情報通信審議会　情報通信技術分科会

放送システム委員会　報告（案）

情報通信審議会諮問第２０３１号「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」について

目　次

Ⅰ　検討事項

情報通信審議会諮問第２０３１号「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」のうち「放送設備のＩＰ化に伴う安全・信頼性に関する技術的条件」について検討を行い、本報告を取りまとめた。

Ⅱ　委員会及び作業班の構成

放送システム委員会の構成員は、別表１のとおり。

なお、検討の促進を図るため、委員会の下に放送設備安全信頼性検討作業班を設置し、検討を行うこととした。放送設備安全信頼性検討作業班の構成員は、別表２のとおり。

Ⅲ　検討経過

１　委員会での検討

・第 76 回委員会（令和４年 10 月 27 日）

検討内容、検討項目及び検討スケジュール等について、検討を行った。また、検討の促進を図るため、作業班において検討を行うこととした。

・第 79 回委員会（令和５年９月 19 日）

放送設備安全信頼性検討作業班報告を受けて、放送システム委員会報告（案）について、検討を行った。また当該報告（案）について速やかにパブリックコメントを行うこととした。

２　作業班での検討

・第１回作業班（令和４年 12 月６日）

放送システム委員会からの指示を受けて、今後の調査の進め方を確認した。また、放送設備のＩＰ化・クラウド化・集約化に関する技術動向について NHK 放送技術研究所及び構成員から状況を聴取した。

・第２回作業班（令和５年１月 30 日）

放送設備に関連する業務及びサイバーセキュリティに関する動向について構成員から状況を聴取した。また、検討対象となる番組送出設備の標準モデルを検討した。

・第３回作業班（令和５年２月 21 日）

放送事業者における設備の状況について構成員から状況を聴取した。また、

番組送出設備の標準モデルに基づく技術的条件等を検討した。

・第４回作業班（令和５年３月 15 日、非公開で開催）
　詳細な技術情報の開示がサイバー攻撃等を誘発するリスクを含むため、非公開の会合にて審議を行った。
　放送設備の IP 化に関する導入計画等についてテレビ大阪株式会社及び構成員から状況を聴取した。また、番組送出設備の標準モデルに基づく技術的条件等を検討した。

・第５回作業班（令和５年３月 27 日、非公開で開催）
　詳細な技術情報の開示がサイバー攻撃等を誘発するリスクを含むため、非公開の会合にて審議を行った。
　放送設備の IP 化に伴うサイバーセキュリティ対策の方向性について構成員から状況を聴取した。

・第６回作業班（令和５年６月 22 日、非公開で開催）
　詳細な技術情報の開示がサイバー攻撃等を誘発するリスクを含むため、非公開の会合にて審議を行った。
　米国及び欧州における番組送出設備のＩＰ化・クラウド化に係る最新動向等に関する調査結果について株式会社三菱総合研究所から状況を聴取した。また、番組送出設備の標準モデルに基づく技術的条件等を検討するとともに、作業班報告の構成等について調査を行った。

・第７回作業班（令和５年７月 14 日）
　放送設備安全信頼性検討作業班報告（案）の検討を行った。

・第８回作業班（令和５年９月４日～９月８日、メール審議を実施）
　放送設備安全信頼性検討作業班報告を取りまとめた。

Ⅳ　検討概要

別紙のとおり。

別表 1

情報通信審議会 情報通信技術分科会
放送システム委員会 構成員

（敬称略）

氏 名		所属・役職
主査 委員	伊丹 誠	東京理科大学 先進工学部 電子システム工学科 教授
主査代理 専門委員	甲藤 二郎	早稲田大学 基幹理工学部 教授
主査代理 専門委員	都竹 愛一郎	名城大学 理工学部 教授（第 76 回まで）
委員	大島 まり	東京大学 大学院 情報学環／生産技術研究所 教授（第 76 回まで）
〃	高田 潤一	東京工業大学 環境・社会理工学院 学院長／教授
専門委員	雨宮 明	一般社団法人日本 CATV 技術協会 筆頭副理事長
〃	井家上 哲史	明治大学 理工学部 教授
〃	岩崎 裕江	東京農工大学 大学院工学研究院 先端情報科学部門 教授/東北大学 タフ・サイバーフィジカル AI 研究センター 特任教授
〃	上園 一知	一般社団法人日本ケーブルラボ 技術部 主任研究員
〃	大槻 知明	慶應義塾大学 理工学部 情報工学科 教授
〃	児玉 俊介	一般社団法人電波産業会 専務理事
〃	後藤 薫	国立研究開発法人情報通信研究機構 電磁波研究所 電磁波標準研究センター 電磁環境研究室 標準較正グループ グループリーダー
〃	関根 かをり	明治大学 理工学部 教授
〃	丹 康雄	北陸先端科学技術大学院大学 副学長（リカレント教育担当）・先端科学技術研究科 教授
〃	豊嶋 守生	国立研究開発法人情報通信研究機構 ネットワーク研究所ワイヤレスネットワーク研究センター 研究センター長
〃	山田 孝子	関西学院大学 副学長（教務機構長） 総合政策学部 教授

別表 2

情報通信審議会 情報通信技術分科会 放送システム委員会
放送設備安全信頼性検討作業班 構成員

（敬称略）

氏 名		所属・役職
主　　任	甲 藤　二 郎	早稲田大学 理工学術院 基幹理工学部 教授
	新 井　勇 太	一般社団法人日本民間放送連盟 企画部 主事
	井 上　大 介	国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所 サイバーセキュリティネクサス ネクサス長
	上 原　道 宏	一般社団法人ICT-ISAC 事務局 次長
	奥 沢　賢 一	株式会社文化放送 アドミニストレーション局長 兼 テックイノベーション部長
	小田島　健秀	株式会社フジテレビジョン 技術局 局次長職 放送技術担当
	川 島　　修	株式会社エフエム東京 執行役員 管理本部 技術局長
	木 村　正 人	日本電信電話株式会社 技術企画部門 セキュリティ・アンド・トラスト室 次長
	倉 田　晃 二	日本放送協会 技術局 管理部（施設） エキスパート
	佐々木　博之	パナソニック エンターテインメント＆コミュニケーション株式会社 VSBU 技術センター ソフト開発部 アライアンス推進課
	杉 澤　洋 輝	一般社団法人 日本コミュニティ放送協会 副代表理事
	鈴 木　英 樹	株式会社日立国際電気 プロダクト本部 放送機器改革推進プロジェクト 副技師長
	砂 崎　俊 二	株式会社放送衛星システム 総合企画室 専任部長
	田 中　亮 一	日本電気株式会社 クロスインダストリーBU メディア統括部 第二メディアグループ 第四メディア営業チーム ソリューションプロフェッショナル
	樽 見　敏 夫	株式会社テレビ東京 技術局 専任局長
	秦　　慎 二	スカパーJSAT株式会社 メディア事業部門 メディア技術本部 アップストリーム部 部長
	藤 田　和 義	株式会社テレビ朝日 技術局 技術業務部 渉外担当部長
	三 腰　稔 洋	東芝インフラシステムズ株式会社 社会システム事業部 通信放送システム技術部 放送技術担当 マネージャ
	村 上　信 高	株式会社TBSテレビ メディアテクノロジー局 ステーション統括部 担当部長
	室 田　孝 昭	日本テレビ放送網株式会社 技術統括局 放送実施部 部長
	山 森　尋 史	一般社団法人衛星放送協会 技術委員会 委員
	横 山　敦 司	株式会社WOWOW 技術センター運用技術ユニット ユニット長
	吉 岡　克 成	横浜国立大学大学院 環境情報研究院 教授

別紙

検　討　概　要

第１章　背景

１－１　放送ネットワークインフラの将来像

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）を中心として、放送設備のＩＰ化・クラウド化・集約化が進むものと想定される。

「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（番組送出設備）に関する現状と課題、並びに今後の方向性を取りまとめた上で、「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」と提言されている。

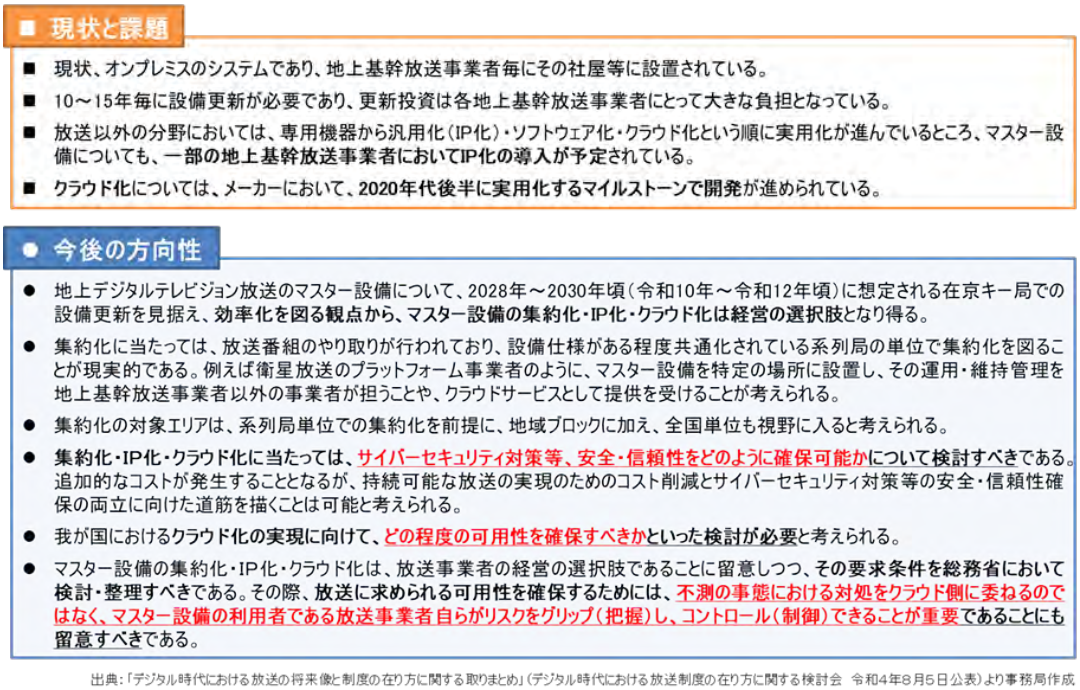


図１－１－１　**マスター設備（番組送出設備）に関する動向**

放送は、緊急災害時を含め、常に国民生活に必需な情報をあまねく届けるという高い公共性を持つことから、その安全・信頼性が求められる。そのため、放送の施設設備に対しては事故の発生を未然に防止するための措置及び発生した時の

早期の復旧を目指した措置を求めている。具体的には、予備機器の配備、停電対策、故障検出、応急復旧機材の配備、サイバーセキュリティの確保等、安全・信頼性に関する技術基準を設けているとともに、重大事故が発生した場合における報告等を義務付けている。

放送設備のＩＰ化・クラウド化・集約化が進展することで、放送設備がインターネット等の外部ネットワークに接続され、その設置場所及び維持・管理の様態が変化する可能性があることから、放送の安全・信頼性確保に関する新たな技術課題が生じることが想定される。

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、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行う必要がある。

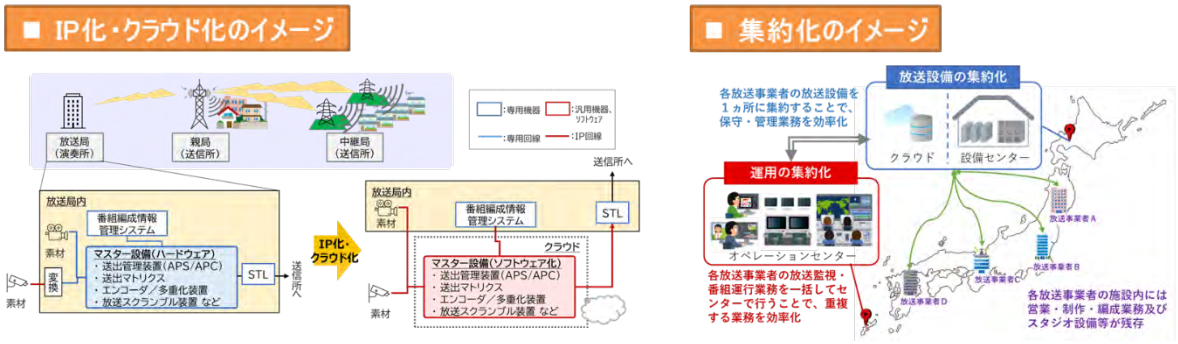


図１－１－２　**放送設備のＩＰ化・クラウド化・集約化のイメージ**

１－２　放送分野におけるＩＰ化・クラウド化等の動向

１－２－１　放送設備のＩＰ化・クラウド化・集約化の概要

（１）　放送設備のＩＰ化の概要

従来の地上デジタルテレビジョン放送の放送設備では、主としてＳＤＩ（Serial Digital Interface）と呼ばれる高速シリアル・インタフェース規格により各装置が接続されている。ＳＤＩは、非圧縮のデジタル映像信号とデジタル音声信号を、1本の同軸ケーブルで送ることができる。

ＳＤＩは放送設備において長年使用されてきた規格であるものの、放送業界の技術進歩に対応する上で、下記のような問題点が発生している。

- 伝送速度が最大でも 12 Gbps 程度にとどまる。
- 機器間を１対１で接続するため、送出マトリクス等には多数のケーブルを接続しなければならない。
- 同軸ケーブルを使用した場合、信号減衰により伝送距離が最大 100m 程度である。
- 同軸ケーブルは、曲がりにくく取り回しが不便。
- ＩＰ化された放送設備との親和性が悪い（装置間の接続において、ＩＰ／ＳＤＩの変換が必要）。
- ソフトウェア化やコストダウンに繋がるＰＣサーバやネットワークスイッチなどの汎用ＩＴ機器の利用が妨げられている。
- ＳＤＩ対応の機器やケーブルが将来的に安定供給されない可能性がある。

放送設備のＩＰ化とは、放送設備における装置および伝送回線等がＩＰに対応したものに置き換わることである。ＳＤＩとＩＰインタフェースの伝送速度を図１－２－１－１に、ＳＤＩとＩＰインタフェースの特徴を図１－２－１－２に示す。

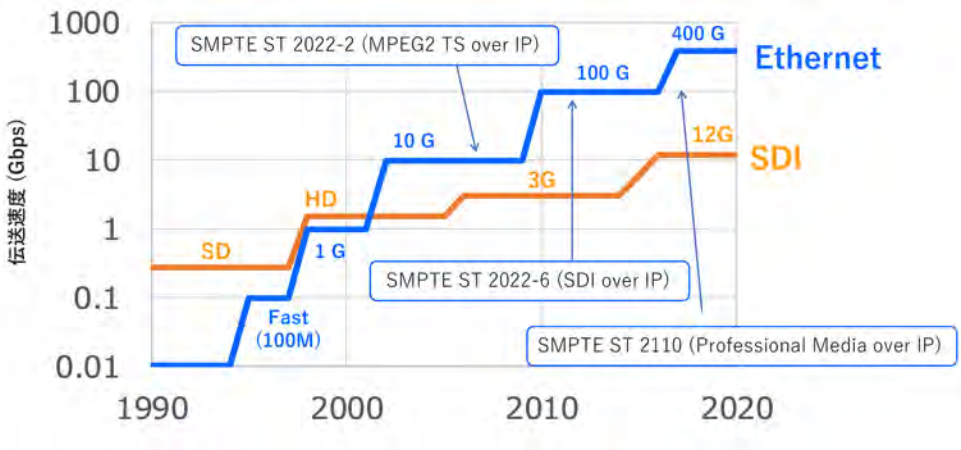


図１－２－１－１　ＳＤＩとＩＰインタフェースの伝送速度

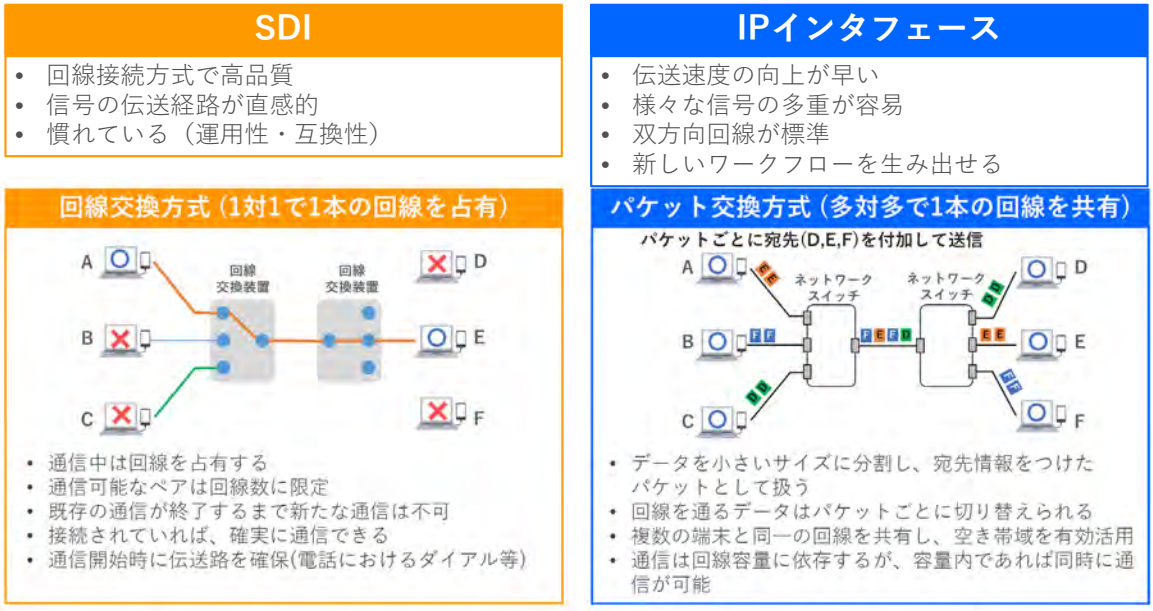
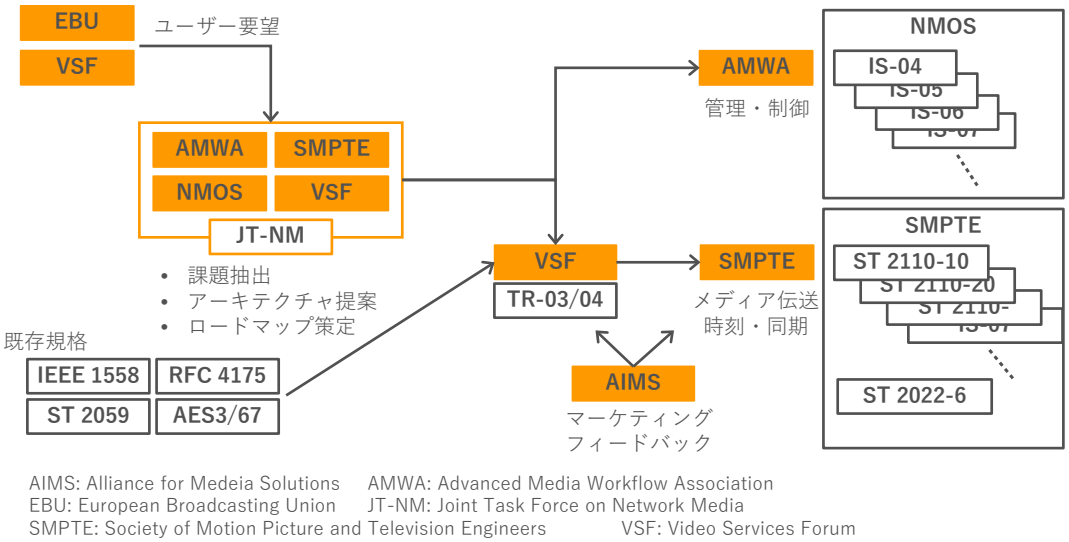


図１－２－１－２　ＳＤＩとＩＰインタフェースの特徴

また、放送設備のＩＰ化に関する標準化も進みつつある。

国際的には、ＥＢＵ（European Broadcasting Union）、ＶＳＦ（Video Services Forum）、ＡＭＷＡ（Advanced Media Workflow Association）、ＳＭＰＴＥ（Society of Motion Picture and Television Engineers）等の業界団体および標準化団体において、ＩＰインタフェースによるメディア伝送、時刻・同期、制御、設定・監視、セキュリティ等に関する標準化が行われている。



AIMS: Alliance for Medeia Solutions　AMWA: Advanced Media Workflow Association
EBU: European Broadcasting Union　JT-NM: Joint Task Force on Network Media
SMPTE: Society of Motion Picture and Television Engineers　VSF: Video Services Forum

図１－２－１－３　放送設備のＩＰ化に関する国際標準化活動

国内では、電波産業会（ARIB）において番組制作用ＩＰインタフェースに関する標準化活動が行われており、SMPTE 文書および AMWA 文書等の国際規格に準拠しつつ国内の放送の実情も踏まえて、国内への技術普及を目的とした日本語規格の策定、放送事業者の利便性向上に寄与する技術文書の策定等の取組が進められている。

（２）放送設備のクラウド化の概要

「クラウド」とは、「クラウドコンピューティング（Cloud Computing)」を略した呼び方で、データやアプリケーション等のコンピューター資源をネットワーク経由で利用する仕組みのことである。クラウドにより、ユーザは大規模なインフラやソフトウェアを持たずとも、インターネット上で必要に応じてサービスを利用できる。この仕組みを用いて提供されるサービスを「クラウドサービス」と称する。放送設備のクラウド化とは、クラウドサービスを用いて放送設備の機能を実現することである。

クラウドには、パブリッククラウド（Public Cloud）とプライベートクラウド（Private Cloud）の２種類がある。

パブリッククラウドは、事業者の施設内に用意したクラウド基盤を、事業者が広く一般の自由な利用に向けて、インターネット経由で提供する。利用者は、ハードウェアやネットワーク、その他のデータセンター設備を所有することはなく、事業者のリソースをマルチテナント（不特定の複数の利用者）で共有する。通信の高速性、安定性、あるいは安全性を確保するために、仮想プライベートネットワーク（ＶＰＮ）や専用線による接続を提供し、プライベートクラウドのように利用できるサービスもある

プライベートクラウドは、単一の企業(組織)、または同じ企業グループ内で使用するための専用のクラウド基盤である。プライベートクラウドは、システム基盤の存在場所によって２つに分類される。１つは自社内でクラウド環境を構築して提供する形態の「オンプレミス型」であり、もう１つは利用者の所有するシステム基盤を事業者が事業者の施設内に用意する「ホスティング型」である。どちらも専有のクラウド環境として提供されるが、前者は独自のカスタマイズや管理が可能であり、後者は導入、管理、運用等の一部を事業者が代行するのが一般的である。

クラウドサービスの利用には下記のメリット[注1]がある。

①コスト構造の平準化
- ・定期的な設備投資が不要
- ・固定資産の削減
- ・予備品不要

②ランニング費の削減
- ・電気代
- ・設置スペース
- ・機器保守費
- ・リプレース不要
- ・保守人員の削減

③利用に応じた課金

④柔軟性、拡張性

・リソース追加の柔軟性

・必要な時にすぐに利用可能

・クラウド前提のサービスとの親和性

注１ 主としてパブリッククラウドおよびプライベートクラウド（ホスティング型）におけるメリットであり、プライベートクラウド（オンプレミス型）には該当しない場合がある。

（３）放送設備の集約化の概要

放送設備の集約化（センター化）は、以下の２つの要素で構成される。

・放送設備の集約化：

各放送事業者の設備を１か所に集約することで、保守・管理業務を効率化

・オペレーションのセンター化：

各放送事業者の放送監視・番組運行業務を一括してセンターで行うことで、重複する業務を効率化

なお、放送設備のＩＰ化およびクラウド化は、集約化を行うための必要条件ではないが、ＩＰ化・クラウド化が進展することにより、ネットワークを介して集約化の実現が容易になると考えられる。

放送設備の集約化に関する想定ケースの例を、図１－２－１－４、図１－２－１－５、図１－２－１－６及び図１－２－１－７に示す。

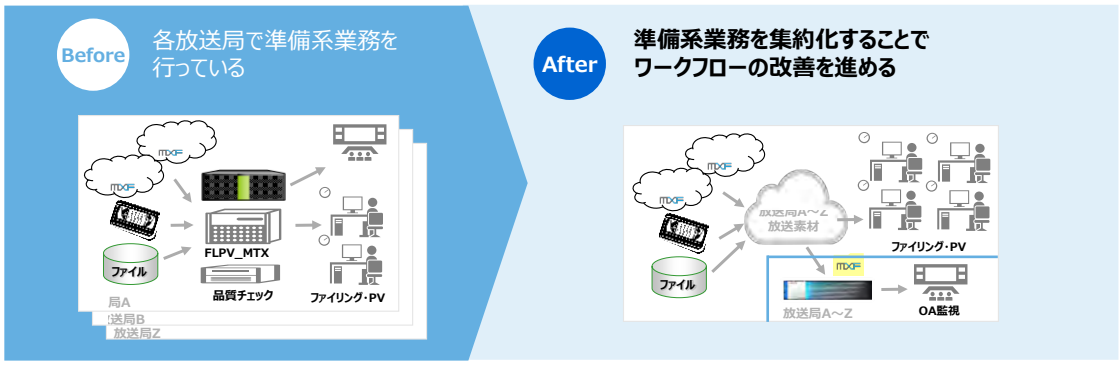


図１－２－１－４　**放送設備の集約化に関する想定ケース例①**

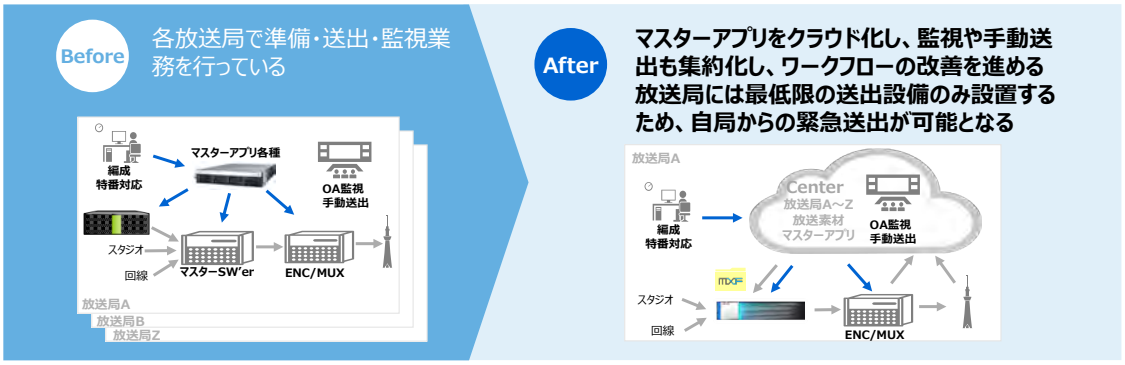


図１－２－１－５　放送設備の集約化に関する想定ケース例②

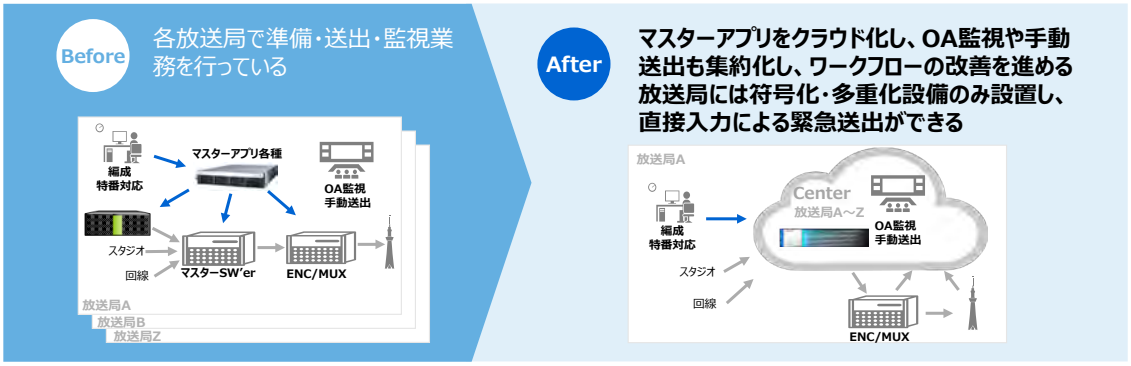


図１－２－１－６　放送設備の集約化に関する想定ケース例③

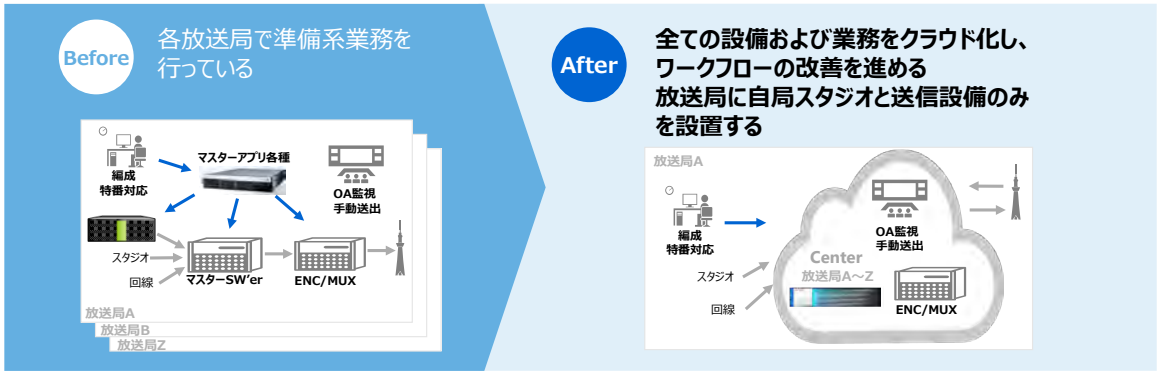


図１－２－１－７　放送設備の集約化に関する想定ケース例④

１－２－２　番組制作環境等におけるＩＰ化の進展

地上デジタルテレビジョン放送の演奏所で行われる業務には、番組送出設備の操作を中心に放送準備、番組送出および放送監視等を実施するマスター業務だけでなく、番組編成業務、番組制作業務、回線業務、データ放送業務および字幕業務等が存在する。マスター業務以外の業務では、演奏所外の施設や設備との間で番組素材等のやりとりを行う場合が多く、マスター業務に先行してＩＰ化が進んでいる状況にある。

図１－２－２－１　地上デジタルテレビジョン放送の演奏所業務

また、番組制作環境をＩＰ化することにより、演奏所外を含めた業務の効率化が実現される可能性が高まる。

例えば、図１－２－２－２に示すリモート制作では、中継先での機材や人員を減らすことが可能である。また、図１－２－２－３に示すリソース共有では、離れた場所の機材が使用可能になり、稼働率の向上が期待できる。一方で、ネットワーク回線のための費用は増加すると考えられる。

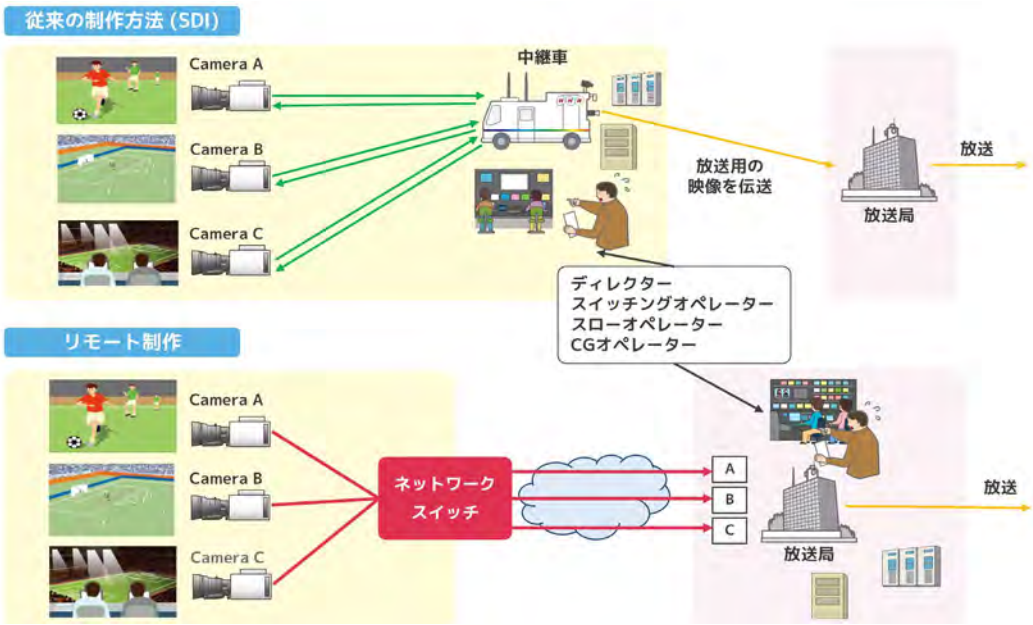


図１－２－２－２　ＩＰ化により実現できるリモート制作の例

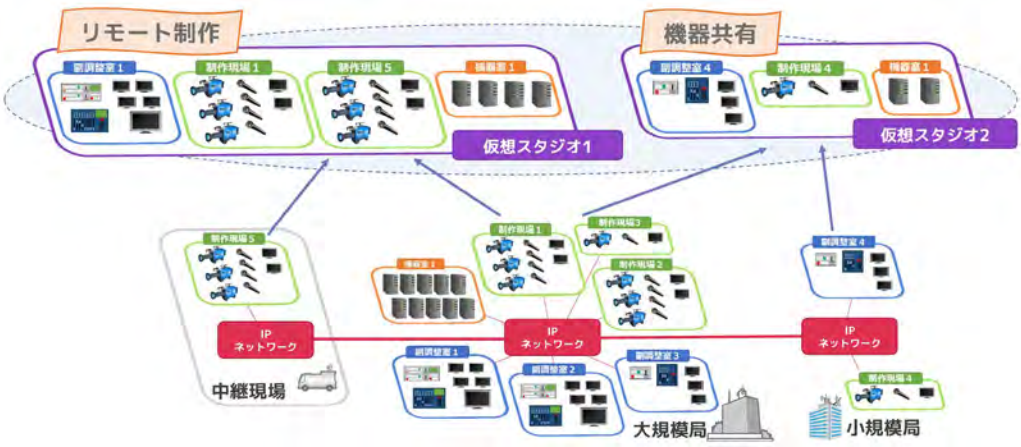


図１－２－２－３　ＩＰ化により実現できるリソース共有の例

１－２－３　日本における放送設備のＩＰ化に係る動向

１－２－３－１　技術開発動向

放送関係のＩＰ化は番組制作環境において先行してきたが、番組送出設備についても2016年頃より技術展示等が見られるようになった。

各放送設備開発メーカは放送局内設備全体のＩＰ化を進めるために、ＩＰマスターシステムの開発を進めている。ＩＰマスターシステムの主な機能は、番組送出プログラムに基づく番組やＣＭの送出、緊急放送などの割り込みが発生した場合の切り替え､字幕やＬ字情報の生成､運用状況の監視や放送品質のチェックなどである。また、番組やＣＭのサーバ機能も一体化することにより、効率的な送出管理を実現しようとしている。なお、放送信号へのエンコード、多重化、スクランブル化などについてはＩＰマスターシステムの開発対象外となっており、従来の設備を利用することを前提としている。

現在は、衛星放送や地上デジタルテレビジョン放送で導入が始まりつつある状況にある。また、Inter BEE 2022等で最新の機能をコンパクトな筐体で実現し、従来設備と同等の性能及び機能が実現できることを実証する展示が行われた。また、SMPTE ST 2110規格、AMWA NMOS仕様等の国際的な標準規格を採用するとともに、ARIB標準規格等に基づく伝送方式（ISDB-T方式／ISDB-S方式）やデータ放送、電子番組表等の機能にも対応した製品が開発されている。

１－２－３－２　放送事業者の導入状況

（１）　地上デジタルテレビジョン放送におけるＩＰ化の導入事例

ある放送事業者は、演奏所の建替・移転の機会をとらえて、番組送出設備、スタジオ設備､回線設備をすべてＩＰに対応したシステムで構築する予定である｡また、番組送出設備に関する状況としては、複数の放送事業者（同じ民放系列局）で設備仕様の一部を共通化し、同時期にＩＰマスターを導入する計画がある。

放送設備のＩＰ化の目的としては、下記のことが挙げられる。

- ネットワーク技術を採用することにより拡張性を持たせ、将来サービスの多様化に対応しやすくする。
- 放送専用機器を広く普及している汎用性のある情報システム機器に置き換えることで、機器の調達をしやすくする。
- 将来的なクラウドへの移行を視野に入れて、クラウドと親和性のあるＩＰに対応したシステムを構築することが効率的である。

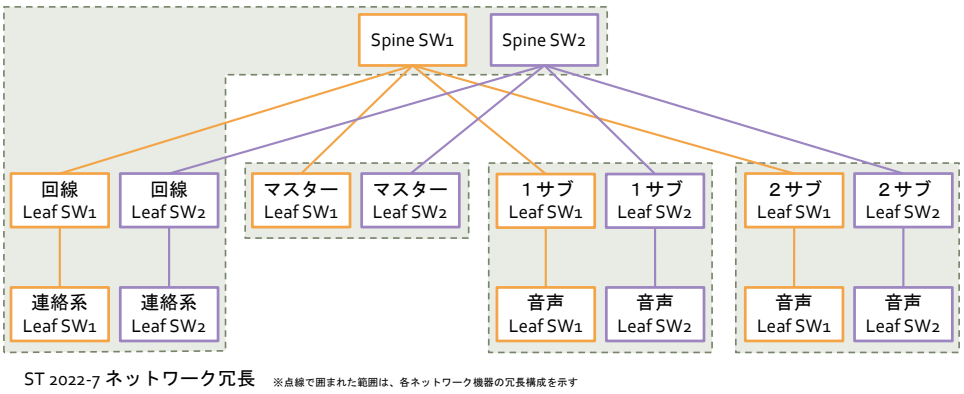


図１－２－３－２－１　地上デジタルテレビジョン放送におけるＩＰ化のネットワーク構成例

（２）　衛星基幹放送におけるＩＰ化の導入事例

ある放送事業者では、新４Ｋ８Ｋ衛星放送の開始および放送設備全体の更新の機会をとらえ、番組送出設備およびその関連設備に関してＩＰ化を順次進めている。

具体的には、多チャンネル化に対応するために送出マトリクスをＩＰ化するとともに、プレイアウト設備やエンコーダについても可能な範囲でソフトウェア化を実施している。

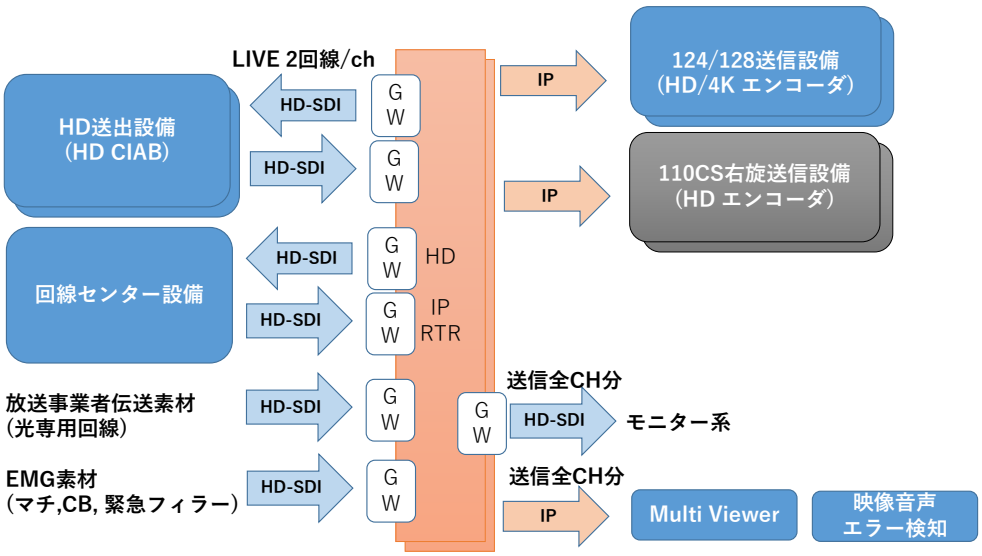


図１－２－３－２－２　**衛星基幹放送におけるＩＰ化の事例**

（３）地上デジタルテレビジョン放送におけるクラウド化の導入事例

ある放送事業者では、編成営業放送システム（営放システム）におけるクラウド活用が進んでいる。営放システムはテレビ局の基幹となるシステムであり、番組編成情報の管理、ＣＭ販売に関わる営業情報の管理、番組やＣＭを放送するための放送準備情報の管理、ＣＭ送出順やＣＭ素材の指定などの機能をもつ。民放系列局が個別に設備投資するのではなく、系列共通でサービス利用することによる効率化を図ることを目的として、標準的な営放システムをクラウド環境に実装し、系列局全体で利用している。クラウド実装された営放システムの導入効果を表１－２－３－２－１に示す。

表１－２－３－２－１　**クラウド実装された営放システムの導入効果**

課題	解決方法	導入効果
設備投資	サービス利用化	初期導入費、保守費の削減
設備の維持管理	設備の非所有	保守の労力、時間の削減
IT部門の体制の確保増強 担当者のスキルの維持向上	設備の共同利用、共同運営	運用ノウハウ共有、運用負荷軽減
災害対策	バックアップセンターとリソース確保	災害時でも通常と同じパフォーマンスを維持

また、同放送事業者では、放送コンテンツや番組素材に関して、マルチユースの促進や管理システムの統合によるコスト削減および業務効率化を目的として、複数

のサービス（地上波、ＢＳ、ＣＳ、配信、番組販売等）および系列局全体で放送コンテンツを共用することを可能とする総合コンテンツ管理システムをクラウドサービスを活用して構築している。クラウドサービスを活用した総合コンテンツ管理システムの構成例を図１－２－３－２－３、導入効果を表１－２－３－２－２に示す。

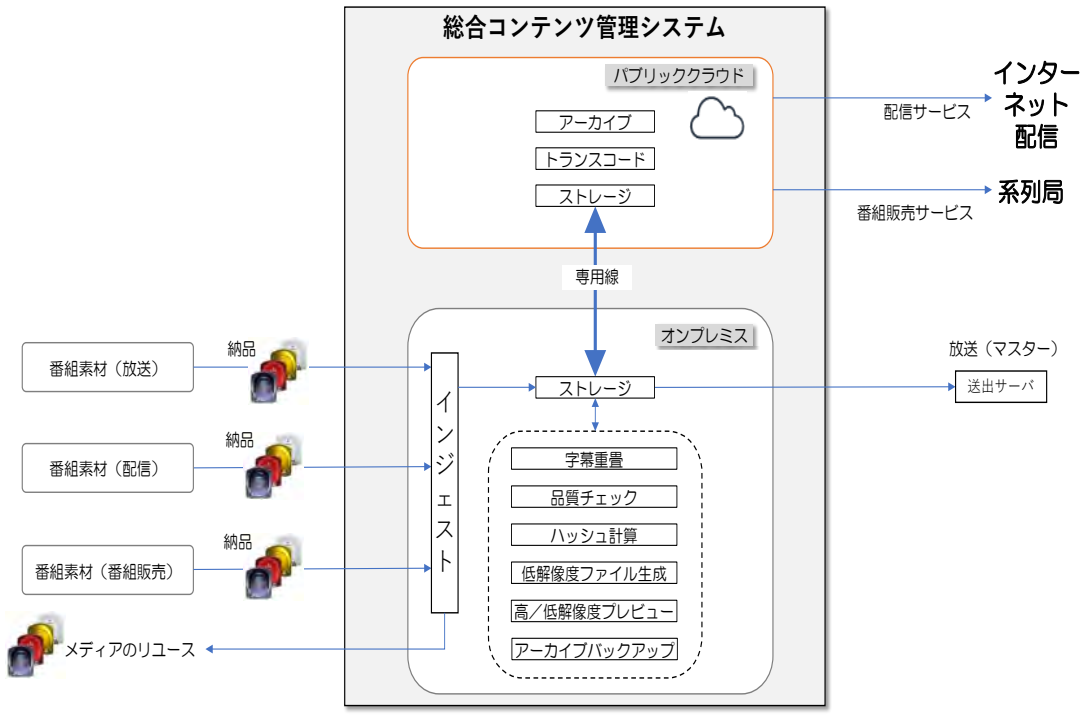


図１－２－３－２－３　クラウドサービスを活用した総合コンテンツ管理システムの構成例

表１－２－３－２－２　クラウドサービスを活用した総合コンテンツ管理システムの導入効果

従来	現在	導入効果
全て設備投資	設備投資＋従量課金。結果、保守費も削減	**設備投資費を抑えられる**
設計段階で最大値を見込んでおく	利用状況に応じて台数やスペックを変更	**サーバースペックを容易に変更可能**
システム全体でのコスト算出	コストの明細化が可能	**コストの見える化**
物理メディアを倉庫から出庫して運搬	端末操作でのオンラインアクセス	**番組素材に即アクセス可能**
メディアで保管	ファイルでクラウド保存	**メディアのリユースが可能**
手動でメディア変換（ダビング）	保存用メディアに依存しないため、原則不要	**アーカイブのマイグレーションが可能**

１－２－４　諸外国におけるＩＰ化・クラウド化等の動向

海外、特に米国及び欧州において、放送設備のＩＰ化・クラウド化に関する技術の進展が見られる。具体的には、業界団体や標準化団体において標準規格が策定され、放送設備メーカ等において番組送出設備を含む放送設備のＩＰ化・クラウド化に関する技術開発がなされ、実際に放送事業者における設備導入が進んでいる状況にある。

１－２－４－１　技術開発動向

米国及び欧州における放送設備メーカの取組については、ネットワーク機器の開発ベンダであるCisco Systemsや Rohde&Schwarzにより、放送分野がネットワーク機器の重要な導入分野の一つとして認識され、放送事業者における放送設備のＩＰ化に対する積極的な貢献が確認されるとともに、放送映像機器メーカであるImagine Communicationsや Grass Valleyによる、クラウド化も見据えたＩＰ化トータルソリューションの提供が行われている。

放送設備メーカによるＩＰ化の開発は、衛星放送、地上デジタルテレビジョン放送、音声放送など幅広い放送を対象として行われており、またＩＰ化の対象となる放送設備については、放送事業者の要望に従い、多様性に富んだ導入事例が確認されている。

特に、放送設備のＩＰ化にあたって根底となる伝送部分のＩＰ化については、ネットワーク機器開発ベンダの主力ビジネス領域であることもあり、すべての導入事例でＩＰ化が着手されている。また、Rohde&Schwarz 等により、メディア関係者が複数の映像コンテンツの制作作業を行う上で有益なソフトウェア等の提供が行われている。

１－２－４－２　放送事業者の導入状況

１－２－４－２－１　ＩＰ化の導入事例

米国及び欧州では、2017 年頃より放送設備のＩＰ化を積極的に進める放送事業者が複数確認されている。また、対象の放送設備もスタジオ設備、伝送、プロダクション（番組制作）、プレイアウト（番組送出）と幅広い適用ケースがある。

表１－２－４－２－１－１　米国及び欧州における放送事業者のＩＰ化事例

事業者	Sinclair Broadcast Group(Tennis Channel)	Sinclair Broadcast Group(RSN)	AP	BBC Wales［公共放送］	CANAL+	M6 Group	BCE	SVT［公共放送］	TV2［公共放送］
国	米国	米国	米国	英国	仏国	仏国	ルクセンブルク	スウェーデン	ノルウェー
IP化開始時期	2020年12月～	2021年6月～	2017年3月～	2020年9月～	・2016年11月～ ・2020年4月～	2022年7月～	2017年9月～	2019年2月	・2017年8月～ （一部導入予定）
IP化した場所	・伝送 ・プロダクション ・プレイアウト	・伝送 ・プロダクション ・プレイアウト	・伝送	・スタジオ設備 ・伝送 ・プロダクション ・プレイアウト	・スタジオ設備 ・伝送 ・プロダクション ・プレイアウト	・伝送 ・プロダクション ・プレイアウト	・スタジオ設備 ・伝送 ・プレイアウト	・スタジオ設備 ・伝送	・スタジオ設備 ・伝送 ・プロダクション ・プレイアウト
主な放送設備メーカ	・Diversified ・Imagine Communications	・Arista ・Diversified ・Encompass ・Imagine Communications	［公開情報なし］	・Cisco Systems ・dB Broadcast ・EVS ・Grass Valley ・VizRT	・Audinate ・Cisco Systems ・Grass Valley ・Lawo ・Videlio ・EVS ・Red Bee Media	・Evertz ・Harmonic	・Arista ・Grass Valley ・Harmonic ・Isilon ・Juniper ・Lawo ・SAM	・Arista ・Clear-Com ・Grass Valley ・Net Insight	・Cisco Systems ・Lawo ・Nevion ・Telenor
導入規格	・SMPTE ST 2110	・SMPTE ST 2110	・SMPTE ST 2022-6 ・SMPTE ST 2022-7	・SMPTE ST 2022-7 ・SMPTE ST 2110 ・AMWA/NMOS ・AES67	・SMPTE ST 2022-6 ・AES67 ・SMPTE ST 2059 ・SMPTE ST 2110	・SMPTE ST 2110	・SMPTE ST 2022-6/7 ・SMPTE ST 2110 ・AES67 ・VSF TR-04 ・PTPv2、PTPv1	・SMPTE ST 2110	・SMPTE ST 2022 ・SMPTE ST 2110 ・AES67

表１－２－４－２－１－２　参考：ＩＰ化に関する標準規格

団体	規格名	内容
SMPTE(Society of Motion Picture and Television Engineers)	SMPTE ST 2110	IPネットワークによるメディア伝送
	SMPTE ST 2022-6	SDI信号を丸ごとパケット化しIPネットワークで伝送を行う
	SMPTE ST 2022-7	冗長化された伝送路のシームレスな信号切り換え
	SMPTE ST 2059-1	時刻・メディア同期に関する規格（Epoch，及びEpoch時点の各A/V信号位相の定義）
	SMPTE ST 2059-2	時刻・メディア同期に関する規格（業務用A/V用途のPTPプロファイル）
AMWA(Advanced Media Workflow Association)	AMWA/NMOS	IPネットワークシステム間の接続制御やIPアドレスなどの管理・制御を行う。
AES(Audio Engineering Society)	AES67	オーディオ over IPに関する技術標準
VSF(Video Services Forum)	VSF TR-04	VSFが開発したスタジオ用IPマッピングの勧告

（１）　Sinclair Broadcast Group（その１）

Sinclair Broadcast Group（米国）の Tennis Channel は、2020 年 12 月より SMPTE ST 2110 をベースとする新たな放送設備へ移行した。

利用されている放送設備は、Imagine Communications 社（米国）が提供する統合プレイアウトプラットフォーム、Versio であり、SMPTE ST 2110 によるＩＰでのメディア伝送が実現されている。

Versio 上で動作する Versio Automation により、プレイアウト機能を AWS 上でクラウド化することも可能である。2021 年３月のマイアミ・オープンではクラウドからライブ中継を実施した実績を有しており、大規模なスポーツイベントをクラウド中継で放送した。

（２）　Sinclair Broadcast Group（その２）

Sinclair Broadcast Group の Bally Sports を始めとした RSN(Regional Sports Net)は、2021 年６月より SMPTE ST 2110 をベースとした施設へ移行した。

こちらも Versio が導入されており、ＩＰ化によって、ＳＤＩで必要だったサーバ数に比べ、大幅な削減を実現した。

災害復旧用プレイアウトやアーカイブの保存など、一部の機能をクラウドに移行している。

（３）　The Associated Press

The Associated Press（AP、米国）は、2017 年３月、新しい本社ビルにおいてＳＤＩとＩＰのハイブリッド伝送の機能を有するスタジオ、ニュースルーム、マスターコントロールルームを用いた放送を開始した。

利用されている規格は SMPTE ST 2022-6,-7 であることを踏まえると、上記の放送設備における伝送が主なＩＰ箇所であることが推察される。

ＩＰ化により得られた効果として以下をあげている：

・拡張容易性の向上
・テストケース機会の提供
・長距離ケーブルの整備

（４）　BBC Wales

BBC Wales（英国）は、2020 年 10 月より、英国で初めてとなる制作と放送の両方でＩＰ技術を用いる施設へ移行し、放送を開始した。

システム全体の構築は Grass Valley 社（米国）、dB Broadcast 社（イタリア）が担当しており、SMPTE ST 2110 によるＩＰでのメディア伝送、AMWA/NMOS による制御を行っている。

Grass Valley 社の GV Orbit により放送設備の制御を行っており、スタジオ設備からプレイアウトまでＩＰ化を実施している。

（５）　CANAL+

2015 年、CANAL+（仏国）の親会社である Vivendi グループは、以前 Euromedia が運営していた Boulogne スタジオを買収した。同スタジオは、CANAL Factory と改称され、Videlio 社（仏国）と Grass Valley 社、Cisco Systems 社（米国）、Lawo 社が主に担当し、2016 年 11 月にＩＰベースのシステムに移行した。

スタジオにはＩＰ化に対応したカメラ（Grass Valley LDX 86）があり、スタジオからコントロールルームへの伝送はＩＰによって行われる。

移行時点では完全にＩＰベースになっておらず、カメラやミキサーなどの機器の一部に入力/出力用に HD-SDI ケーブルを残している。

2022 年７月、CANAL+は新本社の CANAL+ One に EVS 社のソリューションで構築されたＩＰベースのインフラに移行した。新本社にはマスターコントロールルーム、プレイアウト、プロダクションのワークフローを集約させた。

EVS 社は Red Bee Media 社（イギリス）と共同で、SMPTE ST 2110 に対応したインフラを構築しており、クラウド型ライブ映像制作のプラットフォームである Grass Valley 社の GV AMPP を採用している。

プレイアウトを担当する Cast と呼ばれる施設と CANAL Factory、CANAL+ One の計 3 施設はダークファイバー等によって接続されている。

（６）　M6 Group

2020 年４月、M6 Group（仏国）は Evertz 社（カナダ）、Harmonic 社（米国）の技術を導入しマスターコントロールルーム（※プレイアウト等を含むマスター全体と想定される）をＩＰ化した。ＳＤＩからＩＰ（SMPTE ST 2110）への切り替えにより、新たな配信プラットフォームや Ultra HD 4K や 8K といった新しいビデオフォーマ

ットを容易に取り入れることが可能になった。

新たなマスターコントロールではM6をはじめ、W9、Série Clubなどの11チャンネルのプレイアウトが行われている。

ＩＰ化したマスターコントロールルームは従来のマスターコントロールルームと同じ場所に設置したため、段階的な作業を要した。

（７） BCE

RTLの子会社であるBroadcasting Center Europe（BCE、ルクセンブルク）は、2017年９月にＩＰベースの放送施設へ移行した。

ラジオとテレビのプロダクションとプレイアウトセンターの業務には、Arista社（米国）、Grass Valley社、Lawo社（独国）などの放送設備メーカによる最新のＩＰ対応機器が使用されている。

BCEは様々な地域で35以上のチャンネルのプレイアウトを担当しており、新たな施設ではＩＰ対応したプレイアウトよりこれらのチャンネルの24時間365日放送を行っている。

（８） SVT

SVT（スウェーデン）は、2019年２月に開催されたアルペンスキー世界選手権においてＩＰネットワークによるリモートプロダクションを実現した。ＩＰ伝送に対応した80台のカメラ（Grass Valley LDX 86）で撮影した映像をNet Insight社（スウェーデン）のNimbra Solutionsによって伝送し、現地から600km離れた拠点で映像の編集・切り替え・ライブ中継を実施した。

拠点間の伝送にはTelia社（スウェーデン）の100Gbpsの回線を2本使用（1本は予備）しており、機器の制御はGrass Valley社のDirectIPによって行う。

セキュリティの安全性や信頼性を確保するため、EUの個人情報保護を規定する法であるGDPR(General Data Protection Regulation)や、スウェーデン国内における公共放送専用の法律などを遵守している。

（９） TV2

TV2（ノルウェー）は、2017年８月にＩＰ化した施設をベルゲンに建設した。2017年11月にオスロに建設した施設もＩＰ化されており、両施設間(460km)をＩＰネッ

トワークで接続させた。

Lawo 社の VSM(Virtual Studio Manager)によって放送システムのＩＰ制御と監視を統合して実施している。

各地点のスタジオやギャラリーなどの部屋はスパインリーフトポロジー[注1]によって接続されている。ＩＰスイッチには Cisco 9000 シリーズ、Nevion eMerge を採用している。

注 1 拡張性に優れたネットワーク構成の一つ

SMPTE 2022、SMPTE 2110、AES67、Ember+[注2]によって音声、映像の伝送、制御を行う。

注 2 Lawo 社の VSM におけるプロトコル

プレイアウトの設備があるベルゲンの施設において、UHD 信号の受信から OTT プラットフォームへの配信までの流れを示す。

① 放送局より衛星を経由して映像を受信
② 映像から音声を分離、UHD 信号を HD 信号に変換
③ 映像と音声の遅延を設定
④ プレイアウトに HD 信号を送信
⑤ 映像に CM を挿入
⑥ プレイアウトから送られてくる映像を UHD に変換、音声の埋め込み
⑦ OTT プラットフォームに配信

2022 年９月、TV2 は Nevion 社（ノルウェー）と通信サービスプロバイダーの Telenor 社（ノルウェー）と共に、SMPTE ST 2110 に対応した VideoIPath を始めとした Nevion ソリューション、製品、サービスを使用してスポーツ番組制作のインフラを構築すると発表した。

60 以上の会場で複数の試合が同時に行われるため、TV2 は複数の制作会社と契約してコンテンツを制作している。すべての試合はリモートで制作され、最終的に放送される番組は TV2 が制作しており、分散制作となる。

セキュリティ対策のため、マイクロセグメンテーションによって各サーバを分離させており、外部インターネットとも接続しないようにしている。プロダクションにおけるクラウド化も検討段階である。

１－２－４－２－２　クラウド化導入事例

クラウド化については、ＩＰ化導入に伴いそのまま一部をクラウド化する事例も含め、一部の放送事業者では様々な放送設備において導入がされている。

（１）　Discovery

2021 年、米国 Discovery は、グローバルのリニアプレイアウトシステムをクラウドに移行した。プレイアウトは AWS で構築されており、Amazon EC2 と Amazon S3 を用いてクラウドベースのプレイアウト基盤を作成、また AWS DirectConnect を使用して、プレイアウト場所からイギリス・ロンドン、米国・バージニア州スターリングにある同社のオンプレミス配信施設、世界中のパートナーのアップリンク、テレポート施設にデータを送信する。

クラウド導入による主な効果は以下の通り。

- ・クラウド化により運用コストを 50%削減
- ・TCO（Total Cost of Ownership）が 61%削減
- ・イノベーションに時間を投入できるエンジニアが 50%から 80%に増加
- ・自動監視への移行により生産性が 13 倍向上

（２）　FOX

2019 年３月、FOX（米国）は生放送を含む全ての放送のマスターシステムを含め、クラウドベースのメディア制作・配信プラットフォームを実現するための複数年にわたる戦略的提携契約を締結したと発表した。具体的には以下の内容が含まれる。

- ・リニア放送のワークフロー、ケーブルテレビ、衛星事業者、通信会社等のハードウェア事業者への伝送、視聴者への OTT 向けコンテンツの配信を全て AWS 上で実現する。
- ・AWS Outposts により、リニアビデオ編集や画像グラフィックスワークフローなどの低遅延処理が必要となるビデオ処理は全てオンプレミスで実現する。
- ・Amazon Kinesis などの AWS 分析サービスと Amazon SageMaker などの機械学習サービスを使用してライブビデオストリームを強化し、リアルタイムのデータ分析を行う。

第２章　現行法令における放送設備の安全・信頼性に係る技術基準の現状

２－１　技術基準の概要

２－１－１　設備の損壊又は故障の対策

放送の安全・信頼性に係る技術基準については、「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（平成 23 年５月 17 日）」に係る情報通信審議会一部答申に基づき、設備の損壊又は故障の対策として、12 項目の措置が放送法令において定められた。

さらに、「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（令和元年 12 月 24 日）」に係る情報通信審議会一部答申に基づき、サイバーセキュリティの確保に関する措置が追加された。

これらの措置事項は、表２－１－１－１に示すように、地上放送及び衛星放送に対して共通的に定められている。

表２－１－１－１　**設備の損壊又は故障の対策に係る技術基準の概要**

原因	措置	地上系及び衛星系の放送	根拠規定
設備故障	予備機器等	予備機器の設置もしくは配備、故障等の発生時に予備機器に速やかに切替	放送法施行規則第104条
	故障検出	① 故障等の発生時にこれを直ちに検出し、運用者へ通知する機能 ② やむを得ず①の措置を講ずることができない設備は、故障等の発生時にこれを目視または聴音等により速やかに検出し、運用者へ通知可能な措置	放送法施行規則第105条
	試験機器及び応急復旧機材の配備	① 設備の点検及び調整に必要な試験機器の配備 ② 故障等の発生時に応急復旧措置を行うために必要な機材の配備	放送法施行規則第106条
	機能確認	① 予備の機器に係る定期的な機能確認等の措置 ② 放送設備の電源設備に係る定期的な電力供給状況の確認に係る措置	放送法施行規則第108条
	誘導対策	近接した場所に設置する放送設備などにおける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の実施	放送法施行規則第110条
自然災	耐震対策	① 設備の据付けに当たって、地震に　よる転倒または移動を防止するための耐震措置 ② 地震による設備構成部品の接触　不良及び脱落を防止するための耐震措置	放送法施行規則第107条

害等		③ ①、②の耐震措置は大規模な地震を考慮	
	耐雷対策	雷害を防止するための措置	放送法施行規則 第114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の実施	放送法施行規則 第111条
	屋外設備	① 空中線等屋外設備は、気象の変化、振動、衝撃、圧力その他外部環境の影響を容易に受けないこと ② 屋外設備は、公衆が容易に触れることができないよう設置	放送法施行規則 第112条
	収容する建築物	① 堅固で耐久性に富むこと ② 放送設備の安定動作が維持できること ③ 公衆が容易に立ち入り、または、放送設備に触れることができないための措置	放送法施行規則 第113条
停電	停電対策	① 自家用発電機または蓄電池の設置 ② 自家用発電機等の燃料について、必要な量の備蓄または補給手段の確保	放送法施行規則 第109条
その他	宇宙線対策 （人工衛星に設置する放送設備）	宇宙線による影響を容易に受けないための構成部品の使用その他の措置	放送法施行規則 第115条
	サイバーセキュリティの確保	サイバーセキュリティの確保のために必要な措置	放送法施行規則 第115条の2

２－１－２　放送種別と技術基準の適用

技術基準の適用については、設備構成の差異を考慮して、放送の種別ごとに定められており、各放送種別においてその設備規模や故障等による受信者への影響の波及度合いを考慮して、措置の範囲が定められている。

例えば、事故により放送設備の損壊又は故障の影響を広範囲に及ぼす設備（番組送出設備、地上デジタルテレビジョン放送の親局、衛星放送の送信設備等）に対しては、放送の停止等を未然に防ぐ、又は、それから即座に復旧させるための措置が必要である。

一方、地上デジタルテレビジョン放送の小規模な中継局等、放送の停止の影響を及ぼす範囲が限定的な設備に対しては、経済合理性の観点から、主に事故の長時間化を防ぐための措置が必要とされている。

その適用の概要は、表２－１－２－１のとおりである。

表２－１－２－１　放送種別と技術基準の適用状況について

技術基準＼放送種別		地上デジタルテレビジョン放送及び中波放送					超短波放送及び短波放送					マルチメディア放送				コミュニティ放送			衛星基幹放送及び衛星一般放送			
			中継回線設備		放送局の送信設備			中継回線設備		放送局の送信設備				放送局の送信設備								
原因	措置	番組送出設備	親局へ送信	プラン局へ送信	親局	プラン局	番組送出設備	親局へ送信	中継局へ送信	親局	中継局	番組送出設備	中継回線設備	大規模な放送局	小規模な放送局	番組送出設備	中継回線設備	放送局の送信設備	番組送出設備	中継回線設備	地球局設備	放送局の送信設備
設備故障等	予備機器等	○	○	○	○	○	○	○	－	○	－	○	○	○	－	○	－	－	○	○	○	○
	故障検出	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
	試験機器及び応急復旧機材の準備	○	○	○	○	○	○	○	○	○	○	○	○	○	○	－	－	－	○	○	○	－
	機能確認	○	○	○	○	○	○	○	－	○	－	○	○	○	－	－	－	－	○	○	○	○
	誘導対策	○	○	○	○	○	○	○	○	○	○	○	○	○	○	－	－	－	○	○	○	－
自然災害等	耐震対策	○	○	○	○	○	○	○	－	○	－	○	○	○	○	－	－	－	○	○	○	－
	耐雷対策	○	○	○	○	○	○	○	○	○	○	○	○	○	○	－	－	－	○	○	○	－
	防火対策	○	○	○	○	○	○	○	○※1	○	○※1	○	○	○	○	○	－	○	○	○	○	－
	屋外設備	－	○	○	○	○	－	○	○※2	○	○	－	○	○	○	－	－	○	－	○	○	－
	収容する建築物	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	－	○	○	○	○	－
停電	停電対策	○	○	○	○	○	○	○	－	○※1	－	○	○	○	○	－	－	－	○	○	○	－
その他	宇宙線対策	－	－	－	－	－	－	－	－	－	－	－	○	－	－	－	－	－	－	－	－	○
	サイバーセキュリティの確保	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

「○」は適用、「－」は適用外を示す。

※1 短波放送の場合は「-」　※2 超短波放送の場合は「-」

２－２　技術基準の対象となる設備の概要

２－２－１　地上系の放送設備

・地上系の放送設備は、大別すると次の３つに分類できる。

① 番組送出設備

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。

② 中継回線設備

番組送出設備から送出された放送番組を放送局の送信設備まで伝送する機能を有する電気通信設備、異なる場所に設置した放送局の送信設備の間で放送番組を伝送する機能を有する電気通信設備（放送波により中継を行う場合は、その受信設備を含む。）又は異なる場所に設置した番組送出設備間に設ける電気通信設備。

③ 放送局の送信設備

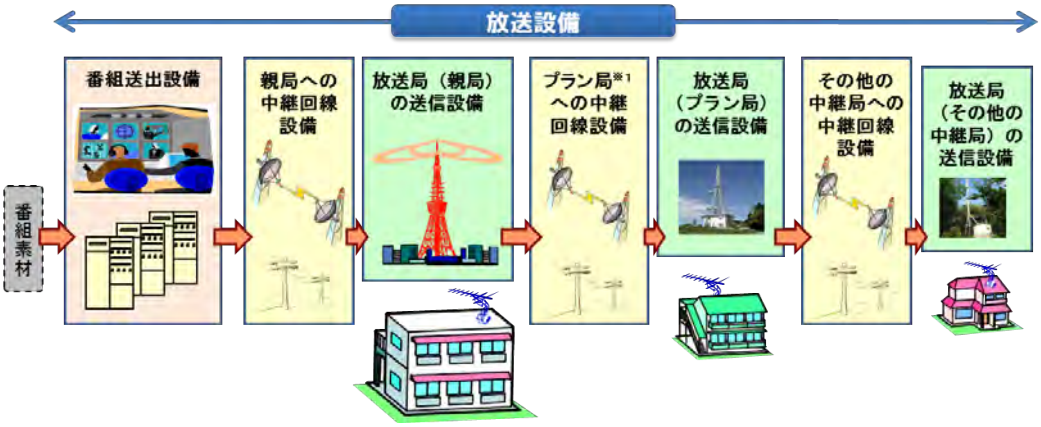
放送をする無線局の送信設備。

・地上系の放送においては、番組送出設備が設置された場所（演奏所）と、実際に放送を送信する場所（送信所）が異なる場所に設置され、その間を中継回線設備で結ぶ構成が取られている。

・地上系の放送設備の構成について、放送種別ごとに整理したものを以下に示す。

２－２－１－１　地上系放送の放送種別ごとの設備構成

２－２－１－１－１　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

図２－２－１－１－１　**地上デジタルテレビジョン放送に関する設備の構成例**

・地上デジタルテレビジョン放送における設備構成は、図２－２－１－１－１のとおりである。地上デジタルテレビジョン放送における放送局は、主として県庁所在地周辺や広域都市圏を対象とする親局、中小都市周辺を対象とするプラン局、その他小規模な地域を対象とするその他の中継局の３種類に区分しており、これらを組み合わせることで、広く放送を提供するための放送網を構成している。

・放送設備の主な構成機器は、映像や音声の信号を選択する送出マトリクス、入力された信号を変換するエンコーダ、番組の送出を管理、制御する送出管理装置、中継回線設備として用いられるＳＴＬ（Studio to Transmitter Link)、ＴＴＬ（Transmitter to Transmitter Link）及び放送局から実際に放送を送信する送信装置や空中線である。

２－２－１－１－２　中波放送（ＡＭ放送）

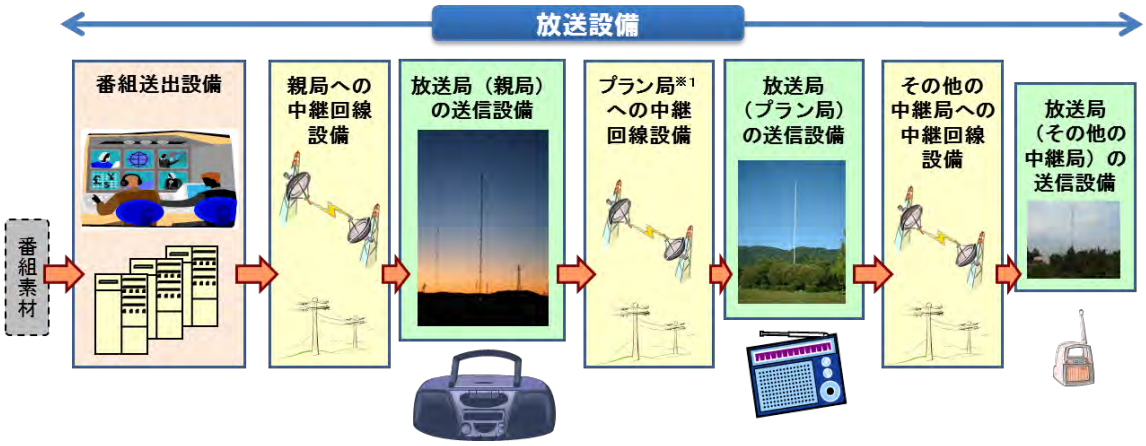


図２－２－１－１－２　**中波放送に関する設備の構成例**

・中波放送における設備構成は図２－２－１－１－２のとおりであり、全体的な放送の流れは地上デジタルテレビジョン放送と同様である。放送に使用する周波数の性質から、放送局、特に親局の空中線は大規模なものとなるため、設置には広大な敷地を必要とする。

・放送設備の主な構成機器は、音声素材を放送番組とするための調整を行う音声調整装置や番組の送出を管理、制御する送出管理装置、中継回線設備として用いるＳＴＬ、ＴＴＬ及び放送局から実際に放送を送信する送信装置や空中線である。

２－２－１－１－３　短波放送

・短波放送における設備構成は、図２－２－１－１－３のとおりである。短波は特有の伝搬特性を持っており、国内放送は親局１箇所とプラン局１箇所からの構成で日本全国をカバーする放送が行われ、国際放送は国内の親局１箇所から放送が行われている。

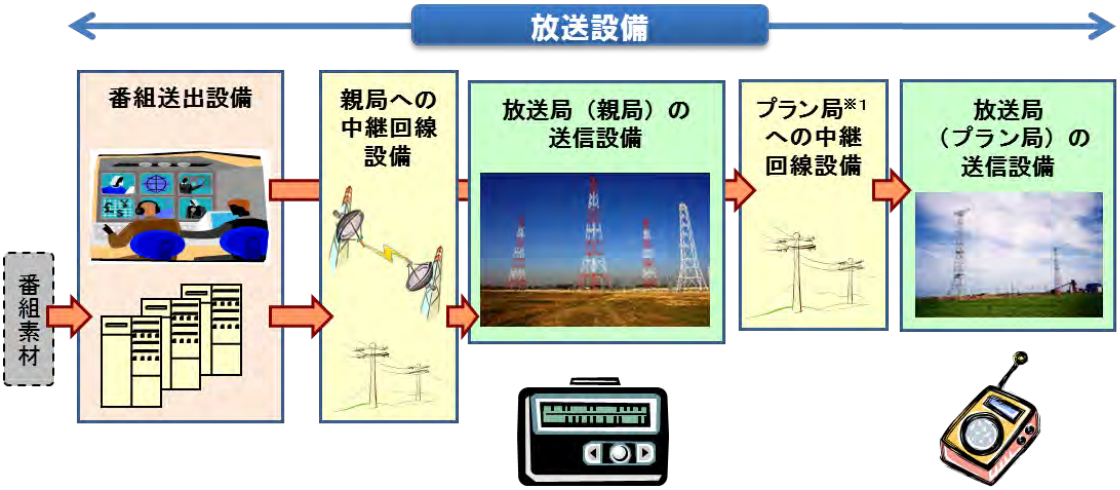


図２－２－１－１－３　**短波放送に関する設備の構成例**

・放送設備の主な構成機器は、音声素材を放送番組とするための調整を行う音声調整装置や番組の送出を管理、制御する送出管理装置、中継回線設備として用いるＳＴＬ及び放送局から実際に放送を送信する送信装置や空中線である。

２－２－１－１－４　超短波放送（ＦＭ放送）

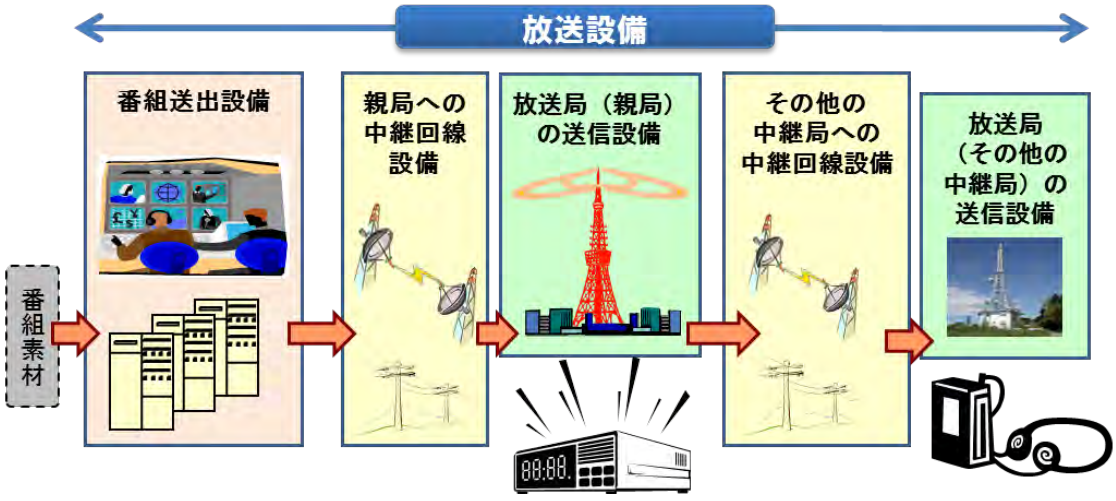


図２－２－１－１－４　**超短波放送に関する設備の構成例**

・超短波放送における設備構成は、図２－２－１－１－４のとおりである。超短波放送の放送局は、地上デジタルテレビジョン放送と同様の場所に設置されている事例もある。

・放送設備の主な構成機器は、音声素材を放送番組とするための調整を行う音声調整装置や音声のステレオ信号に対応したステレオ変調装置、番組の送出を管理、制御する送出管理装置、中継回線設備として用いるＳＴＬ、ＴＴＬ及び放送局から実際に放送を送信する送信装置や空中線である。

・なお、超短波放送のうちコミュニティ放送は、設備の面では超短波放送と同様の構成となっている。

２－２－１－２　地上系放送設備に含まれる装置等

・技術基準の適用対象となる地上系放送の設備に含まれる装置等の例に関しては、表２－２－１－２－１のようになっている。なお、それぞれの設備の構成装置等については、事業者によって異なるものとなっている。

表２－２－１－２－１　地上系放送の放送設備に含まれる装置等の例

放送種別	番組送出設備※1	中継回線設備	放送局の送信設備
地上デジタルテレビジョン放送	・送出マトリクス※2 ・エンコーダ※3 ・多重化装置※4 ・送出管理装置※5 ・基準信号発生装置※6 等	・STL※7 ・TTL※8 ・一事業者内の演奏所間回線 ・放送波中継用の受信装置　等	・基準信号発生装置※6 ・伝送路符号化装置 ・送信装置 ・空中線　　等
中波放送（AM放送）	・送出マトリクス※2 ・音声調整装置(主) ・送出管理装置※5 等	・STL※7 ・TTL※8 ・一事業者内の演奏所間回線 等	・送信装置 ・空中線　　等
短波放送	・送出マトリクス※2 ・音声調整装置(主) ・送出管理装置※5 等	・STL※7 等	・送信装置 ・空中線　　等
超短波放送（FM放送）	・送出マトリクス※2 ・音声調整装置(主) ・送出管理装置※5 ・ステレオ変調装置 等	・STL※7 ・TTL※8 ・一事業者内の演奏所間回線 ・放送波中継用の受信装置　等	・送信装置 ・空中線　　等
コミュニティ放送	・送出マトリクス※2 ・音声調整装置(主) ・ステレオ変調装置　等	・STL※7 ・TTL※8 等	・送信装置 ・空中線　　等
マルチメディア放送	・送出マトリクス※2 ・エンコーダ※3 ・多重化装置※4 ・送出管理装置※5 ・基準信号発生装置※6 等	・番組送出設備から放送局の送信設備間の回線	・基準信号発生装置※6 ・伝送路符号化装置 ・送信装置 ・空中線　　等

※1 スタジオ設備は含まない。
※2 送出する番組の素材を切り替える機能を有する装置。
※3 映像、音声等の信号を MPEG-2 Video、MPEG-2 Audio AAC 等の方式に符号化する機能を有する装置。
※4 符号化された映像、音声等の複数の信号を多重化する機能を有する装置。
※5 放送番組の送出スケジュール等を管理し、主として番組送出を制御する機能を有する装置。
※6 機器の同期をとるためのクロック信号を発生させる装置。
※7 Studio to Transmitter Link の略。
※8 Transmitter to Transmitter Link の略。

２－２－２　衛星系の放送設備

・衛星系の放送設備は、大別すると次の４つに分類できる。

① 番組送出設備

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（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。

② 中継回線設備

番組送出設備から送出された放送番組を地球局設備まで伝送するための電気通信設備。

③ 地球局設備

人工衛星の放送局の送信設備まで放送番組を伝送するための地球局の送信設備。

④ 放送局の送信設備

人工衛星の放送局の送信設備（地球局から伝送された放送番組を受信するための電気通信設備を含む。）。

・衛星放送にはＢＳ放送及び東経１１０度ＣＳ放送に分類される衛星基幹放送と、東経１２４／１２８度ＣＳ放送に分類される衛星一般放送が存在するが、両者の設備構成には大きな差異がないため、以下では併せて説明する。

・衛星放送における設備構成は、図２－２－２－１のとおりである。番組送出設備から送出された放送番組は、中継回線設備及び地球局設備を経由して人工衛星の放送局の送信設備へ伝送され、日本全国を放送対象地域として放送される。

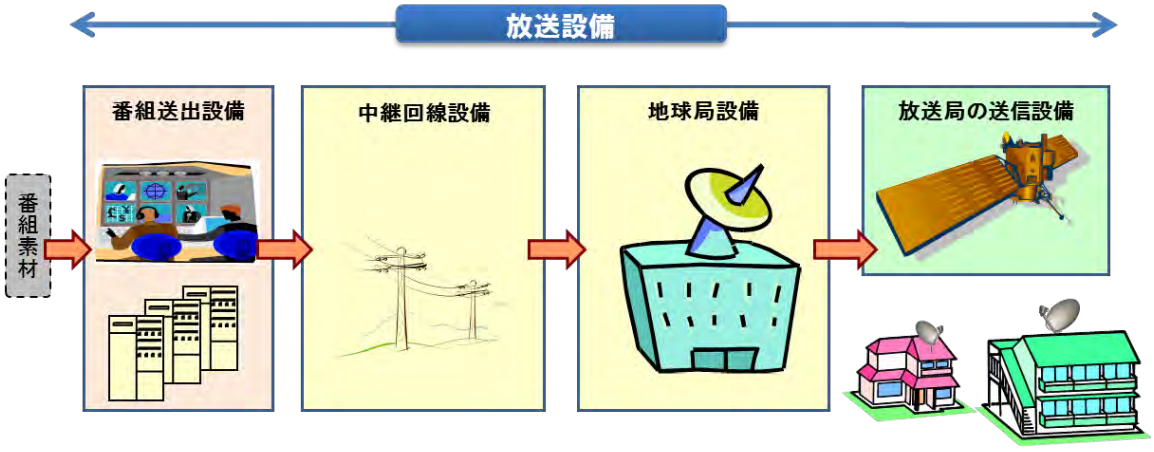


図２－２－２－１　衛星放送に関する設備の構成例

・放送設備の主な構成機器は、番組送出設備を構成する送出管理装置やエンコーダ、中継回線設備となる番組送出設備から地球局設備間の回線、地球局で衛星向けに電波を送出する送信装置や伝送路符号化装置及び衛星に搭載された送信装置や空中線である。

・技術基準の適用対象となる衛星系放送の放送設備の例に関しては、表２－２－２－１のようになっている。なお、それぞれの放送設備に含まれる装置等については、事業者によって異なるものとなっている。

表２－２－２－１　衛星系放送の放送設備に含まれる装置等の例

放送種別	番組送出設備※1	中継回線設備	地球局設備	放送局の送信設備
BS／東経１１０度CS放送	・送出マトリクス※2 ・エンコーダ※3 ・多重化装置※4 ・送出管理装置※5 ・基準信号発生装置※6 等	・番組送出設備から地球局設備間の回線	・TS合成装置 ・伝送路符号化装置 ・送信装置 ・空中線　等	・送信装置 ・空中線 等
東経１２４／128度CS放送	・送出マトリクス※2 ・エンコーダ※3 ・多重化装置※4 ・送出管理装置※5 ・基準信号発生装置※6 等	・番組送出設備から地球局設備間の回線	・伝送路符号化装置 ・送信装置 ・空中線　等	・送信装置 ・空中線 等

※1 スタジオ設備は含まない。
※2 送出する番組の素材を切り替える機能を有する装置。
※3 映像、音声等の信号をMPEG-2 Video、MPEG-2 Audio AAC等の方式に符号化する機能を有する装置。
※4 符号化された映像、音声等の複数の信号を多重化する機能を有する装置。
※5 放送番組の送出スケジュール等を管理し、主として番組送出を制御する機能を有する装置。
※6 機器の同期をとるためのクロック信号を発生させる装置。

第３章　放送設備のサイバーセキュリティ確保に関する対策技術等の現状

３－１　サイバー脅威の動向

３－１－１　サイバー攻撃の巧妙化および深刻化

情報通信技術の浸透や国際情勢の緊張を背景として、サイバー攻撃が巧妙化・深刻化しており、サイバー脅威によるセキュリティリスクが高まっている。重要インフラを含む各分野においてＩＰ化・クラウド化等のＤＸ（デジタルトランスフォーメーション）が進展しつつあり、各分野の情報システムを狙ったサイバー攻撃が増大するとともに、攻撃手段も時々刻々巧妙化しており、被害が深刻化している。

近年のサイバー攻撃の傾向として、攻撃の頻度、規模および対象が拡大していることが挙げられる。具体的には、なりすましメール（Emotet 等）やフィッシング等の手段による不特定多数への繰り返しの攻撃、携帯電話等の大規模な電気通信サービスへの攻撃、重要インフラや IoT 機器等の脆弱性を持つ可能性のある情報システムを狙う攻撃等による「量」的な脅威の増大が見受けられる。

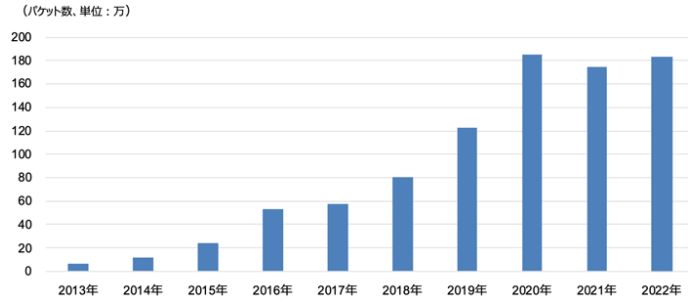


図３－１－１－１　１ＩＰアドレスあたりの年間総観測パケット[注1]数[1]

注１ NICTER プロジェクト（サイバー攻撃等を観測・分析する情報通信研究機構のプロジェクト）で観測しているダークネット（インターネット上で到達可能かつ未使用の IP アドレス空間）の範囲に届いたパケットの個数の推移であり、サイバー攻撃の件数の推移を示すものではない。

[1] 情報通信研究機構　NICTER 観測レポート 2022 の公開
https://www.nict.go.jp/press/2023/02/14-1.html

さらに、サイバー攻撃の高度化、組織化およびビジネス化が進展していることが挙げられる。具体的には、人間の油断や隙といった人の脆弱性を狙ったソーシャルエンジニアリング攻撃、セキュリティ対策の脆弱な組織を経由して当該組織とつながりのある組織にも攻撃を拡大させるサプライチェーン攻撃、ソフトウェア等の脆弱性に対する情報公開や対策が講じられる前に攻撃を行うゼロデイ攻撃、世論操作や心理的誘導を巧みに利用した攻撃等による「質」的な脅威の増大が見受けられる。

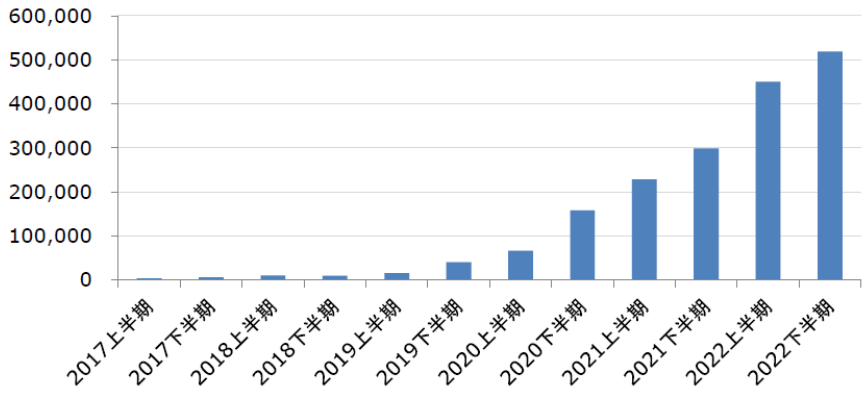


図３－１－１－２　国内のフィッシング[注2]情報の届出件数[2]

注 2 心理的誘導により、実在する組織を騙って、ユーザネーム、パスワード、アカウント ID、ATM の暗証番号、クレジットカード番号といった個人情報を詐取するサイバー攻撃の手段。

また、サイバー攻撃のビジネス化が進展していることを示す顕著な例として、「Cybercrime-as-a-Service（CaaS）」の登場が挙げられる。Software-as-a-Service（SaaS）がソフトウェアをサービスとして提供するのに対し、Cybercrime-as-a-Service（CaaS）はサイバー攻撃手段をサービスとして提供する。当該サービスの利用により、攻撃者は、情報システムやサイバーセキュリティに関する専門知識や技術を持ち合わせていなくてもサイバー攻撃を行うことが可能となる。

CaaS によってサービス提供される攻撃手段には、下記のようなものがある。

・漏えいデータマーケット
・ボットネット
・踏み台サービス
・ゼロデイ攻撃販売

[2] フィッシング対策協議会　フィッシングレポート 2023
https://www.antiphishing.jp/report/phishing_report_2023.pdf

・スパム送信用ホスト販売
・DoS 攻撃代行
・アクセス権販売
・報奨金（攻撃者向けの脆弱性発見）

攻撃対象から直接金銭を得るための手段として、ランサムウェアを活用したサイバー攻撃が世界的規模で増大しているとともに、ビジネスモデル化も進展している。ランサムウェア攻撃は、マルウェアを用いて攻撃対象の情報システムやデータをロックや暗号化等により使用不能にした後、解除のために身代金を支払うよう脅迫するものであるが、近年では、攻撃者が攻撃の手順を下記のような段階に分けて組織化・分業・アウトソースすることにより効率化することで、一つのビジネスモデルとして確立している。

・組織に侵入
・内部情報の暗号化、外部持ち出し
・持ち出し情報の評価（価値の値踏み）
・支払い手段の確保、支払い金の追跡困難性確保
・脅迫（被害者との交渉）
・暗号化されたデータの復元
・支払わない場合の対応（持ち出し情報の暴露・公開・第三者への販売）

３－１－２　重要インフラ（放送を含む）へのサイバー攻撃事例

我が国においては、情報通信(主要な地上基幹放送事業者を含む)、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む)、医療、水道、物流、化学、クレジット、石油の 14 分野が重要インフラに位置づけられている。

海外では、重要インフラに関連するサイバー攻撃が多数発生しており、大きな被害が発生している。

例えば、2021 年には、米大手パイプライン会社コロニアル・パイプライン社がランサムウェア攻撃を受けている。同社は米国東海岸で消費される燃料の約 45%を扱っており、６日間続いたパイプラインの停止は市民生活に大きな影響を与えた。当該攻撃では、情報システムの復旧と引換えに身代金を要求するだけでなく、データを搾取し身代金を支払わない場合は搾取したデータを公開するとの脅迫がなされた。また、CaaS の一種である Ransomware-as-a-Service（RaaS）により、ランサムウェア攻撃に必要な攻撃手段が攻撃者に提供されたとの情報もある。当該攻撃に係る経緯や発生要因をまとめると、下記のようになる。

・ＶＰＮ装置には多要素認証が適用されていたものの未使用のレガシープロファイルが存在し、ＩＤ/パスワードのみでログイン可能だったとされる。
・利用されたパスワードはダークウェブに漏洩していた。

・情報系から侵入を受け、制御系に影響が派生するという典型的な攻撃の流れをたどった。
・制御系まで攻撃が到達していなくても、攻撃が発覚した時点で影響を考慮して制御系を止めざるを得なかった。
・バックアップは存在していたが、安全に使用可能か短時間で判断がつかず、身代金支払い(4 億 8 千万円)に応じざるを得なかった。

ランサムウェアによる攻撃事例としては、2018 年、世界的な半導体企業である TSMC（台湾）の工場ネットワークがランサムウェアの一種である WannaCry の被害を受けている。３日間の生産停止による損害額は最大 190 億円にのぼるとされ、発生原因はマルウェアに感染した端末の工場内への持込みとされている。

TSMC に被害をもたらした WannaCry は、Microsoft Windows を標的とした自動感染拡大機能を持つワーム型ランサムウェアである。2017 年頃には 150 か国 30 万台以上（日本国内では 600 か所以上）で感染が発生したと推定される。

その他にも、イラン核燃料施設に対する破壊目的のサイバー攻撃によりウラン濃縮用遠心分離機約 1000 台が稼働不能に陥った事例（2010 年)、ウクライナにおけるサイバー攻撃により変電所の遮断機が切断した大規模停電の事例(2015 年及び 2016 年)、アルミニウム生産企業最大手のノルスク・ハイドロ社（ノルウェー）の生産設備管理システムと IT システムがランサムウェアに感染した事例（2019 年)、システム管理ツールの開発会社ソーラーウインズ社（米国）への侵入を発端に顧客（米国政府、米軍、米国大手重要インフラ企業を含む）が連鎖的に攻撃を受けた事例（2020 年）等がある。

一方、放送分野へのサイバー攻撃としては、下記のような事例がある。

2015 年に、フランスの国際テレビネットワーク TV5MONDE(TV サンクモンド：(フランス語の国際総合チャンネル)の 12 チャンネルがサイバー攻撃により 18 時間放送不能になった。また同時に、Web サイト、E メール、Twitter、Facebook のアカウントも攻撃を受け、乗っ取り（改ざん）の被害が発生した。

2013 年には、韓国の金融機関や主要放送局への同時多発サイバー攻撃が発生し、複数の放送事業者が多大な被害を被った。韓国放送公社（KBS）では、ＰＣ端末約 5000 台が被害を受け、基幹業務システムにも影響が及んだ。韓国文化放送（MBC）では、ＰＣ端末約 800 台(社内全台数の半数程度)が被害を受けた。ケーブルテレビ・衛星向けにニュースチャンネルを配信するニュース専門放送局である Your True Network（YTN）では、ＰＣ端末約 500 台及びサーバ５～６台が被害を受けた。

2019 年には、フランス大手民放テレビ局である M6 がランサムウェア感染の被害を受けたものの、感染拡大を防いだ結果、10 のテレビチャンネルやラジオ局等は放

送停止には至らなかった[3]。

2021 年には、Cox Media Group（米国）がランサムウェア攻撃の被害を受け、テレビとラジオの放送中断が発生した[4]。

同じく 2021 年には、米大手テレビ放送局運営会社 Sinclair Broadcast Group がランサムウェア攻撃を受け、複数の放送局で放送が停止する事態となった。その被害として、広告収入に 6,300 万ドルの損失が生じたと伝えられている[5]。

過去に発生した重要インフラへの攻撃事例の概略を記載したが、それらの傾向や特徴から以下の３つのことがいえる。

① 重要インフラは高度かつ執拗な攻撃の対象であること

一般的にサイバー攻撃は、攻撃対象の価値に見合うコストをかけた周到な準備を経た上で、継続的で執拗な攻撃が行われる。過去の攻撃事例における被害者の損害額から見ても、重要インフラが攻撃対象となり得ることは明白である。

② サイバー攻撃では、あらゆる侵入経路が狙われること

情報システムへのＩＰ化やクラウド化の導入は利用者の利便性を高めるが、それはサイバー攻撃を行う者にとっても同様である。ネットワーク等でつながれたすべての関係者が攻撃対象となり得る。また、テレワーク等のリモート接続による業務形態を想定すると、さらに侵入経路が増加することになる。

③ 破壊・妨害を目的としたサイバー攻撃が特に脅威であること

一般的にサイバー攻撃には、不正操作や改ざんよりも破壊・妨害を目的とした攻撃の方が実行しやすく防御しにくいという特性がある。重要インフラは、正常に動作していること自体に高い価値があるため、機能の破壊および動作の妨害を目的としたサイバー攻撃が特に脅威となる。

現時点では、日本国内においてサイバー攻撃に起因する放送停止事故が発生した

---

[3] ZDnet 記事
https://www.zdnet.com/article/m6-one-of-frances-biggest-tv-channels-hit-by-ransomware/

[4] Security Affairs 記事
https://securityaffairs.com/123136/malware/cox-media-group-ransomware.html

[5] CyberScoop 記事
https://cyberscoop.com/sinclair-broadcast-group-ransomware-ongoing-disruption-macaw/

という事実は顕在化していないが、放送が重要インフラの一分野であることを踏まえると、サイバー攻撃の対象になる可能性は常にあることに留意する必要がある。

３－２　サイバー脅威と対策の事例

３－２－１　セキュリティ対策技術の典型例

サイバー攻撃を防ぐための対策技術について、いくつかの典型例を解説する。

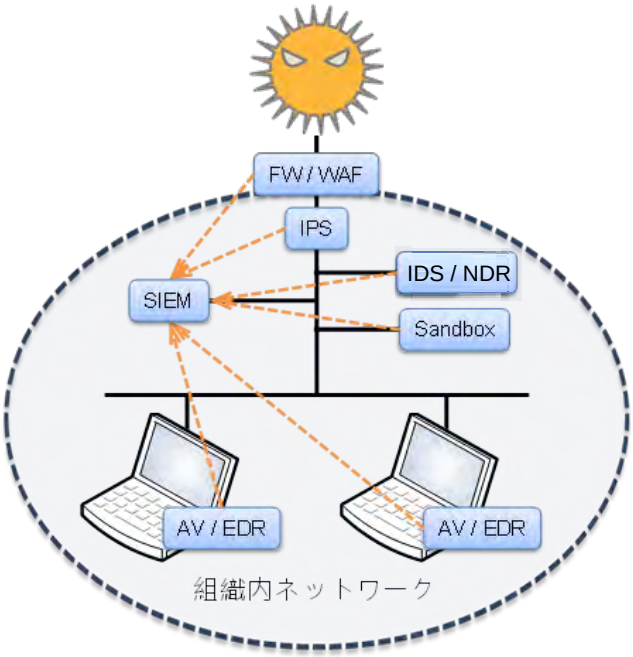


図３－２－１－１　**ネットワーク内におけるセキュリティ対策技術の動作箇所**

図３－２－１－１は、ネットワークのどの箇所で各セキュリティ対策技術が動作するかを示した模式図である。点線は、組織内のネットワークと外部のネットワークの境界線を表している。

FW（Firewall：ファイアーウォール）または WAF（Web Application Firewall ：Web アプリケーションファイアーウォール）は、組織内のネットワークと外部ネットワークの境界に設置され、ネットワーク層／トランスポート層／アプリケーション層でパケット通過の可否を判定する。FW または WAF はインライン（直列）に接続され、外部ネットワークから組織内のネットワークへの不正な侵入を遮断する。

IDS（Intrusion Detection System：侵入検知システム）は、シグネチャを用いて攻撃を検知し、アラートを発報する。また、NDR（Network Detection and Response）は、ネットワークトラフィックを分析することにより攻撃を検知する。IDS や NDR はポートミラーリング機能やネットワークタップ（TAP：Terminal Access Point）を用いて取り出したパケットを分析して異常を検知する。

IPS（Intrusion Prevention System：侵入防止システム）は、シグネチャを用い

て攻撃を防止する。IPS はインラインに接続されるので、攻撃を遮断することができる。

Sandbox（箱庭環境）は、隔離された仮想環境でファイルを実行しマルウェアを検知する。例えば、ポートミラーリング機能やネットワークタップを用いて取り出した添付ファイルなどを実行して、その挙動を分析する。通常の領域からは隔離されているため、ファイルの実行による被害を防ぐことができる。

AV（Anti-Virus：アンチウイルス）や EDR（Endpoint Detection and Response：エンドポイントでの検出と対応）は、シグネチャベースでマルウェア検知し、端末内の各種情報を収集・対応する。AV や EDR はエンドポイント、すなわちネットワーク内の PC 等の端末で動作するため、各端末内にインストールする必要がある。

SIEM（Security Information and Event Management：セキュリティ情報イベント管理）は、上記の各種セキュリティ機器からのログやアラートを集約して一元管理する。SIEM は、組織内ネットワークに適宜設置され、横断的に取得したログやアラートを解析し、インシデントにつながる脅威を検知する。

３－２－２　ゼロトラスト・アーキテクチャ

従来のサイバーセキュリティ対策は、主に境界防御型であった。すなわち、ネットワークを内側と外側に分け、組織内のネットワークという場所を静的に保護しようという考え方である。しかしながら、サイバー脅威の巧妙化・深刻化により、境界防御型の対策では攻撃者の侵入をネットワークの境界で完全に防ぐことは難しくなってきている。また、クラウドや仮想環境の利用拡大でネットワークの境界が曖昧になってきているという実態もある。

これらを背景として、サイバーセキュリティ対策の新しい概念として、ゼロトラスト・アーキテクチャ（ZTA）という考え方が主流になりつつある。ゼロトラスト・アーキテクチャは下記の特長をもつ。

・データソースや計算サービスなどをリソースとみなす
・全ての通信の安全性確保
・セッション単位のリソースへのアクセス許可
・動的なポリシによるリソースへのアクセス判断
・全ての機器の監視と計測
・アクセス前の認証・認可の動的・厳格な実施
・機器の状態やインフラ・通信状態の情報を収集し利用

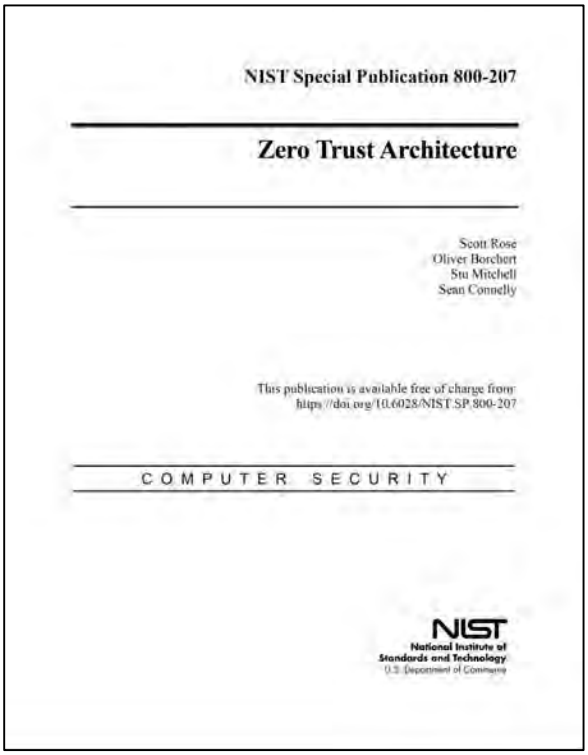


図３－２－２－１　NIST “SP 800-207, Zero Trust Architecture（ゼロトラスト・アーキテクチャ）”

ゼロトラスト・アーキテクチャを構成する一つ一つの技術要素は 10 年以上前から存在していたものであり、それらを導入する際に、導入者の状況に合わせてどのように適用していくのかが課題となる。また、ゼロトラストはセキュリティ対策の概念であり、単一の技術や製品の導入により実現可能なものではないことに留意する必要がある。

３－２－３　サイバーレジリエンス

昨今のサイバー攻撃は多様化・悪質化しており、すべてのサイバー攻撃を防ぎきることは困難になってきている。そのため、サイバー攻撃による被害を受けることがあるという前提で対策を考える必要がある。サイバー攻撃を受けた際には、いかに早く気づいて対処するのか、被害が発生した場合はいかに早く回復し、問題点を発見・改善するのかという点が重要となる。サイバー攻撃への対処のための体制や手順を事前に整備し、被害を最小限にとどめ、なるべく早く機能を復旧させる能力を示す、サイバーレジリエンスという概念が注目されている。

サイバーレジリエンスにより、サイバーセキュリティのリスクを把握・管理しておき、サイバー攻撃を受けた場合に被害を小さくすることが可能となる。具体的に

は、サイバー攻撃による被害を局所化し、縮退運用により事業を継続し、短時間で復旧できるようにすることにより、事業継続性が高まる。

サイバーレジリエンスの必要性が高まってきている理由は、下記のとおりである。

- サイバー攻撃自体が、量的にも質的にも増えてきている。
- 従来は外部ネットワークからの攻撃を組織内のネットワークとの境界で防御するための対策を施してきたが、ネットワークの境界があいまいになってきている。
- ＤＸ（デジタルトランスフォーメーション）により組織の外に業務システムや情報資産が置かれることがあるため、攻撃対象の領域が拡大している。
- 一見インターネットにつながっているのか分からないものが、実はつながっていて、情報がやり取りされることがある。
- サイバー攻撃は、一度組織内のネットワークに侵入されてしまうと被害が拡大しやすいという性質をもつ。

３－３　放送事業者における取組み

放送は、「重要インフラのサイバーセキュリティ[注1]に係る行動計画（令和４年６月 17 日改定）」（以下、「行動計画」という。）に定める重要インフラに該当し、行動計画において、安全等を維持する観点からサイバーセキュリティ対策を関係法令等における保安規制として位置付けることなど、制度的枠組みを適切に改善する取組みの継続的な実施が提示されている。

注１ サイバーセキュリティとは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、または発信され、伝送され、もしくは受信される情報の漏えい、滅失または毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていることをいう（サイバーセキュリティ基本法第２条から一部抜粋）。

放送は、緊急災害時を含め、常に国民生活に必需な情報をあまねく届けるという高い公共性を持つことから、その安全・信頼性が求められる。そのため、放送の施設設備に対しては事故の発生を未然に防止するための措置及び発生した時の早期の復旧を目指した措置を求めている。具体的には、予備機器の配備、停電対策、故障検出、応急復旧機材の配備等に加え、サイバーセキュリティの確保[注2]を含む安全・信頼性に関する技術基準を設けているとともに、重大事故が発生した場合における報告等を義務付けている。

注２ 令和２年３月 30 日の放送法施行規則等の一部改正により、措置項目として追加。

また、政府の行動計画を踏まえ、放送事業者等関係者による自主的取組みとして、以下のような項目が実施されている。

① 安全基準等の整備・浸透
② 情報共有体制の強化
③ 防護基盤の強化

こうした取組みにおいては、一般社団法人日本民間放送連盟（以下、「民放連」という。）と日本放送協会（以下「NHK」という。）が共同で事務局を務める放送セプターが重要な役割を果たしている。なお、セプターは、各分野の重要インフラ事業者等の情報共有を担う組織である（CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response）。

放送セプターは NHK、主な地上系民間基幹放送事業者、民放連の 194 社２団体で構成されている[注3]。

注３　令和５年３月末日現在

各取組みの概要については、以下のとおりである。

① 安全基準等の整備・浸透

放送セプターでは、ICT-ISAC（一般社団法人 ICT-ISAC の概要は後述する。）が 2020 年 9 月に策定した「放送における情報インフラの情報セキュリティ

確保に関わる『安全基準等』策定ガイドライン」(統合初版)を共用している。これは放送全般の情報セキュリティに関するものであり、放送設備のサイバーセキュリティについては、ICT-ISAC が策定した「放送設備サイバー攻撃対策ガイドライン」を共用し、対策に活用している。

また、2020 年３月に「放送法施行規則」および「放送法関係審査基準」が改正され、基幹放送の安全・信頼性に関する技術基準に放送設備のサイバーセキュリティ確保が追加されたことを受け、ICT-ISAC が免許・再免許等の手続きに必要なサイバーセキュリティ対策を整理した「放送設備サイバーセキュリティ対策（参考資料)」も同様に共用し、活用している。

② 情報共有体制の強化

放送セプターでは IT 障害に関し、内閣サイバーセキュリティセンター（以下、「NISC」という。）から提供される情報及びこれを補完する情報を適切に放送事業者に提供し、共有を図る機能を有している。放送セプター事務局と放送事業者は緊急時連絡網を構築しているほか、掲示板型情報共有ツールを運用し、インシデント情報や NISC の注意喚起、ニュースレターなどの情報をセプターごとに共有している。

また、セプターでの情報伝達訓練を実施し、セプター内での情報共有が適切に行われていることを定期的に確認している。

なお、民放連では、サイバーセキュリティ対策についてセミナーや説明会を会員の民間放送事業者等を対象に随時開催し、情報共有に努めている。

③ 防護基盤の強化

NISC の分野横断的演習、警視庁の重要インフラ分野別演習（放送分野）などに放送事業者が積極的に参加し、防護基盤の強化を図っている。

３－４　セキュリティ情報共有組織（ISAC）を通じた取組

1998 年米国にて、クリントン政権の国家の重要インフラを防護する政策として、重要インフラを構成する各業種において設置が促されたことを契機として、ISAC （Information Sharing and Analysis Center)が生まれた。ISAC は、リスクを軽減し回復力を高めるため、脅威情報を収集・分析し、共有することを目的として、事業分野ごとに設立される組織である。

日本においては、2002 年７月に通信事業者の商用サービスの安全かつ安心な運用の確立を目的に日本で最初の ISAC である Telecom-ISAC Japan が発足した。その後、2016 年３月に ICT 全体を俯瞰した新たな ISAC 活動を目的とした組織である ICT-ISAC が発足し、2016 年６月に通信事業者に加え、放送事業者、セキュリティベンダー等もメンバーに加わり、2016 年７月より、本格的活動を開始した。ICT-ISAC は、ICT に関わるセキュリティの対策・対応レベルの向上に資する活動を行うために、会員企業間の幅広い相互連携を図り、安定した情報流通、情報伝達を維持することで、安全な ICT 社会の形成に寄与することを目的としている。

放送設備は可用性を極めて重視する設備であり、一般的にセキュリティ対策が困難である。対策は放送運行に影響を与えない範囲に限定して行う必要があり、セキュリティソフトの利用、セキュリティパッチ等に制約を伴う。そのため ICT-ISAC の放送設備サイバー攻撃対策 WG では、放送局に特化したセキュリティ確保の取り組み（放送事業者による情報交換、放送局のための各種ガイドライン策定と普及、並びに放送設備メーカとの情報交換及び働きかけ）を行っている。

その取り組みの一環として現在 ICT-ISAC では、３つのガイドライン等を策定している。

放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン（2020 年９月：放送と CATV のガイドラインを統合・改訂）は、国の安全基準等策定指針をベースとし、放送事業者の情報セキュリティ管理に関する社内規程の策定や改正を支援するものである。

放送設備サイバー攻撃対策ガイドライン（2018 年７月：策定、2020 年２月：第３版改訂）は、放送事業者が放送設備におけるセキュリティの確保等に取り組むにあたり、適切な放送設備の開発・整備・運用を支援し、放送の安全性確保の推進を目的としたものである。

放送設備サイバーセキュリティ対策（参考資料）（2021 年３月：第１版策定）は、放送法施行規則等が改正（2020 年３月施行）され、放送設備に関するサイバ

ーセキュリティ対策の確保が技術基準に位置づけられたことを受け、免許・再免許等の手続きに必要なサイバーセキュリティ対策を整理したものである。

３－５　サイバーセキュリティ確保に関する主な対策技術

放送設備のＩＰ化に伴い、インシデント発生により放送停止となる可能性のある項目を重点的に対応するとともに、レジリエンス性も考慮したサイバーセキュリティ確保に関する主な対策について、代表例をまとめた。

３－５－１　不正接続対策

外部および内部からの不正アクセスやDoS攻撃等によりサービス拒否を引き起こした場合放送停止につながる可能性があり、不正接続への対策が重要となる。不正接続への対策技術としては、以下のような例がある。

①　サーバ要塞化

サーバ等の稼働機器のリスク耐性を高めるため OS をセキュアな構成（リスク考慮の設定）にする。

- [パスワードの表示]ボタンの非表示
→ パスワードののぞき見防止

- 共有フォルダへの安全でないゲストログオンを無効にする
→ 認証されていないアクセスを無効化することで不要なアクセスを防止する

- リモートデスクトップ接続時に常にクライアントにパスワードを要求する
→リモートデスクトップ接続のショートカットにパスワードを保存した場合などのオートログインを防止

- 「ネットワークの場所」設定時にユーザーに管理権限を要求する
→ 通常のユーザーが「ネットワークの場所」を設定できるとリスクや攻撃対象が増大する

- イベントログのログ最大ファイルサイズをデフォルト値よりも増加させ記録できる量を増やす
→ 初期値ではサイズが小さいため調整

図３－５－１－１　サーバ要塞化の設定例

（導入効果と機能）

・OS の各種設定をセキュリティ的に堅牢な設定で構築（要塞化）する。
・最新版へのアップデート、不要なプログラムや機能の削除・停止、通信可能な相手先の限定、アクセス権限の必要最小限への限定、設定上の問題の修正などを行う。

②　ACL（Access Control List）設定

LAN スイッチにおいては、不要なポートを閉鎖する以外に、ACL を用いて不正通信を防止することが有効である。ACL は LAN スイッチを通過する不要な通信を制限する。

ACL による不正通信の防止措置は、他システムからの侵入や冗長化している系統間でのマルウェア拡散対策として有効である。特に、番組送出設備では決められた装置以外と通信を行うことはないため、ACL による対策は効果的と考えられる。

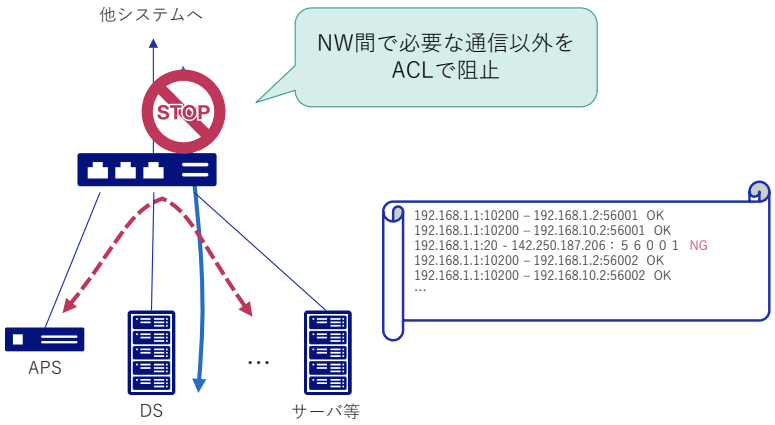


図３－５－１－２　**ACL の動作イメージ**

（導入効果と機能）

・L3 スイッチ（レイヤ３スイッチ）を通過する通信をチェックし、不正な通信を阻止する。
・他システムからの不正な侵入を阻止する。

③　ファイアーウォール、次世代型ファイアーウォール導入

ファイアーウォールは他システムと接続するネットワーク境界点に設置され、必要な通信のみ許可することで、他システムからの侵入・不正通信を抑止する。ファイアーウォールは、外部ネットワーク等との接続において ACL よりも強力な通信制限をかけることができる。

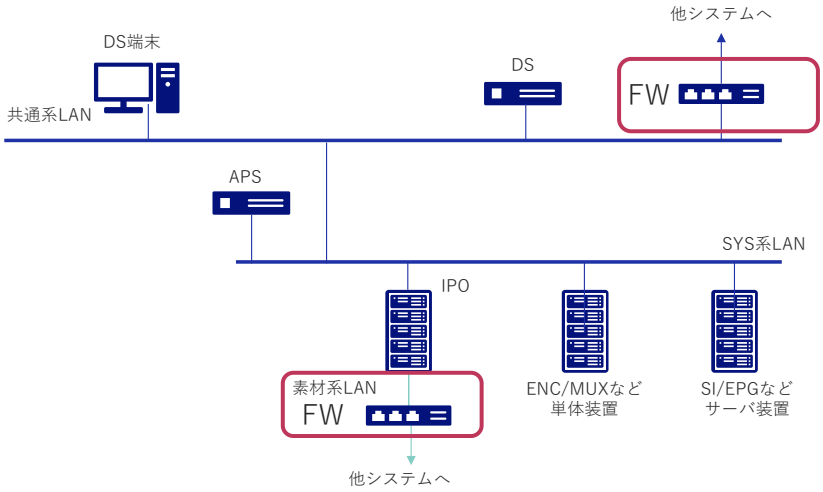


図３－５－１－３　**ファイアーウォールの動作イメージ**

（導入効果と機能）

・次世代型ファイアーウォールは、IPS やアプリケーション層レベルのパケットフィルタ、ウイルスチェック等の機能が追加された、より強固なファイアーウォールである。

・次世代型ファイアーウォールでは、従来型のファイアーウォールではチェックしていない、上位レイヤーでの通信制限が可能となる。

④　IDS／IPS 導入

IDS とは、外部から送信されるパケットをチェックして、不正アクセスと判断されるパケットが発見された場合には、管理者に連絡する機能を持つシステムである。一方、IPS とは、侵入検知システム機能に加えて、不正なパケットを自動的に遮断する機能を持っている。

なお、IDS 及び IPS はシグネチャ更新のためにネットワーク接続が必要なため、外部システムとの接続環境があるネットワークへの設置が必要となる[注1]。

注１　IPS の機能を含む次世代型ファイアーウォールも同様に、外部システムとの接続環境があるネットワークへの設置が必要となる。

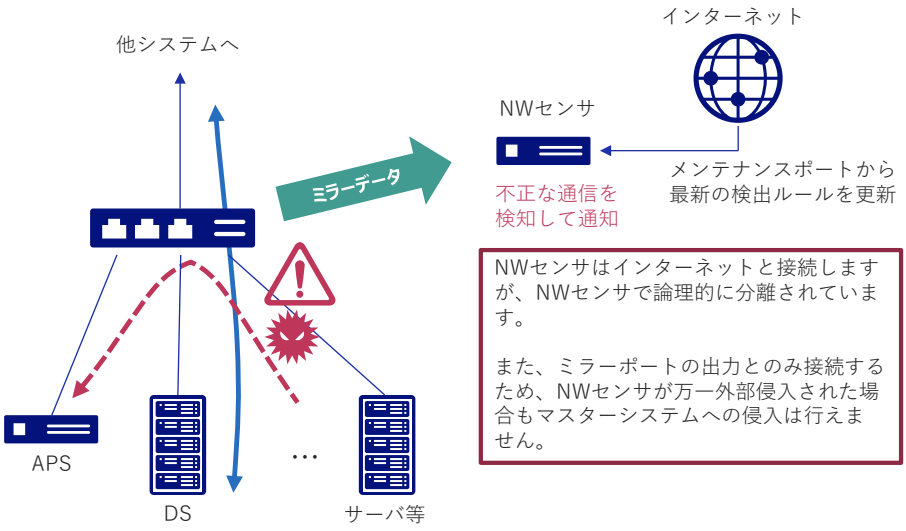


図３－５－１－４　IDS／IPS の動作イメージ

（導入効果と機能）

・番組送出設備の内部で用いられる LAN に IDS 又は IPS を導入することにより不正接続検出が可能となる。
・USB メモリ等を介して侵入したマルウェアなどによる内部の不正通信も検知可能となる。
・IDS はミラー出力のパケットを利用するため、本来の通信に影響を与えず機能の追加が可能（IPS はネットワーク内に設置する必要がある）である。
・他システムからの侵入やマルウェア感染の兆候を検知可能となる。

⑤　中継サーバ導入

中継サーバとは、目的の機器にログインするために用いるサーバであり、踏み台サーバやジャンプサーバとも呼ばれる。外部からの直接アクセスを許容せず、一旦中継サーバにログインした上で、中継サーバからさらに目的の機器にログインさせることで、誰がいつ、どのリソースにアクセスしているかを管理することができる。

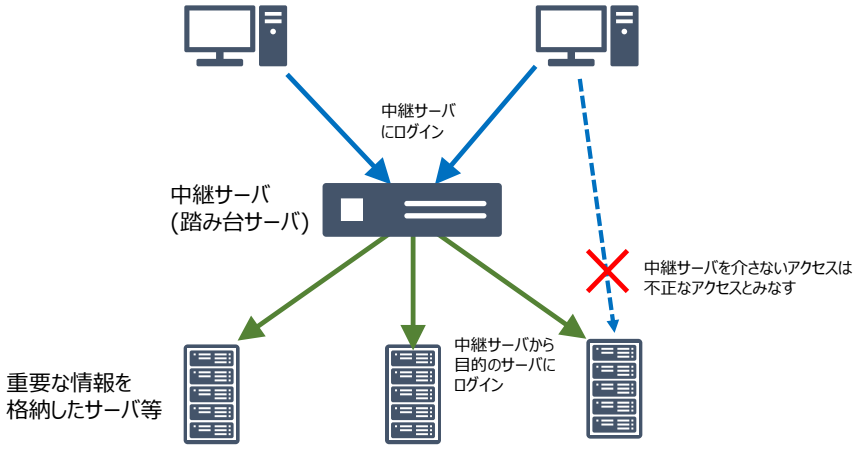


図３－５－１－５　**中継サーバの動作イメージ**

（導入効果と機能）

・中継サーバを監視することにより、監視・保守等の外部からのアクセスを一元的に管理できる。[注 2]

・中継サーバを経由していないアクセスは不正なアクセスとみなせる。

・中継サーバをシャットダウンすることにより、外部からのアクセスを遮断できる。

注 2 外部からのアクセスが一元化されるため、中継サーバのセキュリティ対策についてはより確実に実施する必要がある。

３－５－２　マルウェア感染対策

マルウェア感染により改ざん、サービス拒否（サービスが提供できない状態、処理が実行できない状況等）が発生した場合、放送停止につながる可能性がある。マルウェア感染への対策技術としては、以下のような例がある。

①　許可リスト型マルウェア対策

汎用 OS に対して、実行可能なプログラムを許可リストで管理し、リストにないプログラムは実行させない対策である。アプリケーション許可リストの導入は、アプリケーション起動時にチェックを行う仕組みのため、リアルタイム制御への影響が小さいウイルス対策である。また、実行ファイルの起動時にハッシュ情報をチェックするため、改ざんされたアプリケーションへの対策も行える。

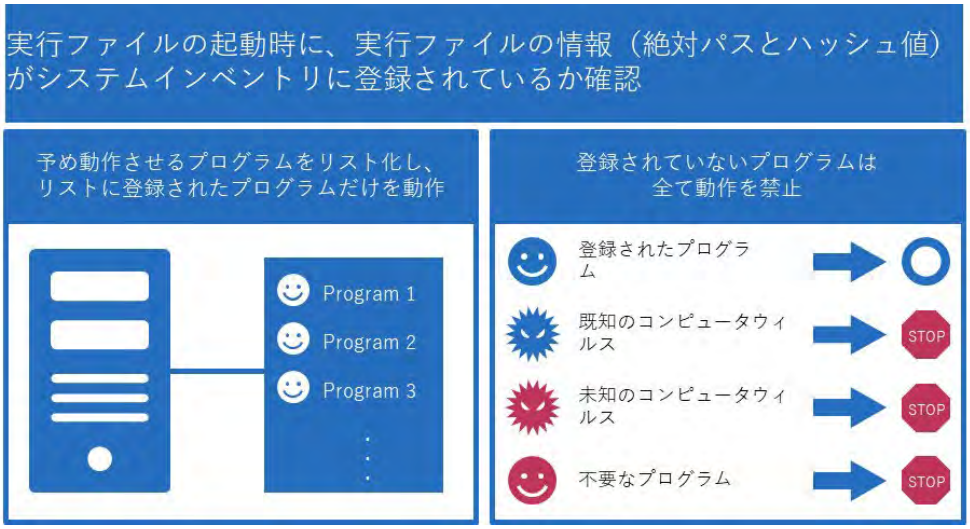


図３－５－２－１　**アプリケーション許可リストの動作イメージ**

（導入効果と機能）

- 起動を許可するアプリケーションを事前に設定し、未設定のアプリケーションの起動を禁止する。
- 万が一マルウェアが混入した場合もマルウェアの起動を抑止できる。
- 一般的なアンチウイルス（ウイルス対策）ソフトと比較して負荷が小さくリアルタイム制御への影響を最小化できる。

②　USB（Universal Serial Bus）メモリ持ち込み対策

USB メモリは可能な限り使用しないことが基本的な対策である。また、誤接続を防止するために、使用予定のない USB ポートは無効化又は閉塞処理を行うことも有効である。

やむをえず USB メモリを使用する場合は、使用前に専用端末にてウイルスチェックを実施することが望ましい。

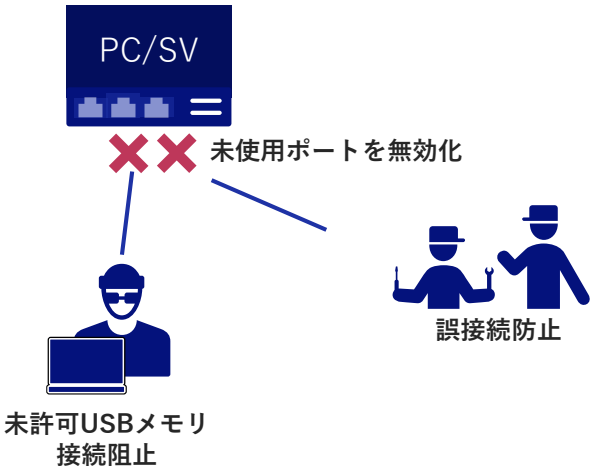


図３－５－２－２　**USB メモリ持ち込み対策**

（導入効果と機能）

・USB メモリを可能な限り使用しないことで、USB メモリを介したマルウェア感染を防止できる。
・USB メモリの紛失などによる情報漏洩を防止できる。

③　非常駐型ウイルスチェックツール導入

放送設備、特に番組送出設備では、番組の送出制御に影響が出るため常駐型のアンチウイルスソフトの導入が困難である。また、機器の保守時やソフトウェアアップデート時にウイルスチェックが必要となるが、インターネット接続がない環境ではシグネチャの更新が困難である。しかしながら、マルウェア感染対策のためには、定期的なウイルスチェックやアプリケーション許可リストでウイルスを検知・動作阻止した後の駆除が必要となる。

USB メモリタイプのアンチウイルスソフトは、機器内に常駐しないため、放送設備の運用休止中に任意のタイミングでウイルスチェックを実行可能である。シグネチャの更新も放送設備とは別のネットワークで可能なため、インターネット

接続が困難な番組送出設備等においてもウイルス情報を最新化してスキャンすることが可能である。

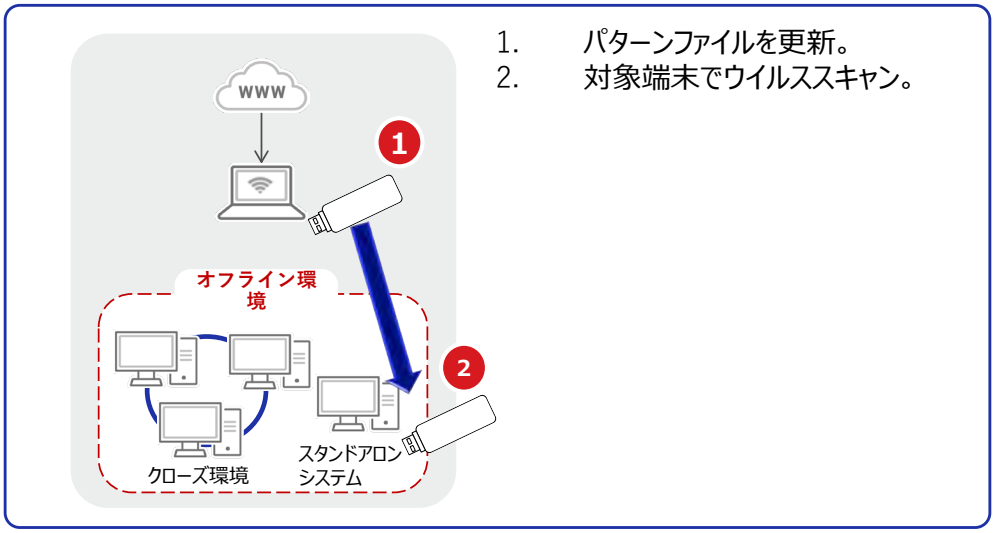


図３－５－２－３　USB メモリタイプのアンチウイルスソフト使用例

（導入効果と機能）

・放送設備の運用休止中などの任意のタイミングでウイルスチェックを実行する。

・処理に影響が出るため常駐型アンチウイルスソフトの導入が困難な設備でも、導入可能。

３－５－３　早期復旧

万が一サイバー攻撃を受け、システムが停止した場合に、早期復旧を行なえるようにする必要がある。

①　バックアップ取得

放送設備を構成する各サーバや装置については、バックアップを取得して、万が一攻撃を受け放送停止となった場合にバックアップにより早期の復旧を行うことが望ましい。バックアップ取得は、機器障害や故障等においても有効である。

番組送出設備はデータ保管システムではないため、バックアップ時にはシステムセットアップと設定情報を取得する。

一方で、復旧のための手法を明確化しておくことも重要である。

（導入効果と機能）

・データや設定情報を複製して保管しておくことで、システムが停止した場合にも早期の復旧が可能となる[注3]。

注3 物理的に別の場所に保管したりオフラインで保管したりすることは、大規模災害やランサムウェア攻撃に対しても有効である。

第４章　放送設備のＩＰ化に伴う安全・信頼性に係る技術基準

４－１　技術基準の検討に関する基本的な考え方

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、安全・信頼性に係る技術基準の検討を開始した。

クラウド化・集約化に伴う技術基準の検討については、ＩＰ化に伴う技術基準の検討後に実施することとするが、ＩＰ化に伴う技術的条件の検討段階において、その後のクラウド化・集約化を見据えた措置を施すことが合理的な場合等については、クラウド化・集約化に伴う技術基準についても考慮しつつ検討を行うこととした。

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。

また、検討の過程において、音声放送及び衛星放送についてもＩＰ化・クラウド化等の技術動向及びニーズが示されたことから、技術基準の検討対象として追加した。

技術基準の具体的な検討については、以下のとおり実施した。

（１）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・クラウド化等の各標準モデルを検討した。

（２）（１）で検討した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、取りまとめた。

なお、必要以上に厳しい技術基準を課した場合は、放送設備のＩＰ化・クラウド化等への移行を阻害する障壁となる可能性があるため、今後、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。

４－２　放送設備のＩＰ化・クラウド化等に係る標準モデル

現行の放送設備からＩＰ化及びクラウド化等への移行過程を明らかにするとともに、放送設備の構成等の変更箇所を特定し、安全・信頼性の確保のために必要な措置及びその対象設備を具体的に検討するため、放送の種別ごとに、各移行段階における標準モデルを策定した。

なお、当該モデルは、放送設備の各装置及びネットワーク等の標準的な構成を示すものであり、実際の構成については事業者によって異なる場合がある。

４－２－１　放送設備の移行過程

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されている。

また、放送設備のなかでも、マスター設備（番組送出設備）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・クラウド化であるとみなすことが可能である。

番組送出設備とは、法令上、「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）と定義されている設備である。

具体的には、以下のような機能を有しており、放送番組やＣＭ、時刻や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である。

- 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

図４－２－１－１　**地上デジタルテレビジョン放送の番組送出**

現行の番組送出設備は、主としてＳＤＩ（Serial Digital Interface）等の映像信号・音声信号を伝送するための専用規格を用いて各装置が接続されているが、今後、図４－２－１－２のようにＩＰ化、ソフトウェア及びクラウド化が進展するものと考えられる。

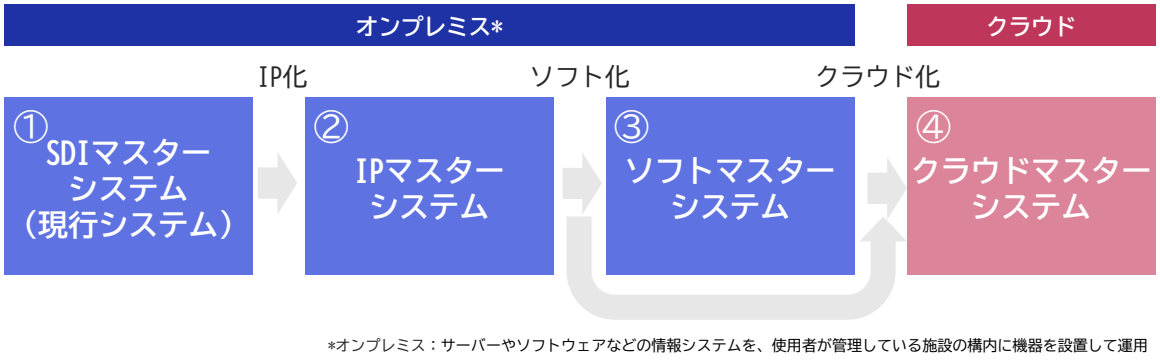


図４－２－１－２　**番組送出設備の移行過程（想定）**

各移行段階における装置やネットワークの構成を検討するにあたり、現行の番組送出設備を「ＳＤＩマスター」、ＩＰ化により実現される番組送出設備を「ＩＰマスター」、ソフトウェア化により実現される番組送出設備を「ソフトマスター」、クラウド化により実現される番組送出設備を「クラウドマスター」とした。

各番組送出設備の定義は表４－２－１－１のとおりである。

表４－２－１－１　**移行過程における各番組送出設備の定義**

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

また、各番組送出設備の特徴は表４－２－１－２のとおりである。なお、クラウドマスターについては、プライベートクラウドとパブリッククラウドに分けて特徴を示す。

表４－２－１－２　移行過程における各番組送出設備の特徴

比較項目	オンプレミス			クラウドマスター	
	SDI マスター	IP マスター	ソフトマスター	プライベート（ホスティング）	パブリック
CAPEX（初期費用）	資産計上	資産計上	資産計上	経費計上 （自社構築カスタマイズ部分は資産計上の場合もあり）	経費計上 （自社構築カスタマイズ部分は資産計上の場合もあり）
OPEX（インフラ）	・保守費 ・オーバーホール費用（専用機器） ・サーバリプレース費用（一部汎用機器）	・保守費 ・オーバーホール費用(一部専用機器) ・サーバリプレース費用（汎用機器）	・保守費 ・サーバリプレース費用（汎用機器）	・クラウド利用料 従量課金：利用分 ＋リソース確保分	・クラウド利用料 従量課金：利用分
OPEX（運用保守体制）	原則、放送局事業者にて体制が必要	原則、放送事業者にて体制が必要	原則、放送事業者にて体制が必要	クラウド事業者への運用委託が可能	クラウド事業者への運用委託が可能
機器更新	専用機器は長期使用が前提	汎用機器は５～７年程度	汎用機器は５～７年程度	不要 ※OS 等のサポート終了後にインフラ環境の再構築が必要な場合あり	不要 ※OS 等のサポート終了後にインフラ環境の再構築が必要な場合あり
機器の調達期間	一般的に専用機器の作りこみの期間が長い	汎用機器利用により機器の調達期間が短くなる	汎用機器の幅広い利用により機器の調達期間が短くなる	アカウント登録後すぐに利用できる。 Web 上から、サーバ台数やスペックを変更できる。 ただし、機器導入のリードタイムがかかる場合がある	アカウント登録後すぐに利用できる。 Web 上から、サーバ台数の増減やスペックを変更できる
機能の変更容易性	専用機器は設計時点で最適化されており機能拡張は限定的 将来的な機能拡張を想定し、導入時に準備しておく必要がある	汎用機器に実装された機能の変更容易性は高い 専用機器については SDI と同等	汎用機器に実装された機能の変更容易性は高い	クラウド上に実装された機能の変更容易性（アップスケール、ダウンスケールを含む）は高い	クラウド上に実装された機能の変更容易性（アップスケール、ダウンスケールを含む）は高い
低遅延性能	専用機器で機能実装しており、SDI から IP への変換も不要のため、最も低遅延	ネットワーク揺らぎを考慮した設計が必要	ネットワーク揺らぎと汎用機器のアーキテクチャを考慮した設計が必要	ネットワーク揺らぎ、汎用機器のアーキテクチャ、クラウド回線接続遅延を考慮した設計が必要	ネットワーク揺らぎ、汎用機器のアーキテクチャ、クラウド回線接続遅延を考慮した設計が必要
セキュリティ脅威	専用機器で機能実装しており、本線系は外部ネットワークから隔離されているため最もセキュリティの脅威が少ない	IP 化に伴い外部ネットワークと接続された状態になると、セキュリティの脅威が増加する	汎用機器化が進むことでセキュリティの脅威がさらに増加する	セキュリティ脅威は増大するため、独自のセキュリティ対策を施した設計・構築が必要	セキュリティ脅威は増大するため、クラウド事業者が提供するセキュリティポリシーも考慮した対策が必要
キャパシティ確保	事前サイジングの通りにキャパシティ確保(占有)される	事前サイジングの通りにキャパシティ確保(占有)される	事前サイジングの通りにキャパシティ確保(占有)される	リソースを動的に確保可能 パブリッククラウドより占有化し易い上、更に拡張が必要な場合も拡張が可能	リソースを動的に確保可能
可用性（業務継続性）	全コンポーネントやネットワークの冗長化、データのオンラインバックアップにより可用性の確保が可能（装置単体での可用性も高い）	全コンポーネントやネットワークの 冗長化、データのオンラインバックアップにより可用性の確保が可能	全コンポーネントやネットワークの 冗長化、データのオンラインバックアップにより可用性の確保が可能	冗長化やデータバックアップに加え、 リージョンやゾーンをまたぐ構成をとることで可用性の確保が可能	クラウドサービスの SLA に依存する （現状は SLA99.99%限度がほとんど）
スケーラビリティ	将来的なリソース増を想定し導入時に準備しておく必要がある	IP ネットワークへの機器の追加/削減は柔軟性がある	IP ネットワークへの機器の追加/削減は柔軟性がある	迅速なスケールアウト／スケールインが行える パブリッククラウドより拡張・縮小の柔軟性は劣る	迅速なスケールアウト／スケールインが行える
災害耐性（被災拠点バックアップ）	局内設置が基本であるため設備を設置した局舎が被災した場合、放送継続が困難となることが想定される	局内設置が基本であるため設備を設置した局舎が被災した場合、放送継続が困難となることが想定される	局内設置が基本であるため設備を設置した局舎が被災した場合、放送継続が困難となることが想定される	一定距離範囲内で複数のデータセンターを提供しており、災害耐性は高い ※データセンターとの回線に関する災害耐性の考慮も必要	一定距離範囲内で複数のデータセンターを提供しており、災害耐性は高い ※データセンターとの回線に関する災害耐性の考慮も必要
セキュリティインシデントの対応	予備系への切替等で対応	予備系への切替等で対応	予備系への切替等で対応	予備系への切替等の他、環境複製による対応も想定される	予備系への切替等の他、環境複製による対応も想定される

４－２－２　地上デジタルテレビジョン放送

（１）ＳＤＩマスターの標準モデル

従来の番組送出設備（ＳＤＩマスター）の標準的な構成は、図４－２－２－１のとおりである。

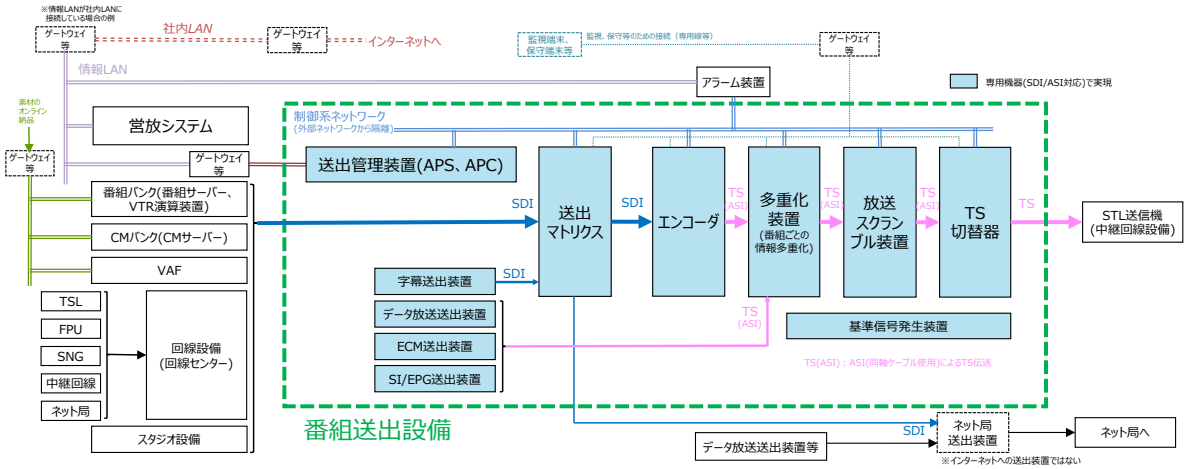


図４－２－２－１　**地上デジタルテレビジョン放送のＳＤＩマスターの標準モデル**

番組送出設備内には、放送本線系信号を伝送するための構成要素として、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及びＴＳ切替器が存在する。

送出マトリクスは、放送番組の放送本線信号を切り替えて出力する装置であり、専用機器（ハードウェア）で実現されている。また、放送本線信号を供給する各装置とＳＤＩ信号を伝送する同軸ケーブルにより１対１で接続される。

エンコーダは、映像及び音声信号を圧縮・符号化することによりＴＳ（Transport Stream）信号を生成する装置である。エンコーダはＳＤＩ対応の専用機器で実現されている。

多重化装置は、１つの番組を構成するための複数のＴＳ信号を多重化する装置である。多重化装置はＳＤＩ及びＡＳＩ対応の専用機器で実現されている。

放送スクランブル装置は、ＴＳ信号にスクランブル（映像信号や音声信号を暗号化し、解読する装置がないと受信機で放送番組が見られないようにする仕組み）をかける装置である。放送スクランブル装置はＡＳＩ対応の専用機器で実現されている。

ＴＳ切替器は、ＴＳ信号の出力先を切り替える装置である。ＴＳ切替器はＡＳＩ対応の専用機器で実現されている。

番組送出設備内には、放送本線系信号を伝送するための構成要素以外の構成要素として、送出管理装置、字幕送出装置、データ放送送出装置、ＥＣＭ（Entitlement Control Message）送出装置、ＳＩ（Service Information：番組配列情報）／ＥＰＧ（Electronic Program Guide：電子番組表）送出装置及び基準信号発生装置が存在する。これらの装置はＳＤＩ対応の専用機器で実現されている。

（２）ＩＰマスターの標準モデル

ＩＰ化された番組送出設備（ＩＰマスター）の標準的な構成は、図４－２－２－２のとおりである。

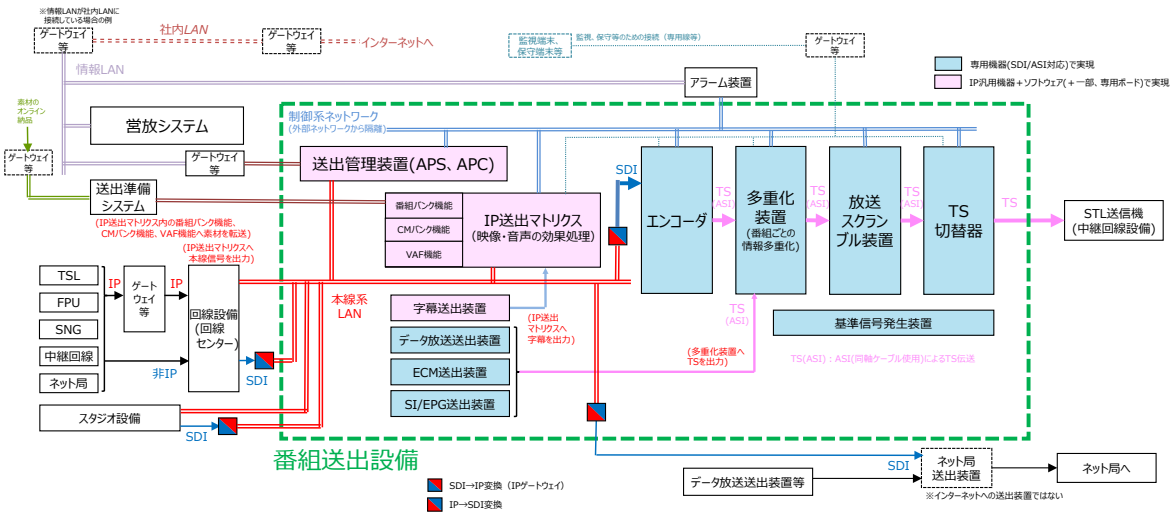


図４－２－２－２　**地上デジタルテレビジョン放送のＩＰマスターの標準モデル**

番組送出設備内には、放送本線系信号を伝送するための構成要素として、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及びＴＳ切替器が存在する。

ＩＰ送出マトリクスはＩＰ対応の汎用機器及びソフトウェアで実現される。ＳＤＩマスターの送出マトリクスは、放送本線信号を供給する各機器とＳＤＩ信号を伝送する同軸ケーブルにより１対１で接続されていたのに対し、ＩＰ送出マトリクスと放送本線信号を供給する各機器はそれぞれ本線系ＬＡＮに接続される。

エンコーダ、多重化装置、放送スクランブル装置及びＴＳ切替器は、ＳＤＩマスターと同様、ＳＤＩ対応の専用機器で実現される。

番組送出設備内には、放送本線系信号を伝送するための構成要素以外の構成要素として、ＳＤＩマスターと同様に、送出管理装置、字幕送出装置、データ放送送出装置、ＥＣＭ送出装置、ＳＩ／ＥＰＧ送出装置及び基準信号発生装置が存在する。これらの装置のうち、送出管理装置及び字幕送出装置は、ＩＰ対応の汎用機器及びソフトウェアで実現される。

ＩＰマスターの標準モデルにおいて、番組送出設備と周辺設備等との接続点は下記のとおりであり、各接続点におけるサイバーセキュリティの脅威について考察する。

① 演奏所内からの本線信号入力

スタジオ設備は演奏所内からＩＰ送出マトリクスへ放送本線信号を供給する。スタジオ設備は他のネットワークと接続しておらず、外部ネットワークから分離した状態にある。

スタジオ設備等の演奏所内設備が他のネットワークと接続していない状態であれば、演奏所内からの本線信号入力については外部ネットワークから隔離されているとみなすことができる。

ただし、近年の機器はネットワーク接続を前提とするものが多く、放送事業者が意識しないまま外部ネットワークに接続されるおそれがある。このことも十分考慮したサイバーセキュリティ対策を行うことが望ましい。

② 演奏所外からの本線信号入力

回線設備は演奏所外からＩＰ送出マトリクスへ放送本線信号を供給する。

回線設備に接続するネットワークとして、専用線、閉域網、放送事業者内で閉じた無線回線等を利用する場合とインターネット等を利用する場合が考えられる。

ＩＰマスターでは、演奏所外から本線信号がＩＰで提供されるため、ファイアーウォール等のサイバーセキュリティ対策が必須となる。

なお、番組送出設備のみをＩＰマスターに置き換え、回線設備等の他の設備は既存のものを用いる場合、演奏所外からの本線信号はＳＤＩ等で提供され、ＩＰに変換された後に番組送出設備に入力される。ＳＤＩ等の信号は、主に同

軸ケーブルを用いて機器同士を１対１で対向に接続し、映像及び音声信号は一方向のみに伝送されることから、演奏所外からの本線信号がＳＤＩ等で提供される場合には、基本的には外部ネットワークから隔離されているとみなすことができる。ただし、技術的には同軸ケーブル上で映像及び音声信号以外の信号を伝送することも可能であるため、同軸ケーブル上を流れる信号から制御信号等を取り出し実行する機能を有していないことを確認すること等が重要となる。

中継現場で用いられる機器等、演奏所外において使用される設備や回線についてもサイバーセキュリティ対策が必要である。なお、演奏所外と演奏所との通信に用いられるＴＳＬ（Transmitter to Studio Link)、ＦＰＵ（Field Pickup Unit)、ＳＮＧ（Satellite News Gathering）等は放送事業者のみが使用する回線であり、インターネットに対して比較的安全な伝送手段であると言える。

③ 中継回線設備へのＴＳ出力

中継回線設備は、ＴＳ切替器からのＴＳ信号を送信所へ伝送する。本標準モデルでは中継回線として固定無線回線であるＳＴＬ（Studio to Transmitter Link）送信機を想定しているが、使用する中継回線が異なる場合には別の装置が用いられる。

本標準モデルでは、ＴＳ切替器とＳＴＬ送信機との間は１対１の対向でＴＳ信号が一方向にのみ流れる接続を想定している。

中継回線は専用線、閉域網、放送事業者内で閉じた無線回線等で構成されており、中継回線の先にある放送局の送信設備も他のネットワークに接続していないことを想定している。

ＴＳ信号は、同軸ケーブル等を用いて機器同士を１対１で対向に接続し一方向のみに伝送されることから、中継回線設備に対してＴＳで出力する場合には、基本的には外部ネットワークから隔離されているとみなすことができる。ただし、技術的には同軸ケーブル上で映像及び音声信号以外の信号を伝送することも可能であるため、同軸ケーブル上を流れる信号から制御信号等を取り出し実行する機能を有していないことを確認すること等が重要となる。

④ ネット局送出装置への出力

系列のネット局へ番組を供給する場合、ＩＰ送出マトリクスはネット局送出装置へ映像及び音声信号を出力する。

本標準モデルでは、ＩＰ送出マトリクスからの出力を伝送する本線系ＬＡＮとネット局送出装置との間にはＩＰをＳＤＩに変換する装置が存在し、当該装置とネット局送出装置との間は１対１の対向でＳＤＩ信号が一方向にのみ流れる接続を想定している。

ネット局送出装置に対してＴＳで出力する場合には、基本的には外部ネットワークから隔離されているとみなすことができる。ただし、技術的には同軸ケーブル上で映像及び音声信号以外の信号を伝送することも可能であるため、同軸ケーブル上を流れる信号から制御信号等を取り出し実行する機能を有していないことを確認すること等が重要となる。

⑤ 送出管理装置と情報ＬＡＮの接続

情報ＬＡＮは、番組制作等の情報をやりとりするためのネットワークである。送出管理装置は情報ＬＡＮに接続され、番組、ＣＭなどの情報や関連業務を一元的に管理する営放システム（営業放送システム）の番組編成情報等を受け取る。

情報ＬＡＮは、社内ＬＡＮ等に接続している場合と接続していない場合がある。一方、社内ＬＡＮは一般的にインターネットと接続している。

ＩＰマスターでは、情報LAN経由でサイバー攻撃が行われた場合、送出管理装置が改ざんされるとともに、本線系LANを介して他の装置に影響を及ぼす可能性があることを考慮して、ファイアーウォール設置等のサイバーセキュリティ対策を行うことが必要となる。

⑥ ＩＰ送出マトリクスと送出準備システムの接続

ＩＰ送出マトリクスは送出準備システムに接続され、番組バンク機能、ＣＭバンク機能及びＶＡＦ（Video Audio File）機能がそれぞれの素材を送出準備システムから受け取る。

本標準モデルでは、ＩＰ送出マトリクスと送出準備システムとの間は１対１の対向接続を想定している。

送出準備システムへの素材の納品には、記録メディアを用いる場合とオンラインで行う場合がある。記録メディアのみで納品される場合には、送出準備システムは他のネットワークに接続しない。

ＩＰマスターでは、送出準備システム経由でサイバー攻撃が行われた場合、バンク機能を含む装置が改ざんされるとともに、本線系ＬＡＮを介して他の装

置に影響を及ぼす可能性があることを考慮して、送出準備システムにオンライン搬入される回線の境界点でのファイアーウォール設置等のサイバーセキュリティ対策を行うことが必要となる。

⑦ 番組送出設備内各機器と制御系ネットワークの接続

制御系ネットワークは、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である。制御系ネットワークには、送出管理装置以外に、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及びＴＳ切替器が接続される。また、番組送出設備内の各機器の異常を知らせるためのアラーム装置は、制御系ネットワークに接続するとともに、情報ＬＡＮにも接続する。

ＩＰマスターの制御系ネットワークはメーカの独自プロトコルを用いており、プロトコル仕様は公開されていないことを想定している。

⑧ 番組送出設備内各機器と監視端末、保守端末等との接続

番組送出設備外から番組送出設備内の各機器の監視、保守等を行うために、監視端末、保守端末等がゲートウェイ等を介して制御系ネットワークに接続する場合がある。

なお、番組送出設備内各機器と監視端末、保守端末等との間は、必要に応じて一時的に接続するように運用されている場合が多い。

現行制度では専用線またはＶＰＮ回線の使用、ポート番号またはＩＰアドレスによる接続制限若しくはＩＤ・パスワードにより権限を有する者だけが接続すること、及び未使用時は回線断とすることが望ましいとされていた。

ＩＰマスターでも、監視端末、保守端末等のサイバーセキュリティ対策が適切に実施されている限り、専用線は安全な伝送手段であると言える。一方、ＶＰＮ回線の使用についても、監視端末、保守端末等のサイバーセキュリティ対策が適切に実施されており、かつＶＰＮ回線を構成する機器の安全性が適切に確保されている限りにおいて、安全な伝送手段であると言える。近年ＶＰＮを介してシステム内部に侵入するサイバー攻撃が多く見られるが、ＶＰＮそのものは安全な技術であり、ＶＰＮを適切に運用していないことによる脆弱性が攻撃者から狙われている。サイバーセキュリティ確保のためには、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が必要である。またＶＰＮには、閉域網内でＶＰＮを構築する場合とインターネット上でＶＰＮを構築する場合（インターネットＶＰＮ）があるが、後者はＶＰＮを使

用していることを攻撃者が検知できることから、特に慎重に運用する必要がある。

ポート番号またはＩＰアドレスによる接続制限は、現在でも有効なサイバーセキュリティ対策である。

権限を有する者だけが接続することは現在でも有効なサイバーセキュリティ対策であるが、ＩＤ・パスワードについては流出できないように管理する必要があり、パスワードはさらに容易に類推できないように設定する必要がある。さらに、所有物認証及び生体認証等などの新しい技術を用いて権限を有する者だけが接続するとともに、複数の認証を組み合わせた多要素認証を使用することは、接続の安全性を高める。

未使用時には物理的に回線の接続を遮断すること等により稼働状態の管理を行うことが必要である。ただし、未使用時に回線の接続を遮断することは、サイバー攻撃の機会を減ずるという点では意味があるが、それのみをもってサイバーセキュリティ確保が達成されるわけではないことに留意すべきである。

（３）ソフトマスターの標準モデル

ソフト化は、ＩＰ化からクラウド化への移行過程において想定される形態であり、ソフト化された番組送出設備（ソフトマスター）は、ほとんどの装置がＩＰ対応の汎用機器及びソフトウェアで実現される。

ソフトマスターは開発段階にあり、放送設備メーカにおいて 2020 年代後半の実用化に向けて開発が進められている。

本作業班で検討したソフトマスターの標準的な構成は、図４－２－２－３のとおりであるが、今後の技術開発動向等を踏まえた見直しを行う必要がある暫定的なものであり、本報告書においては参考情報として掲載する。

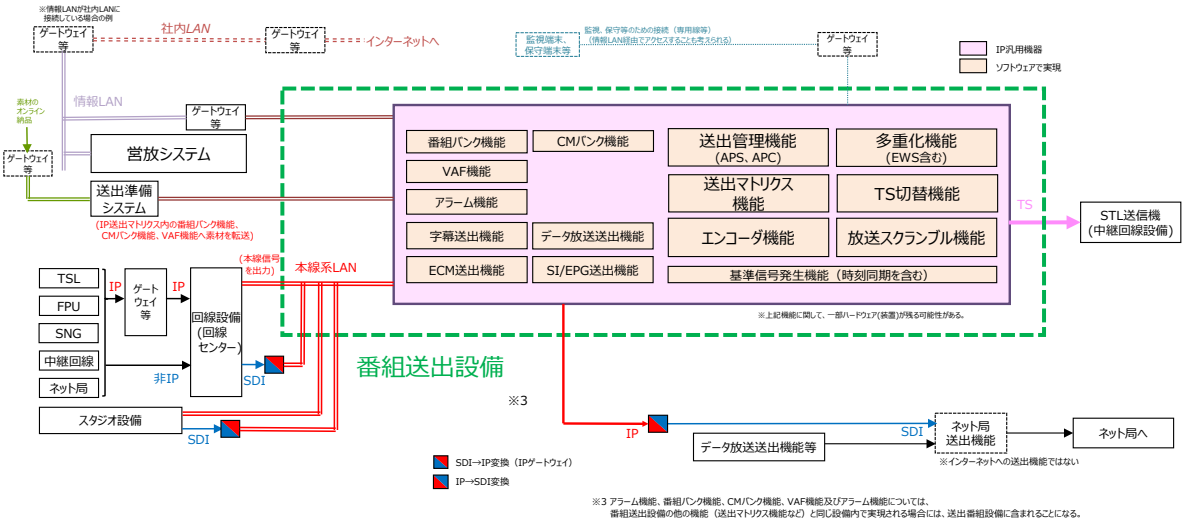


図４－２－２－３　**地上デジタルテレビジョン放送のソフトマスターの標準モデル（暫定）**

（４）クラウドマスターの標準モデル

クラウド化された番組送出設備（クラウドマスター）についても、放送設備メーカにおいて 2020 年代後半の実用化に向けて開発が進められている。

本作業班で検討したクラウドマスターの標準的な構成は、図４－２－２－４のとおりであるが、今後の技術開発動向等を踏まえた見直しを行う必要がある暫定的なものであり、本報告書においては参考情報として掲載する。

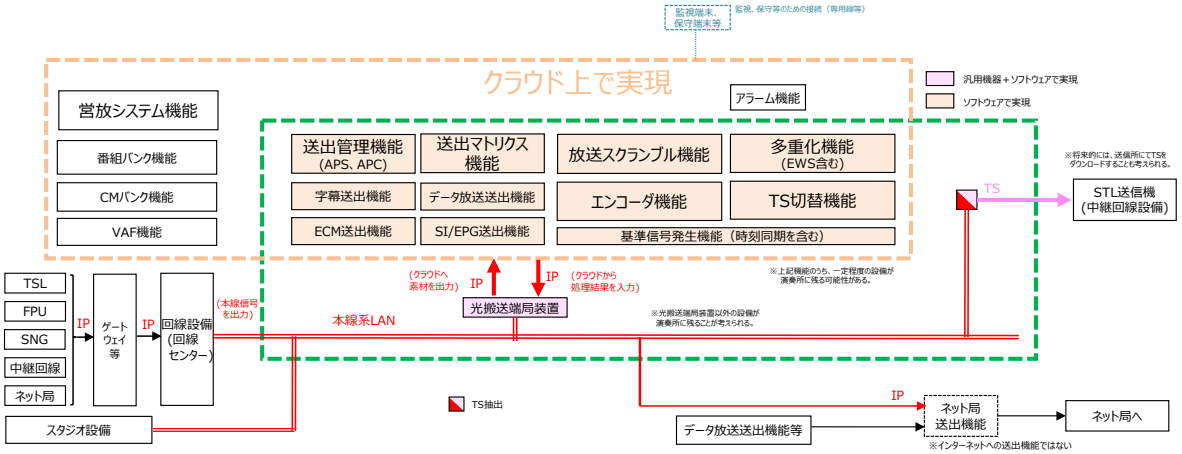


図４－２－２－４　地上デジタルテレビジョン放送のクラウドマスターの標準モデル（暫定）

４－２－３　音声放送

音声放送（ラジオ放送）における従来の番組送出設備では、音声をベースバンド信号で伝送する。音声放送のＩＰ化への移行過程を検討するにあたり、従来の番組送出設備を「ベースバンドマスター」、ＩＰ化により実現される番組送出設備を「ＩＰマスター（システム）」とした。

（１）ベースバンドマスターの標準モデル

従来の番組送出設備（ベースバンドマスター）の標準的な構成は、図４－２－３－１のとおりである。

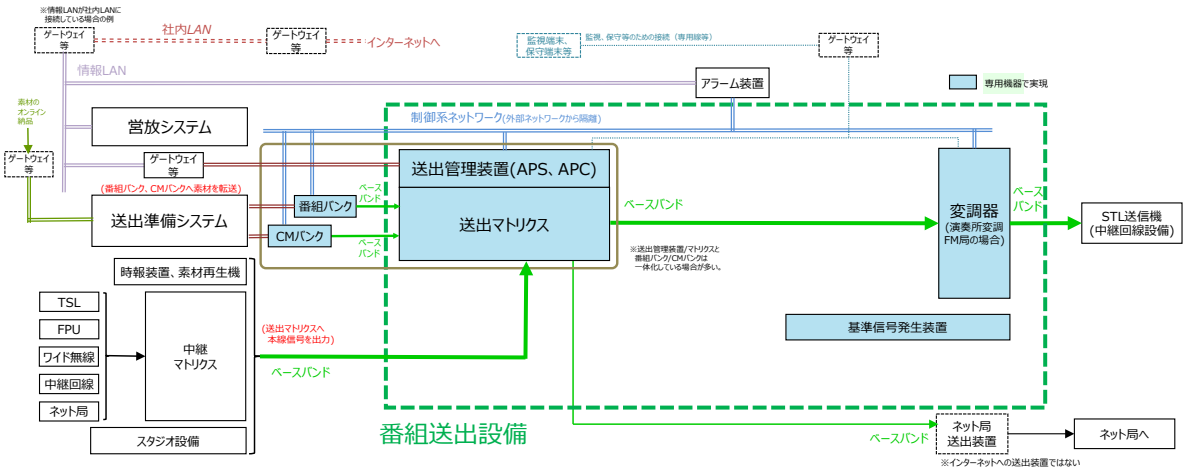


図４－２－３－１　**音声放送のベースバンドマスターの標準モデル**

番組送出設備内には、ベースバンド信号を伝送するための構成要素として、送出管理装置／送出マトリクス及び変調器が存在する。

送出管理装置は自動番組制御装置（APS（Automatic Program control System）又はAPC（Automatic Program Controller））とも呼ばれ、放送本線信号、番組素材等をあらかじめ決められたスケジュールに従って送受するとともに、番組を放送スケジュールに従って出力する。音声放送の送出管理装置は、放送番組のベースバンド信号を切り替えて出力する送出マトリクスと一体になっている。さらに、装置の内部に番組バンク機能及びＣＭバンク機能を備えており、蓄積した素材を送出することが可能である。送出管理装置はベースバンド対応の専用機器で実現されている。

変調器はベースバンド信号をＦＭ変調する装置であり、演奏所にて変調を行うＦＭ放送の場合に設けられる。ＡＭ放送の場合及び送信所にて変調を行うＦＭ放

送の場合、変調器は存在しない。変調器はベースバンド対応の専用機器として実現されている。

番組送出設備内には、放送本線系信号を伝送するための構成要素以外の構成要素として、基準信号発生装置が存在しており、専用機器で実現されている。

（２）ＩＰマスターの標準モデル

ＩＰ化された番組送出設備（ＩＰマスター）の標準的な構成は、図４－２－３－２のとおりである。

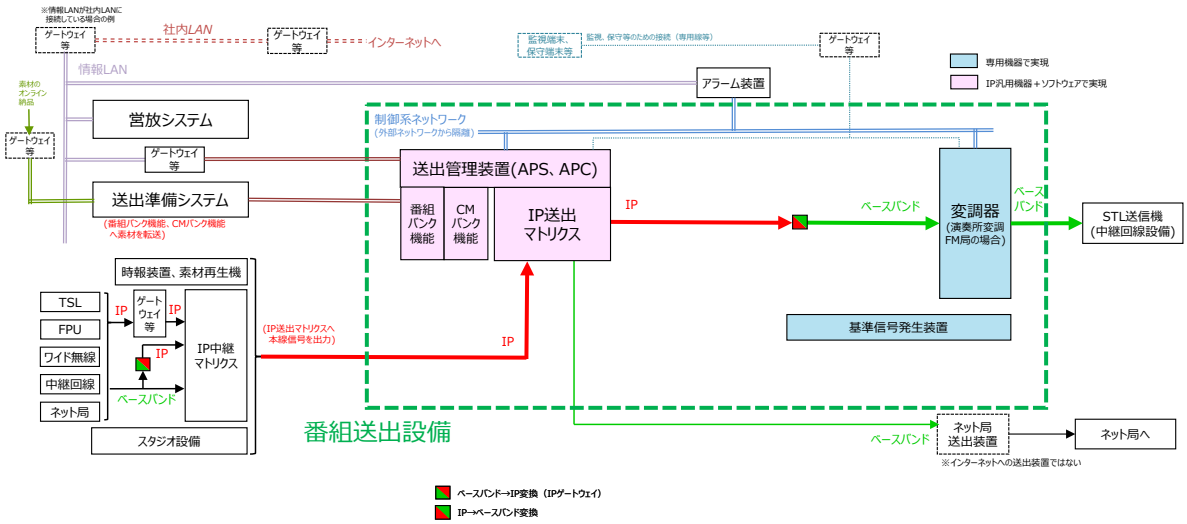


図４－２－３－２　**音声放送のＩＰマスターの標準モデル**

番組送出設備内には、放送本線系信号を伝送するための構成要素として、送出管理装置、変調器及び基準信号発生装置が存在する。

送出管理装置は、ベースバンドマスターと同様、送出マトリクスと一体になっており、装置の内部に番組バンク機能及びＣＭバンク機能を備えている。送出管理装置は、ＩＰ対応の汎用機器及びソフトウェアで実現される。

変調器は、ベースバンドマスターと同様、演奏所にて変調を行うＦＭ放送の場合のみ設けられ、専用機器として実現される。

番組送出設備内には、放送本線系信号を伝送するための構成要素以外の構成要素として、基準信号発生装置が存在しており、ベースバンドマスターと同様、専用機器として実現される。

音声放送のＩＰマスターの標準モデルにおいて、番組送出設備と番組送出設備外との接続点は下記のとおりであり、各接続点におけるサイバーセキュリティの脅威について考察する。

① 演奏所内からの本線信号入力

スタジオ設備は演奏所内からＩＰ送出マトリクスへ放送本線信号を供給する。スタジオ設備は他のネットワークと接続しておらず、外部ネットワークから分離した状態にある。

スタジオ設備等の演奏所内設備が他のネットワークと接続していない状態であれば、演奏所内からの本線信号入力については外部ネットワークから隔離されているとみなすことができる。

ただし、近年の機器はネットワーク接続を前提とするものが多く、放送事業者が意識しないまま外部ネットワークに接続されるおそれがある。このことも十分考慮したサイバーセキュリティ対策を行うことが望ましい。

② 演奏所外からの本線信号入力

ＩＰ中継マトリクスは演奏所外からＩＰ送出マトリクスへ放送本線信号を供給する。

ＩＰ中継マトリクスに接続するネットワークとして、専用線、閉域網、放送事業者内で閉じた無線回線等を利用する場合とインターネット等を利用する場合が考えられる。また、ＩＰ中継マトリクスに接続するネットワークを経由して接続する機器が他のネットワークに接続する場合も考慮する必要がある。

ＩＰマスターでは、演奏所外から本線信号がＩＰで提供されるため、ファイアーウォール等のサイバーセキュリティ対策が必須となる。

なお、番組送出設備のみをＩＰマスターに置き換え回線設備等の他の設備は既存のものを用いる場合に考慮すべき事項、及び演奏所外において使用される設備や回線について考慮すべき事項は、地上デジタルテレビジョン放送のＩＰマスターの場合と同様である。

③ 中継回線設備へのベースバンド出力

中継回線設備は、変調器からのベースバンド信号を送信所へ伝送する。本標準モデルでは中継回線として固定無線回線である STL 送信機を想定しているが、使用する中継回線が異なる場合には別の装置が用いられる。

本標準モデルでは、変調器と STL 送信機との間は１対１の対向でベースバンド信号が一方向にのみ流れる接続を想定している。

中継回線は専用線、閉域網、放送事業者内で閉じた無線回線等で構成されており、中継回線の先にある放送局の送信設備も他のネットワークに接続していないことを想定している。

ベースバンド信号は、同軸ケーブル等を用いて機器同士を１対１で対向に接続し一方向のみに伝送されることから、中継回線設備に対してＴＳで出力する場合には、基本的には外部ネットワークから隔離されているとみなすことができる。ただし、技術的には同軸ケーブル上で音声信号以外の信号を伝送することも可能であるため、同軸ケーブル上を流れる信号から制御信号等を取り出し実行する機能を有していないことを確認すること等が重要となる。

④　ネット局送出装置への出力

系列のネット局へ番組を供給する場合、送出管理装置はネット局送出装置へベースバンド信号を出力する。

本標準モデルでは、送出管理装置とネット局送出装置との間は１対１の対向でベースバンド信号が一方向にのみ流れる接続を想定している。

ネット局送出装置に対してベースバンドで出力する場合には、基本的には外部ネットワークから隔離されているとみなすことができる。ただし、技術的には同軸ケーブル上で音声信号以外の信号を伝送することも可能であるため、同軸ケーブル上を流れる信号から制御信号等を取り出し実行する機能を有していないことを確認すること等が重要となる。

⑤　送出管理装置と情報 LAN の接続

情報 LAN は、番組制作等の情報をやりとりするためのネットワークである。送出管理装置は情報 LAN に接続され、番組、ＣＭなどの情報や関連業務を一元的に管理する営放システムの番組編成情報等を受け取る。

情報 LAN は、社内 LAN 等に接続している場合と接続していない場合がある。一方、社内 LAN は一般的にインターネットと接続している。

ＩＰマスターでは、情報 LAN 経由でサイバー攻撃が行われた場合、送出管理装置が改ざんされるとともに、本線系 LAN を介して他の装置に影響を及ぼす可能性があることを考慮して、ファイアーウォール設置等のサイバーセキュリティ対策を行うことが必要となる。

⑥　送出管理装置と送出準備システムの接続

送出管理装置は送出準備システムに接続され、番組バンク機能及びＣＭバンク機能がそれぞれの素材を送出準備システムから受け取る。

本標準モデルでは、送出管理装置と送出準備システムとの間は１対１の対向接続を想定している。

送出準備システムへの素材の納品には、記録メディアを用いる場合とオンラインで行う場合がある。記録メディアのみで納品される場合には、送出準備システムは他のネットワークに接続しない。

ＩＰマスターでは、送出準備システム経由でサイバー攻撃が行われた場合、バンク機能を含む装置が改ざんされるとともに、本線系 LAN を介して他の装置に影響を及ぼす可能性があることを考慮して、送出準備システムにオンライン搬入される回線の境界点でのファイアーウォール設置等のサイバーセキュリティ対策を行うことが必要となる。

⑦　番組送出設備内各機器と制御系ネットワークの接続

制御系ネットワークは、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である。制御系ネットワークには、送出管理装置以外に、変調器が接続される。また、番組送出設備内の各機器の異常を知らせるためのアラーム装置は、制御系ネットワークに接続するとともに、情報 LAN にも接続する。

ＩＰマスターの制御系ネットワークはメーカの独自プロトコルを用いており、プロトコル仕様は公開されていないことを想定している。

⑧　番組送出設備内各機器と監視端末、保守端末等との接続

番組送出設備外から番組送出設備内の各機器の監視、保守等を行うために、監視端末、保守端末等がゲートウェイ等を介して制御系ネットワークに接続する場合がある。

なお、番組送出設備内各機器と監視端末、保守端末等との間は、必要に応じて一時的に接続するように運用されている場合が多い。

監視端末、保守端末等との接続において考慮すべき事項は、地上デジタルテレビジョン放送のＩＰマスターの場合と同様である。

４－２－４　衛星放送

衛星放送については、ＢＳ放送の場合とＣＳ放送の場合で番組送出設備の構成が大きく異なるため、それぞれについて標準モデルを策定した。

４－２－４－１　ＢＳ放送

ＢＳ放送のＩＰ化への移行過程を検討するにあたり、従来の番組送出設備を「ＳＤＩマスター」、ＩＰ化により実現される番組送出設備を「ＩＰマスター」とした。

（１）ＳＤＩマスターの標準モデル

従来の番組送出設備（ＳＤＩマスター）の標準的な構成は、図４－２－４－１－１のとおりである。

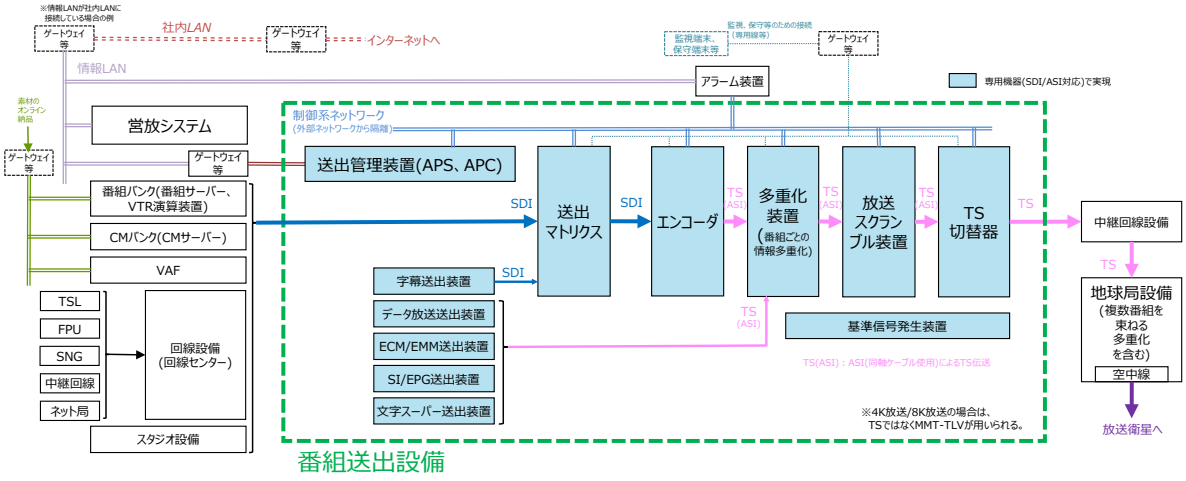


図４－２－４－１－１　**ＢＳ放送のＳＤＩマスターの標準モデル**

全体的に地上デジタルテレビジョン放送のＳＤＩマスターと類似した構成となっており、番組送出設備内には、放送本線系信号を伝送するための構成要素として、地上デジタルテレビジョン放送のＳＤＩマスターと同様、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及びＴＳ切替器が存在する。

これらの装置は、地上デジタルテレビジョン放送のＳＤＩマスターと同様、専用機器で実現されている。

番組送出設備内には、放送本線系信号を伝送するための構成要素以外の構成要素として、送出管理装置、字幕送出装置、データ放送送出装置、ＥＣＭ送出

装置、ＳＩ／ＥＰＧ送出装置、文字スーパー送出装置及び基準信号発生装置が存在しており、いずれの装置も専用機器で実現されている。

（２）ＩＰマスターの標準モデル

ＩＰ化された番組送出設備（ＩＰマスター）の標準的な構成は、図４－２－４－１－２のとおりである。

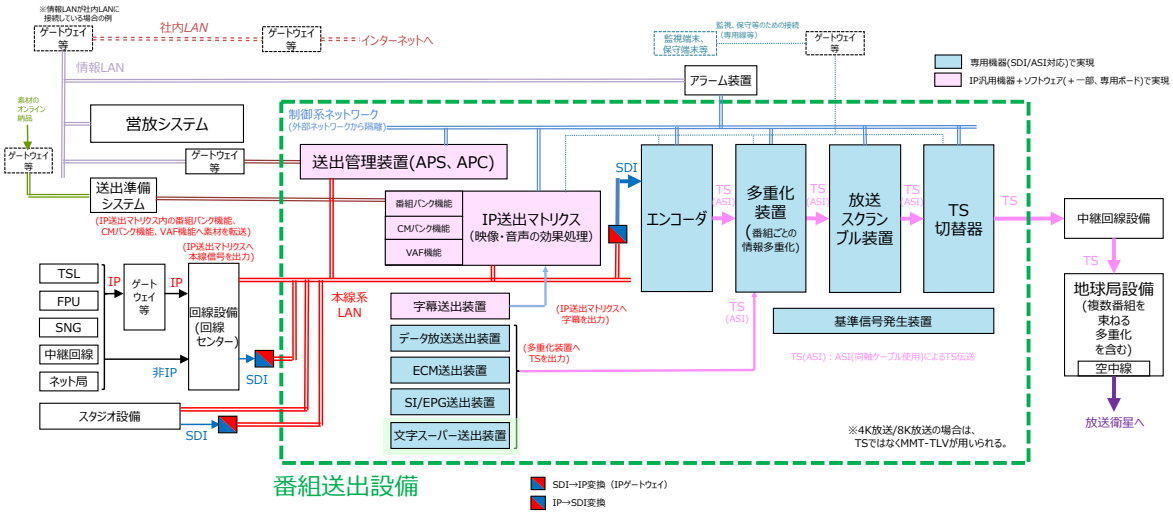


図４－２－４－１－２　**ＢＳ放送のＩＰマスターの標準モデル**

全体的に地上デジタルテレビジョン放送のＩＰマスターと類似した構成となっており、番組送出設備内には、放送本線系信号を伝送するための構成要素として、地上デジタルテレビジョン放送のＩＰマスターと同様、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及びＴＳ切替器が存在する。

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及びＴＳ切替器については、一部に映像・音声信号の伝送規格が異なる部分があるものの、地上デジタルテレビジョン放送のＩＰマスターにおける各装置と同様の構成となっている。

番組送出設備内には、放送本線系信号を伝送するための構成要素以外の構成要素として、送出管理装置、字幕送出装置、データ放送送出装置、ＥＣＭ送出装置、ＳＩ／ＥＰＧ送出装置、文字スーパー送出装置及び基準信号発生装置が存在する。これらの装置のうち、送出管理装置及び字幕送出装置は、ＩＰ対応の汎用機器及びソフトウェアで実現される。

ＢＳ放送のＩＰマスターの標準モデルにおいて、番組送出設備と番組送出設備外との接続点は下記のとおりであり、各接続点におけるサイバーセキュリティの脅威について考察する。

① 演奏所内からの本線信号入力

スタジオ設備は演奏所内からＩＰ送出マトリクスへ放送本線信号を供給する。スタジオ設備は他のネットワークと接続しておらず、外部ネットワークから分離した状態にある。

スタジオ設備等の演奏所内設備が他のネットワークと接続していない状態であれば、演奏所内からの本線信号入力については外部ネットワークから隔離されているとみなすことができる。

ただし、近年の機器はネットワーク接続を前提とするものが多く、放送事業者が意識しないまま外部ネットワークに接続されるおそれがある。このことも十分考慮したサイバーセキュリティ対策を行うことが望ましい。

② 演奏所外からの本線信号入力

回線設備は演奏所外からＩＰ送出マトリクスへ放送本線信号を供給する。

回線設備に接続するネットワークとして、専用線、閉域網、放送事業者内で閉じた無線回線等を利用する場合とインターネット等を利用する場合が考えられる。また、回線設備に接続するネットワークを経由して接続する機器が他のネットワークに接続する場合も考慮する必要がある。

ＩＰマスターでは、演奏所外から本線信号がＩＰで提供されるため、ファイアーウォール等のサイバーセキュリティ対策が必須となる。

なお、番組送出設備のみをＩＰマスターに置き換え回線設備等の他の設備は既存のものを用いる場合に考慮すべき事項、及び演奏所外において使用される設備や回線について考慮すべき事項は、地上デジタルテレビジョン放送のＩＰマスターの場合と同様である。

③ 中継回線設備へのＴＳ出力

中継回線設備は、ＴＳ切替器からのＴＳ信号等を地球局へ伝送する。

本標準モデルでは、ＴＳ切替器と中継回線との間は１対１の対向でＴＳ信号等が一方向にのみ流れる接続を想定している。

中継回線は専用線、閉域網、放送事業者内で閉じた無線回線等で構成されており、中継回線の先にある放送局の送信設備も他のネットワークに接続していないことを想定している。

ＴＳ信号等は、同軸ケーブル等を用いて機器同士を１対１で対向に接続し一方向のみに伝送されることから、中継回線設備に対してＴＳ等で出力する場合には、基本的には外部ネットワークから隔離されているとみなすことができる。ただし、技術的には同軸ケーブル上で映像及び音声信号以外の信号を伝送することも可能であるため、同軸ケーブル上を流れる信号から制御信号等を取り出し実行する機能を有していないことを確認すること等が重要となる。

④ 送出管理装置と情報ＬＡＮの接続

情報ＬＡＮは、番組制作等の情報をやりとりするためのネットワークである。送出管理装置は情報ＬＡＮに接続され、番組、ＣＭなどの情報や関連業務を一元的に管理する営放システム（営業放送システム）の番組編成情報等を受け取る。

情報ＬＡＮは、社内ＬＡＮ等に接続している場合と接続していない場合がある。一方、社内ＬＡＮは一般的にインターネットと接続している。

ＩＰマスターでは、情報ＬＡＮ経由でサイバー攻撃が行われた場合、送出管理装置が改ざんされるとともに、本線系ＬＡＮを介して他の装置に影響を及ぼす可能性があることを考慮して、ファイアーウォール設置等のサイバーセキュリティ対策を行うことが必要となる。

⑤ ＩＰ送出マトリクスと送出準備システムの接続

ＩＰ送出マトリクスは送出準備システムに接続され、番組バンク機能、ＣＭバンク機能及びＶＡＦ機能がそれぞれの素材を送出準備システムから受け取る。

本標準モデルでは、ＩＰ送出マトリクスと送出準備システムとの間は１対１の対向接続を想定している。

送出準備システムへの素材の納品には、記録メディアを用いる場合とオンラインで行う場合がある。記録メディアのみで納品される場合には、送出準備システムは他のネットワークに接続しない。

ＩＰマスターでは、送出準備システム経由でサイバー攻撃が行われた場合、バンク機能を含む装置が改ざんされるとともに、本線系 LAN を介して他の装置に影響を及ぼす可能性があることを考慮して、送出準備システムにオンライン搬入される回線の境界点でのファイアーウォール設置等のサイバーセキュリティ対策を行うことが必要となる。

⑥ 番組送出設備内各機器と制御系ネットワークの接続

制御系ネットワークは、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である。制御系ネットワークには、送出管理装置以外に、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及びＴＳ切替器が接続される。また、番組送出設備内の各機器の異常を知らせるためのアラーム装置は、制御系ネットワークに接続するとともに、情報 LAN にも接続する。

ＩＰマスターの制御系ネットワークはメーカの独自プロトコルを用いており、プロトコル仕様は公開されていないことを想定している。

⑦ 番組送出設備内各機器と監視端末、保守端末等との接続

番組送出設備外から番組送出設備内の各機器の監視、保守等を行うために、監視端末、保守端末等がゲートウェイ等を介して制御系ネットワークに接続する場合がある。

なお、番組送出設備内各機器と監視端末、保守端末等との間は、必要に応じて一時的に接続するように運用されている場合が多い。

監視端末、保守端末等との接続において考慮すべき事項は、地上デジタルテレビジョン放送のＩＰマスターの場合と同様である。

４－２－４－２　ＣＳ放送

ＣＳ放送では、放送設備のＩＰ化が進展しており、ＳＤＩ信号により放送本線系信号を伝送する従来の番組送出設備（ＳＤＩマスター）からＩＰ化により実現された番組送出設備（ＩＰマスター）への移行が進んでいる。そのため、ＣＳ放送の標準モデルについては、「ＩＰマスター」を基本として検討した。

（１）ＩＰマスター

ＣＳ放送では、基幹放送局提供事業者が認定基幹放送事業者より委託を受けて、認定基幹放送事業者に対して番組送出設備を含むプラットフォーム設備を提供している。認定基幹放送事業者が基幹放送局提供事業者のプラットフォーム設備を利用する場合、当該プラットフォームは地球局設備と同一施設内に設置され、認定基幹放送事業者の番組制作設備（番組素材を番組送出設備へ送出するプレイアウト設備等を含む）は、当該プラットフォームと異なる拠点に設置される。

ＩＰマスターの標準的な構成は、図４－２－４－２－１のとおりである。

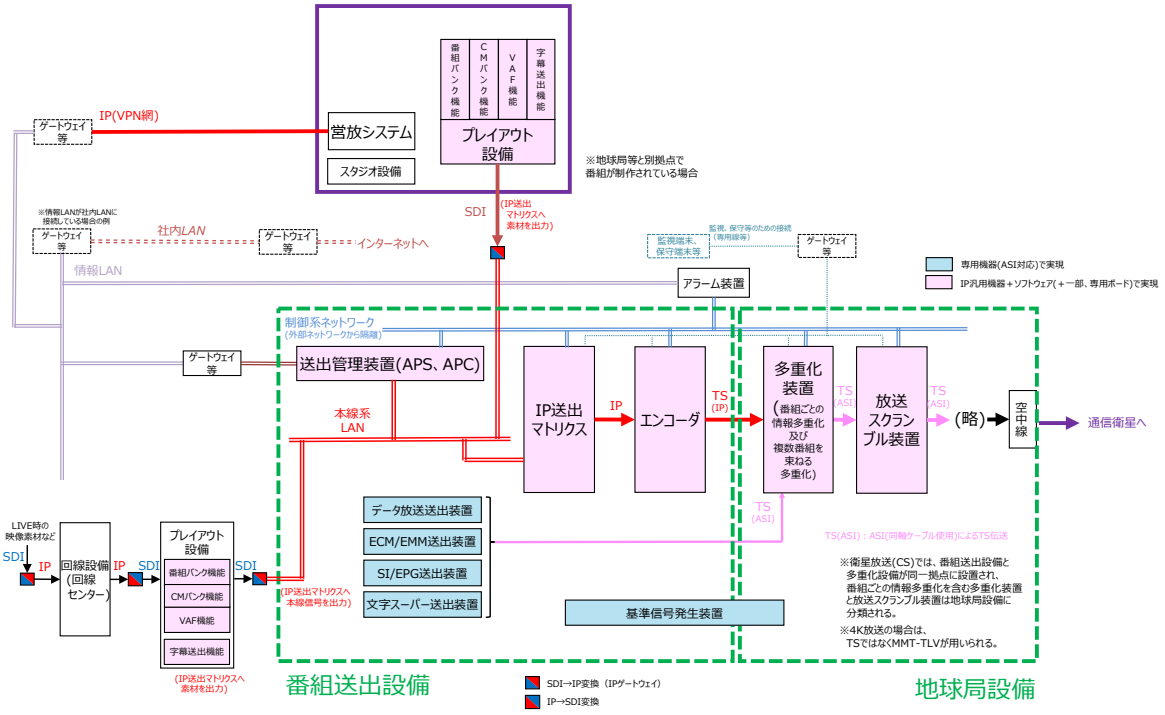


図４－２－４－２－１　ＣＳ放送のＩＰマスターの標準モデル

番組送出設備内には、放送本線系信号を伝送するための構成要素として、ＩＰ送出マトリクス及びエンコーダが存在する。

ＩＰ送出マトリクスは放送番組の素材を切り替えて出力する装置であり、ＩＰ対応の汎用機器及びソフトウェアで実現される。

エンコーダは、映像及び音声信号を圧縮・符号化することによりＴＳ信号を生成する装置であり、ＩＰ対応の汎用機器及びソフトウェアで実現される。

ＢＳ放送のＩＰマスターの標準モデルでは、放送本線系信号を伝送するための構成要素である多重化装置及び放送スクランブル装置が番組送出設備内に存在するが、ＣＳ放送のＩＰマスターの標準モデルでは地球局設備内に多重化装置及び放送スクランブル装置が存在する。

番組送出設備内には、放送本線系信号を伝送するための構成要素以外の構成要素として、送出管理装置、データ放送送出装置、ＥＣＭ／ＥＭＭ（Entitlement Management Message）送出装置、ＳＩ／ＥＰＧ送出装置、文字スーパー送出装置及び基準信号発生装置が存在する。

ＣＳ放送のＩＰマスターの標準モデルにおいて、番組送出設備と番組送出設備外との接続点は下記のとおりであり、各接続点におけるサイバーセキュリティの脅威について考察する。

① 異なる拠点に設けられた放送事業者の施設からの放送本線信号入力

番組送出設備と異なる拠点に設けられた認定基幹放送事業者の施設には、プレイアウト設備（演奏所外）、スタジオ設備、営放システム等が存在する。

プレイアウト設備（演奏所外）は、ＩＰ送出マトリクスへ放送本線信号を供給する設備である。内部に番組バンク機能、ＣＭバンク機能、ＶＡＦ機能及び字幕送出機能を備えており、蓄積した素材を送出することが可能である。また、スタジオ設備からの放送本線信号も、プレイアウト設備（演奏所外）経由でＩＰ送出マトリクスへ供給する。

接続に用いる回線は専用線、閉域網、放送事業者内で閉じた無線回線等で構成されていることを想定している。また、プレイアウト設備（演奏所外）と本線系 LAN との間にはＩＰゲートウェイ（ＳＤＩをＩＰに変換する装置）が存在し、プレイアウト設備（演奏所外）とＩＰゲートウェイとの間は１対１の対向で放送本線信号が一方向にのみ流れる接続を想定している。

ＳＤＩ信号は、機器同士を１対１で対向に接続し、映像及び音声信号は一方向のみに伝送される。接続に用いる回線は専用線、閉域網、放送事業者内で閉じた無線回線等で構成されており、プレイアウト設備のサイバーセキュリティ対策が適切に実施されている限りは安全な伝送手段であると言える。

ただし、接続回線としては安全であっても、プレイアウト設備を含む認定基幹放送事業者の施設のサイバーセキュリティ確保を確実に行う必要がある。

② 演奏所外（①の場合を除く）からの本線信号入力

プレイアウト設備（演奏所内）は回線設備に接続されており、演奏所外からＩＰ送出マトリクスへ放送本線信号を供給する。また、内部に番組バンク機能、ＣＭバンク機能、ＶＡＦ機能及び字幕送出機能を備えており、蓄積した素材を送出することが可能である。

また、プレイアウト設備（演奏所内）と本線系 LAN との間にはＩＰゲートウェイが存在し、プレイアウト設備（演奏所外）とＩＰゲートウェイとの間は１対１の対向で放送本線信号が一方向にのみ流れる接続を想定している。

ＩＰマスターでは、演奏所外から本線信号がＩＰで提供されるため、ファイアーウォール等のサイバーセキュリティ対策が必須となる。

なお、番組送出設備のみをＩＰマスターに置き換え回線設備等の他の設備は既存のものを用いる場合に考慮すべき事項、及び演奏所外において使用される設備や回線について考慮すべき事項は、地上デジタルテレビジョン放送のＩＰマスターの場合と同様である。

③ 多重化装置へのＴＳ出力

エンコーダは、ＴＳ信号等を多重化装置へ伝送する。

本標準モデルでは、エンコーダと多重化装置との間は１対１の対向でＴＳ信号等が一方向にのみ流れる接続を想定している。

多重化装置の後段にある各装置は他のネットワークに接続していないことを想定している。

ＴＳ信号等は、同軸ケーブル等を用いて機器同士を１対１で対向に接続し一方向のみに伝送されることから、中継回線設備に対してＴＳ等で出力する場合には、基本的には外部ネットワークから隔離されているとみなすことができる。ただし、技術的には同軸ケーブル上で映像及び音声信号以外の信号を伝送することも可能であるため、同軸ケーブル上を流れる信号から制御信号等を取り出し実行する機能を有していないことを確認すること等が重要となる。

④ 送出管理装置と情報ＬＡＮの接続

情報ＬＡＮは、番組制作等の情報をやりとりするためのネットワークである。送出管理装置は情報ＬＡＮに接続され、番組、ＣＭなどの情報や関連業務を一元的に管理する営放システム（営業放送システム）の番組編成情報等を受け取る。

情報ＬＡＮは社内ＬＡＮ等に接続しており、社内ＬＡＮはインターネットと接続していることを想定している。

ＩＰマスターでは、情報ＬＡＮ経由でサイバー攻撃が行われた場合、送出管理装置が改ざんされるとともに、本線系ＬＡＮを介して他の装置に影響を及ぼす可能性があることを考慮して、ファイアーウォール設置等のサイバーセキュリティ対策を行うことが必要となる。

⑤ 番組送出設備内各機器と制御系ネットワークの接続

制御系ネットワークは、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である。制御系ネットワークには、送出管理装置以外に、ＩＰ送出マトリクス、エンコーダ、多重化装置及び放送スクランブル装置が接続される。また、番組送出設備内の各機器の異常を知らせるためのアラーム装置は、制御系ネットワークに接続するとともに、情報 LAN にも接続する。

ＩＰマスターの制御系ネットワークはメーカの独自プロトコルを用いており、プロトコル仕様は公開されていないことを想定している。

⑥ 番組送出設備内各機器と監視端末、保守端末等との接続

番組送出設備外から番組送出設備内の各機器の監視、保守等を行うために、監視端末、保守端末等がゲートウェイ等を介して制御系ネットワークに接続する場合がある。

なお、番組送出設備内各機器と監視端末、保守端末等との間は、必要に応じて一時的に接続するように運用されている場合が多い。

監視端末、保守端末等との接続において考慮すべき事項は、地上デジタルテレビジョン放送のＩＰマスターの場合と同様である。

４－３　放送設備のＩＰ化に伴う安全・信頼性に係る技術基準の論点

４－２で検討を行ったＩＰ化に係る標準モデルを踏まえると、各放送種別とも、ＩＰ化に伴い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り、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。

番組送出設備のＩＰ化により、従来の番組送出設備からは、以下の点において変更が生じると考えられる。

（１）放送本線系の伝送回線

従来の番組送出設備において、放送本線系の伝送回線は、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（メタルケーブル）が使用されているが、番組送出設備のＩＰ化に伴い、その一部がＩＰ回線（光ファイバケーブル等）に変更されることになる。

具体的には、番組送出設備の入力端子からＩＰ送出マトリクスの出力までの回線がＩＰ回線に置き換わる一方で、その先、エンコーダの入力から番組送出設備の出力端子までについては、従来どおり放送専用伝送規格の回線が使用される場合が多いと想定される。

（２）構成装置

従来の番組送出設備は、機能ごとに設計された専用機器（ハードウェア）によって構成されており、各機器間は、ＳＤＩ、ＡＳＩ及びベースバンド等の放送専用伝送規格の回線、並びに放送設備製造メーカ独自の通信プロトコルを用いた制御系ＬＡＮにより接続されている。

番組送出設備のＩＰ化に伴い、主に送出管理装置（ＡＰＳ／ＡＰＣ）及び送出マトリクスが、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。また、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となることも想定される。

一方で、オールＩＰ化への移行過程においては、送出マトリクスから先の装置、すなわちエンコーダ、多重化装置、放送スクランブル装置、ＴＳ切替器、変調装置（音声放送の場合）等については、コスト低減等の観点から、既存の専用機器を継続して使用する場合も想定される。その場合は、回線の接続点において、ＩＰからＳＤＩ／ＡＳＩ／ベースバンド等への変換、又はその逆の変換が必要となる。

（３）外部ネットワークとの接続

従来の番組送出設備においては、放送本線系の伝送回線にＳＤＩ、ＡＳＩ及びベースバンド等の放送専用伝送規格の回線が使用されていることをもっ

て、通信方式の異なるインターネット等の外部ネットワークからの隔離が、原則確保されているとみなしている。

番組送出設備のＩＰ化に伴い、放送本線系の伝送回線の一部がＩＰ回線に置き換わることから、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判断される。

なお、外部ネットワークに対して、どのような接続（常時接続か随時接続か等）を行うかについては、各放送事業者において、利便性、安全性及び経済性等を踏まえた上での選択になると想定される。

一方、番組送出設備の設置場所については、従来と同様、放送事業者の施設内（主に演奏所内）であることに変更はない。

以上により、番組送出設備のＩＰ化に伴い、放送本線系が外部ネットワークと接続された状態になり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必要がある。

当該検討にあたっては、従来型のサイバーセキュリティ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することが望ましい。

また、放送継続のために番組送出設備に求められる可用性の担保、並びに措置内容の経済合理性との両立も重要な観点であり、具体的な措置内容については、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である。

なお、番組送出設備の設置場所が放送事業者の施設内であることに変更はないこと等から、安全・信頼性に係る技術基準のうち、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、特段見直しの必要はないものと判断される。

４－４　サイバーセキュリティの脅威と対策例

放送設備をＩＰ化することで、一般的なＩＴ機器と同様の脅威が増加するが、それぞれの脅威に対して運用を考慮した対策を導入することで放送継続を担保できると考えられる。サイバーセキュリティの脅威と対策例について、主要なものを表４－４－１にまとめた。

表４－４－１　サイバーセキュリティの脅威と対策例

脅威		対策例
分類	内容	
改ざん	機器設定、映像素材の改ざん	・入室制限など物理的対策 ・ログの管理 等
	マルウェア感染（本線系 LAN）	・アプリケーション許可リストの導入 ・OS設定の要塞化 ・ファイアウォール、ルータのアクセスコントロール等による不許可通信の拒否 ・早期復旧のためのデータバックアップ 等
	マルウェア感染（情報 LAN 等）	・上記に加えて、持込 USB メモリ等の事前マルウェアチェック 等
特権昇格	汎用機器のソフトウェアの脆弱性を狙った攻撃	・脆弱性診断および診断結果に基づく脆弱性対策 ・脆弱性情報の定期的な確認、OS／ミドルウェア／アプリケーション等へのパッチの適用、 ファイルの実行パーミッションやグループ設定の適切な管理、IDの棚卸管理 等
サービス拒否	マルウェア感染等による内部からの攻撃（DoS 攻撃等）	・ファイアウォール、ルータのアクセスコントロール等による不許可通信の拒否 ・OS設定の要塞化 等
	本線系 LAN からの攻撃（DoS 攻撃等）	

４－５　安全・信頼性確保のための措置の対象となる放送設備

技術基準の適用対象となる地上系放送及び衛星系放送の放送設備については、第２章２－２に掲げるとおり、表４－５－１及び表４－５－２となっている。

放送設備のＩＰ化に伴う安全・信頼性に係る技術基準の見直しにより、新たな措置の適用対象となる設備は、番組送出設備である。

表４－５－１　地上系放送の放送設備

放送の種別	番組送出設備※1	中継回線設備	放送局の送信設備
地上デジタルテレビ放送	・送出マトリクス※2 ・エンコーダ※3 ・多重化装置※4 ・送出管理装置※5 ・基準信号発生装置※6 等	・STL※7 ・TTL※8 ・一事業者内の演奏所間回線 ・放送波中継用の受信装置　等	・基準信号発生装置※6 ・伝送路符号化装置 ・送信装置 ・空中線　等
中波放送（AM放送）	・送出マトリクス※2 ・音声調整装置（主） ・送出管理装置※5 等	・STL※7 ・TTL※8 ・一事業者内の演奏所間回線　等	・送信装置 ・空中線　等
短波放送	・送出マトリクス※2 ・音声調整装置（主） ・送出管理装置※5　等	・STL※7 等	・送信装置 ・空中線　等
超短波放送（FM放送）	・送出マトリクス※2 ・音声調整装置（主） ・送出管理装置※5 ・ステレオ変調装置 等	・STL※7 ・TTL※8 ・一事業者内の演奏所間回線 ・放送波中継用の受信装置　等	・送信装置 ・空中線　等
コミュニティ放送	・送出マトリクス※2 ・音声調整装置（主） ・ステレオ変調装置　等	・STL※7 ・TTL※8 等	・送信装置 ・空中線　等
マルチメディア放送※9	・送出マトリクス※2 ・エンコーダ※3 ・多重化装置※4 ・送出管理装置※5 ・基準信号発生装置※6 等	・番組送出設備から放送局の送信設備間の回線	・基準信号発生装置※6 ・伝送路符号化装置 ・送信装置 ・空中線　等

※1　スタジオ設備は含まない。
※2　送出する番組の素材を切り替える機能を有する装置。
※3　映像、音声等の信号をMPEG-2 Video、MPEG-2 Audio AAC等の方式に符号化する機能を有する装置。
※4　符号化された映像、音声等の複数の信号を多重化する機能を有する装置。
※5　放送番組の送出スケジュール等を管理し、主として番組送出を制御する機能を有する装置。
※6　機器の同期をとるためのクロック信号を発生させる装置。
※7　Studio to Transmitter Linkの略。
※8　Transmitter to Transmitter Linkの略。
※9　現時点において、サービスが提供されておらず、かつ、サービス提供の具体的な計画もないことから、本件の検討対象からは除外した。

表４－５－２　**衛星系放送の放送設備**

放送種別	番組送出設備※1	中継回線設備	地球局設備	放送局の送信設備
BS／東経１１０度CS放送	・送出マトリクス※2 ・エンコーダ※3 ・多重化装置※4 ・送出管理装置※5 ・基準信号発生装置※6 等	・番組送出設備から地球局設備間の回線	・TS合成装置 ・伝送路符号化装置 ・送信装置 ・空中線　等	・送信装置 ・空中線 等
東経１２４／128度CS放送	・送出マトリクス※2 ・エンコーダ※3 ・多重化装置※4 ・送出管理装置※5 ・基準信号発生装置※6 等	・番組送出設備から地球局設備間の回線	・伝送路符号化装置 ・送信装置 ・空中線　等	・送信装置 ・空中線 等

※1　スタジオ設備は含まない。
※2　送出する番組の素材を切り替える機能を有する装置。
※3　映像、音声等の信号をMPEG-2 Video、MPEG-2 Audio AAC等の方式に符号化する機能を有する装置。
※4　符号化された映像、音声等の複数の信号を多重化する機能を有する装置。
※5　放送番組の送出スケジュール等を管理し、主として番組送出を制御する機能を有する装置。
※6　機器の同期をとるためのクロック信号を発生させる装置。

各放送設備を構成する装置等については、放送事業者によって多少異なる場合がある。

また、放送事業者は、放送設備の一部として、他事業者が提供する電気通信設備を利用する場合においても、当該電気通信設備を含めた放送設備全体について、安全・信頼性確保のための措置を行う必要がある。

なお、マルチメディア放送については、現時点において、サービスが提供されておらず、かつ、サービス提供の具体的な計画もないことから、今回の検討対象からは除外することとした。

４－６　安全・信頼性確保のための措置及び解説

○ 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】

・サイバーセキュリティは、人の知覚によっては認識することができない電磁的方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることとされている。

・一般的に、情報システム等では、その脆弱性を完全に除去するのは難しく、意図しない脆弱性が残るものであり、また、悪意のある攻撃者が脆弱性を組み込む場合があり得ることから、放送設備で使用する機器についても、脆弱性があることを認識し、セキュリティ対策が継続的に行われることが必要となる。

・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。また、放送設備については、放送の業務に重大な支障を及ぼす損壊等の発生時には、これを直ちに検出し、放送設備を運用する者に通知することや予備機器に速やかに切り替えられることが求められている。そのため、通信回線を用いた放送設備の監視・制御が行われており、放送設備と同様に、安全性及び信頼性確保のために必要な措置が講じられ、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網等通信ネットワークとはその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ている状態にある。また、予備のため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については、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。

・ここで、「外部ネットワーク」とは、放送事業者が構築した各種ＬＡＮ等の「内部ネットワーク」の外側にある、不特定多数の第三者が接続可能なネットワークである。なお、ＶＰＮ回線[注1]については、「内部ネットワーク」とみなすが、ＶＰＮ回線を構成する装置等セキュリティ確保に十分留意する必要がある。

注１　ＶＰＮ回線には、主に、接続する通信回線が他のネットワークサービスと共用されていない、専用の閉域網を使ったＩＰ－ＶＰＮ及びオープンなネットワークであるインターネット上に構築されたインターネットＶＰＮの二つの種別がある。
ＩＰ－ＶＰＮは、電気通信事業者による専用ＩＰ網を用いて企業等による拠点間通信ネットワークを構築するものである。インターネットを経由しないため、機密性や信頼性に優れているとされている。
インターネットＶＰＮは、インターネット上において、認証や暗号化等を用いて、仮想回線として構成するものである。共用を前提としたセキュリティ対策が必要であり、また、通信速度についても、共用による影響を受けることとなるものの、ＩＰ－ＶＰＮと比較して低コストで構築が可能なものとなっている。
なお、インターネットＶＰＮについては、使用するプロトコルや暗号化の違いなど、電気通信事業者により様々なサービスが提供されており、様々なカスタマイズが可能となっている。設置者は、使用頻度、業務に対する影響、さらには、整備に要するコストなどを踏まえる必要がある。

・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、インターネットのような第三者がアクセス可能な外部ネットワークからの分離について、効率的、効果的にその措置の実施が可能な特徴を有している。併せて、基本的な構成において、方式の違いによって放送ネットワークが分離されている現在の状況は、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。

・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回線となる。当該回線には、放送の映像・音声をＩＰベースで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。

・一方で、放送設備のＩＰ化の標準モデルに示すとおり、番組送出設備は外部ネットワークと直接的に接続されることはなく[注2]、情報系ＬＡＮ、制御系ＬＡＮ若しくは社内ＬＡＮ等の、放送事業者の施設内に構築された内部ネットワークを経由して外部ネットワークと接続されることが一般的である。

注２　監視・制御及び保守に使用される回線の一時的な接続を除く。

・従来の考え方を踏襲すると、番組送出設備における伝送回線がＩＰ化されて

も、外部ネットワークとの間に介在する内部ネットワークがＩＰとは異なる通信方式である場合は、番組送出設備は外部ネットワークから隔離された状態にあるとみなすことが可能と考えられる。

・しかしながら、実際には、番組送出設備と接続される内部ネットワークがすべてＩＰとは異なる通信方式で構成されることは想定されないため、番組送出設備がＩＰ化された場合には、内部ネットワークを介して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。

・具体的な措置内容については、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。

・さらに、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。

・また、本検討における新たな措置内容は、放送設備のＩＰ化を前提として検討したものであるが、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。

・なお、地上系及び衛星系の放送設備におけるサイバーセキュリティの確保については、放送設備に対する措置とともに、その状態が適切に維持管理されていることが求められることから、当該業務を実施するに足りる技術的能力についても、確認されていることが必要となる。

【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＞

・放送設備の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となる。

・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必要がある。

・また、ゼロトラストの観点から、内部ネットワークに侵入したマルウェアを不活性化する措置、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、マルウェア感染防止対策、並びにサイバー事案による障害からの早期復旧対策等を講じる必要がある。

・なお、措置内容に記載した「遮断」とは、内部ネットワークへの不正侵入を遮断することであり、放送本線系の遮断、すなわち放送の即時停止を意味するものではない。ただし、当面の放送継続を重視するあまり放送設備への被害が広範囲に拡大すれば、結果的に放送停止の長期化に繋がるおそれもあることから、放送本線系の遮断についても、被害の最小化の観点で必要な場合には取り得る措置として想定しておくべきである。

・また、措置内容に記載した「検知」とは、必ずしも映像・音声データを含むすべてのトラフィックを監視することを意味しているものではなく、セキュリティ機器の設定等により、映像・音声データ以外の不正な制御プログラム等に限定して監視・検知を行うことも、現実的な措置として想定されるものである。

・さらに、措置内容に記載した「構成装置の各種セキュリティ設定強化」とは、必ずしも最新のセキュリティパッチを定常的に適用し続けることを意味しているのではなく、サーバ装置であれば不要なポートを無効化したり、通信機器であればＩＰアドレスで接続先を限定したりするなど、セキュリティ強化につながるあらゆる設定の見直しが包含される。放送設備導入後においても、構成装置のセキュリティ強化には不断に取り組む必要があることから、運用段階においても継続すべき措置である。

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ことから、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。

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＞

・放送設備においては、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、設備の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、これらに応じてウイルスチェック等の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。

・また、必ずしも放送事業者が自らすべての作業を行う必要はなく、例えば、放送機器メーカとの保守契約の中で実施する等による作業負荷の軽減も考えられるところである。

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。
- 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。

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＞

・放送設備の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ことを前提として、サイバーセキュリティリスクの増大に対応するための措置が求められる。

・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、ゼロトラストの観点からサイバー事案の発生を迅速に検知するための措置やネットワークのセキュリティ監視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。

４－７　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対象設備

放送設備のＩＰ化に伴う安全・信頼性確保のための新たな措置の適用対象となる設備は、番組送出設備である。

当該設備は、故障等により広範囲に放送の停止等を及ぼす設備であることから、サイバーセキュリティの確保に対して、サイバー事案による放送の停止等を未然に防ぐための措置が必要である。

また、当該設備に付随する制御・監視のための電気通信設備、並びに当該設備の保守及びシステム変更時の外部接続（媒体接続を含む）に対しても、同等の措置を講ずることが適当である。

４－６で示したサイバーセキュリティの確保のための措置について、放送種別ごとの措置の対象設備の範囲及び対象設備の規模による措置の要否を、表４－７－１－１～表４－７－１－６及び表４－７－２－１に示す。

４－７－１　基幹放送

① 地上デジタルテレビジョン放送

② 中波放送（ＡＭ放送）

③ 短波放送

④ 超短波放送（ＦＭ放送）

⑤ コミュニティ放送

⑥ ＢＳ放送、東経 110 度ＣＳ放送

４－７－２　一般放送

① 東経 124/128 度ＣＳ放送

また、放送設備のＩＰ化に伴うサイバーセキュリティの確保のための具体的な措置内容の例について、その一覧を表４－７－３に示す。

なお、今回の措置内容は、現時点での放送設備を前提としたものであり、今後新たな放送サービスや技術革新等の環境変化により、放送設備の構成及び形態等が変更される場合においては、安全・信頼性確保のための措置及びその対象となる放送設備の対応についても、適宜、見直しを図ることが必要である。

○ 基幹放送

① 地上デジタルテレビジョン放送

表４－７－１－１　地上デジタルテレビジョン放送に係る措置と対象設備

講じるべき措置（大項目）			講じるべき措置（小項目） ＼ 構成する機器の一例	設備の分類	番組送出設備	中継回線設備			放送局の送信設備		
					・送出マトリクス ・エンコーダ ・多重化装置 ・送出管理装置 ・基準信号発生装置　等	・STL、TTL ・一事業者内の演奏所間回線 ・放送波中継用の受信装置　等			・基準信号発生装置 ・伝送路符号化装置 ・送信装置、空中線　等		
						親局※1へ送信※2	放送用周波数使用計画記載中継局※1へ送信	その他の中継局へ送信※3	親局※1	放送用周波数使用計画記載中継局※1	その他の中継局※4
(1)	予備機器等		予備機器の確保、切替		○	○	○	※5	○	○	※5
(2)	故障検出	①	故障等を直ちに検出、運用者へ通知		○	○	○	○	○	○	○
		②	やむを得ず①の措置を講ずることができない設備について、故障等を速やかに検出、運用者へ通知		※6	※6	○	○	※6	○	○
(3)	試験機器及び応急復旧機材の配備	①	試験機器の配備		○	○	○	○	○	○	○
		②	応急復旧機材の配備		○	○	○	○	○	○	○
(4)	耐震対策	①	設備据付けに関する地震対策		○	○	○	※5	○	○	※5
		②	設備構成部品に関する地震対策		○	○	○	※5	○	○	※5
		③	①、②に関する大規模地震対策		○	○	※7	※5、7	○	※7	※5、7
(5)	機能確認	①	予備機器の機能確認		○	○	○	※5	○	○	※5
		②	電源供給状況の確認		○	○	○	※5	○	○	※5
(6)	停電対策	①	予備電源の確保		○	○	○	○　※8	○	○	○　※8
		②	発電機の燃料の確保		○	○	○	○　※8	○	○	○　※8
(7)	送信空中線に起因する誘導対策		電磁誘導の防止		○	○	○	○	○	○	○
(8)	防火対策		火災への対策		○	○	○	※5	○	○	※5
(9)	屋外設備	①	空中線等への環境影響の防止		※9	○	○	○	○	○	○
		②	公衆による接触の防止		※9	○	○	※5	○	○	※5
(10)	放送設備を収容する建築物	ア	建築物の強度		○	○	○	○	○	○	○
		イ	屋内設備の動作環境の維持		○	○	○	○	○	○	○
		ウ	立ち入りへの対策		○	○	○	○	○	○	○
(11)	耐雷対策		雷害への対策		○	○	○	○	○	○	○
(12)	サイバーセキュリティ		サイバーセキュリティの確保		○※10	○※10	○※10	○※10	○※10	○※10	○※10

○は措置を要することを意味する。

※1　放送用周波数使用計画（昭和六十三年十月一日郵政省告示第六百六十一号）の第７に定める親局及び中継局

※2　一事業者内の演奏所間回線を含む

※3　※4 の中継局へ送信する中継回線設備においては、経済合理性等を勘案しつつ、段階的に放送用周波数使用計画記載中継局へ送信する中継回線設備と同等の措置を講じることが適当。

※4　①放送用周波数使用計画記載中継局へ放送波により中継する中継局
②複数のその他の中継局へ放送波により中継する中継局（当該複数のその他の中継局の放送区域の全体が同一の放送対象地域における放送用周波数使用計画記載中継局の平均的な放送区域と同等となる中継局）のいずれかに該当する中継局においては、経済合理性等を勘案しつつ、段階的に放送用周波数使用計画記載中継局と同等の措置を講じることが適当。

※5　放送の停止等の影響を及ぼす範囲が限定的であるため、経済合理性の観点から、措置を要さない。

※6　番組送出設備、放送番組を親局へ送信するための中継回線設備、及び親局に設置される放送局の送信設備は、放送の停止等の影響を及ぼす範囲が極めて大きく、特に重要な放送設備であるため、これらの設備については、故障等を直ちに検出、運用者へ通知することが適当。

※7　大規模地震対策の措置は、※5 と同様の理由により、特に重要な放送設備(番組送出設備、放送番組を親局へ送信するための中継回線設備、及び親局に設置される放送局の送信設備)に適用することが適当。

※8　大規模災害時における情報伝達の重要性を勘案し、災害により停電が発生した際においても放送が継続できるよう、経済合理性等を勘案しつつ、段階的に措置を講じることが適当。

※9　番組送出設備には、屋外設備は含まれないことから、措置を要さない。

※10　対象設備に付随する制御・監視のための電気通信設備並びに対象設備の保守及びシステム変更時の外部接続（媒体接続を含む）のための電気通信設備についても、所要の措置を講じることが適当。

② 中波放送（ＡＭ放送）

表４－７－１－２　中波放送（ＡＭ放送）に係る措置と対象設備

講じるべき措置（大項目）		講じるべき措置（小項目）		設備の分類：番組送出設備 構成する機器の一例：・送出マトリクス ・音声調整装置（主） ・送出管理装置 等	中継回線設備 構成する機器の一例：・STL ・TTL ・一事業者内の演奏所間回線　等 親局※1へ送信※2	中継回線設備 放送用周波数使用計画記載中継局※1へ送信	中継回線設備 その他の中継局へ送信	放送局の送信設備 構成する機器の一例：・送信装置 ・空中線 等 親局※1	放送局の送信設備 放送用周波数使用計画記載中継局※1	放送局の送信設備 その他の中継局
(1)	予備機器等		予備機器の確保、切替	○	○	○	※3	○	○	※3
(2)	故障検出	①	故障等を直ちに検出、運用者へ通知	○	○	○	○	○	○	○
		②	やむを得ず①の措置を講ずることができない設備について、故障等を速やかに検出、運用者へ通知	※4	※4	○	○	※4	○	○
(3)	試験機器及び応急復旧機材の配備	①	試験機器の配備	○	○	○	○	○	○	○
		②	応急復旧機材の配備	○	○	○	○	○	○	○
(4)	耐震対策	①	設備据付けに関する地震対策	○	○	○	※3	○	○	※3
		②	設備構成部品に関する地震対策	○	○	○	※3	○	○	※3
		③	①、②に関する大規模地震対策	○	○	※5	※3、5	○	※5	※3、5
(5)	機能確認	①	予備機器の機能確認	○	○	○	※3	○	○	※3
		②	電源供給状況の確認	○	○	○	※3	○	○	※3
(6)	停電対策	①	予備電源の確保	○	○	○	○　※6	○	○	○　※6
		②	発電機の燃料の確保	○	○	○	○　※6	○	○	○　※6
(7)	送信空中線に起因する誘導対策		電磁誘導の防止	○	○	○	○	○	○	○
(8)	防火対策		火災への対策	○	○	○	※3	○	○	※3
(9)	屋外設備	①	空中線等への環境影響の防止	※7	○	○	○	○	○	○
		②	公衆による接触の防止	※7	○	○	※3	○	○	※3
(10)	放送設備を収容する建築物	ア	建築物の強度	○	○	○	○	○	○	○
		イ	屋内設備の動作環境の維持	○	○	○	○	○	○	○
		ウ	立ち入りへの対策	○	○	○	○	○	○	○
(11)	耐雷対策		雷害への対策	○	○	○	○	○	○	○
(12)	サイバーセキュリティ		サイバーセキュリティの確保	○※8	○※8	○※8	○※8	○※8	○※8	○※8

○は措置を要することを意味する。

※1　放送用周波数使用計画（昭和六十三年十月一日郵政省告示第六百六十一号）の第２に定める親局及び中継局

※2　一事業者内の演奏所間回線を含む

※3　放送の停止等の影響を及ぼす範囲が限定的であるため、経済合理性の観点から、措置を要さない。

※4　番組送出設備、放送番組を親局へ送信するための中継回線設備、及び親局に設置される放送局の送信設備は、放送の停止等の影響を及ぼす範囲が極めて大きく、特に重要な放送設備であるため、これらの設備については、故障等を直ちに検出、運用者へ通知することが適当。

※5　大規模地震対策の措置は、※3 と同様の理由により、特に重要な放送設備(番組送出設備、放送番組を親局へ送信するための中継回線設備、及び親局に設置される放送局の送信設備)に適用することが適当。

※6　大規模災害時における情報伝達の重要性を勘案し、災害により停電が発生した際においても放送が継続できるよう、経済合理性等を勘案しつつ、段階的に措置を講じることが適当。

※7　番組送出設備には、屋外設備は含まれないことから、措置を要さない。

※8　対象設備に付随する制御・監視のための電気通信設備並びに対象設備の保守及びシステム変更時の外部接続（媒体接続を含む）のための電気通信設備についても、所要の措置を講じることが適当。

③短波放送

表４－７－１－３　短波放送に係る措置と対象設備

講じるべき措置（大項目）			講じるべき措置（小項目）＼構成する機器の一例	番組送出設備 ・送出マトリクス ・音声調整装置（主） ・送出管理装置　等	中継回線設備 ・STL　等 親局※1へ送信	中継回線設備 ・STL　等 放送用周波数使用計画記載中継局※1へ送信	放送局の送信設備 ・送信装置 ・空中線　等 親局※1	放送局の送信設備 ・送信装置 ・空中線　等 放送用周波数使用計画記載中継局※1
（1）	予備機器等		予備機器の確保、切替	○	○	※2	○	※2
（2）	故障検出	①	故障等を直ちに検出、運用者へ通知	○	○	○	○	○
		②	やむを得ず①の措置を講ずることができない設備について、故障等を速やかに検出、運用者へ通知	※3	※3	○	※3	○
（3）	試験機器及び応急復旧機材の配備	①	試験機器の配備	○	○	○	○	○
		②	応急復旧機材の配備	○	○	○	○	○
（4）	耐震対策	①	設備据付けに関する地震対策	○	○	※2	○	※2
		②	設備構成部品に関する地震対策	○	○	※2	○	※2
		③	①、②に関する大規模地震対策	○	○	※2	※4	※2
（5）	機能確認	①	予備機器の機能確認	○	○	※2	○	※2
		②	電源供給状況の確認	○	○	※2	○	※2
（6）	停電対策	①	予備電源の確保	○	○	※2	※5	※2
		②	発電機の燃料の確保	○	○	※2	※5	※2
（7）	送信空中線に起因する誘導対策		電磁誘導の防止	○	○	○	○	○
（8）	防火対策		火災への対策	○	○	○	○	○
（9）	屋外設備	①	空中線等への環境影響の防止	※6	○	※7	○	○
		②	公衆による接触の防止	※6	○	※7	○	○
（10）	放送設備を収容する建築物	ア	建築物の強度	○	○	○	○	○
		イ	屋内設備の動作環境の維持	○	○	○	○	○
		ウ	立ち入りへの対策	○	○	○	○	○
（11）	耐雷対策		雷害への対策	○	○	○	○	○
（12）	サイバーセキュリティ		サイバーセキュリティの確保	○※8	○※8	○※8	○※8	○※8

○は措置を要することを意味する。

※1　放送用周波数使用計画（昭和六十三年十月一日郵政省告示第六百六十一号）の第１の９に定める放送局、第３に定める親局及び中継局

※2　短波放送特有の電波伝搬状況の変化への対策として、難視聴解消のため特定の時間帯に限定した補完的な放送を目的とする中継局であることから、措置を要さない。

※3　番組送出設備、放送番組を親局へ送信するための中継回線設備、及び親局に設置される放送局の送信設備は、放送の停止等の影響を及ぼす範囲が極めて大きく、特に重要な放送設備であるため、これらの設備については、故障等を直ちに検出、運用者へ通知することが適当。

※4　短波放送の親局に設置される送信装置は、構造上、大規模地震対策に関する措置を講じることができない（構成部品として、蒸発冷却式の大型真空管を搭載）ため、措置を要さない。

※5　短波放送の親局に設置される送信装置は、消費電力が極めて大きいため、経済合理性の観点から、予備電源に関する措置を要さない。

※6　番組送出設備には、屋外設備は含まれないことから、措置を要さない。

※7　放送番組を中継局へ送信するための中継回線設備は、屋外設備に該当する設備が無いため、措置を要さない。

※8　対象設備に付随する制御・監視のための電気通信設備並びに対象設備の保守及びシステム変更時の外部接続（媒体接続を含む）のための電気通信設備についても、所要の措置を講じることが適当。

④超短波放送（ＦＭ放送）

表４－７－１－４　超短波放送（ＦＭ放送）に係る措置と対象設備

講じるべき措置（大項目）			設備の分類 ＼ 構成する機器の一例 ／ 講じるべき措置（小項目）	番組送出設備 ・送出マトリクス ・音声調整装置（主） ・ステレオ変調装置 等	中継回線設備 ・STL ・TTL ・一事業者内の演奏所間回線 ・放送波中継用の受信装置 等		放送局の送信設備 ・送信装置 ・空中線 等	
					親局※1へ送信※2	中継局へ送信	親局※1	中継局
(1)	予備機器等		予備機器の確保、切替	○	○	※3	○	※3
(2)	故障検出	①	故障等を直ちに検出、運用者へ通知	○	○	○	○	○
		②	やむを得ず①の措置を講ずることができない設備について、故障等を速やかに検出、運用者へ通知	※4	※4	○	※4	○
(3)	試験機器及び応急復旧機材の配備	①	試験機器の配備	○	○	○	○	○
		②	応急復旧機材の配備	○	○	○	○	○
(4)	耐震対策	①	設備据付けに関する地震対策	○	○	※3	○	※3
		②	設備構成部品に関する地震対策	○	○	※3	○	※3
		③	①、②に関する大規模地震対策	○	○	※3、5	○	※3、5
(5)	機能確認	①	予備機器の機能確認	○	○	※3	○	※3
		②	電源供給状況の確認	○	○	※3	○	※3
(6)	停電対策	①	予備電源の確保	○	○	※3	○	※3
		②	発電機の燃料の確保	○	○	※3	○	※3
(7)	送信空中線に起因する誘導対策		電磁誘導の防止	○	○	○	○	○
(8)	防火対策		火災への対策	○	○	※3	○	※3
(9)	屋外設備	①	空中線等への環境影響の防止	※6	○	○	○	○
		②	公衆による接触の防止	※6	○	※3	○	※3
(10)	放送設備を収容する建築物	ア	建築物の強度	○	○	○	○	○
		イ	屋内設備の動作環境の維持	○	○	○	○	○
		ウ	立ち入りへの対策	○	○	○	○	○
(11)	耐雷対策		雷害への対策	○	○	○	○	○
(12)	サイバーセキュリティ		サイバーセキュリティの確保	○※7	○※7	○※7	○※7	○※7

○は措置を要することを意味する

※1　放送用周波数使用計画（昭和六十三年十月一日郵政省告示第六百六十一号）の第４に定める親局

※2　一事業者内の演奏所間回線を含む

※3　放送の停止等の影響を及ぼす範囲が限定的であるため、経済合理性の観点から、措置を要さない。

※4　番組送出設備、放送番組を親局へ送信するための中継回線設備、及び親局に設置される放送局の送信設備は、放送の停止等の影響を及ぼす範囲が極めて大きく、特に重要な放送設備であるため、これらの設備については、故障等を直ちに検出、運用者へ通知することが適当。

※5　大規模地震対策の措置は、※3と同様の理由により、特に重要な放送設備（番組送出設備、放送番組を親局へ送信するための中継回線設備、及び親局に設置される放送局の送信設備）に適用することが適当。

※6　番組送出設備には、屋外設備は含まれないことから、措置を要さない。

※7　対象設備に付随する制御・監視のための電気通信設備並びに対象設備の保守及びシステム変更時の外部接続（媒体接続を含む）のための電気通信設備についても、所要の措置を講じることが適当。

⑤コミュニティ放送

表４－７－１－５　コミュニティ放送に係る措置と対象設備

講じるべき措置（大項目）			講じるべき措置（小項目） ＼ 設備の分類 構成する機器の一例	番組送出設備 ・送出マトリクス ・音声調整装置（主） ・ステレオ変調装置　等	中継回線設備 ・STL ・TTL　等		放送局の送信設備 ・送信装置 ・空中線　等	
					親局へ送信	中継局へ送信	親局	中継局
（1）	予備機器等		予備機器の確保、切替	○	※1	※1	※1	※1
（2）	故障検出	①	故障等を直ちに検出、運用者へ通知	○	○	※1	○	※1
		②	やむを得ず①の措置を講ずることができない設備について、故障等を速やかに検出、運用者へ通知	○	○	※1	○	※1
（3）	試験機器及び応急復旧機材の配備	①	試験機器の配備	※1	※1	※1	※1	※1
		②	応急復旧機材の配備	※1	※1	※1	※1	※1
（4）	耐震対策	①	設備据付けに関する地震対策	※1	※1	※1	※1	※1
		②	設備構成部品に関する地震対策	※1	※1	※1	※1	※1
		③	①、②に関する大規模地震対策	※1	※1	※1	※1	※1
（5）	機能確認	①	予備機器の機能確認	※1	※1	※1	※1	※1
		②	電源供給状況の確認	※1	※1	※1	※1	※1
（6）	停電対策	①	予備電源の確保	※1	※1	※1	※1	※1
		②	発電機の燃料の確保	※1	※1	※1	※1	※1
（7）	送信空中線に起因する誘導対策		電磁誘導の防止	※1	※1	※1	※1	※1
（8）	防火対策		火災への対策	○	※1	※1	○	※1
（9）	屋外設備	①	空中線等への環境影響の防止	※2	※1	※1	○	○
		②	公衆による接触の防止	※2	※1	※1	※1	※1
（10）	放送設備を収容する建築物	ア	建築物の強度	○	※1	※1	○	○
		イ	屋内設備の動作環境の維持	※1	※1	※1	※1	※1
		ウ	立ち入りへの対策	○	※1	※1	○	○
（11）	耐雷対策		雷害への対策	※1	※1	※1	※1	※1
（12）	サイバーセキュリティ		サイバーセキュリティの確保	○※3	○※3	○※3	○※3	○※3

○は措置を要することを意味する

※1　放送の停止等の影響を及ぼす範囲が限定的であるため、経済合理性の観点から、措置を要さない。

※2　番組送出設備には、屋外設備は含まれないことから、措置を要さない。

※3　対象設備に付随する制御・監視のための電気通信設備並びに対象設備の保守及びシステム変更時の外部接続（媒体接続を含む）のための電気通信設備についても、所要の措置を講じることが適当。

⑥ＢＳ放送、東経 110 度ＣＳ放送

表４－７－１－６　ＢＳ放送、東経 110 度ＣＳ放送に係る措置と対象設備

講じるべき措置（大項目）		講じるべき措置（小項目）		設備の分類：構成する機器の一例	番組送出設備 ・送出マトリクス ・エンコーダ ・多重化装置 ・送出管理装置 ・基準信号発生装置　等	中継回線設備 ・番組送出設備から地球局設備間の回線	地球局設備 ・伝送路符号化装置 ・送信装置 ・空中線　等	放送局の送信設備 ・送信装置 ・空中線 等
（1）	予備機器等		予備機器の確保、切替		○	○	○	○
（2）	故障検出	①	故障等を直ちに検出、運用者へ通知		○	○	○	○
		②	やむを得ず①の措置を講ずることができない設備について、故障等を速やかに検出、運用者へ通知		※1	※1	※1	※1
（3）	試験機器及び応急復旧機材の配備	①	試験機器の配備		○	○	○	※2
		②	応急復旧機材の配備		○	○	※3	※2
（4）	耐震対策	①	設備据付けに関する地震対策		○	○	○	※2
		②	設備構成部品に関する地震対策		○	○	○	※2
		③	①、②に関する大規模地震対策		○	○	○	※2
（5）	機能確認	①	予備機器の機能確認		○	○	○	○
		②	電源供給状況の確認		○	○	○	○
（6）	停電対策	①	予備電源の確保		○	○	○	※2
		②	発電機の燃料の確保		○	○	○	※2
（7）	送信空中線に起因する誘導対策		電磁誘導の防止		○	○	○	※2
（8）	防火対策		火災への対策		○	○	○	※2
（9）	屋外設備	①	空中線等への環境影響の防止		※4	○	○	※2
		②	公衆による接触の防止		※4	○	○	※2
（10）	放送設備を収容する建築物	ア	建築物の強度		○	○	○	※2
		イ	屋内設備の動作環境の維持		○	○	○	※2
		ウ	立ち入りへの対策		○	○	○	※2
（11）	耐雷対策		雷害への対策		○	○	○	※2
（12）	宇宙線対策		宇宙線等への対策		※5	※5	※5	○
（13）	サイバーセキュリティ		サイバーセキュリティの確保		○※6	○※6	○※6	○※6

○は措置を要することを意味する

※1　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、いずれも放送の停止等の影響を及ぼす範囲が極めて大きく、特に重要な放送設備であるため、故障等を直ちに検出、運用者へ通知することが適当。

※2　放送局の送信設備として人工衛星を利用することから、措置を要さない。

※3　地球局設備は、10GHz 超の周波数帯を使用するため、ケーブル繋ぎ替え等の応急復旧により設備の動作不良を誘発する恐れが極めて高いことから、措置を要さない。

※4　番組送出設備には、屋外設備は含まれないことから、措置を要さない。

※5　番組送出設備、中継回線設備及び地球局設備には、人工衛星は利用されないことから、措置を要さない。

※6　対象設備に付随する制御・監視のための電気通信設備並びに対象設備の保守及びシステム変更時の外部接続（媒体接続を含む）のための電気通信設備についても、所要の措置を講じることが適当。

○ 一般放送

①東経 124／128 度ＣＳ放送

表４－７－２－１　東経 124／128 度ＣＳ放送に係る措置と対象設備

講じるべき措置（大項目）		設備の分類 / 講じるべき措置（小項目）		番組送出設備 ・送出マトリクス ・エンコーダ ・多重化装置 ・送出管理装置 ・基準信号発生装置 等	中継回線設備 ・番組送出設備から地球局設備間の回線	地球局設備 ・伝送路符号化装置 ・送信装置 ・空中線　等	放送局の送信設備 ・送信装置 ・空中線 等
（1）	予備機器等		予備機器の確保、切替	○	○	○	○
（2）	故障検出	①	故障等を直ちに検出、運用者へ通知	○	○	○	○
		②	やむを得ず①の措置を講ずることができない設備について、故障等を速やかに検出、運用者へ通知	※1	※1	※1	※1
（3）	試験機器及び応急復旧機材の配備	①	試験機器の配備	○	○	○	※2
		②	応急復旧機材の配備	○	○	※3	※2
（4）	耐震対策	①	設備据付けに関する地震対策	○	○	○	※2
		②	設備構成部品に関する地震対策	○	○	○	※2
		③	①、②に関する大規模地震対策	○	○	○	※2
（5）	機能確認	①	予備機器の機能確認	○	○	○	○
		②	電源供給状況の確認	○	○	○	○
（6）	停電対策	①	予備電源の確保	○	○	○	※2
		②	発電機の燃料の確保	○	○	○	※2
（7）	送信空中線に起因する誘導対策		電磁誘導の防止	○	○	○	※2
（8）	防火対策		火災への対策	○	○	○	※2
（9）	屋外設備	①	空中線等への環境影響の防止	※4	○	○	※2
		②	公衆による接触の防止	※4	○	○	※2
（10）	放送設備を収容する建築物	ア	建築物の強度	○	○	○	※2
		イ	屋内設備の動作環境の維持	○	○	○	※2
		ウ	立ち入りへの対策	○	○	○	※2
（11）	耐雷対策		雷害への対策	○	○	○	※2
（12）	宇宙線対策		宇宙線等への対策	※5	※5	※5	○
（13）	サイバーセキュリティ		サイバーセキュリティの確保	○※6	○※6	○※6	○※6

○は措置を要することを意味する。

※1　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、いずれも放送の停止等の影響を及ぼす範囲が極めて大きく、特に重要な放送設備であるため、故障等を直ちに検出、運用者へ通知することが適当。

※2　放送局の送信設備として人工衛星を利用することから、措置を要さない。

※3　地球局設備は、10GHz 超の周波数帯を使用するため、ケーブル繋ぎ替え等の応急復旧により設備の動作不良を誘発する恐れが極めて高いことから、措置を要さない。

※4　番組送出設備には、屋外設備は含まれないことから、措置を要さない。

※5　番組送出設備、中継回線設備及び地球局設備には、人工衛星は利用されないことから、措置を要さない。

※6　対象設備に付随する制御・監視のための電気通信設備並びに対象設備の保守及びシステム変更時の外部接続（媒体接続を含む）のための電気通信設備についても、所要の措置を講じることが適当。

表４－７－３　放送設備のＩＰ化に伴う**サイバーセキュリティ確保のための具体的な措置内容の例**

項番	具体的な措置内容の例
（１－１）サイバーセキュリティ（放送本線系に係る不正接続対策及びマルウェア感染防止対策）	
ア	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
（１－２）サイバーセキュリティ（サイバー事案による障害からの早期復旧を図るための措置）	
ア	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
（２）サイバーセキュリティ（監視・制御等回線に係る不正接続対策）	
ア	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・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　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
（３－１）サイバーセキュリティ（設備の導入時及び保守時における不正プログラム感染防止措置）	
ア	設備の導入・保守・点検時等において、不正プログラムによる被害を防止するための、 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
（４－１）サイバーセキュリティ（放送設備に対する物理的なアクセス管理（入退室管理等））	
ア	番組送出設備に対し、ＩＤカード、テンキー錠、シリンダー錠又は有人による入退室の管理等を行う措置 監視・制御回線に関す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
（４－２）サイバーセキュリティ（放送設備に対する物理的なアクセス管理（外部記録メディア接続））	
ア	外部記録メディア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
（５）サイバーセキュリティ（組織体制の構築及び社内規程類の整備）	
ア	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

※ 下線部は、新たな措置内容の例を示す。

第５章　今後の課題

５－１　放送設備のクラウド化・集約化に伴う安全・信頼性に係る技術基準の検討に向けて

放送設備のクラウド化・集約化に伴う安全・信頼性に係る技術基準の検討にあたっては、クラウド化・集約化を行った場合の各放送設備の装置及びネットワーク等の構成を明らかにすることで標準モデルを確立し、現行の放送設備やＩＰ化した放送設備からの変更点を分析した上で、安全・信頼性確保のための措置の内容及びその対象設備等を精査していく必要がある。

これまでの検討で策定したクラウド化の標準モデル案については、クラウドの適用範囲、各装置の設置場所及びネットワーク構成等に関して未確定な部分があることから、今後の技術開発動向及び放送事業者の導入計画等を踏まえた詳細検討が必要とされている。

また、「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）によれば、地上テレビジョン放送の番組送出設備のクラウド化については、2028（令和 10）～2030（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て、製造メーカにおいて、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とされている。

今後、放送事業者、放送設備製造メーカ及びクラウド提供事業者等の関係者がクラウド化の実現に向けた建設的な議論・調整を継続することにより、可能な限り早期の段階で、関係者の共通認識として、我が国における放送設備のクラウド化の具体像が確立され、製造メーカにおける技術開発や放送事業者における導入検討が着実に進捗することが望まれる。

一方、放送設備の集約化についても、「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」等を踏まえ、放送設備の維持・管理費用の低減及び運用業務の効率化等の観点から、放送事業者における具体的な検討が開始されることが想定される。

これらの状況を踏まえて、放送事業者が経営の選択肢として放送設備のクラウド化・集約化を選択した場合に安心かつ円滑に導入することができるよう、諸動向を踏まえつつ、安全・信頼性に関する技術基準を適時適切に策定するための検討を進めていく必要がある。