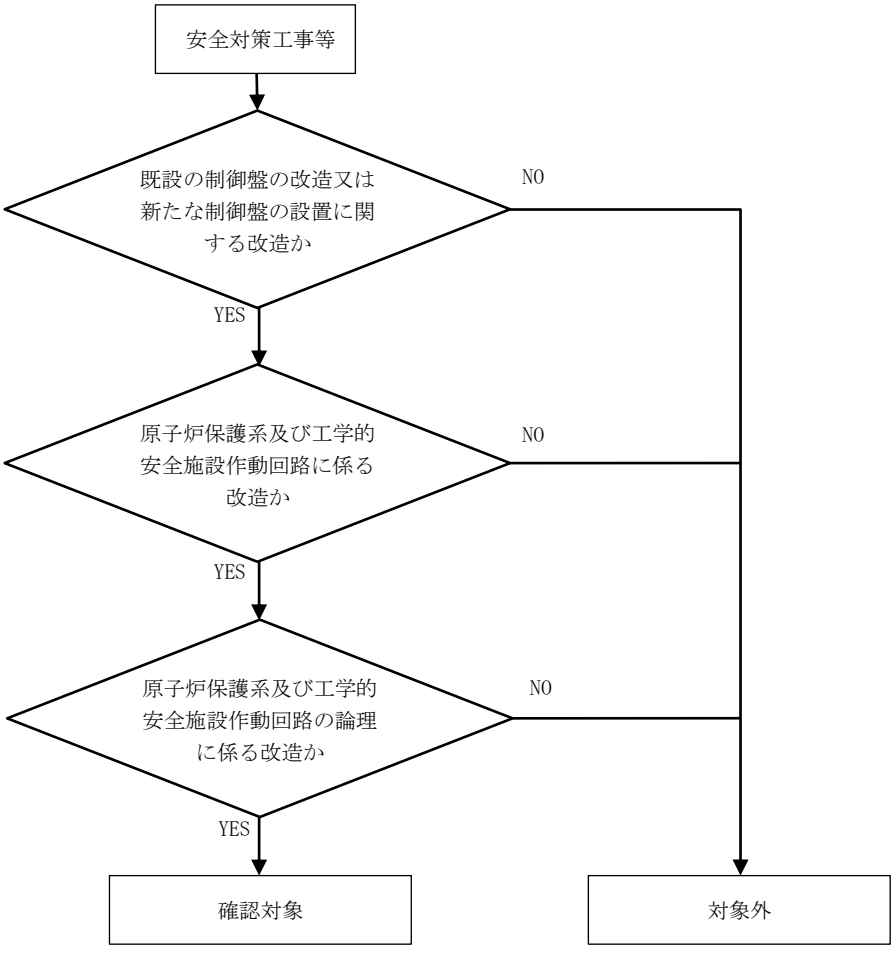
別紙２　今回の設置許可申請に関し，安全保護回路に変更を施している場合の基準適合性

安全対策工事等のうち，安全保護回路の変更に係る工事を抽出し，確認を行った。抽出フローを第１図に示す。

既設の制御盤の改造及び新たな制御盤の設置に関する改造から，安全保護回路及び工学的安全施設作動回路の論理に係る改造を確認対象として抽出した結果，３件が抽出された。いずれの改造も既設の安全保護回路へ影響が無いよう対策が図られていることを確認するとともに，重大事故等対策による改造であっても，既設の安全保護回路へ影響が無いことを確認した。

安全保護回路の変更に係る設備の抽出結果並びに抽出された設備についての個別の確認結果を第１表に示す。

なお，ＡＴＷＳ緩和設備（代替制御棒挿入機能）及び代替自動減圧ロジック（代替自動減圧機能）については，安全保護回路に変更を施しておらず，安全保護回路と電気的・物理的に分離されており安全保護回路に悪影響を与えない設計としている（参考１）。詳細は各条文の基準適合性説明資料にて説明する。



第１図　安全保護回路の論理に係る改造抽出フロー

第１表　安全保護回路の論理に係る改造の抽出結果

改造概要	条文	安全保護回路への影響評価
ＡＴＷＳ時に自動減圧系の作動を阻止する手動回路を追加する。	44 条 46 条	自動減圧系の手動阻止回路は自動減圧系論理回路の関連回路として安全保護回路と同等に扱うものとする。これらは安全保護回路と同様，計測制御系統施設や他の重大事故等対処設備から物理的，電気的に分離する。さらに，安全保護回路として多重化しそれぞれの区分は互いに物理的，電気的に分離する。
ＡＴＷＳ時に原子炉の緊急停止操作を実施する手動回路を追加する。	44 条	緊急停止操作の手動回路は緊急停止系論理回路の関連回路として安全保護回路と同等に扱うものとする。これらは安全保護回路と同様，計測制御系統施設や他の重大事故等対処設備から物理的，電気的に分離する。さらに，安全保護回路として多重化しそれぞれの区分は互いに物理的，電気的に分離する。
自動減圧系の作動条件に低圧ＥＣＣＳ系ポンプが運転状態であることを追加する。	12 条	自動減圧系作動に追加する条件信号回路は，安全保護回路の関連回路として安全保護回路と同等に扱うものとする。これらは安全保護回路と同様，計測制御系統施設から物理的，電気的に分離する。さらに，安全保護回路として多重化しそれぞれの区分は互いに物理的，電気的に分離する。

(1)　自動減圧系の手動阻止回路について

a.　目的

原子炉停止機能喪失事象においては，原子炉が臨界状態であるため，急激な低圧注水系流量増加は，正の反応度印加を引き起こし，原子炉出力の急上昇につながる。このため原子炉停止機能喪失事象発生時に自動減圧系及び代替自動減圧機能が作動しないように，手動阻止回路を設置する。

b.　手動阻止回路

自動減圧系手動阻止回路を第２図に示す。自動減圧系（ＤＢ）と代替自動減圧機能（ＳＡ）の論理回路は各々分離しており，追加設置する自動減圧系手動阻止回路は，代替自動減圧機能手動阻止回路とは分離した設計とすることで互いに悪影響を与えない設計とする。

また，自動減圧手動阻止回路は，単一故障等により本来の自動減圧系の多重性，独立性に悪影響を与えないよう区分ごとに設置するものとする。

c.　自動減圧系への影響について

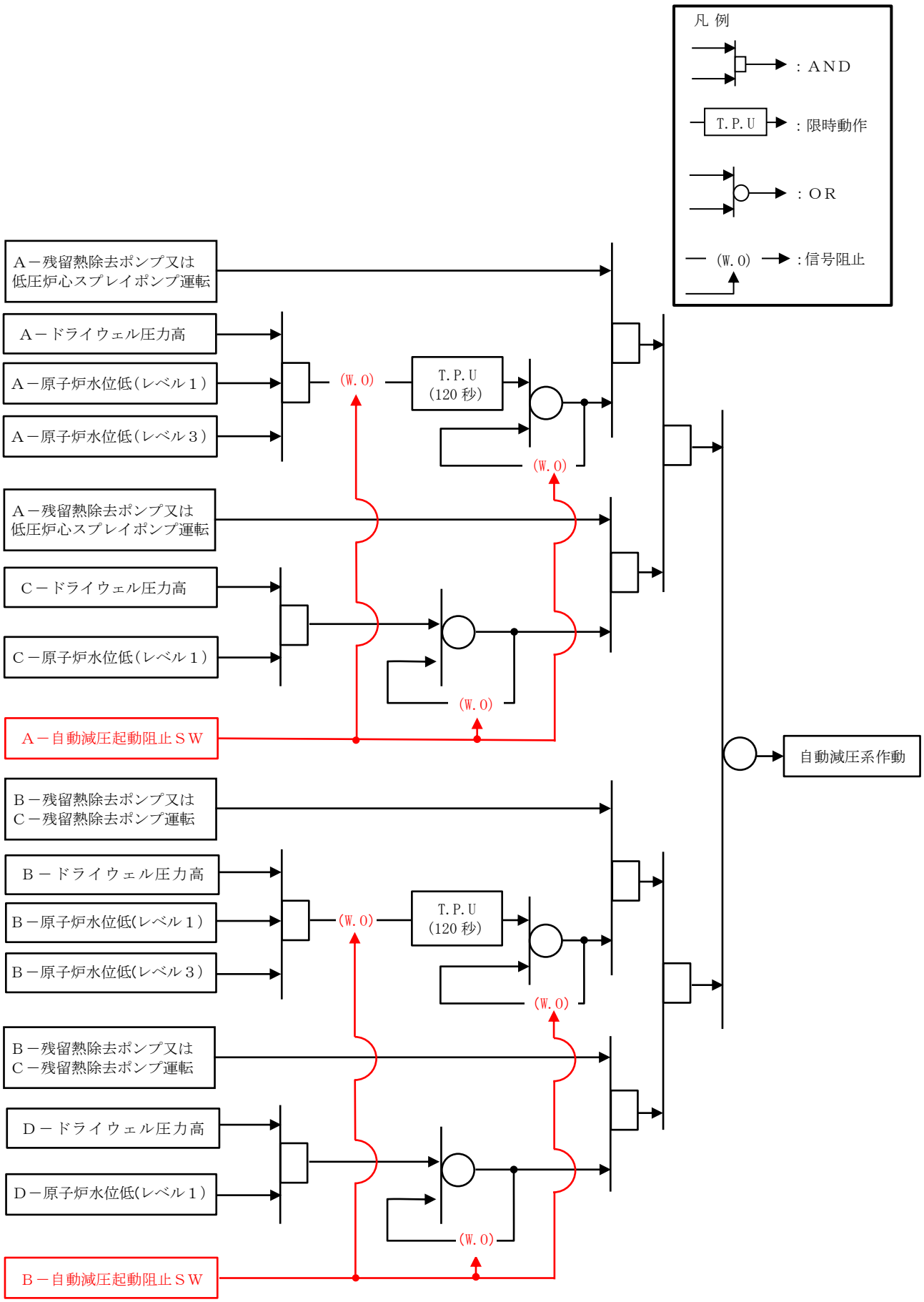
追加設置する自動減圧系手動阻止回路が，自動減圧系に対して悪影響を与えないことを第２表に示す。

第２表　自動減圧系への影響

設置許可基準規則 第二十四条（安全保護回路）	自動減圧系への影響
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。	阻止回路は，原子炉停止機能喪失事象時に手動で自動減圧系を阻止するものであり，運転時の異常な過渡変化時には使用しないため問題ない。
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。	自動減圧系の多重性，独立性に悪影響を与えないよう，区分ごとに阻止回路を設置しているため問題ない。
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。	自動減圧系の多重性，独立性に悪影響を与えないよう，区分ごとに阻止回路を設置しているため問題ない。
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。	自動減圧系の多重性，独立性に悪影響を与えないよう，区分ごとに阻止回路を設置しているため問題ない。

設置許可基準規則 第二十四条（安全保護回路）	自動減圧系への影響
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。	自動減圧系は，駆動源である電源の喪失で系の現状維持（フェイル・アズ・イズ），その他の不利な状況が発生した場合でも多重性，独立性をもつことで原子炉を十分に安全な状態に導くようにしている。追加する阻止回路はこの安全保護動作を阻害するものではない。
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。	阻止回路はアナログで構成しており，不正アクセス行為による影響を受けない。
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。	計測制御系とは共用していないため，影響はない。

設置許可基準規則 第十二条（安全施設）	自動減圧系への影響
４　安全施設は、その健全性及び能力を確認するため、その安全機能の重要度に応じ、発電用原子炉の運転中又は停止中に試験又は検査ができるものでなければならない。	阻止回路を設置することで自動減圧系の試験に影響を与えることはない。



第２図　自動減圧系手動阻止回路図

(2) ＡＴＷＳ緩和設備（代替制御棒挿入機能）の手動起動回路について

a.　目的

発電用原子炉の運転を緊急に停止することができない事象のおそれがある場合において，手動による原子炉の緊急停止操作を実施するため，手動回路を設置する。

b.　手動回路

ＡＴＷＳ緩和設備（代替制御棒挿入機能）の手動回路を第３図に示す。ＡＴＷＳ緩和設備（代替制御棒挿入機能）は，検出器から代替制御棒挿入機能用電磁弁まで設計基準事故対処設備である多重化された原子炉保護系とは独立した構成となっており，多重化された原子炉保護系に悪影響を及ぼさない設計としている。

c.　原子炉保護系への影響について

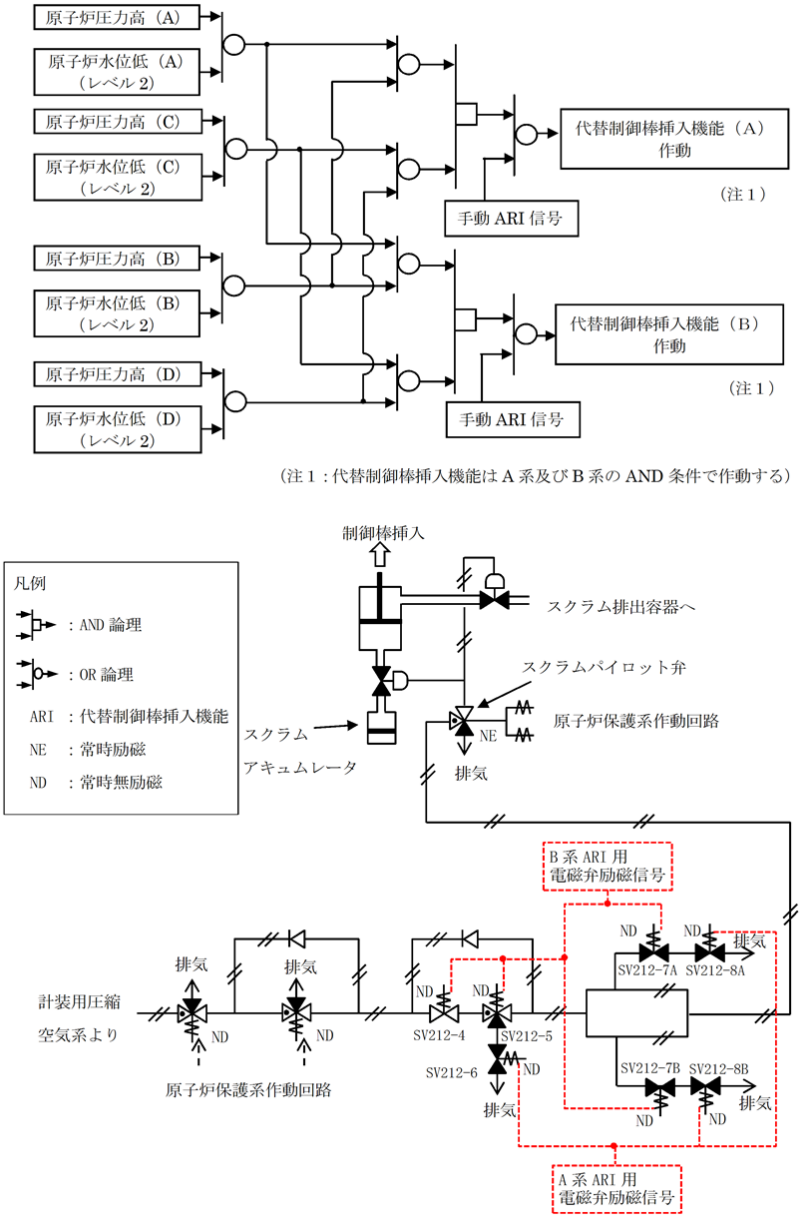
追加設置するＡＴＷＳ緩和設備（代替制御棒挿入機能）の手動回路が，原子炉保護系に対して悪影響を与えないことを第３表に示す。

第３表　原子炉保護系への影響

設置許可基準規則 第二十四条（安全保護回路）	原子炉保護系への影響
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。	運転時の異常な過渡変化時には使用しないため問題ない。
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。	原子炉保護系とは独立した構成となっており悪影響を及ぼさない設計としているため問題ない。

設置許可基準規則 第二十四条（安全保護回路）	原子炉保護系への影響
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。	原子炉保護系の多重性，独立性に悪影響を与えないよう，原子炉保護系とは独立した構成となっているため問題ない。
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。	原子炉保護系の多重性，独立性に悪影響を与えないよう，原子炉保護系とは独立した構成となっているため問題ない。
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。	駆動源の喪失，系統の遮断等においても安全上許容される状態（フェイル・セイフ）になるようにしている。手動回路はこの状態を阻害するものではない。
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。	手動回路はアナログで構成しており，不正アクセス行為による影響を受けない。
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。	計測制御系とは共用していないため，影響はない。

設置許可基準規則 第十二条（安全施設）	原子炉保護系への影響
4　安全施設は、その健全性及び能力を確認するため、その安全機能の重要度に応じ、発電用原子炉の運転中又は停止中に試験又は検査ができるものでなければならない。	手動回路を設置することで原子炉保護系の試験に影響を与えることはない。



第３図　ＡＴＷＳ緩和設備（代替制御棒挿入機能）の手動回路図

(3)　自動減圧系作動の条件信号回路追加について

a.　目的

炉心注水が行われない状態で自動減圧系が作動した場合，原子炉冷却材が急減するおそれがあることから，低圧注水系の待機状態で，自動減圧系を作動させるため，新たに低圧ＥＣＣＳポンプ（残留熱除去ポンプ又は低圧炉心スプレイポンプ）の運転状態を条件信号として，自動減圧系の作動回路に追加する。

b.　条件信号回路

自動減圧系に追加する条件信号回路を第４図に示す。この条件信号回路は，単一故障等により本来の自動減圧系の多重性，独立性に悪影響を与えないよう区分ごとに設置するものとする。

c.　自動減圧系への影響について

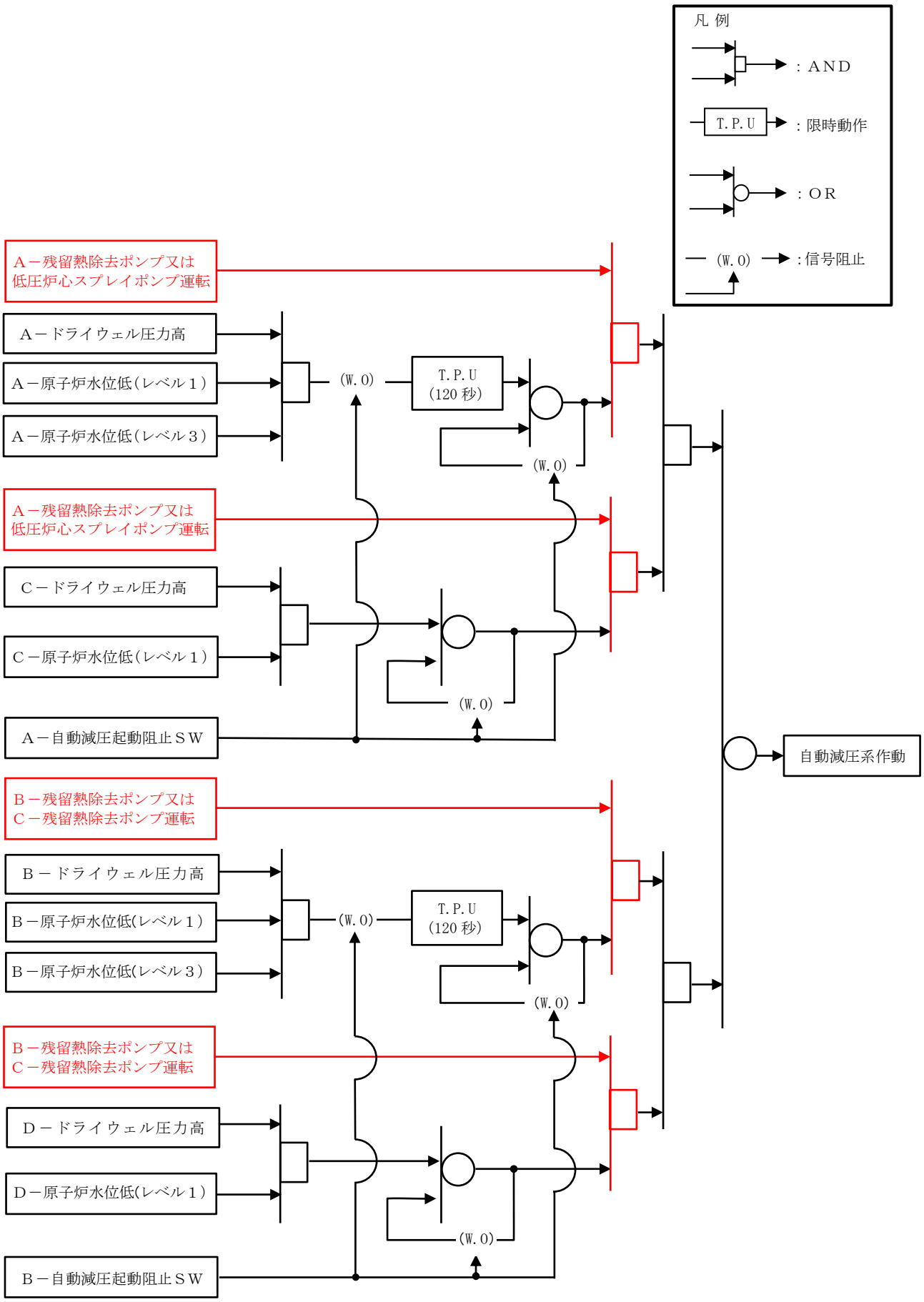
自動減圧系作動回路に追加する条件信号回路が，自動減圧系に対して悪影響を与えないことを第４表に示す。

第４表　自動減圧系への影響

設置許可基準規則 第二十四条（安全保護回路）	自動減圧系への影響
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。	自動減圧系は設計基準事象（中小破断ＬＯＣＡ）の際に使用するものであり，運転時の異常な過渡変化時には使用しないため問題ない。
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。	条件信号回路を追加しても，低圧注水系が待機状態にある場合は，異常な状態を検知し自動的に作動させることができる。 自動減圧系は，低圧炉心注水を促進することを目的とした設備であり問題ない。

設置許可基準規則 第二十四条（安全保護回路）	自動減圧系への影響
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。	自動減圧系の多重性，独立性に悪影響を与えないよう，区分ごとに条件信号回路を設けているため問題ない。
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。	自動減圧系の多重性，独立性に悪影響を与えないよう，区分ごとに条件信号回路を設けているため問題ない。
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。	自動減圧系は，駆動源である電源の喪失で系統の現状維持（フェイル・アズ・イズ），その他の不利な状況が発生した場合でも多重性，独立性をもつことで原子炉を十分に安全な状態に導くようにしている。追加する条件信号回路はこの安全保護動作を阻害するものではない。
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。	条件信号回路はアナログで構成しており，不正アクセス行為による影響を受けない。
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。	計測制御系とは共用していないため，影響はない。

設置許可基準規則 第十二条（安全施設）	自動減圧系への影響
４　安全施設は、その健全性及び能力を確認するため、その安全機能の重要度に応じ、発電用原子炉の運転中又は停止中に試験又は検査ができるものでなければならない。	条件信号回路を設けることで自動減圧系の試験に影響を与えることはない。



第４図　自動減圧系に追加する条件信号回路図

参考１　新規制対応設備の安全保護回路への影響について

1.　代替制御棒挿入機能について

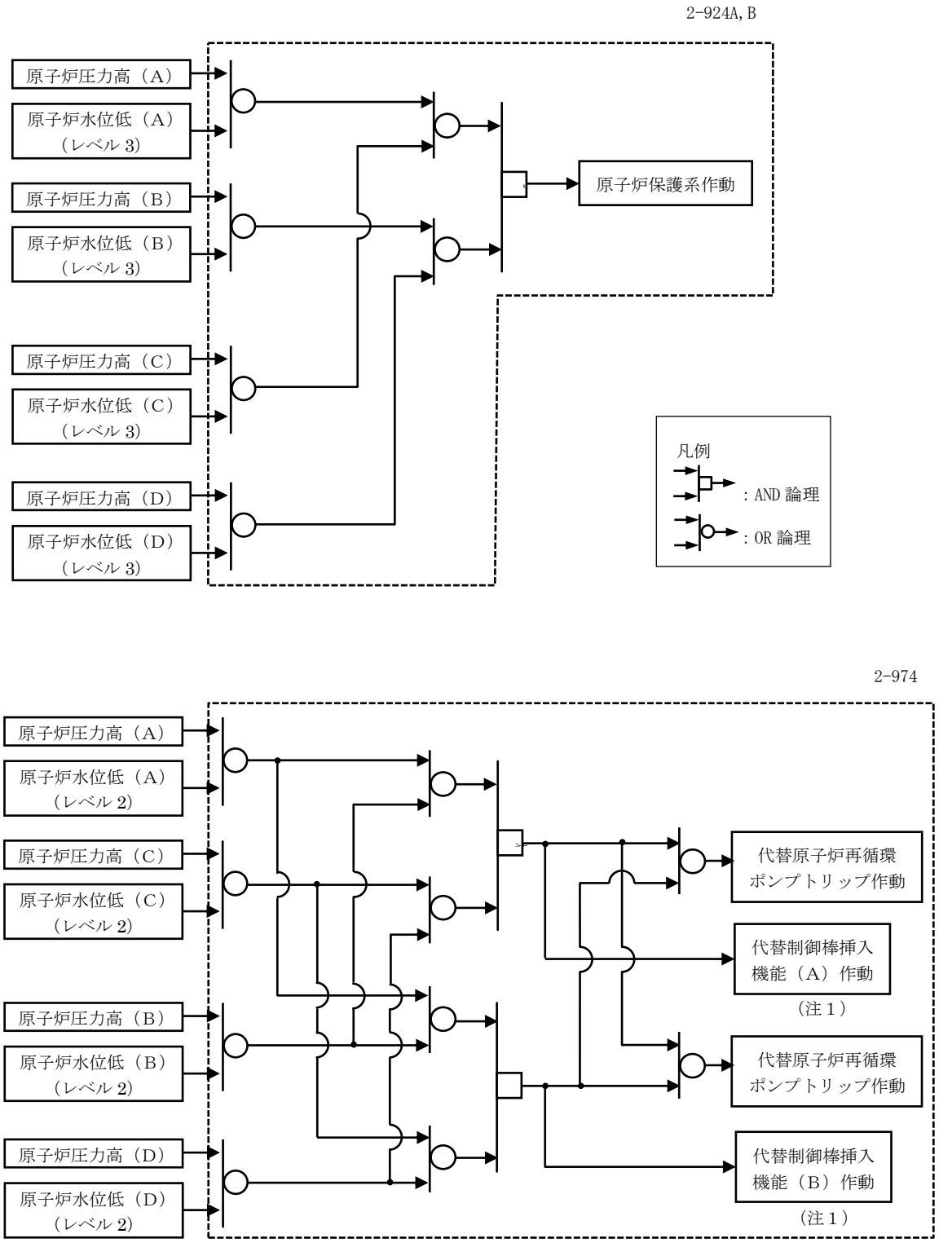
(1)　目的

代替制御棒挿入機能は，制御棒駆動機構を作動させる原子炉保護系の故障によるＡＴＷＳ発生時に，スクラム用計装空気配管に取り付けられた排気弁を開放することによって制御棒を急速に挿入し，原子炉出力を低下させることを目的とする。

(2)　原子炉保護系への影響について

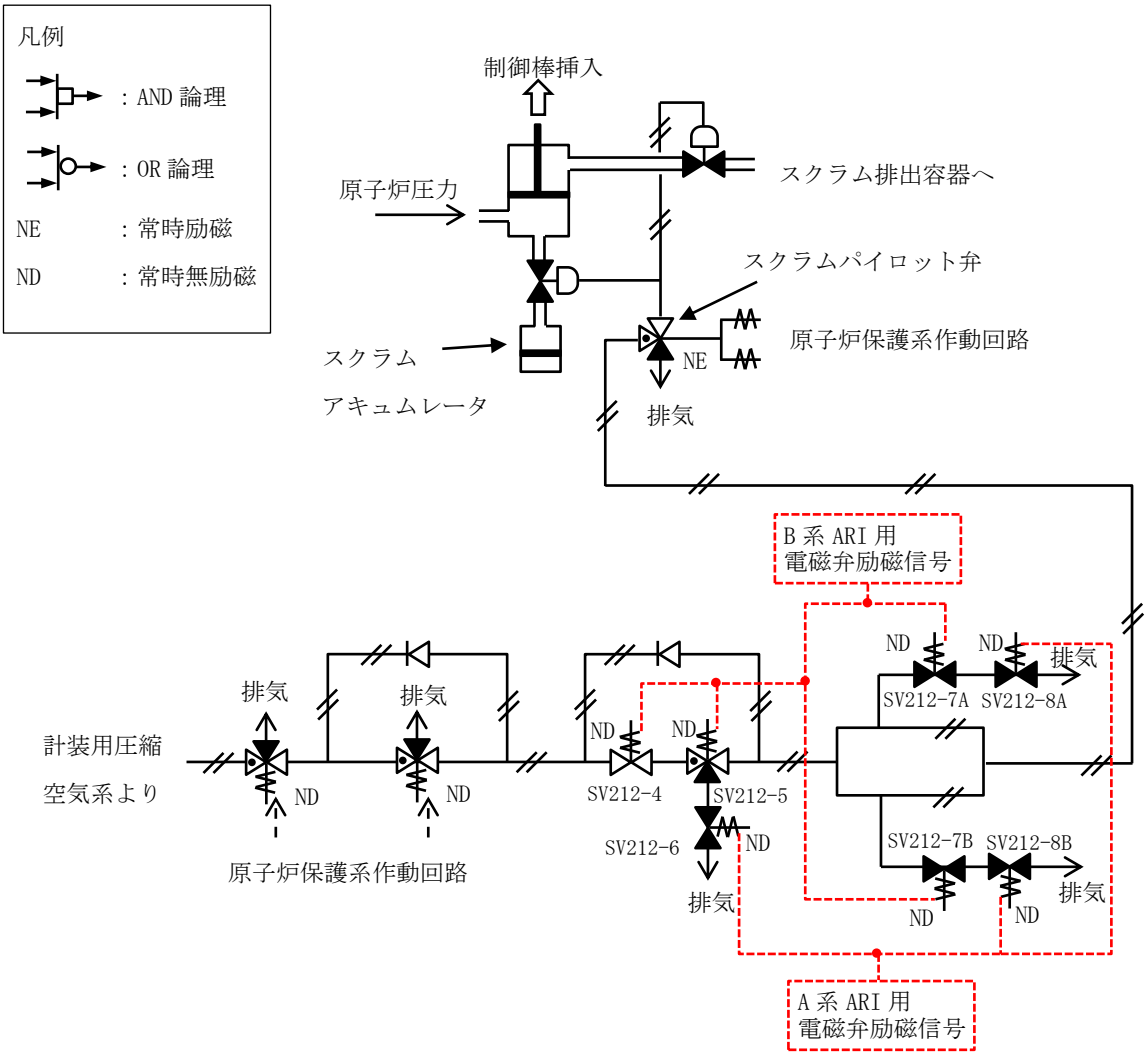
原子炉保護系と代替制御棒挿入機能の論理回路は第１図のとおり，検出器から論理回路まで，原子炉保護系と代替制御棒挿入機能は独立した構成となっており，原子炉保護系に悪影響を与えない設計としている。

なお，第２図のとおり原子炉保護系の作動電磁弁についても，代替制御棒挿入機能と原子炉保護系では独立した構成とする。



（注１：代替制御棒挿入機能は A 系及び B 系の AND 条件で作動する）

第１図　原子炉保護系と代替制御棒挿入機能の論理回路



第２図　電磁弁の分離について

2.　代替自動減圧ロジック（代替自動減圧機能）

(1)　目的

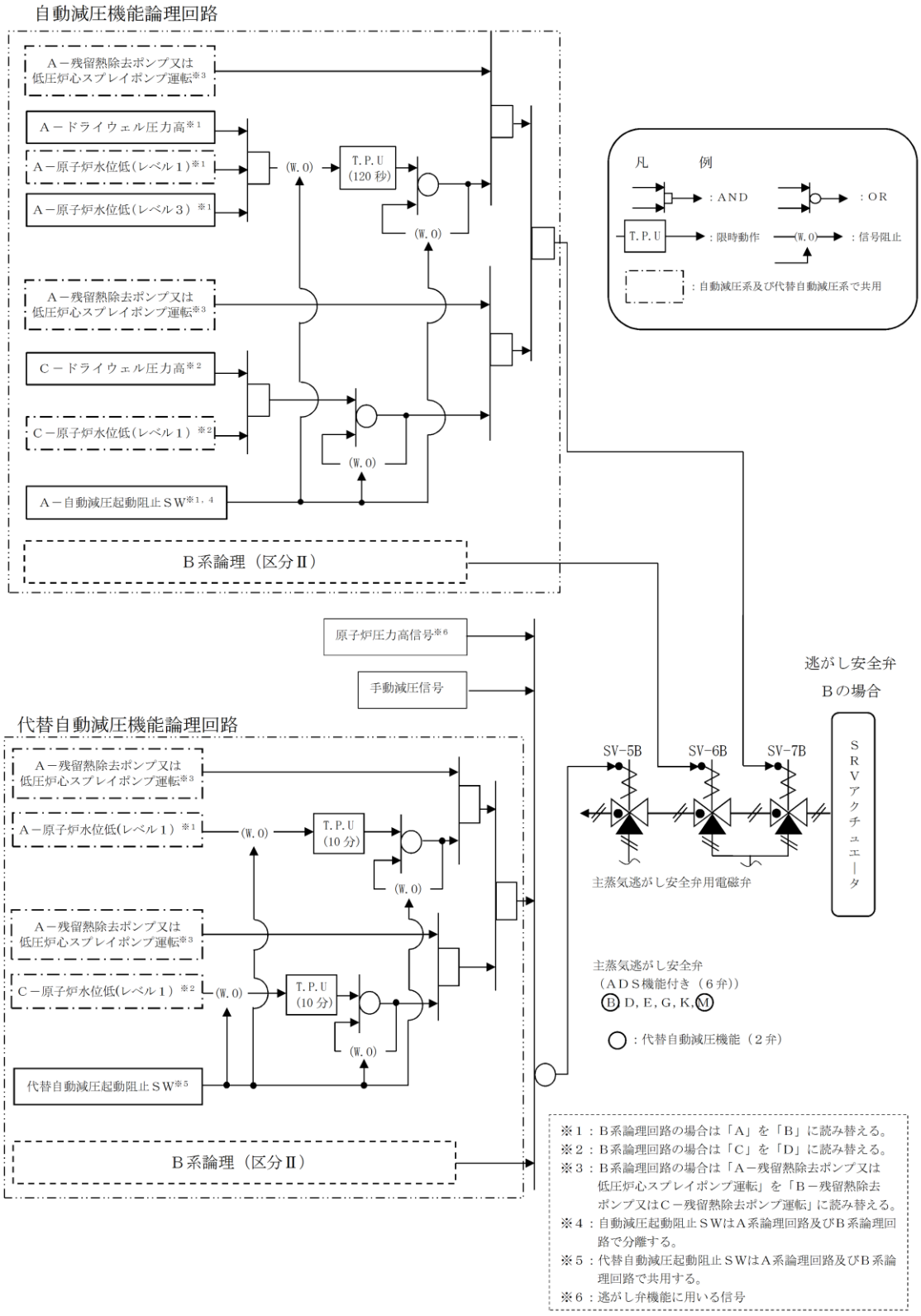
代替自動減圧機能は，原子炉冷却材圧力バウンダリが高圧の場合であって，自動減圧系が有する発電用原子炉の減圧機能が喪失するおそれがある場合又は発生した場合に，原子炉冷却材圧力バウンダリを減圧し，炉心の著しい損傷及び原子炉格納容器の破損を防止することを目的とする。

(2)　自動減圧系への影響について

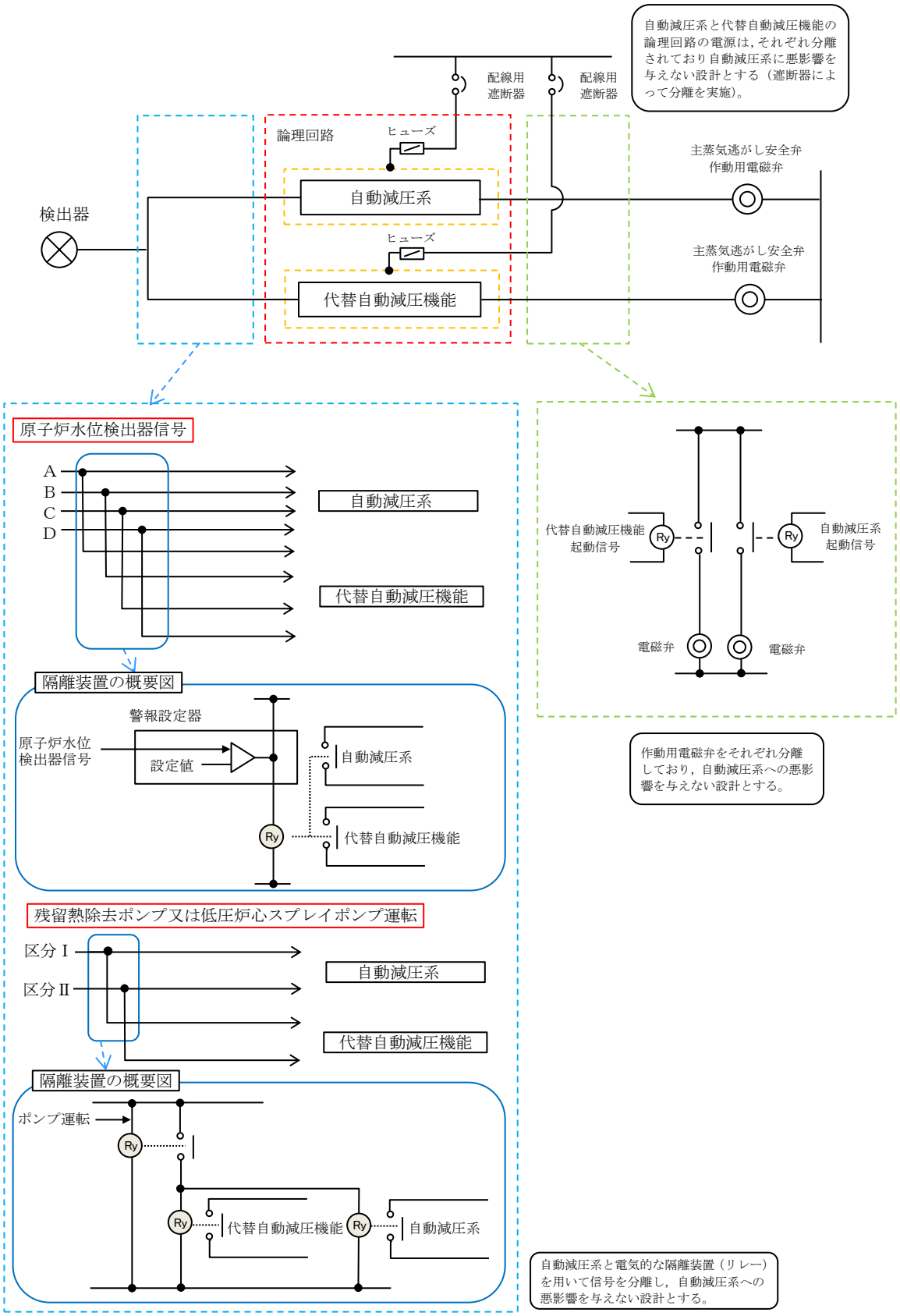
自動減圧系と代替自動減圧機能の論理回路を第３図に示す。自動減圧系に対して独立した論理回路を構成しており，自動減圧系に悪影響を与えない設計としている。

第４図のとおり原子炉水位低（レベル１），低圧炉心スプレイポンプ運転及び残留熱除去ポンプ運転信号については共用しているが，自動減圧系と隔離装置を用いて電気的に分離しており，自動減圧系への悪影響を与えない設計とする。

なお，原子炉スクラム失敗時に自動減圧が自動起動すると，高圧炉心スプレイ系及び低圧注水系から大量の冷水が注水され，出力の急激な上昇に繋がるため，自動減圧系及び代替自動減圧機能の自動起動阻止回路を用いて，自動起動を阻止する設計とする。自動減圧系及び代替自動減圧機能の自動起動阻止回路は，手動阻止スイッチ（ハードスイッチ）を分離することで，自動減圧系に悪影響を及ぼさない設計とする。



第３図　自動減圧系及び代替自動減圧機能の論理回路図



第４図　信号の分離について

別紙３　アナログ型安全保護回路の不正アクセス行為等の防止対策

アナログ型安全保護回路の検出器から論理回路について，検出器はアナログ機器，論理回路はハードワイヤーロジック（リレーや配線によるアナログ回路）で構成しており，一部の安全保護回路への出力信号処理でデジタル装置を使用している。安全保護回路（原子炉保護系，工学的安全施設作動回路）について，検出器から論理回路の入口までの構成機器に対しアナログ・デジタルの有無を抽出した。原子炉保護系の構成例を第１図，抽出結果を第１ 表，第２ 表に示す。

構成機器のうちデジタル処理部のある機器としてプロセス放射線モニタ及び平均出力計装の演算回路がある。ただし，これらのデジタル処理部のある機器は外部ネットワークと直接接続しないことにしている。さらに，出入管理により外部からの妨害行為または破壊行為を防止していることから，不正アクセス行為による被害を受けることはない。

不正アクセス行為等による対策については，「2.１　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」に記載の設計方針としている（下記に，「2.1」の記載内容の一部再掲）。

(1)　物理的アクセス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，出入管理により物理的アクセスを制限し，電気的アクセスについては，安全保護回路を有する制御盤を施錠管理とし，デジタル処理部と接続する保守ツールは施錠管理された場所に保管し，パスワード管理することで管理されない変更を防止している。

(2)　ハードウェアの物理的な分離又は機能的な分離対策

安全保護回路の信号は，安全保護回路→ＳＰＤＳデータ収集サーバ→防護装置→ＳＰＤＳ伝送サーバ→防護装置を介して外部に伝送している。この信号の流れにおいて，安全保護回路からは発信されるのみであり，外部からの信号を受信しないこと及びハードウェアを直接接続しないことで物理的及び機能的分離を行っている。

(3)　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防止対策

安全保護回路の信号で外部ネットワークへのデータ伝送の必要がある場合は，防護装置（通信状態を監視し，送信元，送信先及び送信内容を制限することにより，目的外の通信を遮断）を介して安全保護系盤の信号を一方向（送信機能のみ）通信に制限し外部からのデータ書き込み機能を設けないことでウイルスの侵入及び外部からの不正アクセスを防止している。

(4)　システムの導入段階，更新段階又は試験段階で承認されない動作や変更を防ぐ対策

アナログ型安全保護回路は別紙１の通り

安全保護回路のうちデジタル処理部を持つ機器は，固有のプログラム言語を使用（一般的なコンピュータウイルスが動作しない環境）するとともに，保守以外の不要な演算回路へのアクセス制限対策として入域制限や設定値変更作業での施錠管理及びパスワード管理を行い，関係者以外の不正な変更等を防止している。

(5)　耐ノイズ・サージ対策

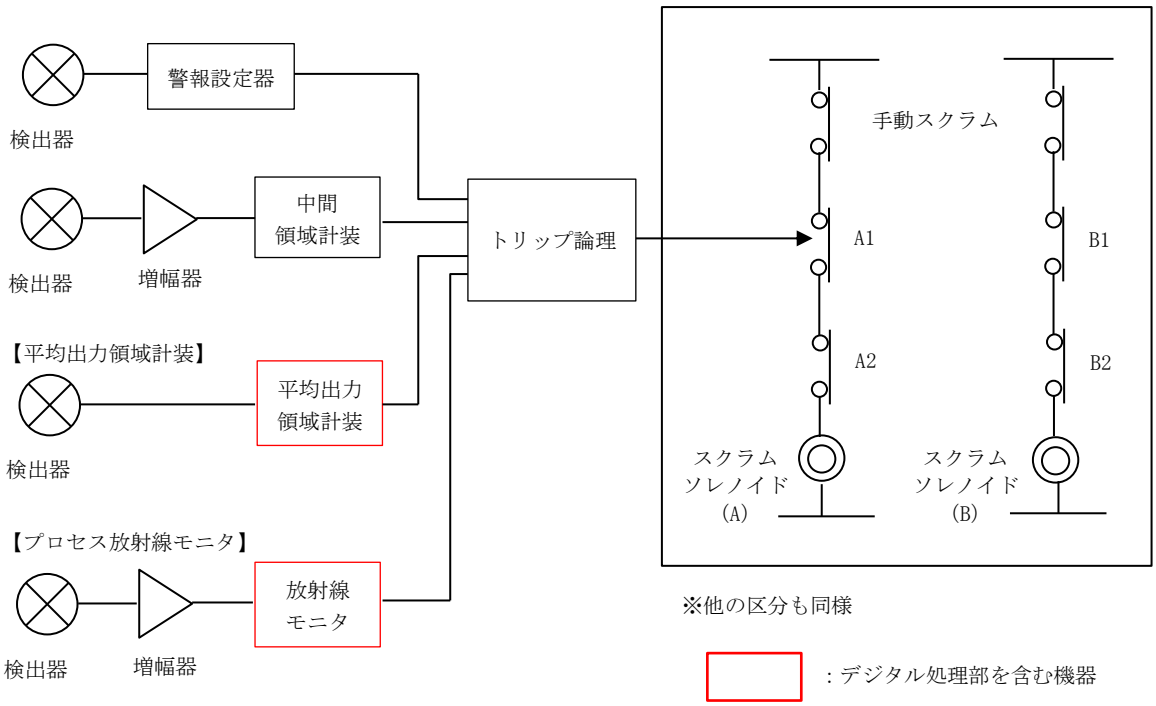
安全保護回路は，雷，サージ・ノイズ，電磁波障害等による擾乱に対して，制御盤へ入線する電源受電部や外部からの信号入出力部にラインフィルタや絶縁回路を設置している。

ケーブルは金属シールド付ケーブルを適用し，金属シールドは接地して電磁波の侵入を防止する設計としている。安全保護回路は，鋼製の筐体に格納し，筐体を接地することで電磁波の侵入を防止する設計としている。

(6) ウイルス侵入防止について，供給者への要求事項及び供給者で実施している対策

ウイルスの侵入防止対策も含め，当社の安全保護系への妨害行為又は破壊行為を防止するため，「2.1（6）」に記載のセキュリティ対策を供給者へ要求することとしている。

アナログ型安全保護回路（A1 チャンネル）の例



第１図　安全保護回路の構成例（原子炉保護系）

第１表　原子炉保護系の構成機器

原子炉スクラム信号の種類		検出器	設定器
原子炉圧力高		アナログ	アナログ
原子炉水位低（レベル３）		アナログ	アナログ
格納容器圧力高		アナログ	アナログ
中性子束高	平均出力領域計装	アナログ	デジタル
	中間領域計装	アナログ	アナログ
中性子計装不作動	平均出力領域計装	アナログ	デジタル
	中間領域計装	アナログ	アナログ
スクラム排出水容器水位高		アナログ（接点）	
		アナログ	アナログ
主蒸気隔離弁閉		アナログ（接点）	
主蒸気止め弁閉		アナログ（接点）	
蒸気加減弁急速閉		アナログ（接点）	
主蒸気管放射線高		アナログ	デジタル
地震大		アナログ（接点）	
手動		アナログ（接点）	
原子炉モードスイッチ「停止」位置		アナログ（接点）	

第２表　工学的安全施設作動回路の構成機器

機能	信号の種類	検出器	設定器
主蒸気隔離弁閉鎖	原子炉水位低（レベル２）	アナログ	アナログ
	主蒸気管圧力低	アナログ	アナログ
	主蒸気管流量大	アナログ	アナログ
	復水器真空度低	アナログ	アナログ
	主蒸気管放射線高	アナログ	デジタル
	主蒸気管周囲温度高	アナログ	アナログ
主蒸気隔離弁以外の主要な隔離弁閉鎖	格納容器圧力高	アナログ	アナログ
	原子炉水位低（レベル３）	アナログ	アナログ
非常用ガス処理系起動	原子炉棟排気放射線高	アナログ	デジタル
	燃料取替階放射線高	アナログ	デジタル
	格納容器圧力高	アナログ	アナログ
	原子炉水位低（レベル３）	アナログ	アナログ
高圧炉心スプレイ系及び同ディーゼル起動	格納容器圧力高	アナログ	アナログ
	原子炉水位低（レベル１Ｈ）	アナログ	アナログ
低圧炉心スプレイ系起動	格納容器圧力高	アナログ	アナログ
	原子炉水位低（レベル１）	アナログ	アナログ

機能	信号の種類	検出器	設定器
低圧注水系起動	格納容器圧力高	アナログ	アナログ
	原子炉水位低（レベル１）	アナログ	アナログ
自動減圧系作動	格納容器圧力高	アナログ	アナログ
	原子炉水位低（レベル１）	アナログ	アナログ
非常用ディーゼル発電機起動	格納容器圧力高	アナログ	アナログ
	原子炉水位低（レベル１）	アナログ	アナログ

別紙４　ソフトウェア更新時の立会における，インサイダー等に対するセキュリティ対策

安全保護回路について，検出器から論理回路入口までの構成機器のうちデジタル処理部がある機器は，放射線モニタと平均出力領域計装である。これらについては，以下の対策を実施している。

・保守ツールについては，施錠管理されたラック内に保管する。また，保守ツール使用には，[redacted] の許可を得る必要があるとともに，パスワードの入力が必要である。

・保守ツール接続のためには制御盤の解錠が必要であり，制御盤の鍵は [redacted] の許可を得た上で貸し出しを行う。これらにより，許可された者のみアクセス可能とする。

[redacted]

・ソフトウェア変更に係わる者は，情報セキュリティ教育を受講している。

本資料のうち，枠囲みの内容は機密に係る事項のため公開できません。

別紙５　安全保護回路のうちデジタル部分のシステムへ接続可能なアクセスについて

安全保護回路の検出器はアナログ機器，論理回路はハードワイヤーロジック（リレーや配線によるアナログ回路）で構成されており，ソフトウェアを用いないアナログ回路であるが，一部の安全保護回路への出力信号処理でデジタル装置を使用している。

安全保護回路のうちデジタル部分のシステムへ接続可能なアクセスとして，保守ツールがある。こちらについては以下のとおり対策する。

(1) 保守ツールによる不正アクセスの防止対策

保守ツールは，出力領域モニタ盤に接続することによりデジタル処理を行う演算回路からデータを受信する機能があるが，保守ツールは施錠管理された場所に保管し，パスワード管理することで管理されない変更を防止している。

(2) 物理的アクセスの制限対策

保守ツールは通常時接続はせず，接続のためには制御盤の解錠を必要とする。

また，施錠管理された場所に保管することで管理されない使用及び変更を防止している。

発電所への入域に対しては，出入管理により物理的アクセスを制限し，管理されない変更を防止している。

別紙６　安全保護回路のうちデジタル部分について，システム設計と実際のデバイスが具備している機能との差（未使用機能等）による影響の有無

システム設計に基づき，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，安全保護回路のうちデジタル処理部がある機器は，工場出荷前試験及び導入時における試験を実施することにより，要求される機能を満足することの確認及び未使用機能等による悪影響がないことの確認が供給者によって確実に実施されていることを確認している。

なお，安全保護回路のうちデジタル部分については，未使用機能がないことを確認している。

別紙７　安全保護系の過去のトラブル（落雷によるスクラム動作事象等）の反映事項

安全保護系に係る過去のトラブル情報を抽出し，島根原子力発電所２号炉の安全保護系の設計面への反映すべき事項を下記のとおり確認した。

(1)　過去の不具合事例の抽出

安全保護系の設計面に反映が必要となる事象の抽出にあたり，以下を考慮した。

①公開情報（原子力施設情報公開ライブラリー「ニューシア」）を対象

②キーワード検索（安全保護系，原子炉保護系，工学的安全施設作動回路，雷，ノイズ，スクラム等）により抽出

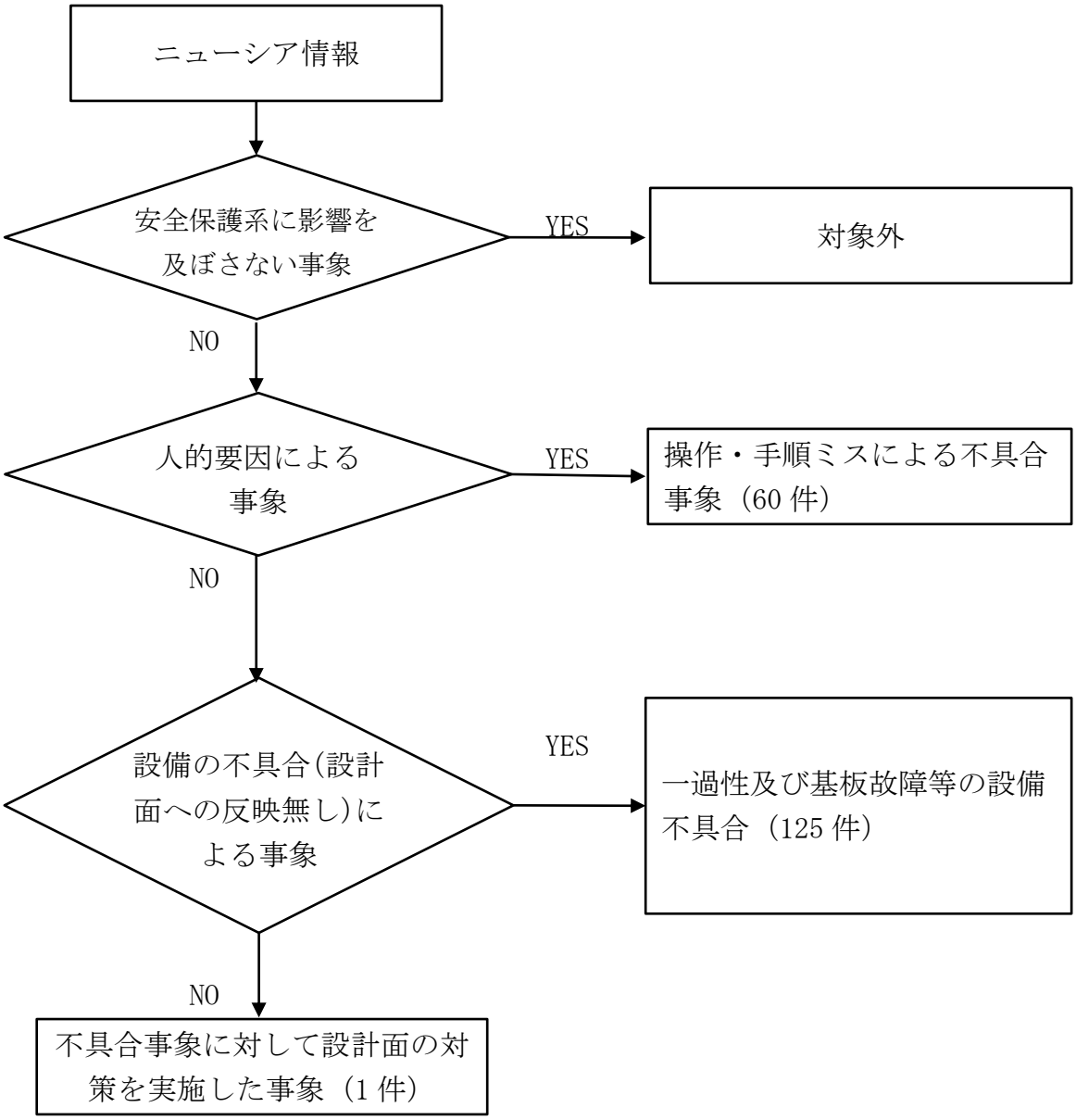
③間接的な影響（他設備のトラブル）によって安全保護系へ影響を与えた事象（安全保護系の正動作は除く）

(2)　反映が必要となる事象の選定

安全保護系の設計面に反映が必要となる事象について，第１図及び第１表に基づき抽出した。抽出された過去の不具合事象を第２表に示す。

(3)　過去の不具合事例への対応について

過去の不具合事例を抽出し，安全保護系の設計面への反映要否について検討を実施した結果，対応済み，もしくは，反映不要であることを確認した。



第１図　設計面へ反映すべき事項の抽出フロー

第１表　設計面へ反映不要とする理由

項目	事象例	理由
人的要因による事象	安全処置の実施又は復旧時のミス，作業手順のミス等	作業手順，作業管理等の人的要因によるものであり，設計面へ反映すべき事項ではない。
設備の不具合（設計面への反応無し）による事象	計器・部品の単品故障・一過性故障・偶発故障等	故障した部品の交換を図ることが基本であり，設計面へ反映すべき事項ではない。

第２表　抽出された過去の不具合事象

件名	島根原子力発電所１号機　「中性子束異常高」信号による原子炉自動停止について
会社名・プラント	中国電力株式会社　島根原子力発電所１号機
発生日	1992 年 02 月 20 日
事象概要	島根原子力発電所１号機は，定格出力（４６０MWｅ）で運転中のところ，平成４年２月２０日１１時３２分「ＡＰRM異常高／不作動」の警報が発生し，原子炉が自動停止した。 調査の結果，平均出力領域モニタ（以下，ＡＰＲＭ）全６チャンネル中３チャンネル（２，３，６）に「中性子束異常高」信号が発生（表示灯が点灯）し，原子炉保護系が動作したものであることが確認された。 また，ＡＰRM記録計のチャートでは，ＡＰRM全６チャンネル中３チャンネル（２，３，６）に，指示値の上昇がわずかに（最大１０３％程度まで）認められた。 一方，原子炉自動停止直前のプラント主要パラメータ（原子炉圧力，原子炉水位，炉心流量等）については，有意な変化は認められなかった。 なお，これによる外部への放射能の影響はなかった。
原因	【原因調査の概要】 （１）「中性子束異常高」信号発生の要因分析 「中性子束異常高」信号の発生する要因としては，原子炉圧力上昇，炉心流量の増加，炉水温度低下，中性子束を上昇させる操作の実施およびＡＰRM誤動作の可能性が考えられる。 要因分析に基づき点検調査を行った結果，「中性子束異常高」信号は，実際に中性子束が異常に上昇して発生したものではなく，落雷に伴うノイズ混入によるＡＰRMの誤動作で発生したものである可能性が強いことがわかった。 （２）落雷に係る調査 ６６ｋＶ鹿島線の避雷器の動作が確認された。また，発電所構内建物，構築物，避雷針について調査したところ，１号機原子炉建物避雷針に新しい落雷の痕跡が認められた。 （３）落雷による中性子計測設備への影響 ａ．１号機原子炉建物避雷針への落雷により，中性子計測設備に誘導電流が生じた。誘導電流はケーブル長に比例するため，ケーブル長の長いチャンネル２，３，６により大きな誘導電流が流れたものと判断された。 ｂ．中性子計測設備のケーブル構成を模擬し，模擬パルス電流を印加して誘導電流を発生させたところ，中性子計測設備のケーブルに「中性子束異常高」スクラム信号レベルを超える信号変化が生じることが確認された。 【事象の原因】 １号機原子炉建物避雷針へ落雷があり，中性子計測設備のケーブルに誘導電流が流れ，これが通常レベルの電流信号に重畳したため，「中性子束異常高」の誤信号が発信したものと推定された。
対策	（１）中性子計測設備およびその他の計測設備の点検を実施し，異常のないことを確認した。 （２）念のため，落雷による影響を低減するため，中性子計測設備および中性子計測設備と同様な設備である原子炉建物換気系モニタについては，信号ケーブルを収納している電線管をアルミで内張りしたしゃへい材で包み込むこととした。

別紙 8　安全保護回路のうち一部デジタル演算処理を行う機器のソフトウェアの検証及び妥当性確認について

安全保護回路のうち，一部デジタル演算処理を行う機器のソフトウェアは，安全保護回路で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，設計，製作，試験，変更管理の各段階で「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，以下「JEAG4609」という。）に準じた検証及び妥当性確認を実施する。

島根原子力発電所２号炉においては平均出力領域計装，放射線モニタ（主蒸気管放射線高，原子炉棟排気放射線高，燃料取替階放射線高）の演算処理においてソフトウェアを用いている。以下にこれらソフトウェアの検証及び妥当性確認の概要を示す。

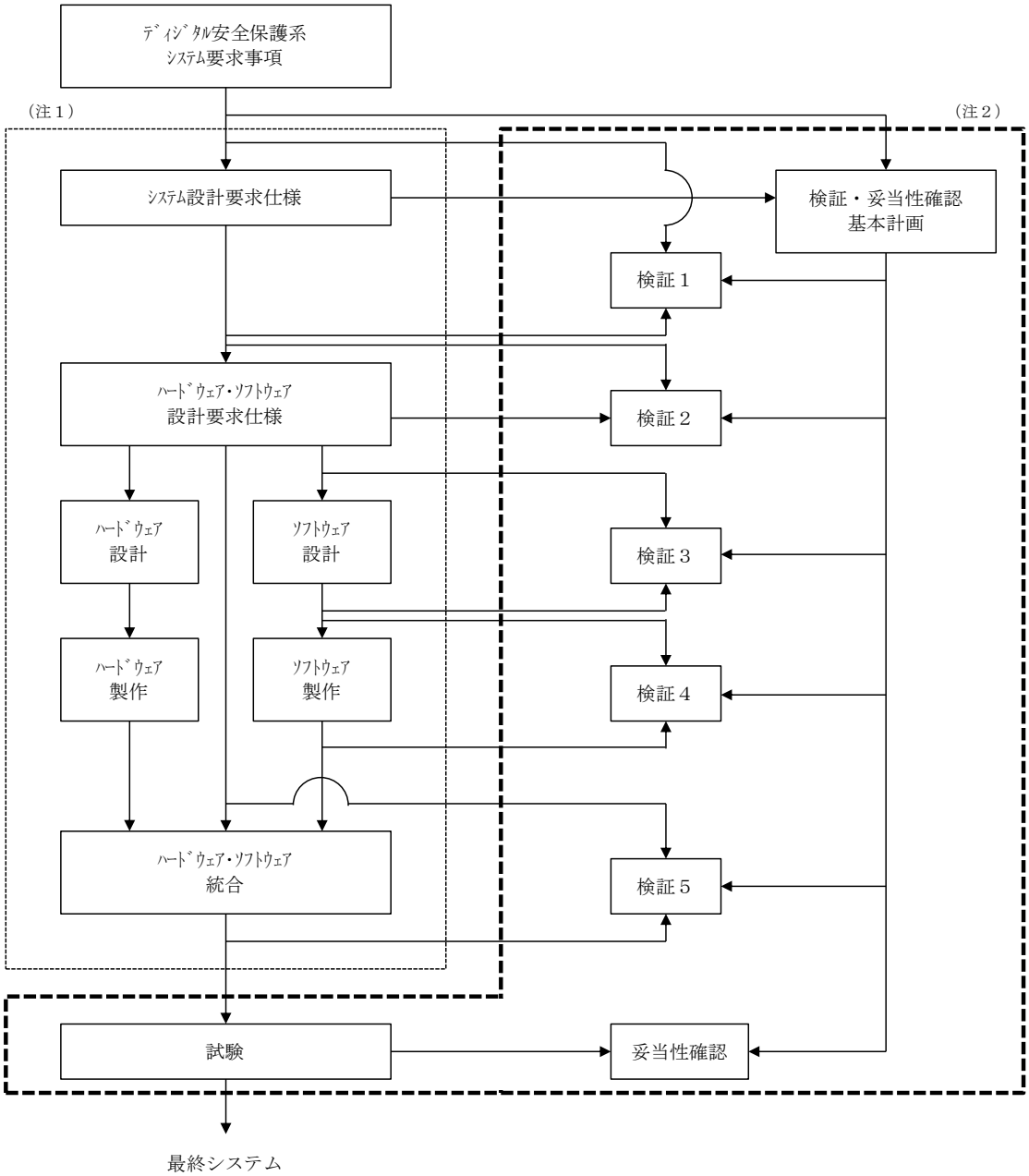
(1) 平均出力領域計装，放射線モニタ（主蒸気管放射線高，原子炉棟排気放射線高，燃料取替階放射線高）

これらに用いるソフトウェアは JEAG4609 に準じた検証及び妥当性確認を実施する。（第１図）

検証は，設計，製作過程のステップごとに上位仕様と下位仕様の整合性チェックを主体として，以下の観点から検証作業を行う。

ａ．安全保護系システム要求事項がシステム設計要求仕様に正しく反映されていること。
ｂ．システム設計要求仕様がハードウェア，ソフトウェアの設計要求仕様に正しく反映されていること。
ｃ．上記設計要求仕様に基づいてソフトウェアが製作されていること。
ｄ．検証及び妥当性確認が可能なソフトウェアとなっていること。

必要な検証を経て製作されたソフトウェアをハードウェアと統合した後の全体システムについて，最終的に安全保護系システム要求事項が正しく実現されていることを確認するために妥当性確認を行う。



検証１・・・システム設計要求仕様検証
検証２・・・ハードウェア・ソフトウェア
　　設計要求仕様検証
検証３・・・ソフトウェア設計検証
検証４・・・ソフトウェア製作検証
検証５・・・ハードウェア・ソフトウェア統合検証

（注１）　は，設計・製作作業の範囲を示す。

（注２）　は，検証・妥当性確認作業の範囲を示す。

第１図 検証及び妥当性確認（JEAG4609）

別　添

島根原子力発電所２号炉

運用，手順説明資料
安全保護回路

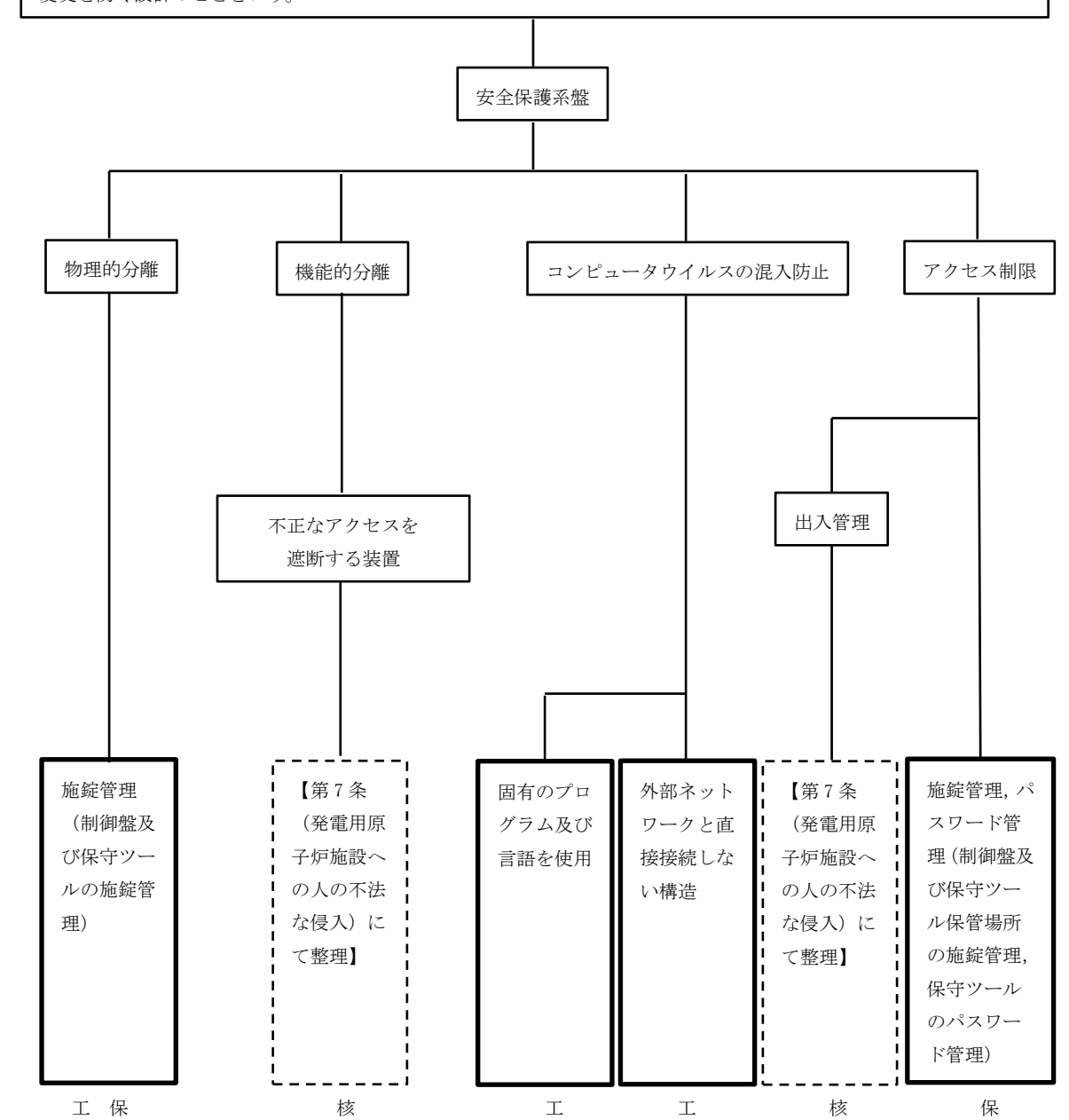
24 条　安全保護回路

設置許可基準　第 24 条第６号

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。

（解釈）

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。



【後段規制との対応】
工：工認（基本方針，添付書類）
保：保安規定（運用，手順に係る事項，下位文書含む）
核：核物質防護規定（下位文書含む）

【添付六，八への反映事項】
：添付六，八に反映
：当該条文に該当しない（他条文での反映事項他）

運用，手順に係る対策等（設計基準）

設置許可基準 対象条文	対象項目	区分	運用対策等
第 24 条 安全保護回路	施錠管理	運用・手順	施錠管理に関する管理方法を定める。
		体制	（運転員，保修員による識別及び施錠管理）
		保守・点検	—
		教育・訓練	—
	パスワード管理	運用・手順	管理（盤のパスワード管理の手順整備含む） 操作（パスワード入力手順の整備含む）
		体制	（保修員によるパスワード管理）
		保守・点検	—
		教育・訓練	—