泊発電所３号炉審査資料	
資料番号	資料２－３
提出年月日	令和4年10月7日

ともに輝く明日のために。
Light up your future.
ほくでん

泊発電所３号炉
第24条　安全保護回路

本資料の位置付け

- まとめ資料より，ヒアリングにて口頭でご説明申し上げる箇所を抜粋したもの。
- 本資料中の[〇〇]は，当該記載の抜粋元として，まとめ資料のページ番号「24条－〇〇」を示している。

令和４年１０月７日
北海道電力株式会社

□：枠囲みの内容は機密情報に属しますので公開できません。

1. 適合のための基本方針

○「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）

・新規制基準としての追加要求事項は「第１項第六号」のみであり，その他の規制要求に変更はない。

・追加要求事項に対する適合の基本方針は以下のとおり。詳細は次頁以降参照。

設置許可基準	適合の基本方針
（安全保護回路） 第二十四条　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。 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。 （解釈） 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。	（物理的分離） ・安全保護設備は，盤の施錠等により，許可された者以外にはハードウェアを直接接続させないことで，物理的に分離している。 ・発電所出入管理により，物理的アクセスを制限している。 ・安全保護設備のシステムへのパスワード管理等により，電気的アクセスを制限している。 （機能的分離） ・安全保護設備の信号を外部へ伝送する場合は，外部ネットワークと直接接続せず，防護装置（一方向のみに通信を許可する装置等）を介した一方向通信に制限し，ハードウェアレベルで外部からの信号を受信しないことで，機能的分離を行っている。 （調達管理） ・安全保護設備は，システムの設計・製作・試験及び変更管理の各段階において，「安全保護系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）に基づき，検証及び妥当性確認がなされたソフトウェアを使用している。 （ソフトウェアの信頼性） ・安全保護設備は，固有のプログラム及び言語を使用し，一般的なコンピュータウイルスが動作しない環境としている。

２．物理的分離（１／２）

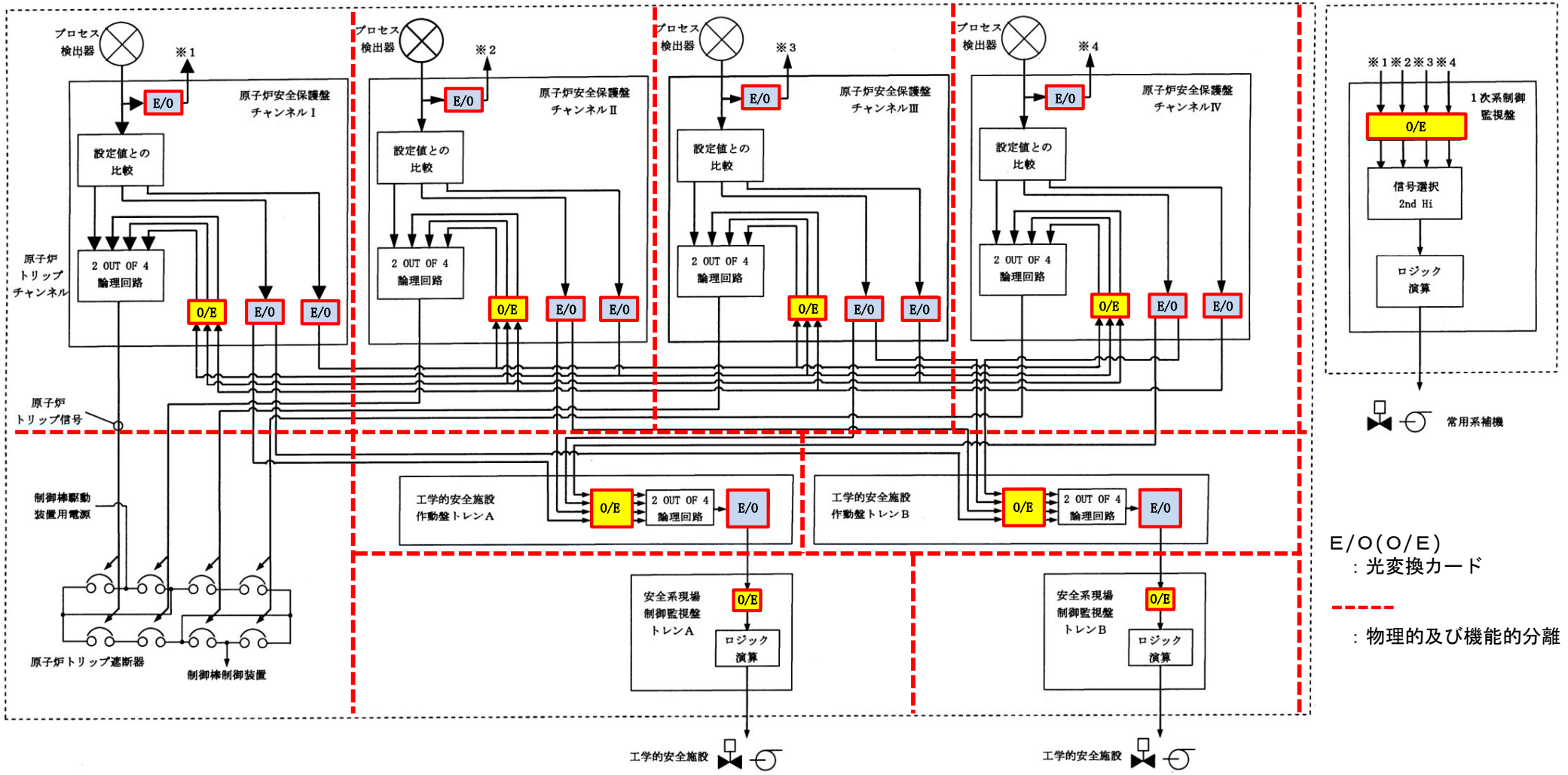
□ 内の内容は先行との差異あり。
「比較結果等をとりまとめた資料」参照。

ともに輝く明日のために。
Light up your future.
ほくでん

・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，各チャンネル間・トレン間及び計測制御系等とは，物理的及び機能的に分離している。[38]

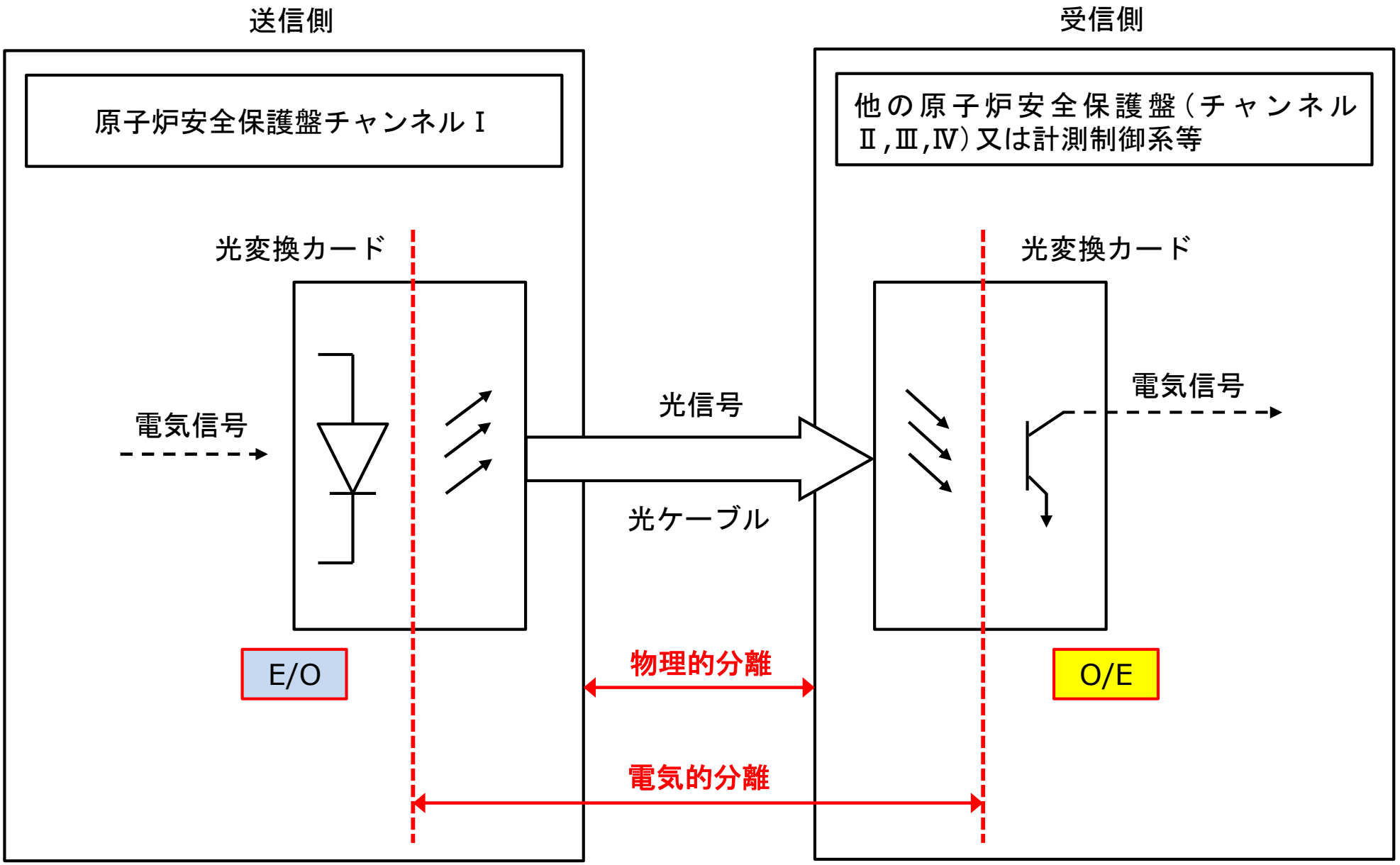
・各盤筐体の施錠等により，許可された者以外がハードウェアを直接接続することを物理的に防止している。[31]

・安全保護設備から他チャンネルや計測制御系等へのデータ伝送にあたっては，光変換カードによって電気信号を光信号に変換することで，物理的および電気的に分離している。[31]



安全保護設備の構成[39]

２．物理的分離（２／２）



光通信における分離概念図[32]

３．機能的分離，物理的及び電気的アクセスの制限（１／２）

○機能的分離

・ソフトウェアを送信ソフトウェアのみとすることで、信号の流れが安全保護設備からデータ収集計算機へ信号を送信するのみの一方向となっている。[37]

・安全保護設備とデータ収集計算機との間に設けた防護装置（　　）により，ハードウェアレベルで信号の流れが安全保護設備から信号を送信するのみの一方向となっている。[37]

・データ収集計算機と外部システムとの間には，防護装置（　　）を介して接続している。[37]

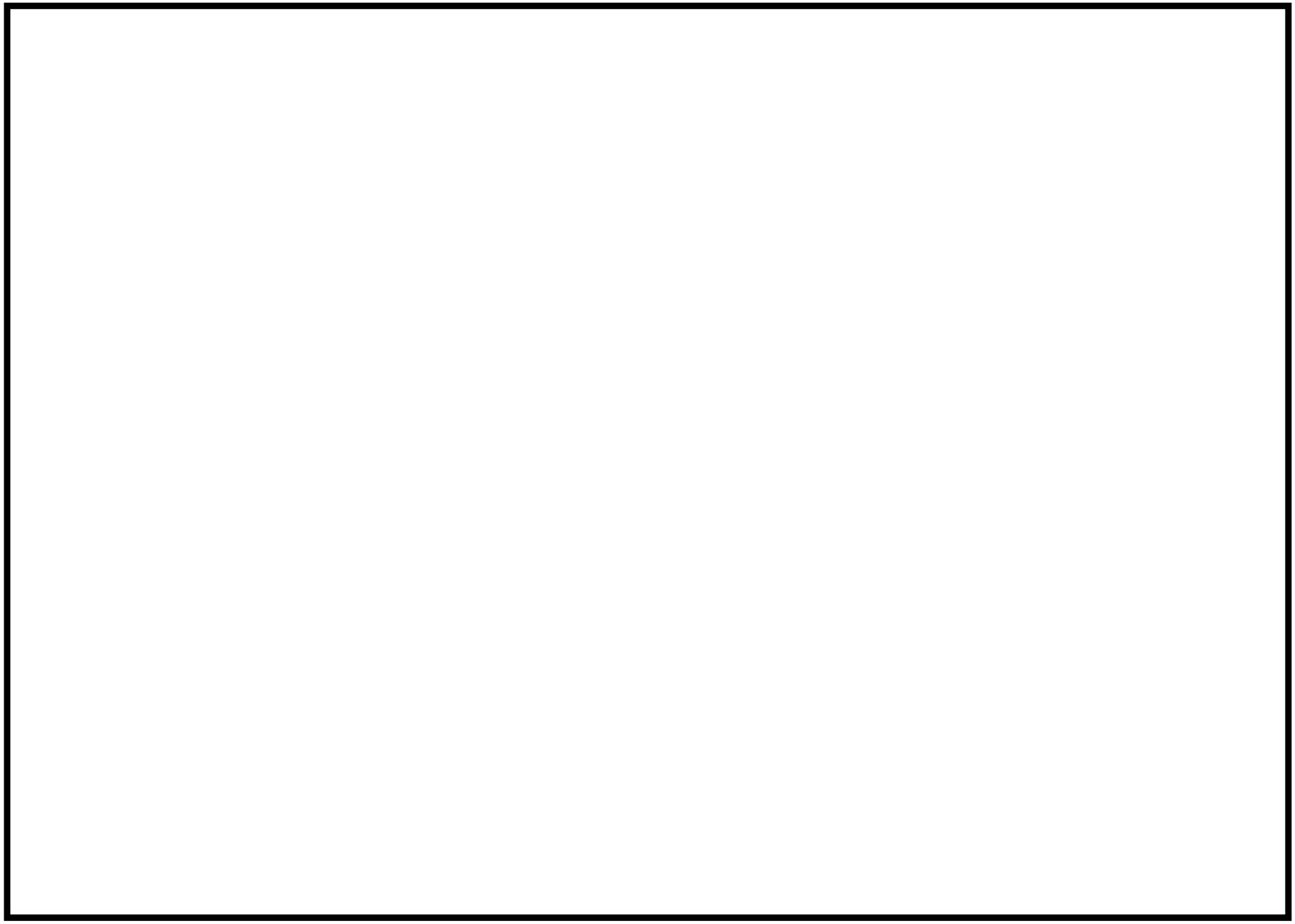
○物理的及び電気的アクセスの制限

・発電所の出入管理，安全保護設備に対する盤の施錠や貸出管理等により，物理的アクセスを制限している。[37]

・安全保護設備のシステムへのパスワード管理等により，電気的アクセスを制限している。[37]

□ 枠囲みの内容は機密情報に属しますので公開できません。

３．機能的分離，物理的及び電気的アクセスの制限（２／２）



枠囲みの内容は機密情報に属しますので公開できません。

不正アクセス防止の概念図[37]

4. コンピュータウイルスによる被害の防止

□枠囲みの内容は機密情報に属しますので公開できません。

ともに輝く明日のために。
Light up your future.
ほくでん

・安全保護設備は，固有のプログラム及び言語を使用することで，一般的なコンピュータウイルスが動作しない環境としている。[33]

・安全保護設備は，パスワード管理等によって，ソフトウェアへの不要なアクセスを制限している。[33]

・安全保護設備は，設計・製作・試験及び変更管理の各段階で，検証及び妥当性確認（コンピュータウイルスの混入防止を含む）がなされたソフトウェアを使用している。[33]

・情報システムセキュリティ計画を策定し，当社原子力施設に係る情報システムへの妨害または破壊行為を防止するための措置を講じるとともに，当該措置の実効性を定期的に確認している。[33]

項目	確認項目
調達に係る対策	
システムの構成に係る対策	
システムの構成要素に係る対策	
アクセスの制御に係わる対策	
パスワードに係わる対策	
バックアップに係わる対策	
媒体に係わる対策	
セキュリティチェック	

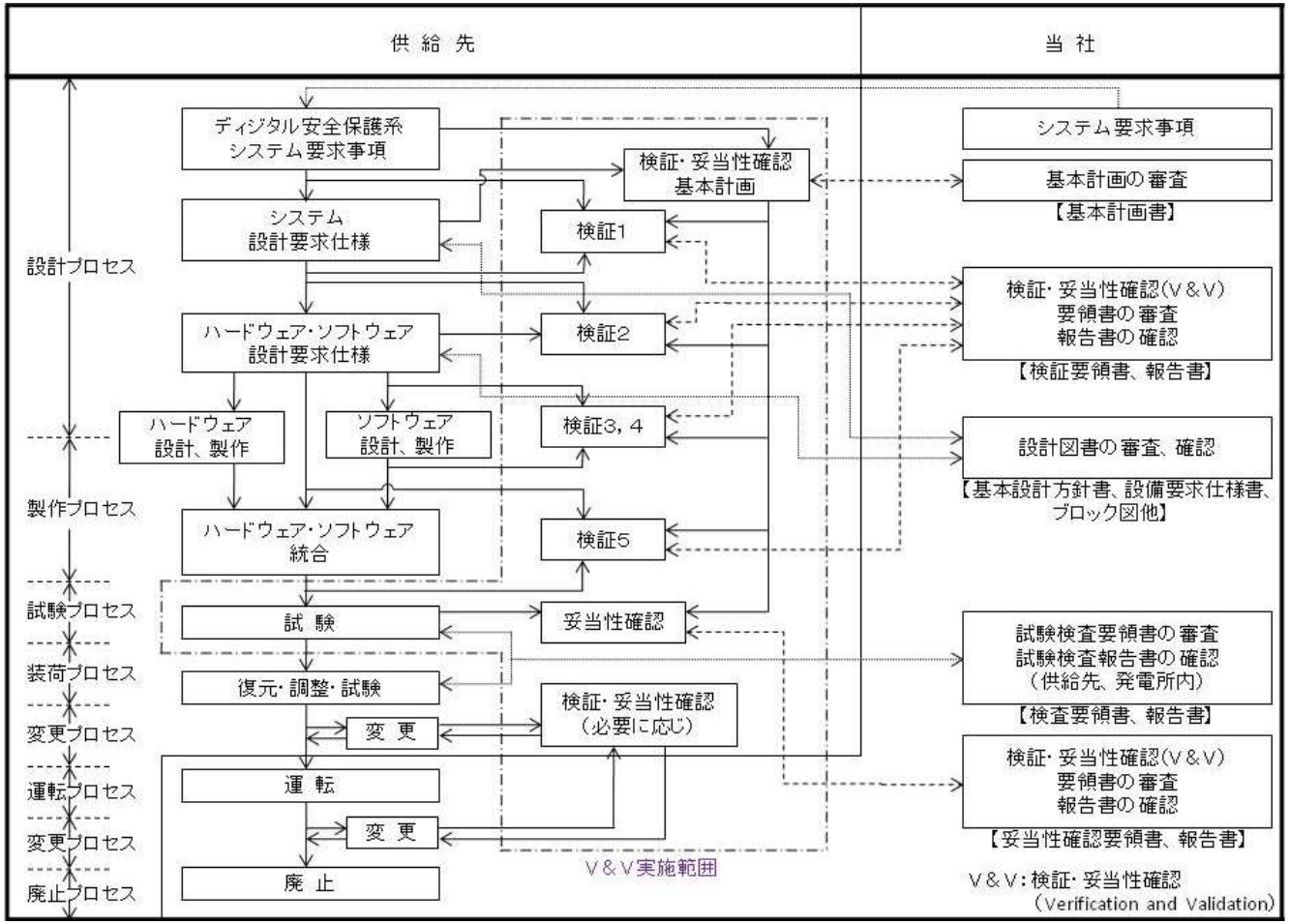
情報システムセキュリティ計画の概要[33]

5. 検証及び妥当性確認

・安全保護設備のプログラムは，工場製作段階からライフプロセスにおける各段階において，想定脅威に対する対策，品質保証活動に基づく検証及び妥当性確認等を実施している。[35]

・安全保護設備のディジタル化にあたっては，システムの設計・製作・試験・変更管理の各段階で，以下の規格及び指針に基づく検証及び妥当性確認がなされたソフトウェアを使用している。[35]

- 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）（建設時～以下の規程及び指針に改定されるまでの間に適用）
- 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）
- 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）



検証項目	検証内容
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
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
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
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
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
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

検証及び妥当性確認の流れ[36]

6. ソフトウェア変更管理

□ 内の内容は先行との差異あり。
「比較結果等をとりまとめた資料」参照。

□ 枠囲みの内容は機密情報に属しますので公開できません。

ともに輝く明日のために。
Light up your future.
ほくでん

・安全保護設備のソフトウェア変更にあたっては，安全系計装盤室内の施錠管理された盤内に設置された専用保守ツールを使用するとともに，専用保守ツールはパスワード管理することで，管理されないソフトウェアの変更を防止している。[40]

・専用保守ツールのパスワードは，関係者に限定して付与するとともに，定期的（定期保安工事毎等）に見直すものとしている。[40]

・インストールしたソフトウェアは，専用保守ツールの保管庫（ハードディスク）に保管するとともに，安全保護設備の改造工事毎にバックアップを採取し，記憶媒体を施錠管理した保管庫（事務所）にて保管している。[40]

ソフトウェア変更の手順[40]