ドラフト

JEAC4620-2020　安全保護系へのディジタル計算機の適用に関する規程
JEAG4609-2020　ディジタル安全保護系の検証及び妥当性確認（V＆V）に関する指針 改定内容について

令和4年1月25日

（一社）日本電気協会　原子力規格委員会

目次

	頁
➢1. JEAC4620-2020/JEAG4609-2020の概要と改定経緯	3
➢2. JEAC4620-2020/JEAG4609-2020の改定目的	4
➢3. JEAC4620-2008/JEAG4609-2008技術評価書を踏まえた改定	5
➢4. 法令改正(新規制基準施行)を踏まえた改定	9
➢5. 関連海外規格の調査	11
➢6. 運転経験, トラブル情報の調査	12
➢7. 安全設計分科会, 規格委員会からのコメントを踏まえた改定	13

1．JEAC4620-2020/JEAG4609-2020の概要と改定経緯

1989年　安全保護系へのディジタル計算機適用に当たり，ソフトウェアの品質確保を目的として，V&V（検証及び妥当性確認）を中心とした手順をガイドラインとして制定。（1999年に定期改定。）

JEAG4609-1989「安全保護系へのディジタル計算機の適用に関する指針」

2008年　省令62号 性能規定化に伴い，ディジタル安全保護系全体に対する性能及び信頼性の面から必要とされる事項全体について規程としてJEAC4620を制定。JEAG4609はV&Vに特化したガイドラインとして改定。

JEAC4620-2008「安全保護系へのディジタル計算機の適用に関する規程」
JEAG4609-2008「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」

2011年　NISA/JNESの技術評価書にて，JEAC4620-2008及びJEAG4609-2008がエンドースされる。（JEAC4620は条件付き）

2013年　技術基準規則の解釈に，2011年の技術評価書の条件を付記した形でJEAC4620-2008及びJEAG4609-2008が引用される。

NISA：旧 原子力安全保安院，JNES：旧 原子力安全基盤機構

2．JEAC4620-2020/JEAG4609-2020の改定目的

規制要求，海外関連規格を調査・検討し，本規程／指針へ必要な事項を反映する。

- NISA/JNESの技術評価書上の条件及び要望事項の確認
- 新規制基準（設置許可基準規則，技術基準規則）上の安全保護系への要求事項の確認
- 最新の関連海外規格の調査
- 運転経験，トラブル情報からの反映事項の確認

3．JEAC4620-2008/JEAG4609-2008技術評価書を踏まえた改定（1/4）

◆JEAC4620

No	NISA/JNES技術評価書の適用条件	JEAC4620への反映
1	①過渡時，事故時及び地震時の機能 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。	「4.1　過渡時及び地震時の機能」及び「4.2 事故時の機能」に左記条件を考慮した記載を追記。 記載内容については，技術基準規則との整合性を考慮して反映。
2	②検証及び妥当性確認 検証と妥当性確認の実施に際して作成された文書は，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。	（解説-23）に左記条件を追記。
3	③環境条件 デジタル計算機を設置するプラントで想定されるサージ電圧や電磁波等の外部からの外乱・ノイズについて，その対策の妥当性が十分であることを確証すること。	2008年版における「4.8　環境条件」を「4.9 外的要因」として，「環境条件」，「耐震性」，「その他の外的要因」に関する要求事項とその確証に関する記載に変更。 「4.9.1　環境条件」に，左記条件を考慮して外部からの外乱・ノイズに関する記載を追記。

3．JEAC4620-2008/JEAG4609-2008技術評価書を踏まえた改定（2/4）

◆JEAC4620

No	NISA/JNES技術評価書の適用条件	JEAC4620への反映
4	④計測制御系との分離 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，又は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。	左記条件を踏まえて，「ディジタル安全保護系は，計測制御系と部分的に共用する場合には，計測制御系で故障が生じてもディジタル安全保護系に影響のないよう，計測制御系と電気的に分離する設計とすること。」を要求事項として，本文に反映。 「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」，及び「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」については，実際の対策例を考慮した上で，（解説-8）にディジタル安全保護系と計測制御系との通信の機能的分離の措置の例として記載。
5	⑤外部ネットワークとの遮断 外部影響の防止された設備とすること。	2008年版における「4.16 外部ネットワークとの遮断」を，「4.18　不正アクセス行為等の被害の防止」の措置の例として，左記条件を考慮して（解説-17）に記載。

3．JEAC4620-2008/JEAG4609-2008技術評価書を踏まえた改定（3/4）

◆JEAC4620

No	NISA/JNES技術評価書の適用条件	JEAC4620への反映
6	⑥アンアベイラビリティ及び誤動作率の評価 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。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。	左記条件については，「4. ディジタル安全保護系に対する要求事項」の本文に，「ディジタル安全保護系は，動作に失敗する確率（アンアベイラビリティ）及び誤動作する頻度（誤動作率）を考慮し，その安全保護機能に相応した高い信頼性を有すること」を記載。 信頼性評価に必要な構成要素については，（解説－4）として左記条件の記載を追記。
7	なお，別記-7 No.10 の要求事項に対して，「デジタル安全保護系規程」には該当する記載がないことから，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。	「ディジタル安全保護系と動作原理等が異なる追加の設備を設けること」については，ディジタル安全保護系への要求事項ではないこと，及び技術基準規則でもJEAC4620の読み替えとはしていないことから，これまでと同様，留意事項にとどめており，要求事項としては反映していない。

3．JEAC4620-2008/JEAG4609-2008技術評価書を踏まえた改定（4/4）

◆JEAG4609

・技術評価書のJEAG4609への条件は無し。

・技術評価書でJEAG4609の規程化の要望あり。

⇒ 規程化しない方針とする

（V＆Vの実施，その体制などの「要求事項」はJEAC4620に記載されている。JEAG4609は解説-1に示す通り，JEAC4620のV&V要求に対しての指針という位置づけであり，規程化する必要性は低いと考える。）

4．法令改正（新規制基準施行）を踏まえた改定（1/2）

◆JEAC4620

（1）設置許可基準規則第24条（安全保護回路）

・第6項の「不正アクセス行為等の被害の防止」を4.18項として追加。
2008年版における以下の項目は具体策として本項の解説に変更
「4.16 外部ネットワークとの遮断」

（2）技術基準規則第35条（安全保護装置）

・第5項は，上記設置許可基準規則第6項と同様

・解釈3に記載のウイルス検出機能に対する考慮事項は，ウイルス検出機能を実装する可能性がほとんどないことから，現段階では追記しない。

・解釈4の「ディジタル」から「デジタル」への読替えに対しては，JISの用語定義に合わせ，現状通り「ディジタル」のままとする。

（3）全交流電源喪失の定義

・全交流電源喪失については，新規制基準前後で大幅に意味合いが異なるため，ディジタル型安全保護系の電源に関する要求事項を明確化した。

４．法令改正（新規制基準施行）を踏まえた改定（2/2）

◆JEAG4609

・新規制基準において，Ｖ＆Ｖに関する新たな要求事項は無い。

５．関連海外規格の調査

① 前回制改定時に調査したディジタル安全保護系関連の海外規格（IEEE, IEC 等）を調査

⇒ 至近で反映すべき内容は無かった。なお，MDEPの動向等についても確認。

② 不正アクセス防止に関し，サイバーセキュリティ関連の海外規格（ 10CFR73.54, RG 5.71, NEI08-09 ）を調査

⇒ サイバーセキュリティに関しては，通信と防護上の話であるため，JEAC4620上で対応を述べるのは困難。
安全保護系としてはJEAC4620の対策（不正アクセス行為等の被害の防止）を遵守することとし，サイバーセキュリティに特化した要求はしない。

③ ディジタルシステムの共通要因故障（CCF）に関して，DAS（Diverse Actuation System）に関するIAEA TECDOCを調査

⇒ CCF対応としてのハードウェア回路の設置はJEAC4620に「5. 留意事項」として位置づけている。現状は改定不要とした。

調査の結果，今回の改定で反映すべき項目は無かった。

６．運転経験，トラブル情報の調査

国内及び国外のディジタル安全保護系に関する

- 運転経験
- トラブル情報（NUCIA等）
- 新規制での安全審査状況

について，反映すべき事項の有無を調査。

運転経験，トラブル状況について反映すべき事項は無かった。

新規制基準に基づく安全審査から得られた知見を考慮して，各要求項目の改定文案を検討した。（要求項目としての追加は無かった。）

7．安全設計分科会，規格委員会からのコメントを踏まえた改定（1/4）

安全設計分科会における審議を踏まえて，主に以下のような点を反映。

・過渡時及び地震時，事故時における要求事項の明確化

⇒過渡時及び地震時における要求事項と事故時における要求事項を分けて記載し，それぞれに対する要求事項を明確化。

・ディジタル計算機を適用していない従来型の安全保護系に対する記載を追加

⇒解説に「ディジタル計算機を適用していない従来型の安全保護系に対しては，「原子力発電所安全保護系の設計規程：JEAC4604-2009」に従う」旨を記載。JEAC4604とJEAC4620の統合については，その可否も含めて今後検討（今回の改定範囲には含めない）。

・地震時における要求事項の明確化（JEAC4620）

⇒地震は基準地震動を想定していること，「燃料許容損傷限界を超えない」とは過渡変化時に対する要求であることを解説として追加。

7．安全設計分科会，規格委員会からのコメントを踏まえた改定（2/4）

・ソフトウェアの管理外の変更防止要求と不正アクセス防止要求の分割

⇒ JEAC4620改定案で不正アクセス防止の手段としていた「ソフトウェアの管理外の変更防止」を個別の要求とし，2008年版の構成に戻した。

・設計側品質保証活動とV&Vとの関係，JEAG4609の位置付けの明確化

⇒指針に「0．序論」を追加し，V&Vの概要，JEAG4609の章構成等を記載。

・故障時の機能に関する記載の適正化（JEAC4620）

⇒故障時の機能について，本文と解説が冗長な記載になっていたところ，記載を見直し，解説を削除することとした。

・動作原理等の異なる追加の設備に関する記載の適正化

⇒「動作原理等の異なる追加の設備」について，本文に設置を推奨する旨を記載。

7．安全設計分科会，規格委員会からのコメントを踏まえた改定（3/4）

・V&Vの実施体制に関する内容の明確化

⇒V&Vを実施する個人又はグループについて「V&Vを実施する力量を有することを組織が認めた者とする」旨の記載に変更。

7．安全設計分科会，規格委員会からのコメントを踏まえた改定（4/4）

原子力規格委員会における審議を踏まえて，主に以下のような点を反映。

・規格の利用者について目的の項に明記

⇒「原子力発電所の事業者及びディジタル安全保護系の供給者」と記載。

・JEAC4111/JEAG4121の品質保証とJEAC4620/JEAG4609のV&Vの関係を明確化

⇒JEAC4111/JEAG4121に従った品質保証活動を実施した上で，ディジタル安全保護系のソフトウェアに対しV&V活動を実施することを記載（目的，用語の定義，品質保証等の項に反映）。

⇒「検証及び妥当性確認」を「V&V」として用語の定義を変更。指針の名称も「ディジタル安全保護系の検証及び妥当性確認（V&V）に関する指針」に変更。