資料２－１

放送設備の安全・信頼性に関する技術基準の概要と最近の動向

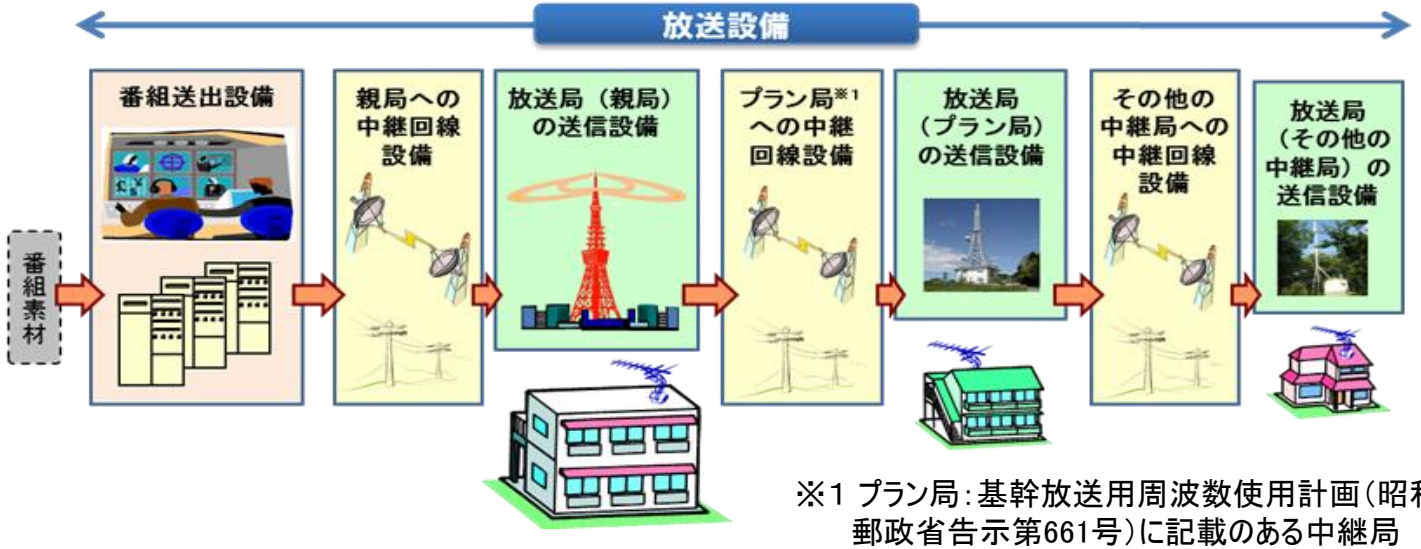
令和6年2月27日

情報流通行政局 放送技術課

放送設備の概要

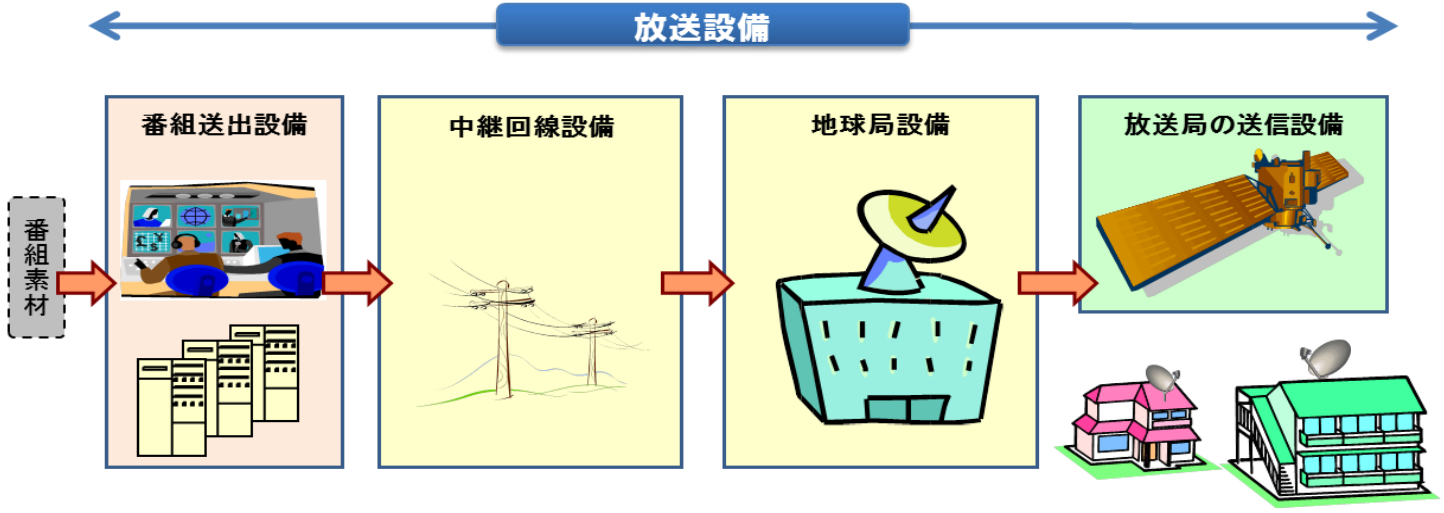
放送設備の構成

■ 地上デジタルテレビジョン放送



※1 プラン局：基幹放送用周波数使用計画（昭和63年郵政省告示第661号）に記載のある中継局

■ 衛星放送



番組送出設備（マスター設備）の概要

- 番組送出設備（マスター設備）は、放送番組及びCM、並びに時刻・天気予報等の付帯するデータ等を、放送時間に合わせて順番どおりに誤りなく送信設備へ送出する、放送局にとっての「心臓部」とも言うべき放送設備。
- 法令上は、「放送番組の素材を切り替え、当該放送番組の素材その他放送番組を構成する映像、音声、文字及びデータに係る信号を調整（デジタル放送の場合にあっては、主として映像、音声及びデータに係る信号を符号化及び多重化することをいう。）し、放送番組として送出し、並びにこれらを管理する機能を有する電気通信設備をいう。」（放送法施行規則第2条第11号）と定義。

映像・音声、時刻などの様々な信号をプログラム通りに送出

緊急時（ニュース速報、地震・災害等）に手動操作で制御

放送運行・放送品質の監視、チェック

放送局にとっての
”心臓部“

出典：情報通信審議会 放送設備安全信頼性検討作業班（第１回）NEC資料より抜粋

番組送出設備に関連する業務（マスター業務）の概要

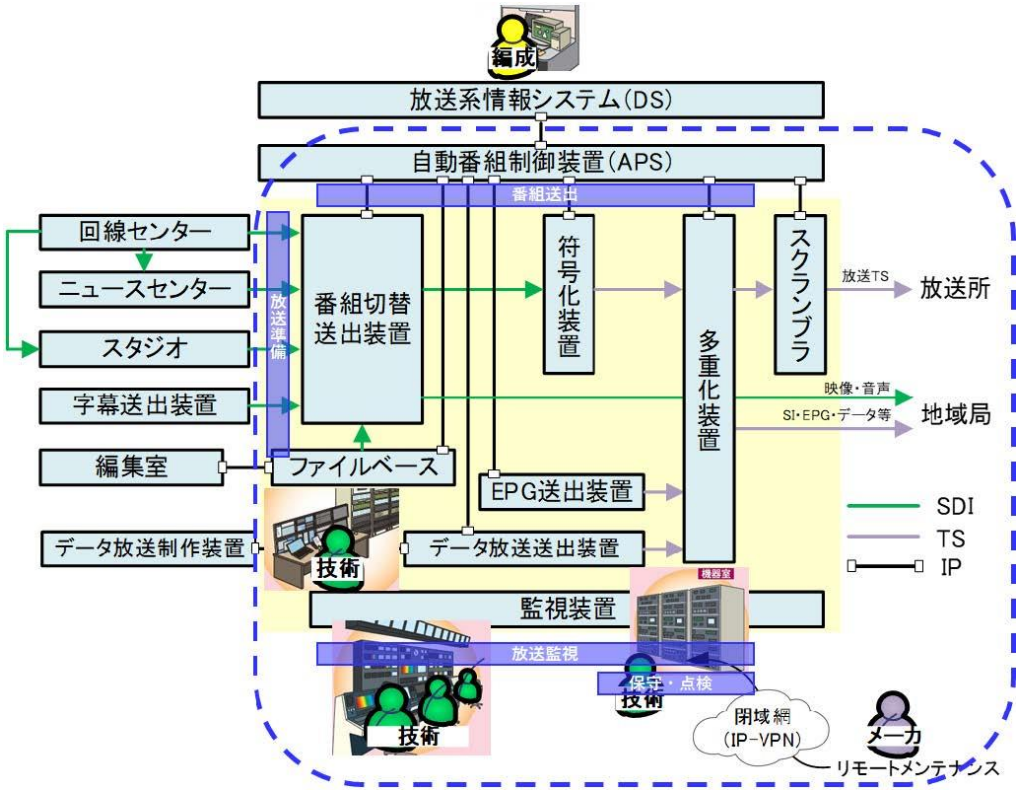
● 技術スタッフにより、放送準備、番組送出及び放送監視の各業務が行われるほか、設備の機能を維持するための保守・点検も実施される。

◆ 放送準備
- 収録した番組ファイルを試写し、映像音声・フォーマットチェック後、ファイルベース設備に登録
- 生放送のスタジオや回線の接続確認

◆ 番組送出
- 運用データに従って番組切替が行われ、データ放送、EPG、字幕を自動送出
- 緊急ニュースやスポーツ中継では、編成と技術が連携して放送時間の変更やスーパー対応を実施

◆ 放送監視
- 運行表をもとに24時間正しく放送されているか監視
- 設備故障時に予備機器に切替え、放送を確保

◆ 保守・点検
- 機器点検や定期保守、故障機器の交換
- 不具合発生時、メーカによるリモートメンテナンス

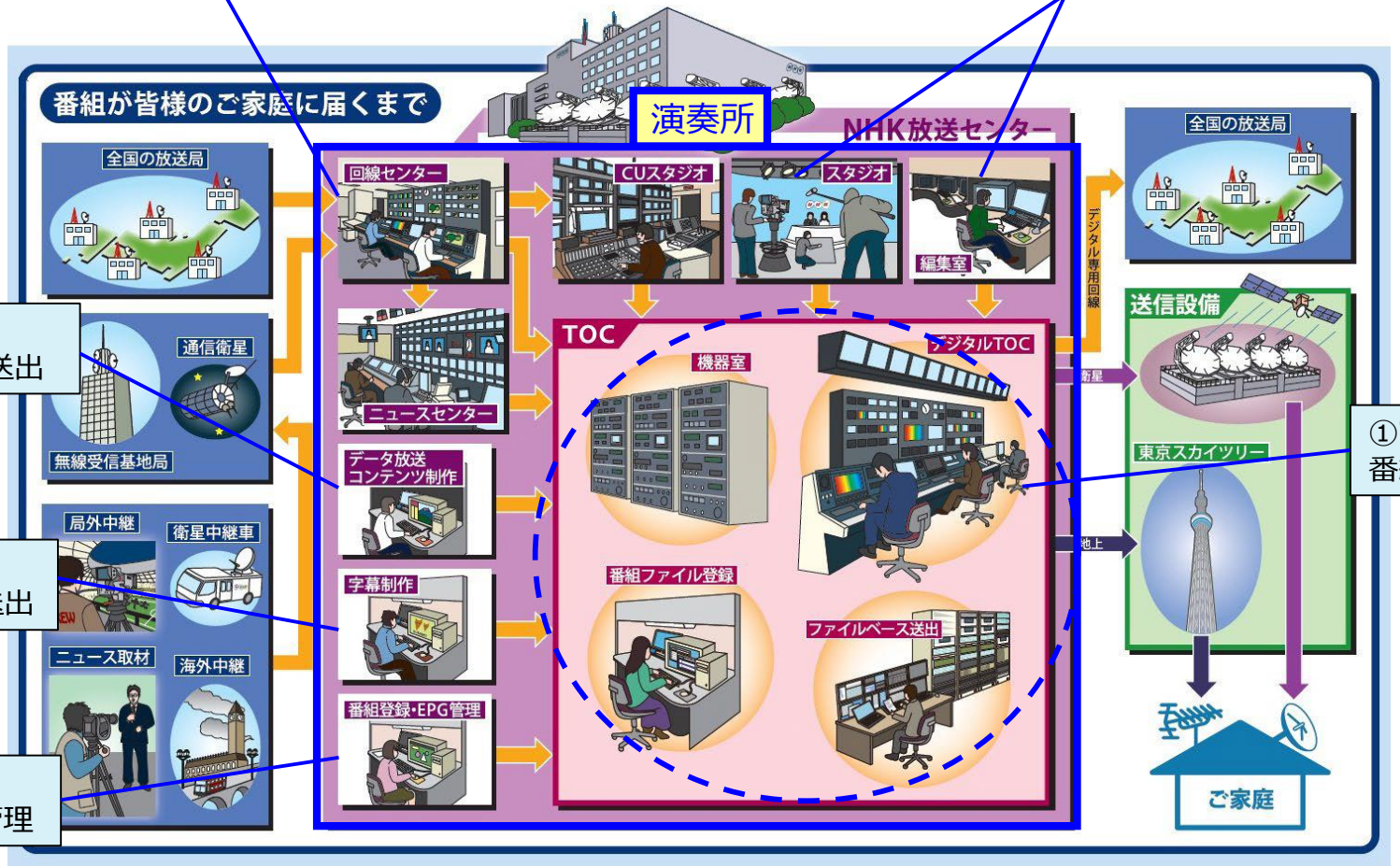


出典：情報通信審議会 放送設備安全信頼性検討作業班（第２回）NHK資料より抜粋

【参考】演奏所で行われる業務の概要

④回線業務
素材伝送回線構築と局内外への分配

③番組制作業務
スタジオ、ニュースセンターで生放送や番組収録
編集室で収録した映像・音声の編集・加工



⑤データ放送業務
データ放送の制作と送出

⑥字幕業務
字幕放送の制作と送出

②番組編成業務
番組編成の決定・管理

①マスター業務
番組の送出と監視

出典：情報通信審議会 放送設備安全信頼性検討作業班（第２回）NHK資料より抜粋

放送設備の安全・信頼性確保に関する規定

放送設備に係る技術基準適合維持義務

■ 放送法に規定する技術基準適合維持義務

・特定地上基幹放送事業者においては、法第112条
・基幹放送局提供事業者においては、法第121条
・登録一般放送事業者においては、法第136条
に、技術基準への適合維持義務を規定。

（設備の維持）

第111条　認定基幹放送事業者は、基幹放送設備を総務省令で定める技術基準に適合するように維持しなければならない。

2　前項の技術基準は、これにより次に掲げる事項が確保されるものとして定められなければならない。

一　基幹放送設備の損壊又は故障により、基幹放送の業務に著しい支障を及ぼさないようにすること。

二　基幹放送設備を用いて行われる基幹放送の品質が適正であるようにすること。

◆ 放送法施行規則（省令）に安全・信頼性に関する技術基準を規定

- 予備機器等
- 故障検出
- 試験機器及び応急復旧機材の配備
- 耐震対策
- 機能確認
- 停電対策
- 送信空中線に起因する誘導対策
- 防火対策
- 屋外設備
- 放送設備を収容する建物
- 耐雷対策
- 宇宙線対策
- サイバーセキュリティの確保

◆ 放送品質に関する省令を規定

- 中波放送に関する送信の標準方式
- 標準テレビジョン放送等のうちデジタル放送に関する送信の標準方式
- 衛星一般放送に関する送信の標準方式
- 超短波データ多重放送に関する送信の標準方式
- 超短波放送に関する送信の標準方式
- 超短波音声多重放送及び超短波文字多重放送に関する送信の標準方式
- 有線一般放送の品質に関する技術基準を定める省令

放送設備の安全・信頼性に関する技術基準の概要（1）

■ 放送法施行規則（省令）に規定する技術基準

・衛星一般放送に係る電気通信設備の技術基準については、第148条に規定。
・有線一般放送に係る電気通信設備の技術基準については、第151条ー第154条に規定。

第４章第５節　基幹放送に用いる電気通信設備
第１款　設備の損壊又は故障の対策（第102条ー第115条の2）

措置項目	措置内容	条文
予備機器等	• 機能を代替することができる予備機器の設置もしくは配備、かつ、その損壊又は故障の発生時に当該予備機器への速やかな切替。	第104条
故障検出	• 電源供給停止、動作停止、動作不良その他放送の業務に直接係る機能に重大な支障を及ぼす損壊等の発生時、これを直ちに検出し、放送設備を運用する者に通知する機能の具備。 • やむを得ず当該機能を備えることができない放送設備は、損壊等の発生時にこれを目視又は聴音等により速やかに検出し、当該設備を運用する者に通知することが可能となる措置。	第105条
試験機器及び応急復旧機材の配備	• 放送設備の点検及び調整に必要な試験機器の配備。 • 放送設備の損壊等が発生した場合における応急復旧工事、電力の供給その他の応急復旧措置を行うために必要な機材の配備。	第106条
耐震対策	• 放送設備の据付けに当たって、通常想定される規模の地震による転倒又は移動を防止する、床への緊結その他の耐震措置。 • 通常想定される規模の地震による構成部品の接触不良及び脱落を防止する、構成部品の固定その他の耐震措置。 • その損壊等により放送の業務に著しい支障を及ぼすおそれのある放送設備は、上記の耐震措置は大規模な地震を考慮したものであること。	第107条
機能確認	• 予備機器に対する、定期的な機能確認等の措置。 • 放送設備の電源設備に対する、定期的な電力供給状況の確認等の措置。	第108条

放送設備の安全・信頼性に関する技術基準の概要（2）

■ 放送法施行規則（省令）に規定する技術基準

措置項目	措置内容	条文
停電対策	• 自家用発電機又は蓄電池の設置その他これに準ずる措置。 • 自家用発電機の設置又は移動式の電源設備の配備を行う場合、使用される燃料について、必要な量の備蓄又は補給手段の確保。	第109条
送信空中線に起因する誘導対策	• 送信空中線に近接した場所に設置するものは、送信空中線からの電磁誘導作用による影響を防止する措置。	第110条
防火対策	• 自動火災報知設備及び消火設備の適切な設置その他これに準ずる措置。	第111条
屋外設備	• 通常想定される気象の変化、振動、衝撃、圧力その他設置場所における外部環境の影響を容易に受けないものであること。 • 公衆が容易にそれに触れることができないように設置されること。	第112条
放送設備を収容する建築物	• 放送設備を安全に設置することができる堅固で耐久性に富むものであること。 • 放送設備が安定に動作する環境を維持することができること。 • 公衆が容易に立ち入り又は放送設備に触れることができないようにする施錠その他必要な措置。	第113条
耐雷対策	• 落雷による被害を防止するための耐雷トランスの設置その他の措置。	第114条
宇宙線対策	• 人工衛星に設置する放送設備は、宇宙線による影響を容易に受けないための放射線対策が講じられた構成部品の使用その他の措置。	第115条
サイバーセキュリティの確保	• 放送設備及び当該放送設備を維持又は運用するために必要な設備は、放送の業務に著しい支障を及ぼすおそれがないよう、サイバーセキュリティの確保のために必要な措置。	第115条の2

放送設備の安全・信頼性に関する技術基準の概要（3）

■ 放送法関係審査基準（訓令）に規定する措置内容

【別添1】 1　基幹放送に用いる電気通信設備の損壊又は故障に対する措置

（13）サイバーセキュリティの確保

● **放送本線系入力となる番組送出設備について、外部ネットワークから隔離するための次の措置又はこれと同等と認められる措置**
• 原則として、第三者が接続可能な外部ネットワークとの接続を行わない措置 • やむを得ず接続を行う場合には、ファイアーウォールの設置又は不正接続対策等の措置
● **放送設備に接続される監視・制御及び保守に使用される回線について、外部ネットワークからの不正接続対策を行うための次の措置又はこれと同等と認められる措置**
• 専用回線又はVPN回線の使用、ポート番号若しくはIPアドレスによる接続制限又はID及びパスワードにより権限を有する者だけが接続できるようにする措置 • 未使用時は回線を通じた接続を遮断する等の措置
● **設備の導入時及び運用・保守時におけるソフトウェアの点検について、不正プログラムによる被害を防止するため、放送設備のネットワークからの分離・遮断の措置及び不正プログラムの感染防止の措置**
● **放送設備に対する物理的なアクセス管理について、機密性が適切に配慮されるための次の措置又はこれと同等と認められる措置**
• 番組送出設備に対しIDカード、テンキー錠又は有人による入退室の管理等を行う措置及び監視・制御回線、保守回線に係る機器の設置場所に対し公衆が容易に立ち入ることができないよう施錠その他の必要な措置 • 外部記録メディア等を介した不正プログラムへの感染防止の措置
● **放送設備の運用・保守に際して、業務を確実に実施するための組織体制の構築及び業務の実施に係る規程若しくは手順書の整備に関する次の措置又はこれと同等と認められる措置**
• サイバー事案の発生時の対応策及び再発防止策について、事故報告を含む事後対応を迅速かつ確実に実施するための規程又は手順書を整備する措置 • サイバー事案が発生した場合の連絡先の整備及び報告実施等の手順書化、放送設備のソフトウェアの更新等設備の運用・保守等について、実施方法を定める規程又は手順書を整備する措置

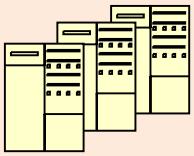
【参考】技術基準の適用範囲のイメージ（地上デジタルテレビジョン放送）

放送設備

設備構成

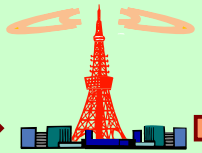
番組素材

番組送出設備



親局への中継回線設備

放送局（親局）の送信設備



放送エリア：
県庁所在地周辺、広域都市圏における、数10万世帯以上

プラン局への中継回線設備

放送局（プラン局）の送信設備

放送エリア：
中小都市周辺の、概ね数万世帯

その他の中継局への中継回線設備

放送局（その他の中継局）の送信設備

放送エリア：
山間部等の小規模な地域における、概ね数千世帯以下

広範囲 ← 【放送の停止等の影響の及ぶ範囲】 → 限定的

各設備における措置（概要）

- 予備機器等
- 機能確認
- 耐震対策
- 防火対策

当該設備には、予備機器等の措置を求めないが、以下の速やかな故障検出及び応急復旧の措置により放送の再開につなげる。

- 停電対策
- 故障検出
- 試験機器及び応急復旧機材の配備
- 耐雷対策
- 放送設備を収容する建築物
- 送信空中線に起因する誘導対策
- サイバーセキュリティの確保
- 屋外設備

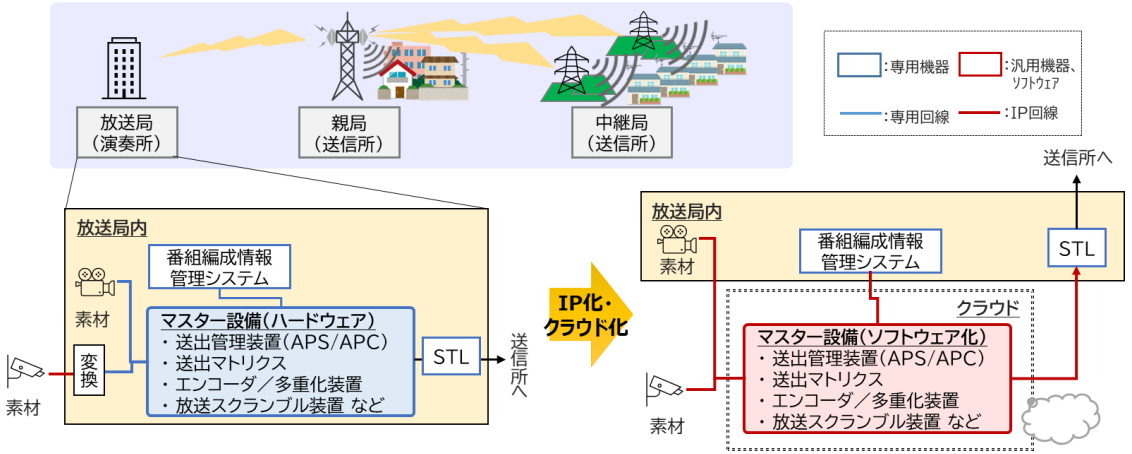
放送設備のIP化に伴う安全・信頼性に関する技術基準の見直し

放送設備のIP化に伴う安全・信頼性に関する技術的条件の検討

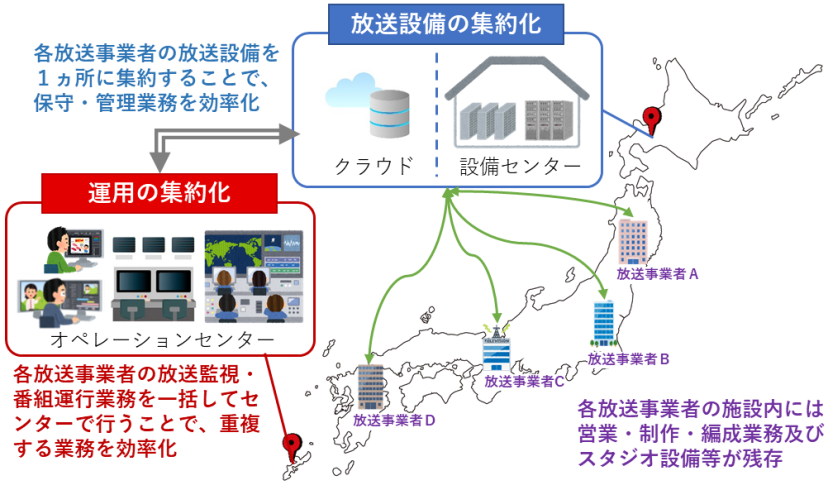
検討の背景・目的

- ICTの進展に伴い、IP化・クラウド化・集約化による柔軟な機能拡張や効率的なリソース共有を実現する技術が各分野で活用されており、今後は放送分野においても、利便性向上、運用効率化及びコスト低減等の観点から、マスター設備（番組送出設備）を中心に放送設備のIP化・クラウド化・集約化が進むものと想定。
- 「デジタル時代における放送の将来像と制度の在り方に関する取りまとめ」（デジタル時代における放送制度の在り方に関する検討会　令和４年８月５日公表）においては、「マスター設備の集約化・IP化・クラウド化は、放送事業者の経営の選択肢であることに留意しつつ、その要求条件を総務省において検討・整理すべきである」と提言。
- これらを受けて、放送設備のIP化・クラウド化・集約化に伴い新たに措置すべき安全信頼対策等、**放送に係る安全・信頼性に関する技術的条件**（※）のうち、**地上デジタルテレビジョン放送等の安全・信頼性に関する技術的条件**の検討を開始。
  ※情報通信審議会諮問第2031号（H22.12.21）
- 放送設備への実装が実用化段階にあり、放送事業者の導入計画が具体化している**IP化について**、令和５年11月21日、**情報通信審議会から一部答申**。当該答申を踏まえ、**令和５年度内に関連規程の整備を実施**。

■ IP化・クラウド化のイメージ



■ 集約化のイメージ



【参考】番組送出設備（マスター設備）に関する動向

■ 現状と課題

- 現状、オンプレミスのシステムであり、地上基幹放送事業者毎にその社屋等に設置されている。
- 10～15年毎に設備更新が必要であり、更新投資は各地上基幹放送事業者にとって大きな負担となっている。
- 放送以外の分野においては、専用機器から汎用化（IP化）・ソフトウェア化・クラウド化という順に実用化が進んでいるところ、マスター設備についても、**一部の地上基幹放送事業者においてIP化の導入が予定**されている。
- **クラウド化**については、メーカーにおいて、**2020年代後半に実用化するマイルストーンで開発**が進められている。

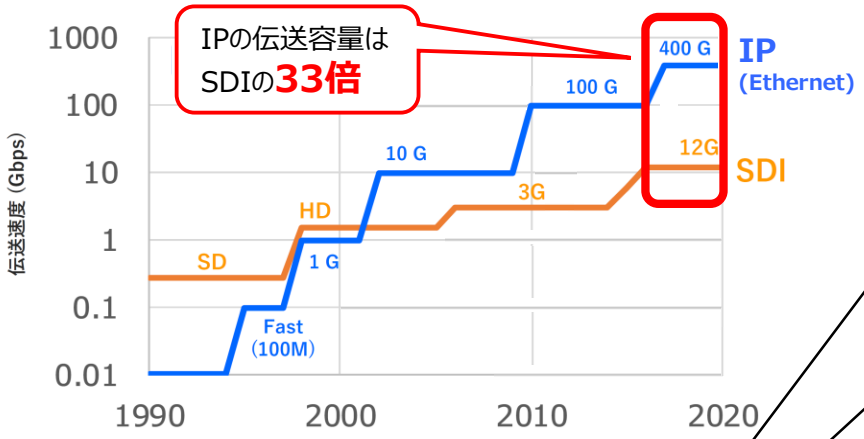
● 今後の方向性

- 地上デジタルテレビジョン放送のマスター設備について、2028年～2030年頃（令和10年～令和12年頃）に想定される在京キー局での設備更新を見据え、**効率化を図る観点から、マスター設備の集約化・IP化・クラウド化は経営の選択肢**となり得る。
- 集約化に当たっては、放送番組のやり取りが行われており、設備仕様がある程度共通化されている系列局の単位で集約化を図ることが現実的である。例えば衛星放送のプラットフォーム事業者のように、マスター設備を特定の場所に設置し、その運用・維持管理を地上基幹放送事業者以外の事業者が担うことや、クラウドサービスとして提供を受けることが考えられる。
- 集約化の対象エリアは、系列局単位での集約化を前提に、地域ブロックに加え、全国単位も視野に入ると考えられる。
- **集約化・IP化・クラウド化に当たっては、サイバーセキュリティ対策等、安全・信頼性をどのように確保可能かについて検討すべき**である。追加的なコストが発生することとなるが、持続可能な放送の実現のためのコスト削減とサイバーセキュリティ対策等の安全・信頼性確保の両立に向けた道筋を描くことは可能と考えられる。
- 我が国における**クラウド化の実現に向けて、どの程度の可用性を確保すべきかといった検討が必要**と考えられる。
- マスター設備の集約化・IP化・クラウド化は、放送事業者の経営の選択肢であることに留意しつつ、**その要求条件を総務省において検討・整理すべき**である。その際、**放送に求められる可用性を確保するためには、不測の事態における対処をクラウド側に委ねるのではなく、マスター設備の利用者である放送事業者自らがリスクをグリップ（把握）し、コントロール（制御）できることが重要であることにも留意すべき**である。

出典：「デジタル時代における放送の将来像と制度の在り方に関する取りまとめ」（デジタル時代における放送制度の在り方に関する検討会　令和４年８月５日公表）より事務局作成

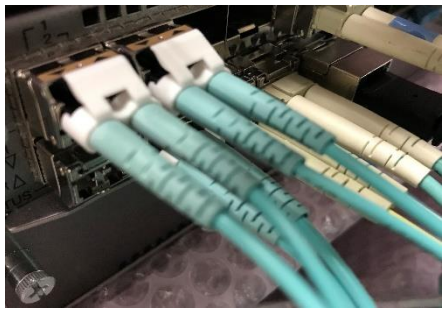
【参考】番組送出設備のIP化に伴う効率化等の効果

伝送容量の高速化

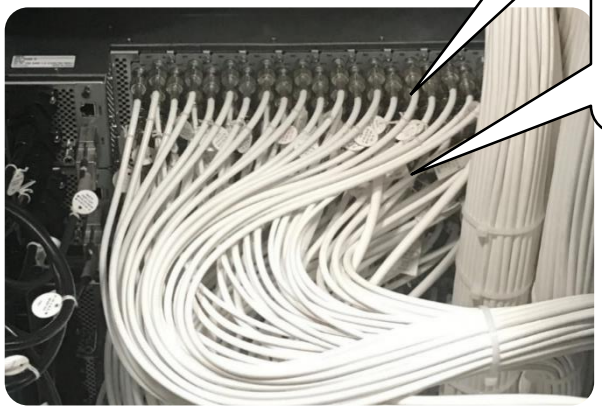


<従来>
SDIのインタフェース
（同軸ケーブル用コネクタ）

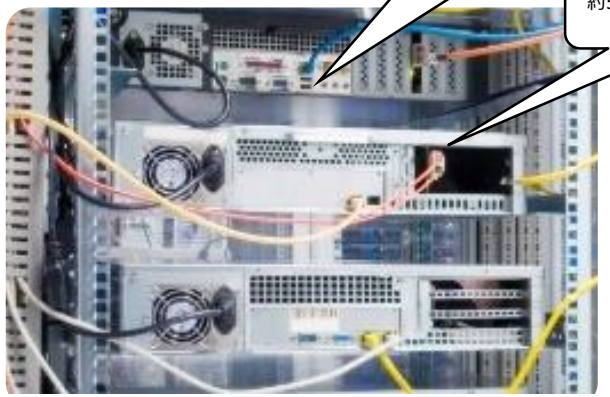
<ＩＰ化>
IPのインタフェース
（光ケーブル用コネクタ）



接続配線のスリム化



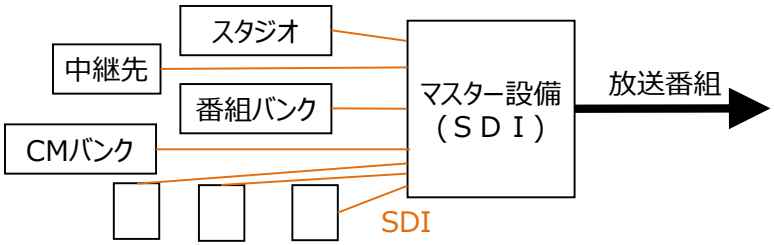
最大
10.2mm

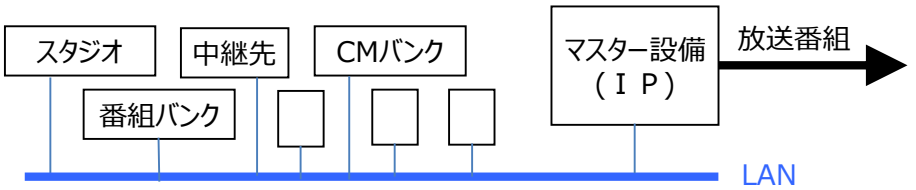


約5.7mm

<従来>
各装置間を
同軸ケーブルで
１対１接続

<IP化>
複数の装置を
光ケーブルで
LANを形成して
接続





技術的条件の検討経過

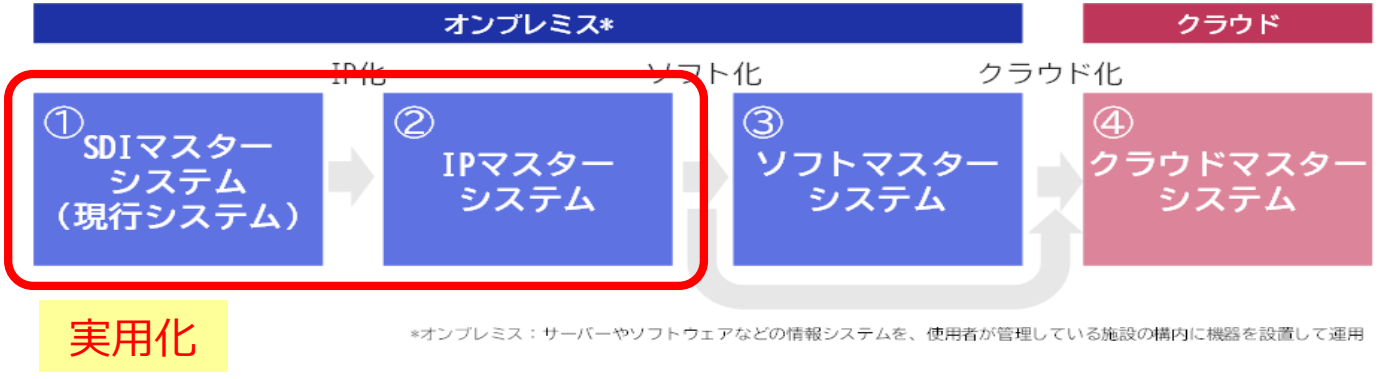
- IP化・クラウド化・集約化のうち、放送設備への実装が実用化段階にあり、放送事業者への設備導入に係る計画が具体化している**IP化を対象として検討を開始**した。
- クラウド化・集約化に伴う技術的条件の検討については、IP化に伴う技術的条件の検討後に実施することとした。
- 放送の種別については、IP化・クラウド化等の方向性が示されている**地上デジタルテレビジョン放送を対象として検討を開始**した。
- 検討の過程において、IP化・クラウド化等の技術動向及びニーズが示された**音声放送及び衛星放送についても検討対象として追加**した。
- 技術的条件の具体的な検討は、以下のとおり実施した。

  - 放送機器メーカ、放送事業者、学術研究機関、情報セキュリティ関係団体その他の関係者によるプレゼンテーションから、技術開発動向、国内外の標準化動向、機能要件及び導入計画、安全・信頼性上の課題等を調査し、現行設備からIP化及びクラウド化等への移行過程、並びにIP化等の標準モデルを検討した。
  - IP化の標準モデルに基づき、安全・信頼性の確保のために必要な措置の対象となる放送設備を特定するとともに、受信者への影響の波及度合い等を考慮した上で具体的な措置内容を検討した。

- 放送事業者がIP化・クラウド化等を選択した場合に安心かつ円滑に導入できるよう、**安全・信頼性の確保のために必要十分な技術基準を策定**することを念頭に置いて検討を進めた。

放送設備のIP化・クラウド化等への移行過程

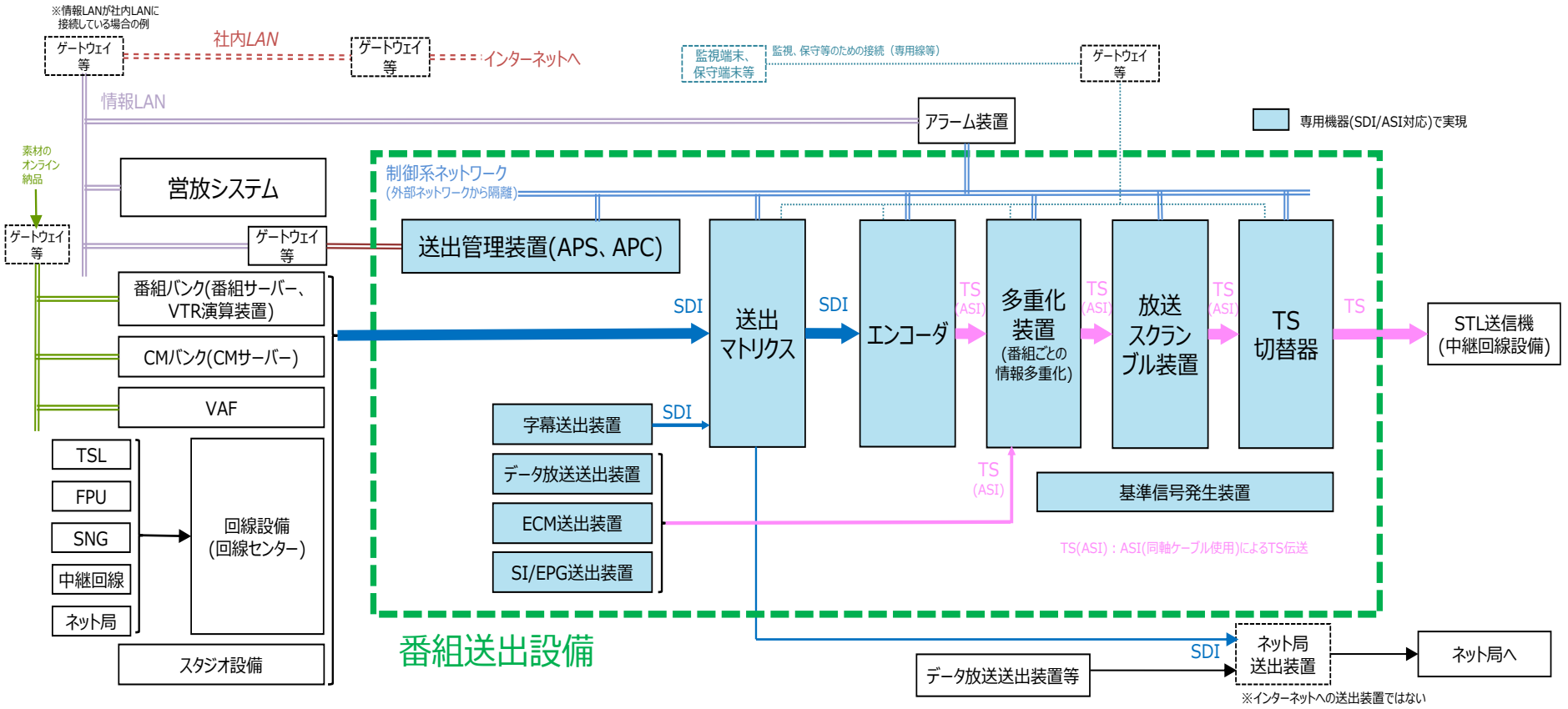
- 放送設備は、他の情報システムと同様に、**IP化からソフトウェア化を経てクラウド化に移行**すると想定。
- 番組送出設備（マスター設備）を中心にIP化・クラウド化等が進展すると想定されており、現時点において、**放送設備のIP化・クラウド化とは、番組送出設備のIP化・クラウド化とみなす**ことが可能。



マスターの種類	定義
SDIマスター	・局内に設置（オンプレミス） ・局内外からの本線信号をSDIで伝送し送信機へ送出する従来型のマスター ・多くの構成品は本線信号の伝送や映像処理をSDI信号に対応した専用機器で構成
IPマスター	・局内に設置（オンプレミス） ・局内外からの本線信号をIPで伝送し送信機へ送出する新型のマスター ・多くの構成品は汎用機器＋ソフトウェアで実現 ・性能保証が満足しない一部機器は専用ボードまたは専用機器で構成
ソフトマスター	・局内に設置（オンプレミス） ・局内外からの本線信号をIPで伝送し送信機へ送出する将来実現されるマスター ・本線信号の伝送ならびに映像処理の全てを汎用機器＋ソフトウェアで実現
クラウドマスター	・局内に設置する一部の機器を除きクラウド上に配置 ・局内外からの本線信号をIPで伝送し送信機へ送出する将来実現されるマスター ・ソフトマスターをクラウド環境に移行 ・本線信号の伝送ならびに映像処理の全てをクラウド上のリソース＋ソフトウェアで実現

現行マスター設備の標準モデル（地上デジタルテレビジョン放送）

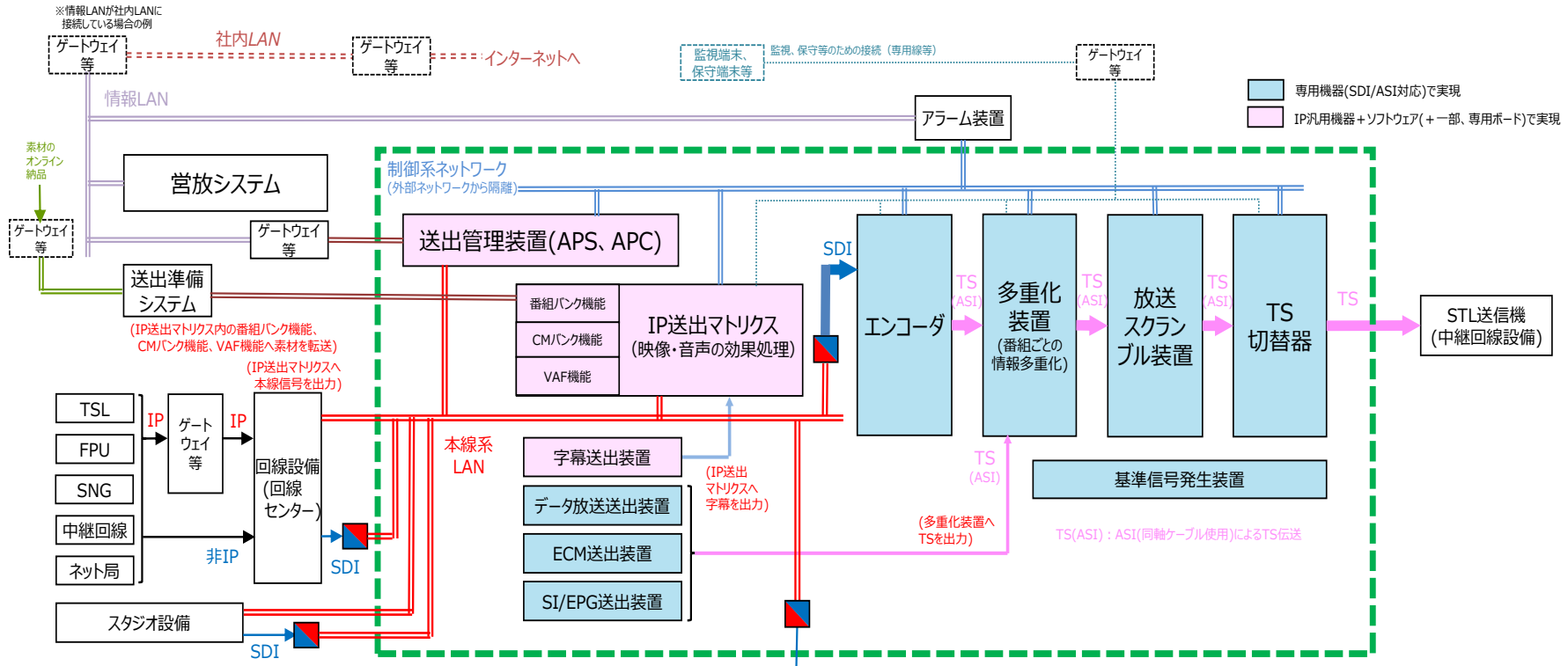
- 放送本線系は、送出マトリクス、エンコーダ、多重化装置、放送スクランブル装置等で構成
- 構成装置は、放送専用の伝送規格（SDI及びASI）に対応した専用機器（ハードウェア）
- 各構成装置の間は、SDI信号又はASI信号を伝送する同軸ケーブルにより1対1で接続



情報LAN：番組制作等の情報をやりとりするためのネットワーク
制御系ネットワーク：送出管理装置が番組送出設備内の
　　各機器を制御するためのネットワーク
社内LAN：放送事業者の社内ネットワーク

IP化されたマスター設備の標準モデル（地上デジタルテレビジョン放送）

- 放送本線系は、IP送出マトリクス、エンコーダ、多重化装置、放送スクランブル装置等で構成
- 一部の構成装置（送出管理装置（APS、APC）及びIP送出マトリクス等）は、IP対応の汎用機器（ハードウェア）及びソフトウェアで実現
- IP送出マトリクスと放送本線系信号を供給する各構成装置の間は、光ケーブルによりLANを形成して接続
- 従来は番組送出設備外に設置されていた番組バンク及びCMバンク等のバンクシステムが、IP送出マトリクスと一体化して番組送出設備の構成装置の一部になる場合もあり



本線系LAN：放送本線系を構成するネットワーク
情報LAN：番組制作等の情報をやりとりするためのネットワーク
制御系ネットワーク：送出管理装置が番組送出設備内の各機器を制御するためのネットワーク
社内LAN：放送事業者の社内ネットワーク

放送設備のIP化に伴う安全・信頼性に関する技術的条件の論点

- IP化に伴って放送設備の構成等に変更が生じるのは、**番組送出設備のみ**である（中継回線設備、地球局設備及び放送局の送信設備の変更は想定されない）。

  - 放送本線系の伝送回線の一部が、SDI、ASI及びベースバンド等の放送専用の伝送規格に準拠した回線（同軸ケーブル）から、IP回線（光ケーブル等）に変更される。
  - 構成装置が、機能ごとに設計された専用機器（ハードウェア）から、IP対応の汎用機器（ハードウェア）及び当該機器上で動作するソフトウェアに置き換わる。
  - IP回線及びIP対応機器に置き換わることで、通信方式の違いを根拠として外部ネットワークから隔離されているとみなすことは困難となる。

- 番組送出設備の設置場所は、**放送事業者の施設内（演奏所内）**であることに変更はない。

□ 放送本線系が外部ネットワークと接続された状態になることで、サイバー脅威が増大することを踏まえ、**サイバーセキュリティの確保の観点から新たな措置を検討することが必要**

- 従来型の対策である境界防御の強化のほか、ゼロトラスト及びサイバーレジリエンス等の新しいセキュリティ対策の概念についても考慮
- 放送継続のために求められる可用性の担保及び経済合理性との両立も重要な観点であり、具体的な措置内容は、放送事業者の責任及び判断に基づく選択を可能とすることが適当

□ 番組送出設備の設置場所に変更はないこと等から、**サイバーセキュリティの確保以外の措置項目については見直しの必要なし**

番組送出設備のIP化に伴うサイバーセキュリティ確保のための措置

＜従来の番組送出設備＞

- 放送専用規格に対応した専用ハードウェアで構成
- 各装置は同軸ケーブルにより1対1接続
- 365日24時間有人管理のマスター室に設置され、室内の専用端末で操作

■ 外部ネットワークから原則隔離された状態で運用

＜IP化された番組送出設備＞

- IPに対応した汎用ハードウェアとソフトウェアで構成
- 各装置はIPに対応したLANケーブル1本で接続
- 放送事業者のネットワーク(社内LAN等)上の汎用端末からも操作可能

■ 外部ネットワークと接続された状態で運用

サイバーセキュリティ確保のための新たな措置内容

① 放送本線系に係る不正接続対策等

- ファイアーウォールの設置に加えて、**不正侵入の検知及び当該侵入の遮断**等、不正接続を防止するための措置
- **不正プログラムの実行阻止、構成装置の各種セキュリティ設定強化**等、マルウェア感染防止のための措置
- **構成装置のシステム設定等に関する定期的なバックアップの実施**等、早期復旧のための措置

② 監視・制御回線に係る不正接続対策

- **VPN回線を構成する機器の安全性確保のための措置**、ID・パスワードに加えて、**所有物認証、生体認証又は多要素認証**等により、権限を有する者だけが接続できるようにする措置

③ ソフトウェア点検時の不正プログラム対策

- **定期的なウイルスチェック等、不正プログラムの早期検出のための措置**

④ 規程・手順書等の整備

- **サイバー事案の発生を迅速に検知するための定常的な監視、早期復旧及び対応能力向上**の観点も踏まえ、事故報告を含む対応を迅速かつ確実に実施するための規程又は手順書を整備する措置

【参考】放送設備のIP化に伴う安全・信頼性確保のための措置及び解説（1）

○ サイバーセキュリティの確保

放送設備（番組送出設備、中継回線設備、地球局設備及び放送局の送信設備）は、放送の業務に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保しなければならない。

【措置についての解説】

・放送設備については、情報の発信、伝送及び受信のための設備として、番組の送出に係る番組送出設備、放送本線系（放送局の送信設備及び当該設備までの中継回線設備）に対して、安全性及び信頼性確保のために必要な措置が講じられるとともに、その状態が適切に維持管理されることが必要となる。

・現行の放送設備において、番組送出設備及び放送本線系は、映像伝送や音声伝送のための通信方式（ＳＤＩ、ＡＳＩ等）及び直接受信のための放送方式により運用されており、インターネット・ＩＰ網等とは通信方式が異なっていることで、それら外部のネットワークから分離された状態にある。また、予備の通信回線及び監視・制御等放送設備に付随して使用される通信回線は、閉域網の使用など適切な防御対策を行った上で使用されている。

・また、放送本線系は１対多による片方向のネットワーク構成となっており、その起点となる番組送出設備に対策を行うことで、効率的・効果的に外部ネットワークからの分離の実施が可能な特徴を有し、併せて、**通信方式の違いによって外部ネットワークから分離されている現状は、結果的にサイバーセキュリティの確保に対して優位な構成になっている**ものと考えられる。

【参考】放送設備のIP化に伴う安全・信頼性確保のための措置及び解説（2）

【措置についての解説（続き）】

・放送設備のＩＰ化に伴い、番組送出設備における伝送回線の一部又は全部がＩＰ回線となり、当該回線には、放送の映像・音声を伝送するための専用規格（SMPTE2110等）が用いられるものの、広義においてはインターネット・ＩＰ網等と同じ通信方式となる。

・番組送出設備がＩＰ化された場合には、放送事業者の施設内に構築された情報系ＬＡＮ、制御系ＬＡＮ、社内ＬＡＮ等の内部ネットワークを介して、**インターネット等の第三者がアクセス可能な外部ネットワークと接続された状態になることを前提としたサイバーセキュリティ確保のための措置が必要**となる。

・具体的な措置内容は、従来からの境界防御の強化のほか、**ゼロトラストやサイバーレジリエンス等の新しいセキュリティ対策の概念も考慮**したものであるほか、**放送継続のために求められる可用性の担保及び経済合理性との両立についても考慮**する必要がある。

・放送設備の安全・信頼性の確保については、従来から規模の異なる様々な放送事業者が事業環境や影響の度合いなどを勘案しながら、経済合理性も踏まえて適切な対策を講じてきたこと、並びにサイバーセキュリティを取り巻く環境の変化に伴い有効な措置内容も時々刻々と変化する可能性があること等を踏まえて、**放送事業者がその責任と判断において現実的な対策を柔軟に選択できるよう、対策の目的や概略を示しつつも具体的な措置内容については幅を持たせることが望ましい**。

・放送設備のＩＰ化を前提として検討した新たな措置内容については、サイバー脅威の巧妙化・深刻化およびサイバーセキュリティ対策技術の高度化等の状況を踏まえると、現行の放送設備においても適用が推奨され得るものと考えられる。

【参考】放送設備のIP化に伴う安全・信頼性確保のための措置及び解説（3）

【具体的な措置内容の例】

１．放送本線系入力となる番組送出設備について、外部ネットワークからの不正接続対策、マルウェア感染防止対策、サイバー事案による障害からの早期復旧を図るための次の措置又はこれと同等と認められる措置

- 外部ネットワークとの接続を行う場合において、ファイアーウォールの設置、内部ネットワークへの不正侵入の検知及び当該侵入の遮断、許可リスト等に基づく不正プログラムの実行阻止、構成装置の各種セキュリティ設定強化等の措置を講じること。
- 構成装置のシステム設定等に関して、初期整備および変更等の機会をとらえたバックアップの実施等の措置を講じること。

※下線部は、現行の措置内容からの変更点。

＜具体的な措置内容についての解説＞

・ＩＰ化に伴い番組送出設備が外部ネットワークと接続された状態になるため、障害発生時、その原因がサイバー事案によるものか否かを切り分け、迅速な対応を行うための措置が必要があり、具体的には、既定のファイアーウォール設置のほか、**外部ネットワークから内部ネットワークへの不正侵入の検知・遮断等の不正接続対策を講じることが必要**である。

・また、ゼロトラストの概念を踏まえつつ、内部ネットワークに侵入したマルウェア等を不活性化する措置が必要であり、**許可リスト等に基づく不正プログラムの実行阻止等のマルウェア感染防止対策を講じることが必要**である。

・さらに、サイバーレジリエンスの観点から、サイバー事案による障害から早期に放送を復旧するための措置も重要であり、**初期整備および変更等の機会をとらえたバックアップの実施等の早期復旧対策を講じることが必要**である。

【参考】放送設備のIP化に伴う安全・信頼性確保のための措置及び解説（4）

【具体的な措置内容の例】

２．放送設備に接続される監視・制御及び保守に使用される回線について、外部ネットワークからの不正接続対策を行うための次の措置又はこれと同等と認められる措置

- 専用回線又はＶＰＮ回線（インターネット等の公衆回線網上において、認証や暗号化等の技術を利用して保護された仮想専用線をいう。）※１の使用、ポート番号（インターネットに接続された電気通信設備において通信に使用されるプログラムを識別するために割り当てられる番号をいう。）若しくはアイ・ピー・アドレスによる接続制限又はＩＤ及びパスワード、所有物認証及び生体認証等※２により、権限を有する者だけが接続できるようにする措置を講じること。

※１ ＶＰＮ回線を構成する機器の安全性確保に留意し、ソフトウェアの更新及びセキュリティパッチの適用等を適時適切に実施する必要がある。

※２ 複数の認証を組み合わせた多要素認証を使用することが望ましい。

- 未使用時は、当該回線の接続を断とする措置を講じること。

※下線部は、現行の措置内容からの変更点。

＜具体的な措置内容についての解説＞

・ＶＰＮ回線の使用は、放送設備に外部からセキュアに接続するための手段として有効であるが、ＶＰＮ回線を構成する機器の脆弱性を悪用したサイバー事案が頻発している状況を踏まえ、ソフトウェアの更新及びセキュリティパッチの適用等を適時適切に実施することで、**ＶＰＮ機器を最新の状態に維持する必要がある旨を追記**する。

・アクセス権限の設定について、ＩＰ及びパスワードによる「知識認証」のほか、ワンタイムパスワードや電子証明書による「所有物認証」、指紋・顔・声紋・虹彩等の身体的な特徴を用いる「生体認証」等、**よりセキュリティレベルの高い認証方法を明記するとともに、これらを組み合わせた「多要素認証」の使用を推奨する旨を追記**する。

【参考】放送設備のIP化に伴う安全・信頼性確保のための措置及び解説（5）

【具体的な措置内容の例】

３．設備の導入時及び運用・保守時におけるソフトウェアの点検について、不正プログラムによる被害を防止するための次の措置又はこれと同等と認められる措置

- 放送設備のネットワークからの分離・遮断の措置及び不正プログラムの感染防止の措置を講じること。
- 定期的なウイルスチェック等による不正プログラムの早期検出の措置を講じること。

※下線部は、現行の措置内容からの変更点。

＜具体的な措置内容についての解説＞

・放送設備については、いかなる時も放送を継続するための可用性を確保する必要があり、動作に影響を与える可能性のある常駐型ウイルス対策ソフト等を使用することは困難である。

・それゆえに、設備の導入時及び運用・保守時におけるソフトウェアの点検においては、最新のウイルス定義（シグネチャ）でのウイルスチェック等による不正プログラムの早期検出の措置を講じる必要があることから、**非常駐型のツール等を使用した定期的なウイルスチェックを具体的な措置内容として追記**する。

・なお、一度の保守作業において対象となる設備及び作業時間には制約があると考えられることから、これらに応じて対象設備を限定するなど、放送継続に影響を及ぼさないことを前提として措置すべき内容である。

【参考】放送設備のIP化に伴う安全・信頼性確保のための措置及び解説（6）

【具体的な措置内容の例】

４．放送設備に対する物理的なアクセス管理について、機密性が適切に配慮されるための次の措置又はこれと同等と認められる措置

- 番組送出設備に対し、ＩＤカード、テンキー錠又は有人による入退室の管理等を行う措置及び監視・制御回線、保守回線に係る機器の設置場所に対し公衆が容易に立ち入ることができないようにするための施錠その他の必要な措置を講じること。
- 外部記録メディア等を介した不正プログラムへの感染防止のための不要なポート／スロットの無効化又は閉塞処理、外部記録メディア接続前のウイルスチェック等の措置を講じること。

※下線部は、現行の措置内容からの変更点。

＜具体的な措置内容についての解説＞

・外部記録メディアを介した不正プログラムへの感染の防止について、**不要なＵＳＢポートやＳＤカードスロット等を無効化又は閉塞処理すること、外部記録メディアを放送設備に接続する前にウイルスチェックを行うことを具体的な措置内容として追記**する。

【参考】放送設備のIP化に伴う安全・信頼性確保のための措置及び解説（7）

【具体的な措置内容の例】

５．放送設備の運用・保守に際して、業務を確実に実施するための組織体制の構築及び業務の実施に係る規程若しくは手順書の整備に関する次の措置又はこれと同等と認められる措置

- サイバー事案の発生を迅速に検知するための定常的な監視、並びに発生時の対応策及び再発防止策について、早期復旧及び対応能力向上の観点も踏まえ、事故報告を含む対応を迅速かつ確実に実施するための規程又は手順書を整備する措置を講じること。
- サイバー事案が発生した場合の連絡先の整備及び報告実施等の手順書化、放送設備のソフトウェアの更新等設備の運用・保守等について、実施方法を定める規程又は手順書を整備する措置を講じること。

※下線部は、現行の措置内容からの変更点。

＜具体的な措置内容についての解説＞

・サイバー脅威は日々高度化・巧妙化しており、その被害も深刻度を増している状況にあることから、サイバー事案を防止するための対策を講じるだけでなく、ゼロトラストの概念を踏まえつつ、サイバー事案の発生を迅速に検知するための措置を定常的に実施するとともに、サイバー事案が発生した場合の体制や手順を事前に整備し、被害を最小限にとどめ、なるべく早く業務を復旧させる能力、いわゆるサイバーレジリエンスの向上を図ることも重要である。

・これらを踏まえ、サイバー事案の発生時の対応策及び再発防止策に関する規程若しくは手順書の整備に際しては、**サイバー事案の早期検知のための定常的なセキュリティ監視、放送停止等の障害からの早期復旧及びサイバー事案に対する対応能力の向上についても重要な観点として考慮すべきである旨を追記**する。

安全・信頼性に関する技術基準への反映（1）

IP化に伴う措置内容	現行の措置内容
➢ 放送本線系入力となる番組送出設備について、外部ネットワークから**の不正接続対策、マルウェア感染防止対策、サイバー事案による障害からの早期復旧を図る**ための次の措置又はこれと同等と認められる措置	➢ 放送本線系入力となる番組送出設備について、外部ネットワークから隔離するための次の措置又はこれと同等と認められる措置
• **外部ネットワークとの**接続を行う場合**において、**ファイアーウォールの設置**、内部ネットワークへの不正侵入の検知及び当該侵入の遮断、許可リスト等に基づく不正プログラムの実行阻止、構成装置の各種セキュリティ設定強化**等の措置 • **構成装置のシステム設定等に関して、初期整備および変更等の機会をとらえたバックアップの実施等の措置**	• 原則として、第三者が接続可能な外部ネットワークとの接続を行わない措置 • やむを得ず接続を行う場合には、ファイアーウォールの設置又は不正接続対策等の措置
➢ 放送設備に接続される監視・制御及び保守に使用される回線について、外部ネットワークからの不正接続対策を行うための次の措置又はこれと同等と認められる措置	➢ 放送設備に接続される監視・制御及び保守に使用される回線について、外部ネットワークからの不正接続対策を行うための次の措置又はこれと同等と認められる措置
• 専用回線又はVPN回線※1の使用、ポート番号若しくはアイ・ピー・アドレスによる接続制限又はID及びパスワード**、所有物認証及び生体認証等**※2により、権限を有する者だけが接続できるようにする措置 **※1 回線を構成する機器の安全性確保に留意し、ソフトウェアの更新及びセキュリティパッチの適用等を適時適切に実施する必要がある。** **※2 複数の認証を組み合わせた多要素認証を使用することが望ましい。** • 未使用時は回線を通じた接続を遮断する等の措置	• 専用回線又はVPN回線の使用、ポート番号若しくはアイ・ピー・アドレスによる接続制限又はID及びパスワードにより権限を有する者だけが接続できるようにする措置 • 未使用時は回線を通じた接続を遮断する等の措置

安全・信頼性に関する技術基準への反映（2）

IP化に伴う措置内容	現行の措置内容
➢ 設備の導入時及び運用・保守時におけるソフトウェアの点検について、不正プログラムによる被害を防止するための次の措置又はこれと同等と認められる措置	➢ 設備の導入時及び運用・保守時におけるソフトウェアの点検について、不正プログラムによる被害を防止するため、放送設備のネットワークからの分離・遮断の措置及び不正プログラムの感染防止の措置
・放送設備のネットワークからの分離・遮断の措置及び不正プログラムの感染防止の措置 ・**定期的なウイルスチェック等による不正プログラムの早期検出の措置**	
➢ 放送設備に対する物理的なアクセス管理について、機密性が適切に配慮されるための次の措置又はこれと同等と認められる措置	➢ 放送設備に対する物理的なアクセス管理について、機密性が適切に配慮されるための次の措置又はこれと同等と認められる措置
・番組送出設備に対し、IDカード、テンキー錠又は有人による入退室の管理等を行う措置及び監視・制御回線、保守回線に係る機器の設置場所に対し公衆が容易に立ち入ることができないようにするための施錠その他の必要な措置 ・外部記録メディア等を介した不正プログラムへの感染防止**のための不要なポート／スロットの無効化又は閉塞処理、外部記録メディア接続前のウイルスチェック等**の措置	・番組送出設備に対しIDカード、テンキー錠又は有人による入退室の管理等を行う措置及び監視・制御回線、保守回線に係る機器の設置場所に対し公衆が容易に立ち入ることができないよう施錠その他の必要な措置 ・外部記録メディア等を介した不正プログラムへの感染防止の措置

安全・信頼性に関する技術基準への反映（3）

IP化に伴う措置内容	現行の措置内容
➢ 放送設備の運用・保守に際して、業務を確実に実施するための組織体制の構築及び業務の実施に係る規程若しくは手順書の整備に関する次の措置又はこれと同等と認められる措置	➢ 放送設備の運用・保守に際して、業務を確実に実施するための組織体制の構築及び業務の実施に係る規程若しくは手順書の整備に関する次の措置又はこれと同等と認められる措置
• サイバー事案の発生**を迅速に検知するための定常的な監視、並びに**発生時の対応策及び再発防止策について、**早期復旧及び対応能力向上の観点も踏まえ、**事故報告を含む対応を迅速かつ確実に実施するための規程又は手順書を整備する措置	• サイバー事案の発生時の対応策及び再発防止策について、事故報告を含む事後対応を迅速かつ確実に実施するための規程又は手順書を整備する措置
• サイバー事案が発生した場合の連絡先の整備及び報告実施等の手順書化、放送設備のソフトウェアの更新等設備の運用・保守等について、実施方法を定める規程又は手順書を整備する措置	• サイバー事案が発生した場合の連絡先の整備及び報告実施等の手順書化、放送設備のソフトウェアの更新等設備の運用・保守等について、実施方法を定める規程又は手順書を整備する措置