第４回デジタル安全保護系に関する日本電気協会規格の
技術評価に関する検討チーム
議事録

１．日時

令和４年８月２５日（木）１４：３０～１５：４０

２．場所

原子力規制委員会　１３階Ｂ・Ｃ・Ｄ会議室

３．出席者

原子力規制委員会

田中　知	原子力規制委員会委員

原子力規制庁

佐藤　暁	技術基盤グループ長
遠山　眞	技術基盤グループ　技術基盤課長
佐々木　晴子	技術基盤グループ　技術基盤課　企画調整官
今瀬　正博	技術基盤グループ　技術基盤課　原子力規制専門職
濱口　義兼	技術基盤グループ　シビアアクシデント研究部門 主任技術研究調査官
皆川　武史	技術基盤グループ　システム安全研究部門　技術研究調査官
酒井　宏隆	技術基盤グループ　放射線・廃棄物研究部門 上席技術研究調査官
藤澤　博美	技術参与
瀧田　雅美	技術参与

一般社団法人　日本電気協会

高橋　毅	原子力規格委員会　副委員長
遠藤　亮平	計測制御検討会　主査

今野　浩明	計測制御検討会　副主査
内海　正文	計測制御検討会　委員
下野　哲也	計測制御検討会　委員
加藤　守	計測制御検討会　委員
小山　三輝雄	計測制御検討会　委員
西田　直樹	安全設計分科会　幹事
原　勲	計測制御検討会　委員
白澤　寛司	計測制御検討会　常時参加者

４．議題

（１）　デジタル安全保護系に関する日本電気協会規格の技術評価について

５．資料

資料４－１	「デジタル安全保護系に関する日本電気協会規格の技術評価に関する検討チーム会合における日本電気協会への説明依頼事項（案)」に対する回答
資料４－２	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 4620-2020）並びに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（JEAG 4609-2020)」に関する技術評価書（案）
参考資料４－１	デジタル安全保護系に関する日本電気協会規格の技術評価に関する検討チーム会合における日本電気協会への説明依頼事項（案）
参考資料４－２	「デジタル安全保護系に関する日本電気協会規格の技術評価に関する検討チーム会合における日本電気協会への説明依頼事項（その２)」に対する回答（修正版）

６．議事録

○田中委員　それでは、定刻になりましたので、デジタル安全保護系に関する日本電気協会規格の技術評価に関する検討チームの第4回会合を開催いたします。司会進行を務めさせていただきます原子力規制委員会の田中でございます。よろしくお願いします。

本検討チームは、構成員名簿のとおり、原子力規制委員及び原子力規制庁の担当者で構成されております。また、説明者として日本電気協会の方々に御出席いただいております。よろしくお願いいたします。

それでは、事務局から、議事運営について説明をお願いいたします。

○佐々木企画調整官　原子力規制庁、佐々木です。

本日の会合の議事運営ですが、新型コロナウイルス感染症対策のため、テレビ会議システムを用いて実施いたします。

本日の配付資料は、議事次第の配付資料一覧を御覧ください。

なお、注意事項ですが、マイクについては、発言中以外は設定をミュートにする、発言を希望する際は大きく挙手する、発言の際はマイクに近づく、音声が不明瞭な場合は相互に指摘するなど、円滑な議事運営に御協力をお願いします。発言する際には、必ずお名前を名乗ってから発言するようにしてください。また、資料の説明の際には、資料番号及びページ番号が分かるように発言していただき、該当箇所がどこか分かるようにしてください。よろしくお願いします。

○田中委員　よろしくお願いいたします。

それでは、早速本日の議題に入ります。第3回会合では、日本電気協会より、第1回会合、第2回会合におけるデジタル安全保護系、デジタル計算機、ソフトウェアといった用語の定義や適用範囲について、混同していた等の説明がありました。そのため、日本電気協会には、もう一度よく整理して、再度説明してもらうこととなりました。本日は、整理した内容を資料の4-1としていただいておりますので、まず、日本電気協会のほうから説明をお願いいたします。

○日本電気協会（高橋副委員長）　日本電気協会、原子力規格委員会の副委員長の高橋でございます。

これから御説明しますが、冒頭に当たり、一つ御挨拶をさせていただきたいと思います。

今お話がありましたように、今回、技術評価に当たりまして、私どものほうで不手際がございまして、整理して再説明するということになりました。実際、前回のチーム会合では、日本電気協会の説明には失望した、誠に遺憾、そういった厳しい御発言がありまして、実質、当時においては中断せざるを得ない、そういう状況になったわけでございます。これまでの私どもの協会における対応の不備、具体的には、誤った説明をしたとか、あるいは誤解を招くような説明をしたとか、そういうことですが、によりまして、今回の技術評

価作業に悪影響を与えてしまったことについて、誠に申し訳なく思っております。また、そういった中でも、本日検討チーム会合を再開いただいたことに対して、感謝を申し上げる次第でございます。

今回の原因と再発防止対策につきましては、当協会で検討しているところではございますけれども、原因としては、一つには会合での資料説明を間違えたという問題、さらに、回答資料を作成するときにも、その資料について正確ではない記載をしてしまった。今お話あったような、適用範囲とか用語の意味の問題のところですが、そういったことがあったと、そういうふうに認識しています。

今回、第4回目ですが、会合につきましては、事前に回答についてしっかりと確認作業を行ってきましたので、よろしくお願いしたいと思っています。

また、他の規格でも、私ども、技術評価していただいたと、そういうふうに思っておりますが、今後の対応について、今回のような同じようなことが生じないよう、しっかりと技術評価の作業を円滑に進めるように御協力できますよう、当協会内でしっかりと対策を検討しているところでございまして、次回の、ありますれば規格の技術評価対応時には、この対策を講じていきたいというふうに考えておりますので、よろしく御指導願いたいと、そのように思っております。

それでは、資料につきまして、当協会の遠藤のほうから、これから説明させますので、よろしくお願いします。

○日本電気協会（遠藤主査）　それでは、日本電気協会の遠藤です。

資料のほうの御説明のほうに入らせていただきたいと思います。

資料4-1のほうを御覧ください。

まず、1ページ目と2ページ目のほうは、いただいております説明依頼事項ですので、こちらのほうは割愛させていただきまして、3ページ目から、御質問いただきました内容について、一つずつ御説明させていただきたいと思います。

まず、3ページ目の1ポツ目の1の(1)ですけども、こちらのほうは、安全保護系へのデジタル計算機、JEAC4620の2020年版の適用範囲についての御質問で、4ポツの要求事項の規定ごとの適用範囲を説明してくださいということで、こちらのほうは、別添の資料として、PDFの一番最後のページですね、12ページになりますかね、ちょっと通し番号ないのですけど、一番最後のページに整理させていただきましたので、ここは前回の会合でも、ちょっと問題になった部分だと思いますので、説明させていただきたいと思います。

まず、上のほうに用語の意味ということで、デジタル安全保護系、デジタル計算機、それから安全保護系としての機能を実現するソフトウェアの意味を整理させていただいています。

まず、デジタル安全保護系というところは、安全保護系の機能をデジタル計算機のアプリケーションのソフトウェアで実現している場合に、検出器から動作装置入力端子までを含めて、これをデジタル安全保護系としています。

こちらは、下の左側のほうの図を見ていただくと、ここの黄色い範囲ですね、検出器から右側のスクラムパイロット弁と書いてあるところの端子のところまで、こちらがデジタル安全保護系という形になります。

次に、デジタル計算機のほうは、安全保護系としての機能を実現するソフトウェアが実装された計算機、デジタル計算機を指しておりまして、その下の図の真ん中辺ですね、一点鎖線のところの紫色のハッチングを指してございます。

それから、あと、安全保護系としての機能を実現するソフトウェアというところは、今原子炉停止系及び工学的安全施設作動系の演算・論理回路を実装したアプリケーション、ソフトウェアを指していまして、本規程のソフトウェアの要件は、この部分を指しますということで、その下の図の青い作業論理と書いてある四角の中、こちらのソフトウェアのことを指してございます。これは各用語の意味と示す範囲になっていまして、御質問にありました4章の要求事項に対する対応としましては、この右側に項目ごとにまとめさせていただいています。デジタル安全保護系全般への要求としまして、黄色の四角で囲わせていただいたもの、こちらは4.1から4.15までありますけども、こちらは、おおむね黄色いところに該当するデジタル安全保護系全般への要求で。

それから、右側のほうに行きまして、デジタル計算機への要求ということで、紫色の四角で囲わせていただいたところで、4.16、4.18、それに加えて、ソフトウェアの要求。あと青いところ。ソフトウェアの要求は4.17、4.19。こういった整理になってございます。それぞれの言葉の意味と要求事項の対象は、こういった形になっております。

あと、一番下に、一部デジタルの場合とアナログの場合との比較ということで記載させていただいていまして、一番左側にJEAC4620の要求事項、安全保護系への要求と計算機への要求とソフトウェアへの要求という形で整理した場合に、2列目が全てがデジタル安全保護系で、3列目が一部デジタル安全保護系の場合ですけども、この場合は、こういった演算・論理回路をソフトウェアで実装した安全保護機能の検出器から動作装置入力端子ま

でがデジタル安全保護系全般への要求が適用になると。デジタル計算機への要求が適用になるのは、同じように演算・論理回路をソフトウェアで実装した部分のデジタル計算機のみ対象になります。それから、ソフトウェアも演算・論理回路を実装したソフトウェアのみが対象になるという形になりまして、アナログの場合は全て対象外という形になってございます。これが4項の要求事項に対する適用範囲の考え方になります。

以上が1の(1)に対する御説明になります。

次に、(2)のほう、4ページのほうを御覧ください。こちらの御質問は、ソフトウェアの管理に関連する4.17、4.18、4.19について適用範囲の詳細を説明してくださいということで、回答のほうは、下の回答(2)のほうに記載させていただいてございます。

まず、4.17、ソフトウェアの管理外の変更の防止については、こちらのほうは、先ほどの作動論理に用いられるデジタル計算機の安全保護系としての機能を実現するソフトウェアを対象にしています。こちらはソフトウェアの管理ですので、ソフトウェアを対象にしています。

次に、4.18、不正アクセス行為等の被害の防止については、こちらのほうは、デジタル計算機のほうを対象にしてございます。

次に、4.19、品質保証のほうは、こちらはアプリケーションソフトですね、安全保護系としての機能を実現するソフトウェアを対象にしてございまして、ここの理由は、アプリケーションソフトはやはり、設備ごと、プラントごとに固有の設計として確実に作り込む、そういう必要がありますので、ソフトウェアとしてきめ細かく管理するというところがデジタル安全保護系の安全性及び信頼性確保の観点から重要というところで、こういった制定にしてございます。適用範囲の考え方は、2008年版から特に変更はなくて、2020年版でも同じ考え方を一般の原子力品質保証を前提として4620の要求事項を適用するという形になっております。

なお書きですけども、デジタル計算機に用いるハードウェア、それから計算機の基本動作を制御するソフトウェアについては、開発段階で一般の原子力品質保証をきちんと適用して開発、設計プロセス、設計検証、妥当性確認を実施するということにしています。当然、安全保護系としての機能を実現するソフトウェアとこういったものを組み合わせるということが必要になりますので、具体的にデジタル計算機を設計、製作する際には、アプリケーションソフトの品質保証を確実に実施するというところでハードウェアや基本ソフトを組み合わせた仕様を設定しまして、製作して実装すると。これに対する品質保証、ラ

イフサイクルの構成管理、V&Vというところはきちんと組み合わせて実施するということにしてございます。ここはJEAG4609の図にも記載されている部分です。

また、核計装や放射線モニタ、それから温度計装、そういったところの安全保護系の中でデジタル技術を適用している装置は、基本的に一般の原子力品質保証に基づいて設計、製作を行うと。それから、設計、保守用のソフトウェアツールについても、同様に要求されるレベルに応じて原子力品質保証の基で作業環境やツールとして管理をしているといった形になってございます。

最後に、JEAC4620では、原子炉停止系、工学的安全施設作動系の作動論理へのデジタル計算機の適用を基本的に念頭に要求事項を整備してきていますけれども、安全保護系におけるそのほかのデジタル制御装置、それ以外のところにデジタル制御装置を適用した場合の要求事項は、不要というふうに判断しているわけではありませんので、ちょっと今後の課題として整理をして検討していきたいというふうに考えている部分でございます。

引き続きまして、6ページ目のほうに核計装、放射線計装に関する部分について御説明いたします。

まず、(1)のところですけれども、核計装・放射線計装の演算・論理回路をデジタル計算機の対象としていない理由を説明してくださいという部分です。ちょっと長く書いてありますので、少し端折って御説明しますが、回答(1)のほうで、まず、今回のデジタル安全保護系に関する規格というのは、やっぱりソフトウェアの品質確保を目的にV&Vのガイドラインを作るということで、1989年にJEAG4609、ここを制定したところから始まっております。この際に、デジタル計算機の適用については、安全保護系として機能を実現するソフトウェアが実装されたデジタル計算機、ここを対象にしていまして、先ほどから御説明していますアプリケーションソフトウェアとして実装している、ここも計算機を対象としています。V&Vの対象範囲に原子炉停止系及び工学的安全施設作動系の演算・論理回路を実装したアプリケーションソフト。これは、以前もアナログの安全保護系を考えたときに、リレー回路を中心としたハードウェア、そこの論理回路をソフトウェアできちんと品質を確保して実現していく。そういったところに焦点を絞って検討したことが理由なのです。あとは、ここの部分の回路というのは、多重化された装置の論理演算結果を出力したものでありまして、最終的に設備の動作に直結する回路は、そういう意味でも最も重要な部分です。そういったところも関係しています。

あと、核計装、放射線モニタというところでは、1989年当時に核計装、BWR（沸騰水型

炉）プラントでは、既にデジタル制御技術を適用した装置がありまして、ソフトウェアも含めて、先ほどの原子力品質保証の仕組みの中で、十分な検証を実施した上で導入されていまして、問題なく稼働していたというところで、こういったところには含めておりませんでした。逆に、その経験を踏まえて安全保護系の対応方法を検討しているという形でございます。

あと、核計装、放射線モニタのほうは、設定値比較機能をデジタル制御回路で実現しているものがありますけども、判定結果は接点入力で安全保護系のほうに入力するという形になっておりますので、こういった回路は、設定値比較機能がアナログのものではありますけども、ほかにCV急閉の圧力スイッチのもの等ありますので、こういったものは検出器として扱っていまして、同じように核計装、放射線モニタも検出器として扱っているといった形です。こういった点から、JEAC4620では核計装、放射線モニタをデジタル計算機の対象とはしていないというところです。ただ、BWRプラントでは、かなり複数のプラントで核計装、放射線モニタ入ってきていますので、その扱いについては、今後やはり検討すべき課題かなというふうに考えております。

次に、8ページ目、(2)番になります。4.18、不正アクセス行為等の被害の防止は、核計装・放射線計装は適用範囲外、先ほどの別添でも御説明させていただいたのですけども、技術基準規則では、核計装・放射線計装にも適用される要求事項ですというところで、適用対象外とした理由を説明してください。回答(2)のところで、ちょっとここ、先ほどと繰り返しになりますけども、JEAC4620は、原子炉停止系、それから工学的安全施設作動系の作動論理へのデジタル計算機の適用を念頭に要求事項を整備してきた、回答の2の(1)で御説明させていただいたとおりです。そういったところで、JEAC4620としては、核計装・放射線計装については、デジタル計算機への適用事項である4.18のほうは適用対象としてはいません。ただ、これは、そういったもともとの作ったときの経緯がありまして対象とはしていないのですけども、核計装・放射線モニタについて技術基準規則35条を要求しなくていいということではありませんので、そういう意味で記載していることではありません。核計装・放射線計装に限らず安全保護系全体にデジタル装置を適用する場合の要求事項については、この4.18に限らず再整備が必要と考えておりまして、今後考えていきたいというところでございます。

引き続きまして、9ページ目、(3)のほうになります。こちらは、4.16、4.17、4.18、4.19、核計装・放射線計装は適用範囲外ということですが、これらの規定を核計装・放射

線計装に用いることができるか説明してくださいというところで、回答(3)のほうに記載させていただいています。このデジタル安全保護系については、ちょっと繰り返しになりますけど、JEAC4111を中心とした品質保証活動が実施されまして、核計装、放射線モニタについても同様です。一方で、安全保護系としての機能を実現するソフトウェアについては、原子力品質保証活動を前提にして、さらにきめの細かい管理を行うということでV&Vを実施するということにしてございます。デジタル制御装置を適用した核計装、放射線モニタのソフトウェアは、安全保護系としての機能を実現するソフトウェアではありませんので、V&Vの対象とはしておりませんけども、同じように原子力品質保証活動を前提にしてV&Vを実施することで、信頼性を高くするということはできます。ですので、核計装、放射線モニタにこういった項目を適用するということ自体は問題ないというふうに考えてございます。

「また」からですけども、JEAC4620ではデジタル装置を適用した核計装、放射線モニタをデジタル計算機ではなく検出器として扱っていますので、4.16、4.18の適用対象としませんけども、ここも同じように、より信頼性の高い設備を構築するということで、ここに適用することは問題ないというふうに考えております。

引き続きまして、10ページ目です。3番のその他の部分ですけども、ここからは機能的分離を中心に御質問いただいていますが、(1)の計測制御系との分離における通信の定義と機能的分離が適用される範囲というところで、回答(1)に記載させていただいています。通信とは、複数の情報を伝送する手段を指していまして、一般的に言えばネットワーク伝送とかデータリンクになります。機能的に分離するというところは、ハードワイヤード回路を含む全ての安全保護系に適用されますので、JEAC4620の4.5項、4.6項においても、機能的に分離する手段として電気的分離、物理的分離を要求しているという形でございます。これらはチャネル間、計測制御系との間で分離すべき機能が異なる装置で構成されている場合には、装置間で電気的分離、物理的分離を行うことが影響波及を防止するということが必要であるということを示しています。その上で、複数の情報を伝送する手段である通信については、特に注意すべき事項として異区分とか計測制御系からの悪影響を防止するために機能的分離を要求すると、解説にその手段の例示をさせていただいているというものになります。

引き続きまして、最後、11ページです。(2)番のほう、機能的分離には、安全系と非安全系の信号の優先処理部が含まれるのか否かというところと、この処理がFPGA（Field

Programmable Gate Array）で実装される場合に適用範囲となるか否かというところの御質問です。回答(2)のほうに記載させていただいていますが、デジタル安全保護系で優先処理部を使用する場合には、ここはもうソフトウェアで実現するか、ハードウェアで実現するか関係なく、どちらの場合でも安全保護系の一部に位置づけられて、JEAC4620の適用範囲になります。機能的分離としては、安全保護系の動作が優先するほか、最終的に安全機能を阻害しないということが条件になりますし、考慮して設計をするという形でございます。

なお、優先処理部にFPGAのようなプログラマブルなハードウェア素子を適用した場合は、ハードウェアの開発・設計として原子力品質保証活動の中で設計検証、そういったところをやっていきますので、アプリケーションソフトウェアとしては扱っていないというところです。

また、原子炉停止系、工学的安全施設作動系の演算・論理回路の安全保護系としての機能を実現するソフトウェアに相当する機能にFPGAを適用した場合、その品質向上のためにJEAC4620のデジタル計算機への要求を準用するということが考えられますが、現行のものではFPGAを適用した計算機の適用範囲としては、あまり考慮していません。あまり想定はしていませんので、その扱いについてはやはり、今後の検討課題かなというふうに考えてございます。

すみません。ちょっと長くなりましたが、御説明は以上になります。

○田中委員　ありがとうございました。

それでは、ただいまの説明に対して、規制庁のほうから質問、確認等、お願いいたします。

○佐々木企画調整官　原子力規制庁、佐々木です。

御説明ありがとうございました。

資料の一番最後についている別添について、ちょっと確認させていただきたいと思います。質問と感想みたいなことなのかも分からないのですけれども、こちらで整理していただいたので、この規格の規定ごとの適用範囲も多分理解できたというふうに思います。ただ、規格に書いてある定義ですとか要求事項と合っていないとは今でも思っていまして、解説に書いてあることとか、解説の図に書いてあることとかが正になっているということについては、ちょっと規格としては納得していないのですけど、御説明の内容は多分理解できたというふうに思っています。

そうすると、この左のほうの図がありますけれども、これを見ると、デジタル計算機がデジタル化されていた場合、この紫のところの中がデジタル化されていた場合に、デジタル安全保護系となって、この規格が適用になるというふうに理解したのですけど。だとすると、赤で書いてあります核計装、放射線モニタというところがデジタル化されていて、紫のデジタル計算機の中がデジタル化されていなかったら、アナログの安全保護系ということになるのではないかと思うのですけど、そういう理解で正しいですか。実際にそういうプラントはあると思うのですけれども。

○日本電気協会（遠藤主査）　日本電気協会の遠藤でございます。

おっしゃるとおりで、この計算式のところがアナログであれば、全体としてはアナログの安全保護系という形になってございます。

○佐々木企画調整官　そうすると、アナログ安全保護系の規定というのはないですけど、JEAC4604という、前もちょっと議論に出ましたけど、原子力発電所安全保護系の設計規定というのがあって、これはアナログ時代から作られているものだと思うので、こちらが適用図書になるのかなという気がちょっとしますけれども。この中には、デジタル機器はどうしなさいみたいなことは書いていないということになるので、アナログ安全保護系のデジタル化された部分はどうなるのかなという疑問は依然あって。つまり、デジタル安全保護系のアナログ部分については要求事項があるけれど、アナログ安全保護系のデジタルの部分については、どこの規定からもちょっと漏れてちゃっているということになるのかなと思ったので、ちょっとそういうところを含めて、今後検討いただけるということなので、今どうこうしてくださいというつもりはありませんけれども、ちょっとそういうふうに思いましたということをお伝えしたいと思います。

もう一つは、技術評価を我々はしているわけですけども、技術評価は、民間規格の活用についてという委員会文書がございますけれども、効率的な審査に資するということで技術評価を行うとしていますので、できるだけ審査の効率化に資するようになるというのが望ましいのだと私自身は理解していまして。そうすると、今この規格で規定している範囲はちょっと難しいですし、入っていない部分もあって、今申し上げたようなデジタルが入っているアナログ安全保護系の場合は、この規格の適用範囲ではないから別途審査してくださいみたいなことに多分なるということになると思うのですけども、ちょっとそういうことを意図して作られているわけではないと思いますし、皆さんにしても審査の効率化というのは規格を作る上での一つの意味だと思っていますので、そういうことを踏まえて今

後検討されて、効率的な審査に資するような規格になっていくことがいいのではないかなと個人的に思ったので、これは感想ですけれども、お伝えさせていただきたいと思います。

以上です。

○日本電気協会（遠藤主査）　日本電気協会の遠藤です。

御意見ありがとうございました。いただいた御意見を踏まえて、今後もう少し分かりやすい審査に役に立つ規定になるようにしていきたいと思いますので、引き続きよろしくお願いいたします。

以上です。

○田中委員　あと、ありますか。

○今瀬専門職　原子力規制庁、今瀬でございます。

一点だけ、確認なのですけど。回答書でいただいた4ページ目、ソフトウェア管理に関連する4.17から4.19について適用範囲の詳細を説明してくださいということで、16行目以降で、ハードウェアとか基本動作を制御するソフトウェア、OSのことだと思うのですけども、に関する記載があるのですが、その文面の最後で、基本ソフトが適切に組み合わされることを確認していますという表現があるのですけど、これは現行のJEAC/JEAGで対処されているというふうに読めばいいのでしょうか。明示的な記載はないと思うのですけど、常識的にこう解釈するのだという意図なのか、そこを確認させていただきたいのですけども。

○日本電気協会（遠藤主査）　日本電気協会の遠藤でございます。

明示的にというか、フローの中でやはり、アプリケーションソフトだけの検証ってできませんので、当然ハードウェア、それから基本ソフトウェアを組み合わせてちゃんと実現しますということを、この中で一応書いているつもりです。ですので、今、今瀬さんがおっしゃっていただいたとおりの理解で特に問題ありません。

以上です。

○今瀬専門職　分かりました。質問の意図は、V&Vは確かに実施されているのですけど、構成管理ですとかライフサイクル管理については、アプリケーションソフトだけが対象だという説明があったものですから、私の理解としては、そのアプリケーションソフトを管理する上では、それに影響を与え得るOSとかハードウェアというのは、現行のJEAC、JEAGの解釈の基でも対象になると、そういう理解でいいのでしょうかという質問だったのですけど、そういう理解でいいのでしょうか。

○日本電気協会（遠藤主査）　日本電気協会の遠藤でございます。

すみません、ちょっと言葉足らずで。その理解で結構です。

以上です。

○今瀬専門職　分かりました。問題ないと思います。どうもありがとうございました。

○田中委員　あと、ありますか。

○藤澤技術参与　原子力規制庁の藤澤です。

回答ありがとうございました。

資料8ページの(2)のことに関連しての質問です。この(2)では、4.18の不正アクセス行為等の被害の防止については、これは核計装・放射線計装は適用範囲外とのことですが、技術基準規則では適用とされる、要求事項ですよというふうにも書いていまして、それに対して、回答は、それを肯定している形で書かれております。つまり、適用対象としていないということなのですけども、JEAC4620-2020の最初から2枚目のところの原子力規格委員会安全設計分科会の分科会長が書かれた「安全保護系へのデジタル計算機の適用に関する規定について」という文言がございますけども。これを読みますと、まず、安全保護系は、設計に関する要求事項というのが我々原子力規制庁のオーダーしている技術基準規則とか、そういうふうなものに示されておりますということが書かれております。それに対して、下のほうに、2011年に発行された原子力安全・保安院と（独）原子力安全基盤機構によるJEAC4620-2008、JEAG4609-2008に対する技術評価書及び2013年に施行された新規制基準を踏まえて、デジタル安全保護系に関する最新の規制要求事項を確認するとともに、国際規格を最新の国内外における関連規格ですね、こういうふうなものと、それから運転経験、トラブル情報とかの知見を調査して、その結果を踏まえて本規定を改定することといたしましたというふうに書かれております。こう書かれますと、この4620-2020というのは、技術基準規則に適合していますよというふうに書いてあるように、実は思えるのですけども、先ほどの資料のほうにあった回答は、これは適用範囲外というふうに書かれております。この矛盾について、どういうふうに理解すればいいのか、説明をお願いします。

○日本電気協会（遠藤主査）　日本電気協会の遠藤でございます。

解釈の違いかなと思いますけども、このJEAC4620では、御説明させていただいたとおり、原子炉停止系、工学的安全施設作動設備の作動論理のところをデジタル計算機というふうに設定をしてございまして、それはやはり、経緯があってそういったところを中心に、この規格としては記載させていただいた。そこのデジタル計算機に対して不正アクセス等の

防止を定義しますと、今回のような記載なので、4620としては、デジタル計算機に対して4.18を適用対象としていまして、核計装、放射線モニタは、デジタル計算機としては扱っていませんので、ここは適用対象外。4620としては、この4.18項を適用していませんという形なのですけども、ただ、規制要件としては、当然、技術基準規則に35条という形で記載されていることは認識していますので、そこを満足するように、技術者としてはきちんと設計をしてございますし、そこは認識しているつもりでございます。

先ほどの冒頭の記載については、技術基準規則をきちんと確認しまして、この4620としては原子炉停止系と工学的安全施設作動設備もデジタル計算機ということで要求事項をまとめてございますので、そこの部分はきちんと反映したと。核計装、放射線モニタまでというところについてはやはり、ちょっと今後の課題かなと考えて、規格には反映していないというところでございまして、特に無視したりとか、そういうことではございません。

以上です。

○藤澤技術参与　藤澤です。

回答ありがとうございました。安全設計分科会の分科会長が書かれている内容は、くどいですけども、技術基準規則には適合していますよというふうな文章だと私は理解しているのですけども、今の遠藤さんの発言の内容は、そうはいっても一部は違うのですよというふうなことなので、ちょっとそういう意味でも、規定の上位の審議機関、規格委員会とか、それから安全設計分科会の審議レベルと、それから計測制御検討会の審議のときに、何か少し差があるのではないかなと、私は理解についての差があると思います。そういうところをぜひ今後、皆さんでもって見直していただければと思います。

以上です。この件についての回答は要りません。

○田中委員　あと、ございますか。

○今瀬専門職　原子力規制庁、今瀬でございます。

回答書の11ページ、(2)機能的分離で、優先処理回路にFPGAが使われる場合というケースについて質問させていただいた部分なのですけど、回答の7ページ目以降、なお、優先回路にFPGAのようなプログラマブルなハードウェア素子を適用した場合にはというところで、ハードウェアの開発・設計として原子力品質保証活動の中で設計検証などの適切な対応を取るということで記載されておりますけども、ここでいうハードウェアの開発・設計としてという言葉の意味なのですけど、データの部分とハードウェアという意味ではなくて、自分の解釈としては、こういった優先回路にFPGAを使う場合はハードウェアとみなし

て、その全パス試験をやるとか、いわゆるV&Vよりは少し高い基準の品質維持を狙ったハードウェアとしての検証をやるというふうにこの文章を読んだのですが、そういう理解でよろしいでしょうか。

すみません、ちょっと質問の趣旨が伝わらなかったかもしれません。FPGAをこういった優先回路に使うときには、FPGAプラスソフトウェアのV&V手法を準用してというやり方もあれば、米国で言えばBTP7-19の最新版では、全パス試験という表現が適切かどうか分からないですけど、all executable logic pathのような表現が取られていて、自分はそれを全パス試験と言っているのですけど、これをやればCCF（共通原因故障）のリスクを排除できるようなV&V以外にそういった手法もあって、海外では認められているというふうに理解しているんですけど。それで、ここの文章を読んだときに、ハードウェアの開発設計として原子力品質保証活動の中でということで、ハードウェア全体、FPGAの回路全体をハードウェアとみなして、そういった全パス試験みたいなことをやるというふうに読めれば非常にいいのかなと思ったんですけど、ここで書かれた意図がそれでいいのか確認させていただければと思います。

○日本電気協会（遠藤主査）　日本電気協会の遠藤でございます。

御質問の趣旨は理解いたしました。ここでは、すみません、ちょっと言葉もちょっと意味の取り方によっちゃうんですけど、ハードウェアの開発設計というふうに記載させていただいたんですけども、そのほかのところにソフトウェアと記載させていただいているんですが、要はFPGAを使うなら、FPGAに合った検証、妥当性確認をすると。

今まで、ソフトウェアって基本的に安全保護系としての機能を実現するソフトウェアを意識していますので、それ以外のものはちょっとハードウェアみたいなちょっと書き方をしてございますが、ここで言うところは、FPGAを検証するのに一番いいやり方を採用しますという意味で書かせていただいていまして、それがV&Vより上か下かとか、そういったところはあまり関係なくて、やっぱりきちっと設計をする、検証、妥当性確認をするというところは、当然間違いなく信頼性高いものをつくるというところは変わりませんので、そういう意味でFPGAに対して必要な品質保証を確保するような設計検証、妥当性確認をしていきますといったところの意味になります。

○田中委員　よろしいですか。

○今瀬専門職　原子力規制庁、今瀬でございます。

回答の内容は分かりました。後ほど私どもの評価書の説明があると思いますけど、2020

年版の、JEACのほうのそういったところを保安活動の重要度に応じて当該処理部に装荷するソフトウェアの品質を確保することが重要とか、V&V以外の手法も許容するような形で、先ほど自分のほうが説明したような意図を酌んだ形で、今、評価書は書いているのですけど、そこの部分をよく読んで、もし御意見があればお願いしたいと思います。先走ってしまって、すみません。

○日本電気協会（遠藤主査）　日本電気協会の遠藤でございます。

ありがとうございます。基本的に、でも記載いただいた趣旨と私どもの活動とそんなに違ったところはないというふうに認識してございます。

以上です。

○今瀬専門職　はい、分かりました。

○田中委員　あと、ありますか。いいですか。

それでは、次に、技術評価書（案）について、資料4-2に基づきまして、佐々木企画調整官から説明をお願いいたします。

○佐々木企画調整官　原子力規制庁、佐々木です。

それでは、資料4-2に基づいて御説明させてください。こちらは技術評価の検討チームを行い、また面談で資料を頂いたりとかして、私どものほうで技術評価をこういうふうにしたらどうかという案を御提示するものになっています。

それで、皆さん、日本電気協会で今見ていただいてますけれども、今日配付されたものになっていると思いますので、詳しく読むのにお時間がかかると思いますけれど、今回、特に今日説明いただいたところに関係するところで御説明して、もし御意見、御質問がある前に、聞いておいたほうがいいかなと思うところを中心に説明させていただきたいと思います。

めくっていただきまして、次のページから目次になっておりまして、1、2、3のところは技術評価をどういうふうにやったかという説明になっておりまして、4のところから技術評価の内容ということで、具体的な評価の内容を記載してございます。

たくさん書いてあるんですけども、ちょっと大事なところだけ説明することにさせていただいて、5、6、7のところには、このような条件をつけて使わせていただくことにしたいと思いますというようなことになっていまして、6、7で要望事項ということがまとめてございます。

同じ資料の、まず12ページのところを開いていただければと思います。12ページの上か

ら2行目のところに①ということで、安全保護系の定義と適用範囲ということで、今日御説明いただいた内容を中心に記載してございます。

まず最初に、四角で囲ってありますが、3.2安全保護系ということで、ここに記載されている内容は、JEACの定義が転記してございます。この内容については、特段、違和感はございませんで、これをベースに、この同じページの真ん中辺りにありますが、かぎ括弧としてディジタル安全保護系、ディジタル計算機の範囲について説明をいただいたところになります。

その辺の説明が、次の13ページのところにも書いてありまして、この絵でこういう形になっていますということを説明いただいています。

13ページの丸二つありますけど、その下のところに安全保護系に属するデジタル化された核計装や放射線計装などの装置に関する論理・演算部は、ディジタル計算機に入りますかということについては、入りませんという説明を受けたところでございます。

その下に、またということで、ディジタル計算機の対象としていない理由は何ですかということで、これは今日説明していただいたことは記載されています。

めくっていただきまして、14ページの下から4行目のところからは、規定ごとの適用範囲について詳しく説明してくださいということに対して、15ページの図がありますけれども、このような形で説明いただいたということになります。

その図の下の2個目の段落のところですけれども、ソフトウェアに関連する規定の適用範囲をさらに詳細に説明してくださいというふうなお願いをしたところ、その下の丸と書いてありますけれども、そこのところにそれぞれの要求事項が書いてありまして、上の図を詳しく説明していただいたというふうに理解しています。

めくっていただきまして、16ページに先ほど質問も出ましたけれど、真ん中辺りにまたということで、不正アクセス行為等の被害の防止について、どうして核計装、放射線計装は入ってないんですかということについての説明いただいた内容が記載してございます。

さらに、17ページのところに行って、四角で図がありますけど、その下の二つ目の段落のところになりますが、仮に適用になっていない規定について、核計装、放射線計装に適用した場合は適用できるのですかという質問も、今日お答えいただいていて、問題ないと考えますということをいただいています。

18ページ、次のページめくっていただきまして、そういう説明を、一連の説明を受けた結果、私どもとしては、下から2個目の段落になりますが、「したがって」というところに

まとめて書いておりまして、今後は、デジタル安全保護系規程の2020年版も2008年版も適用範囲については、日本電気協会の説明によらず、核計装、放射線計装を含む検出器側のデジタル化された演算・処理部についても含むこととして、それに対応する読み替えをしたいと思っていまして、規程上、ディジタル計算機と書いてある部分は、これは原子炉停止系及び工学的安全施設作動系の演算・論理回路ということになりますので、ここの部分をデジタル安全保護系のデジタル化された演算・論理処理部というふうに読み替えて、核計装、放射線計装も含む安全保護系全体ということにしてはどうかというふうに考えています。

ここで、ちょっと一つ、皆さんに確認していただきたいと思っていることがありまして、今まで御説明いただいた内容は、核計装、放射線計装が入っていても適用して問題ないということは確認していたんですが、それ以外に、意図せず入ってしまう、ちょっと分からないですけど、例えば圧力とか温度とかですかね、にデジタル化された部分があって、それに適用すると安全上問題があるとか、成立しないとかいうところの詳細までは、ちょっと私どもでは完全には理解できないところもありますので、そういう点で問題があるかどうかということは、日本電気協会の専門の皆さんにも御確認いただいたほうがいいかなというふうに思っています。それが一点目になります。それについては、ちょっと後ほど補足してもらおうと思いますので、そこで議論していただければと思います。

それから、もう一つが、19ページの真ん中辺りに(a)としてソフトウェアの範囲というふうに書いてあります。その下のところには、まず規程の中には「ソフトウェア」という定義はないんですけれども、解説-3のところに、本規程におけるソフトウェアとは、特にことわりのない場合、安全保護系としての機能を実現するソフトウェアを示すということで、ソフトウェアと言っているものの範囲は限定された、いわゆる原子炉停止系、工学的安全施設作動系の演算・論理回路を実装したアプリケーションのソフトウェアということで、ちょっとこれをアプリケーションソフトと呼びますけど、アプリケーションソフトに対する要求事項ですという御説明がありました。

これにつきましても、ちょっと品質保証に関係する記載内容になりますので、ちょっと品質保証は別のところにまとめて書いているので少し飛びますけれども、後ろのほうに行っていただきまして、58ページを見ていただければと思います。

この58ページのところに、4.1.9ということで検証及び妥当性確認（V&V）と品質保証ということで、ここにまとめて書いてありますけれども。ちょっと今日議論したところと関

係ないところもありますので、少し飛ばせていただいて、65ページを見ていただければと思います。

この65ページのところに四角で囲った部分がありますけども、ここは日本電気協会の規格から転記してきているものでして、この4.19の品質保証のところは、具体的にはディジタル安全保護系に用いられるディジタル計算機は、以下の手法によりソフトウェアの健全性を確保することとして、1個目のポチとして、ソフトウェアライフサイクル及び構成管理手法を含めた品質保証活動、2個目のポチとしてV&V活動というふうに書いてございます。これは先ほどからの日本電気協会の説明からすると、アプリケーションソフトウェアについての要求事項ということになっていて、このポチ二つの方法を使って健全性を確保するというふうに書いてあるというふうに理解しています。

その下にある（a）ソフトウェアの品質保証というところで、その内容が書いてありまして、そこの段落の4行目ぐらいからですけど、アプリケーションソフトウェアの品質保証について規定していて、それ以外については規定していないのはなぜですかということに対する御回答をいただいています。

同じページの一番最後の段落ですけれども、ここから私どもがどう思っているかということが書いてございますけれども、まず、保安活動については、品質保証は我々の観点からすると保安活動ということになりますけれども、別の規則がありまして、原子力施設の保安のための業務に係る品質管理に必要な体制の基準に関する規則というのがありまして、ここには原子力事業者等は、保安活動の重要度に応じて、品質マネジメントシステムを確立し、運用しなければならないということで規定しています。この保安活動の重要度に応じてというのは、いわゆるグレーデッドアプローチを適用してという意味になってまして、そのときに考慮すべき事項については、この第4条のところに書いてあるんですけれども、ちょっとここには書きませんでしたけども、そういうふうに要求されていまして、したがって、今の規格のようにアプリケーションソフトウェアであるのかないのかのところで境目をつくって、品質保証のこのグレーデッドをするのは、ちょっと私どもとしては違和感があるというところです。

それから、もう一つは、次のページの66ページの2個目の段落ですか、「また」というところにありますけれども、さっき言いましたように、ソフトウェアの健全性を確保する手法として二つの方法が列記されているんですけど、品質保証は今いろいろな手法でやるものになりまして、もともとこの日本電気協会の規程にも含めた品質保証活動と書いてあり

ますけども、ちょっと限定しているようにも見えますので、特に限定する必要があるわけでありませんので、必要な品質保証活動をしてもらえればいいというふうに思っています。

また、4.17のソフトウェアの管理外の変更の防止というのについては、アプリケーションソフトウェアは変更管理をするけれど、それ以外はちょっと違うグレードの管理をしますみたいなふうに読めるわけですけれども、ソフトウェアの変更管理というのは安全保護系だったら全部されるべきものじゃないかと思いますので、そういうことが書いてございます。

それで、その下の「したがって」というところになりますけれども、品質保証については、デジタル安全保護系を構成する全てのソフトウェアを対象に保安活動の重要度に応じて実施してほしいと思いますので、以下の手法によりソフトウェアの健全性を確保することと書いてあるのは、保安活動の重要度に応じ、以下に掲げる事項その他の適切な手法によりソフトウェアの健全性を確保することというふうに読み替えて使うようにしたいというふうに思っています。

それから、その下に「また」とありますけども、ソフトウェアの管理外の変更の防止については、今はアプリケーションソフトは管理外の変更を防止する設計とすることというふうになってますけれども、ここの部分はデジタル安全保護系のデジタル化された演算・論理処理部に装荷するソフトウェアは、管理外の変更を防止する設計とすることというふうに読み替えてはどうかというふうに思っています。

今、御説明した内容は、もともとJEACの規程を素直に読めば、そういうふうに書いてあるように、特に私なんかは思っていますので、非常に何かを付加したというつもりではないんですけれども、皆さんの説明でも、核計装や放射線計装に適用しても大丈夫だという説明もありましたし、ソフトウェアについても必要な確認はしているということでしたので、それほど認識には大きな違いはないのではないかと思っています。

私の説明は以上ですので、補足をお願いしたいと思います。

○今瀬専門職　原子力規制庁の今瀬でございます。

先ほど説明があった、保安活動の重要度に応じてというふうな表現をとった背景といいますか、関連する事項を補足させていただきたいと思います。

今回表現の記載がディジタル計算機をディジタル安全保護系のデジタル化された演算・論理処理部と解釈を読み替えますので、我々が意図しないところで違う読み方をされる場合もあるのではないかなと、そのときには本当に技術的に成立するのかなといったところ

を心配しております。

一つは、4.15の自己診断に関わるところなのですけども、今回こういった記載変更は、核・放射線計装を含むように読み替えたものということで、それ以上の変更を意図するものではないというふうに理解しているんですけど、今回の解釈の文章の変更で、例えば資料4-1で今回、質問回答をさせていただいた優先処理回路のようなところで、一般的にはCCFのリスクが残らないような品質水準でなければならないと理解していますので、この部分は例えばプログラマブルなものではないディスクリートな論理として構成する場合もあるでしょうし、FPGAを使う場合には、いわゆるCCFのリスクが残るようなV&Vではなくて、全パス試験による検証をやると、別の手法を取られるというようなケースがあるのではないのかというふうに考えました。

自己診断に関して言うと、そういった多様性を考慮した設計を優先して、例えばディスクリートな論理回路になったときに、そういったところが今回のJEAC全体の適用範囲になってくると考えたときに、そういった部分が自己診断できるのかなとか、あるいはFPGAを使って自己診断できるにしても、全パス試験のような非常に品質水準の高い検証ができるのかなといったところを心配しております。検討チームとしては、こういった多様性を考慮した自己診断への適正化というのが必要ではないかなというふうに考えているのですが、現状の読み替え案で課題を生じるのかどうかということに関しては、専門的な見地も踏まえて慎重な検討が必要ではないかなと考えています。

文章を解釈した上での懸念事項ですとか、あるいは若干でもその解釈が変わって、適用範囲が広がったときに、技術的な問題が生じないかといった観点から、懸念を感じるようなところ、私どもの案で懸念を感じるようなところがあれば、御意見をいただきたいなというふうに考えております。

もう一点、関連するところでは、先ほどから考え方として佐々木のほうから説明ありましたけど、品質保証の部分について、保安活動の重要度は品質基準規則の4条2項2号または3号で規定されるものというふうに私どもは理解しているんですけども、V&V以外の手法も今回許容するようにしたらいいのではないかと考えた背景は幾つかありまして、代表例を二つ挙げると、先ほどから事例として申し上げている全パス試験なんですけど、CCFのリスクを排除した多様性を考慮した回路にしないといけないという部分で、CCFのリスクを排除するためにハードウェア的な全パス試験をやるという場合は、V&Vに限定している今の表現、ちょっと望ましくないのかなというふうに考えました。

例えば、CCFの残存リスクが許容される部分は、FPGAプラスV&Vでいいんですけども、それが許容されない部分、多様化設備の信号が通るようなところは、FPGAプラス全パス試験で対応する必要があるのではないか。先ほどのちょっと日本電気協会からの答えについて確認させていただいたのは、こういったところで全パス試験による対応が必要であれば、V&Vに限定する表現は望ましくないかなというふうに考えました。

もう一つは、海外では検出器の伝送器のような非常に小規模な回路が対象になると思うのですけど、定性評価と故障影響評価による検証手法というのも認められる例があって、最近の米国の動向で、国内では今すぐに必要はないかもしれないのですけども、伝送器のような検出器に組み込まれるデジタル回路のように、非常に小規模で、なおかつ膨大な適用実績で信頼性を保証することで、CCFの発生頻度も極めて低いことが示すことができる、なおかつ故障影響評価の観点からは、故障時の影響の程度も低いと評価される。こういった場合は、保安活動の重要度は相対的に低くて、必ずしもV&Vに依らない適用実績等による定性評価と故障影響評価でもよいとする考え方があるのではないかなと。

ここら辺りは、海外の最新の動向ですので、日本電気協会においてもよく調査した上で取組を考えていただきたいところなのですけども、今回の評価書としては、海外でこういう動向があるということを踏まえて、V&Vに限定しないような、先ほど説明あったような保安活動の重要度に応じてということで記載することを考えました。

先ほどの回答の趣旨も、先ほど4-1の資料の回答の意図を確認したのも、これとの関連があってなのですけども。今回の私どもの案について、それが適正かどうかは、かなり高度な技術的な評価も必要になるのかなというふうに考えていますので、よく時間を取って読んでいただいた上で、必要な意見があればお願いしたいというふうに考えています。

以上、補足させていただきました。

○田中委員　いいですか、こちら側は。

ということで、この4-2につきまして、現時点において何か質問とか確認したいことありましたらお願いしたいと思いますが、いかがでしょうか。

○日本電気協会（遠藤主査）　日本電気協会の遠藤でございます。

御説明ありがとうございました。要は、JEAC4620自体は、いろいろ御質問回答にも書かせていただいたとおり、安全保護機能を実現する部分のソフトウェアの検証をするためにV&V活動というのを構築して、それはもうやっぱり設計もセットでそういった構築したものをガイドとしてまとめて、それが・・・としていうふうにまとまってきたというもので。

もともとおっしゃっていただいている、重要度に応じた品質保証を強いてやるというところは、もう基本的にやってあるというベースで考えてございまして、その中でさらに安全機能を有するところのソフトウェアにV&Vをというふうに考えてきましたので、求めているところはそんなに変わらないのかなという認識なんですけど、ちょっとここのもともと入口、規格としての入口の書き方が、やっぱりV&V活動をここにやりたいですということで記載させていただいているところに、ちょっと記載として求めているところが若干違いがあるのかなと思いますので、そこはちょっと認識を合わせつつ、全てのものにV&Vをやりなさいみたいな話になると、それはものによってはV&Vがあまり品質保証の役に立たないものも当然ありますので、よくちょっとそこは認識を合わせながら記載をまとめないと、ちょっと変な方向に行くかなというところはちょっとありますので、ちょっと確認させていただいた上で御相談させていただきたいなと思います。

以上です。

○田中委員　はい。あと、ありますか。よろしいですか。現時点では、あとよろしいですか。

分かりました。これはまた後で、また事務局の話ありますけども、評価書（案）について、いつ頃までにちょっと意見をいただきたいということ、後で話があるかと思います。

本日の議題は以上になりますが、全体を通して、ほかに何か御質問、御意見等ございますか。ないようですね。

本日の説明で、論点としていた部分について一通り議論することができたと思いますので、事務局から今後の進め方について説明をお願いいたします。

○遠山課長　原子力規制庁の遠山です。

今日の御説明、それから引き続きの議論、参加ありがとうございます。今日の議論を踏まえ、また、それから今日この資料4-2という技術評価書（案）というのは、本日提示をしたものですので、内容も大部ですから、日本電気協会の皆さんにも、この内容を確認していただいて、コメントなどがありましたら、3週間を目処にいただければというふうに思います。

また、技術評価については、被規制者からの希望を聴取して始めているものでございますので、被規制者からも意見を伺うこととしたいと思います。そのように、今後、手続を進めさせていただきたいと思います。

会議は今回で一旦終わりなのですけれども、もしあれば公開会合等の開催等は、別途検

討させていただきたいと思います。

○田中委員　では、そのように進めていただきたいと思います。

ほか何か全体を通して、何かございますか。日本電気協会、事務局のほうから特にないですか。

ないようですので、それでは、デジタル安全保護系に関する日本電気協会規格の技術評価に関する検討チームを終了いたします。ありがとうございました。