特集論文

米国原子力プラント向けデジタル計装システムの規制対応活動

平畠将士*
稲葉隆太*
那須ひとみ*

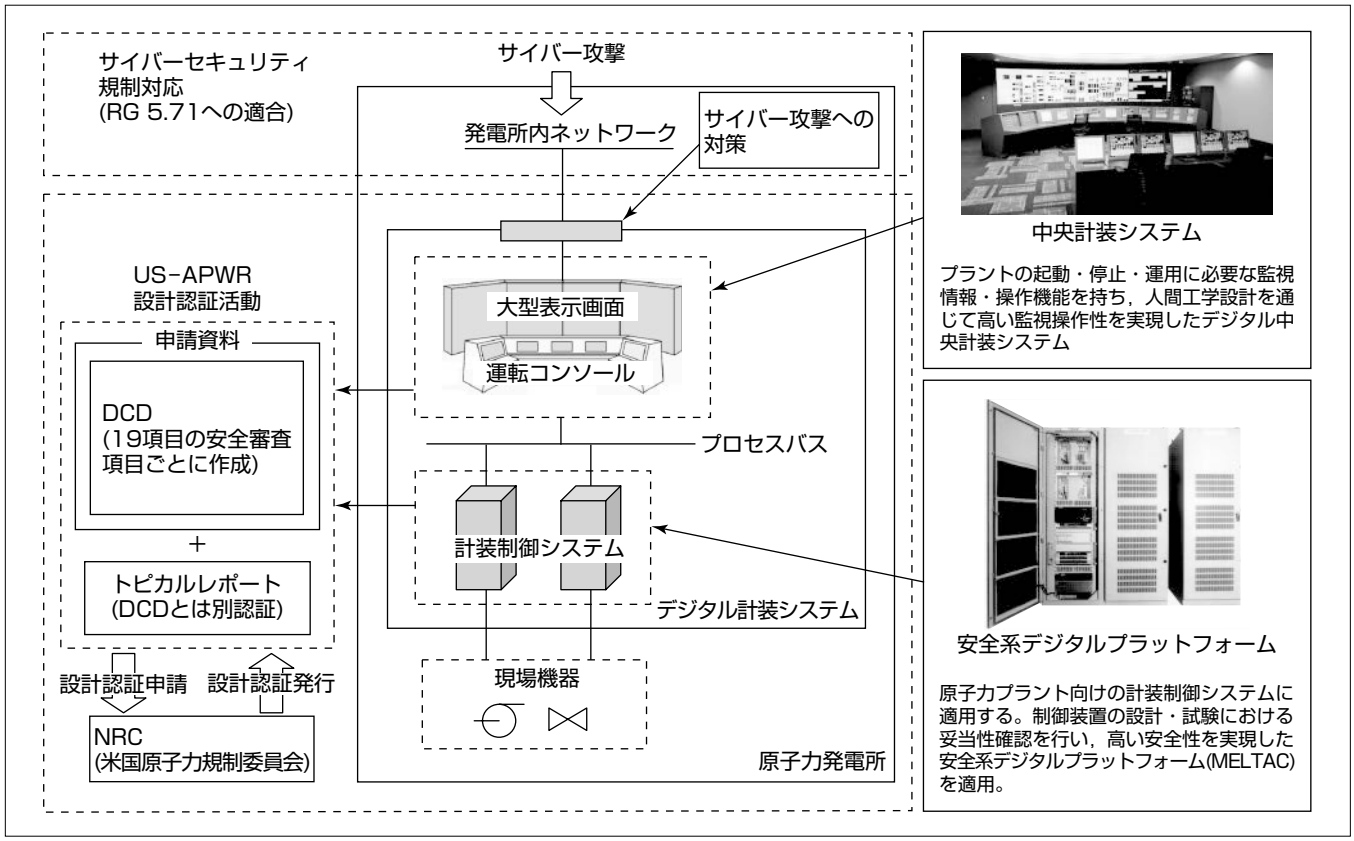
Activities for Complying with Requlations for US−APWR Digital Instrumentation and Control Systems

Masashi Hirahatake, Ryuta Inaba, Hitomi Nasu

要　旨

三菱電機は，三菱重工業㈱とともに，米国市場向け最新型加圧水型軽水炉としてUS-APWRの設計認証活動を推進しており，三菱重工業㈱は，米国標準審査指針で定められる19項の安全審査項目ごとに設計認証の申請資料を米国原子力規制委員会(NRC)へ提出している(1)。当社は，19項の安全審査項目のうち，人間工学設計と計装制御システムの設計認証で必要となる活動に取り組んでいる。三菱重工業㈱と当社は，この活動を通じて，これら2つの安全審査項目に関する米国規制指針への適合性を示し，これらの審査項目に関する申請資料に対してドラフト版安全評価書(Safety Evaluation Report：SER)がNRCから発行された。今後，原子力安全諮問委員会(Advisory Committee on Reactor Safeguards：ACRS)の審査を経て，最終版SERが発行される。

また，サイバーテロの脅威が増加し，サイバーセキュリティ対策の必要性が高まる中，米国では，2010年に原子力発電所のサイバーセキュリティに関する規制指針(RG 5.71)が制定された。このため，三菱重工業㈱と当社は，この規制指針への適合に向けたサイバーセキュリティ対策の開発を進めており，当社では，データダイオードとセキュリティ管理システムの開発を進めている。



当社が関係するUS-APWR 設計認証活動

三菱重工業㈱は，プラント全体(炉型)の設計認証の申請資料として，DCD(Design Control Document)，及びトピカルレポート，テクニカルレポートをNRCに提出している。当社では，19項の安全審査項目のうち，人間工学設計，計装制御システムの設計認証活動に協力しており，申請資料の評価レポートであるSERを受け，当社設備をUS-APWRに適用する計画である。

*電力システム製作所

1. まえがき

当社は，三菱重工業㈱とともに，米国市場向け最新型加圧水型軽水炉（US-APWR）に関して，米国原子力規制委員会（NRC）による設計認証の取得活動を推進している。当社は，この設計認証活動のうち，人間工学設計と計装制御システムに関する設計認証活動に取り組んでいる。

また，米国では，2010年に原子力発電所のサイバーセキュリティに関する規制指針“Regulatory Guide 5.71（RG 5.71）”が制定された。三菱重工業㈱と当社（以下“三菱”という。）は，この規制指針への適合を進めている。

本稿では，人間工学設計，及び計装制御システムについてドラフトSER発行に至るまでの活動と，サイバーセキュリティ規制指針への適合に向けた当社活動について述べる。

2. 設計認証活動とサイバーセキュリティ規制対応

2.1 US-APWRの設計認証活動

米国での原子力プラント建設・運転に向け，三菱重工業㈱は，米国標準審査指針で定められる19項の安全審査項目ごとに設計認証の申請資料をNRCに提出しており[1]，当社は，これらの安全審査項目のうち，人間工学設計と計装制御システムの設計認証に必要な活動に取り組んでいる（**図1**）。

当社は，この活動を通じて，人間工学設計及び計装制御システムの米国規制指針への適合性をNRCへ示し，これら2つの安全審査項目の申請資料に対して，NRCからドラフトSERが発行された。

2.1.1 人間工学設計の設計認証活動

三菱では，人間工学設計の規制ガイドラインである人間工学プログラムのレビュー基準（NUREG-0711），及び中央計装システムの設計ガイドライン（NUREG-0700）への適合性を示すために，三菱の設計プロセス及び米国標準仕様を申請資料に定めている。また，これらの規制ガイドラインへの適合性を示すために，当社の米国拠点（MEPPI：Mitsubishi Electric Power Products，Inc.）に構築した検証設備（**図2**）を用いて，米国運転員による運転検証を実施した[2]。運転検証結果は，米国標準仕様として申請資料に反映しており，NRCによる技術監査の中で，規制ガイドラインへの適合性が確認され，人間工学設計の申請資料に対するドラフトSER発行に至った。

3章で，運転検証以降に実施した米国標準仕様の確立に向けた活動と，NRCによる技術監査の結果を述べる。

2.1.2 計装制御システムの設計認証活動

計装制御システムの設計認証取得のためには，計装制御システムの中でも原子炉の保護機能をつかさどる安全系に適用するプラットフォーム“MELTAC”に関して，米国規制指針への適合性を示す必要がある。当社は，米国原子力安全系向け品質保証プログラム（10CFR50 Appendix B）に準拠した品質保証プログラムを新たに策定し，MELTACの技術要素とともに申請資料としてまとめた[2]。2010年以降は，策定した品質保証プログラムに基づき，MELTACの再評価活動を実施し，NRCによるQA（Quality Assurance）審査，技術監査を経て，米国原子力安全系向け品質保証プログラムへの適合性が確認された。この結果を受け，MELTACを含む計装制御システムの申請資料に対するドラフトSER発行に至った。

図2．中央計装システムの運転検証設備

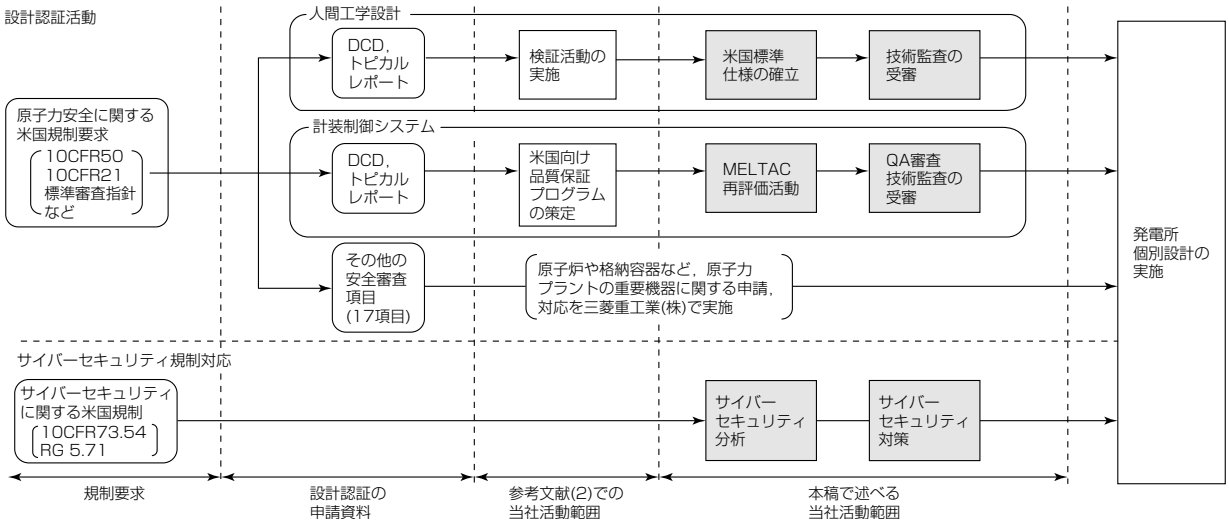


図1．米国規制対応に向けた三菱活動

4章で，策定した品質保証プログラムに基づき実施した米国規制指針に適合するためのMELTAC再評価活動，及びNRCによるQA審査，技術監査の内容を述べる。

2.2　サイバーセキュリティ規制対応

近年，マルウェアや不正アクセス等によるソフトウェア改ざん，データ傍受，現場設備の不正制御等，監視制御システムに対するサイバーテロの脅威が増加しており，社会や米国電力会社を含む事業者に被害を与えている。サイバーセキュリティ対策の必要性が高まる中，米国では2010年に原子力発電所のサイバーセキュリティに関する規制指針（RG 5.71）が制定された。当社では，RG 5.71への適合に向けたサイバーセキュリティ対策の開発を進めており（**図1**），**5章**でその取組みを述べる。

3. 人間工学設計の設計認証活動

3.1　米国標準仕様の確立

設計認証活動で必要となる米国標準仕様を確立するため，人間工学プログラムのレビュー基準（NUREG-0711）に基づいた設計プロセスを定め，運転検証を実施した。運転検証結果については，この設計プロセスに従い，米国標準仕様に反映した。三菱では，米国運転員を含めた評価チームを編成し，運転検証結果の反映仕様をレビューすることで，米国標準仕様が規制ガイドラインに適合していることを確認した。次に，運転検証結果の反映仕様例について述べる。

【運転検証結果の反映仕様例】

運転員は，運転手順書に従った監視操作を行っており，この監視操作をサポートする機能として，電子化手順書システムに次の機能を設けた。

⑴　電子化手順書上でのステータス管理機能（**図3**）

複数の運転員による手順書の進捗を管理するため，手順書の操作手順ごとで“開始”“完了”“対応不要”等，複数のステータス管理を可能とした。

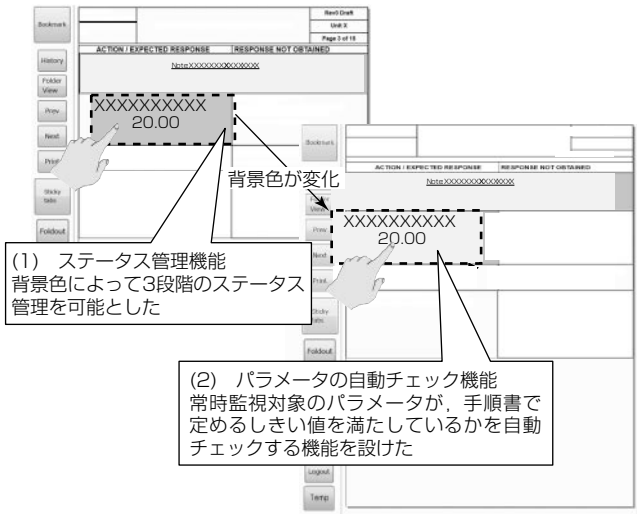


図3．ステータス管理機能及び自動チェック機能

⑵　パラメータの自動チェック機能（**図3**）

運転手順書の中で常時監視が要求されるパラメータについて，常時監視する負担を軽減するために，対象パラメータの状態を計算機が常時チェックし，状態変化時には運転員に告知する機能を設けた。

3.2　NRCによる技術監査

人間工学設計の設計認証活動では，2007年に申請図書の提出以降，NRCによる審査を受審してきた。この審査では，申請資料で定めた三菱の設計プロセスと米国標準仕様が，規制ガイドラインに適合していることをNRCが確認した。次に，NRC評価の観点と評価結果を示す。

⑴　設計プロセスの適合性

三菱の設計プロセスが，人間工学プログラムのレビュー基準（NUREG-0711）に定める要求を満足している。

⑵　画面設計方針の適合性

監視操作画面などの仕様が，中央計装システムの設計ガイドライン（NUREG-0700）に定める要求を満足している。

⑶　運転員のワークロード評価

デジタル中央計装システムの適用によって，ハードウェアの操作器，指示計等を主体に構成した中央計装システムに比べ，運転員のワークロードを軽減しており，人間工学プログラムのレビュー基準（NUREG-0711）の要求を満足している。

これらの評価結果を踏まえ，トピカルレポートで定めた設計プロセスと策定した米国標準仕様が米国規制ガイドラインの要求を満足していることをNRCが確認し，2012年3月にドラフトSER発行に至った。

4. 計装制御システムの設計認証活動

4.1　米国規制適合に向けたMELTACの再評価活動

安全系計装制御システムに適用するMELTACは，米国原子力安全系向け品質保証プログラム（10CFR50 Appendix B）の要求への準拠が必要である。そのため，この要求事項を満足した当社の品質保証プログラムの下，日本国内原子力発電所に納入してきた開発済みMELTACに対して，再評価活動を実施した。

開発済みMELTACは，日本国内原子力安全系向け品質保証プログラム（ISO9001，JEAG等）に準拠して開発している。一方で，米国原子力安全系向け品質保証プログラムの下では，日本国内規格で開発済みMELTACは，商用グレード製品（Commercial Grade Item）として扱われるため，EPRI NP-5652（Guideline for the Utilization of Commercial Grade Item in Nuclear Safety Related Applications）の評価手法であるCGD（Commercial Grade Dedication）を用いて，MELTACの再評価活動を実施し，開発済みMELTACが米国原子力向け品質保証プログラムの要求事項を満足し，商用グレード製品を安全系計装制御システムに適用できることを示した。

再評価活動は，開発時点で設計及びV&V（Verification and Validation：検証と妥当性確認）に関わっていない独立した組織に所属する第三者によって実施した。

4.2 NRCによるQA審査と技術監査

2011年12月にNRCによるQA審査と技術監査を受審した。QA審査では，MELTACの開発設計活動や**4.1節**で述べた再評価活動の結果をエビデンスとして，当社の米国原子力安全系向け品質保証プログラムが，規制指針に適合しているか審査を受けた。技術監査では，日本国内でも要求がある安全系計装制御システムの多重性，独立性等の主要技術要素を中心に，米国規制指針への適合性が評価された。この結果を踏まえ，2013年3月に計装制御システムの申請資料に対して，ドラフトSERが発行されており，この中で，MELTACが規制指針へ適合しているとの評価を得た。

5. サイバーセキュリティ規制対応

5.1 RG 5.71のサイバーセキュリティ要求

RG 5.71には，詳細なサイバーセキュリティ対策の要求があり，セキュリティの低いネットワークから高いネットワークへのデータ送信の禁止，ネットワークのセキュリティレベルに応じた分離等の外部脅威(注1)への対策，及びデジタルシステムへの不正アクセス防止のためのアクセス管理，データ改ざん防止のための暗号化等の内部脅威(注2)への対策に分類できる。

また，RG 5.71では，デジタル計装システムのサイバーセキュリティ分析を実施し，セキュリティ対策を行うことを要求している。そこで当社は，この要求に適合するために，RG 5.71で推奨されているセキュリティ分析手法である，National Institute of Standards and Technology（NIST）の“SP800-30：Guide for Conducting Risk Assessments-IT Security”に基づき分析（**図4**）を実施し，内部脅威及び外部脅威への対策を検討した。

（注1） 原子力プラント外からのサイバー攻撃などによる脅威
（注2） 原子力プラント内における不正アクセスなどによる脅威

5.2 サイバーセキュリティ対策

脅威への対策を検討した結果，当社は，外部脅威対策として，物理的な一方向通信を実現するデータダイオード，内部脅威対策として，監視対象装置のセキュリティを統合管理するセキュリティ管理システムの開発を進めている。

外部脅威対策としては，RG 5.71では，セキュリティレベルの異なるネットワーク間にデータダイオード又はファイアウォールを設置し，デジタル計装システムに対するデータアクセスを遮断することを要求している。しかし，ファイアウォール適用時は，21項目の運用面での管理が必要であり，事業者負担が大幅に増加する。そのため，当社ではデータダイオードを採用する方針とし，デバイス開発を進めている。

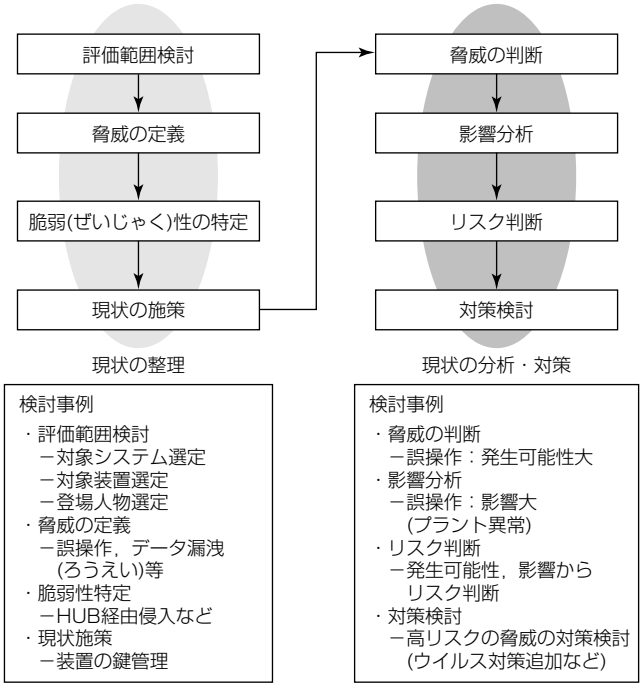


図4．米国規制が推奨するサイバーセキュリティの分析フロー

内部脅威対策としては，ネットワーク上の各装置に対して，各種セキュリティ機能（アクセス管理，暗号化，ウイルス対策等）を実装する必要がある。個別にセキュリティ機能を実装する場合，装置ごとにセキュリティ状態の確認や，ウイルスパターンファイルの更新等を行う必要があり，運用負荷の増大につながる。そのため，当社では，RG 5.71に適合するとともに，セキュリティの統合管理による運用効率化とセキュリティ強化を実現するセキュリティ管理システムを開発した。

6. むすび

3章，**4章**で述べた活動を通じて，人間工学設計，計装制御システムの申請資料に対するドラフトSER発行に至った。2016年までに，三菱重工業㈱は全ての安全審査項目に関する設計認証活動を完了する予定である。認証取得後は，この活動で定めた標準設計を基にUS-APWR適用プラントでの仕様詳細化検討を進める。

また，**5章**で述べたサイバーセキュリティ対策については，日本国内外でも議論されている課題であり，日本国内外の規制動向を踏まえた開発に取り組む計画である。

参考文献

(1) 緒方善樹，ほか：US-APWRにおける電気計装設備の新技術（新型中央制御盤及び非常用ガスタービン発電機の検証），三菱重工技報，**46**，No.4，15～18（2009）
(2) 北村雅司，ほか：米国向け中央計装運転検証設備及び型式認証活動，三菱電機技報，**84**，No.10，542～545（2010）