資料安作3-4

放送設備のIP化に伴う安全・信頼性に関する技術的条件等について

IP化～クラウド化の標準モデル

標準モデル案に対する構成員からのコメント等（1）

■ SDIマスター

- 外部との接続について
  - **情報LAN**は、**社内LAN等の社内システム**とはファイアーウォール等を経由して接続している。
  - **社内システム**は、**インターネット**との境界点に外部ファイアーウォールを設けている。また、内部ファイアーウォールによって**放送設備**との境界点を設けている。
  - **各放送設備**や**放送設備用のLAN**は、**インターネット**に直接は接続していない。**放送設備用のLAN**は、ネットワークスイッチを複数経由して**社内LAN**と限定的に接続している。また、**社内LAN**は、ファイアーウォールを介して**インターネット**と接続している。
  - **番組送出設備**は、**社内LAN**や**インターネット**とは直接接続していない。
- システム不具合時に、（放送設備メーカ等が）専用線またはIP-VPNの閉域網を用いてリモートで対応にあたる場合がある。【第2回会合議事概要(案)より】
- **制御LAN**はメーカ・ローカルなネットワークであるため、（**本線系**のネットワークと）混在することはない。【第1回会合議事概要より】

標準モデル(案)に対する構成員からのコメント等（2）

■ IPマスター

- SDIマスターからIPマスターへの移行段階における専用機器（SDI対応）の扱いについて
  - **移行段階においてはSDI入力が存在すると想定される**ため、SDIやTS(SDI)を併記したほうがよい。
  - 安全・信頼性に関する具体的な措置内容を策定するに当たっては、**SDIが一部残る形態のマスターも想定される**ので、すべてIP化される形態と併記するのがよい。
  - 標準モデルとしては、すべてがIP化されたものをベースに検討し、それに対して**SDIやTSが残る場合は注釈する形での検討がよい**が、**すべてがIP化されたものとソフトマスターとの違いは、どこで動作させるかだけになる**。
- **「本線系を構成するIP回線は、外部ネットワークに接続」とは限らない**のではないか。
- 現行SDIマスターと同様に、**可能な限り外部ネットワークからは隔離することが想定される**。
- 「IPに対応した汎用機器及びソフトウェアで構成」は正しいか。ベンダ固有OS上で動作する「IPに対応した専用機器」ではないか。
- 「IPスイッチャー」と記載された要素については、いわゆるスイッチングハブをイメージされることが多いので、名称がふさわしくない。
- すべての機器がIP化される時期をメーカに伺いたい。

標準モデル(案)に対する構成員からのコメント等（3）

■ ソフトマスター

- ソフトウェア化できないハードウェアについて
  - 性能、機能要件、システム安定性、安全性等を考慮し、**最低限のハードウェアは残る**と思われる。
  - SDIマスターと同等の可用性を実現できない場合などには、**ハードウェアが残ることが想定される**。
  - STLによる番組伝送に必要な精度のクロック信号等が**ソフトウェア（基準信号発生機能）で得られない場合には、ハードウェアが必要となる可能性がある**。
  - **監視機器、映像モニター機器などが残ることが想定される**。
  - ハードウェア装置が残るかの見解をメーカに伺いたい。

標準モデル(案)に対する構成員からのコメント等（4）

■ クラウドマスター

- クラウドマスターについては、**安価で高い安全性が確保できるような状況であれば、演奏所にバックアップ系統を確保しることを前提に、十分に検討にすべきである**。
- **クラウドとの接続構成については、将来的に利用するクラウドベンダー側の要件にも関わってくる**。
- 演奏所に残るハードウェアについて
  - 演奏所には、**光搬送端局装置のみが残ると想定される**。
  - メーカーの開発状況次第では、**光搬送端局装置も残る可能性がある**。また、**多重化装置等の一部の装置が放送事業者の施設内に設置されることが考えられる**。
  - **監視機器、映像モニター機器などが残ることが想定される**。
  - 「不測の事態における対処をクラウド側に委ねるのではなく、マスター設備の利用者である放送事業者自らがリスクをグリップ(把握)し、コントロール(制御)できることが重要」に準拠するには、**すべてをクラウド側に委ねるのではなく、演奏所にも一定程度の設備を設置する検討が必要である**。
  - 光搬送端局装置がIPからTSを抽出する機能を有しているとの理解でよいか。
- クラウドとの接続回線について
  - 安全性を確保する為にも**専用ネットワークでの接続がよい**。
  - 放送継続性の維持を考慮すると、**クラウドとの接続を冗長化することが想定される**。また、セキュアにアクセス制御を行う場合は、**ルータースイッチ、ファイアーウォールの構築なども想定される**。
- **中継回線設備を使用せず、送信局内でクラウドから信号をダウンロードすることも可能ではないか**と思う。

標準モデル(案)に対する構成員からのコメント等（5）

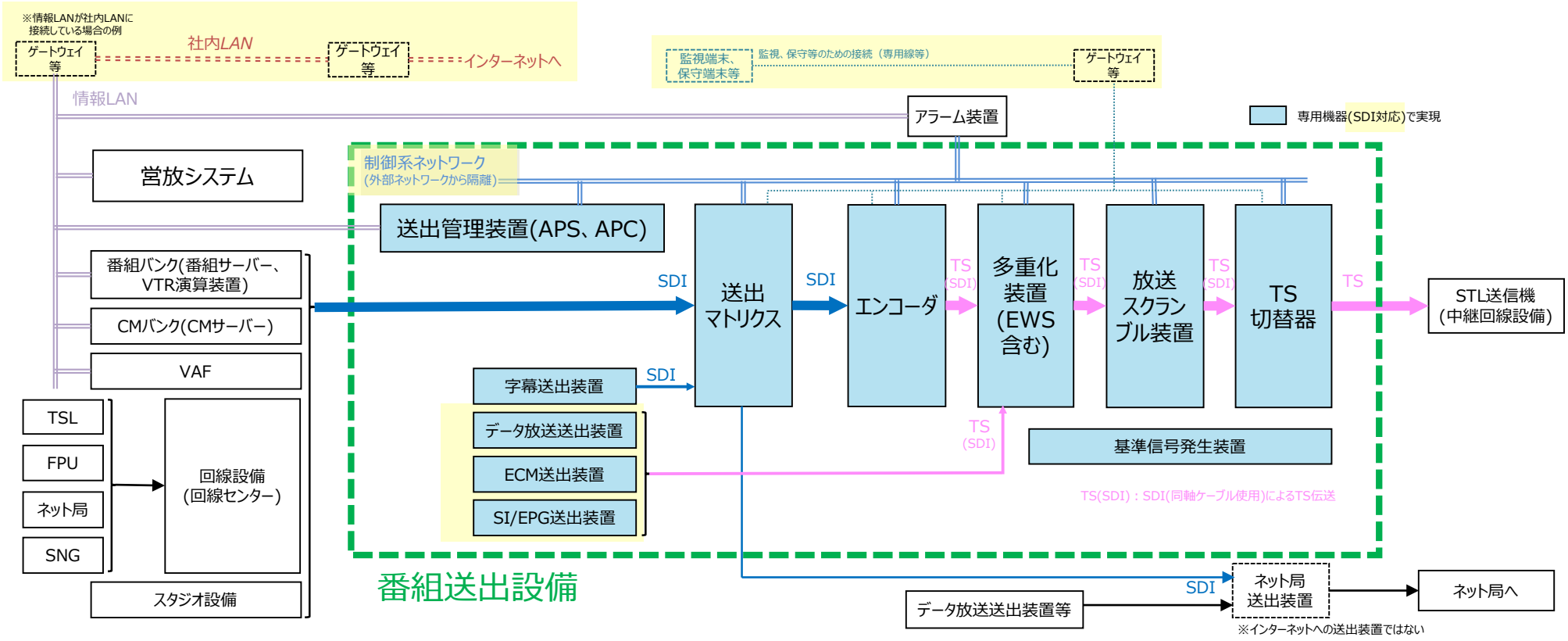
■ 標準モデル(案)全般

- 今後の技術進展のなか、**設備の動作の担保やコスト等を念頭に、装置・機能別にIP化やソフトウェア化、クラウドリフトの検討が必要である**。
- IPマスター、ソフトウェアマスター、クラウドマスターについては、**現行SDIマスターの可用性を維持するために、構成について標準モデル(案)から変動要素がある**と考える。
- プライベートクラウドには、「ホスティング」と「ハウジング」があるが、「ハウジング」の検討も必要ではないか。
- ラジオのマスター設備は、以下の点でテレビと大きく異なることから、ラジオに関する検討はテレビとはある程度切り分けて進めることが必須であると考える。
  - ベースバンドの信号は、「SDI」ではなく「アナログ音声」、「AES」、「MADI」等である。
  - 現状でもIPマスター、ソフトマスターの導入が具体化している。
  - 機器構成、APSの構成範囲が異なる。

SDIマスターの標準モデル（案）※1

※1 地上デジタルテレビジョン放送を想定した標準モデル（案）

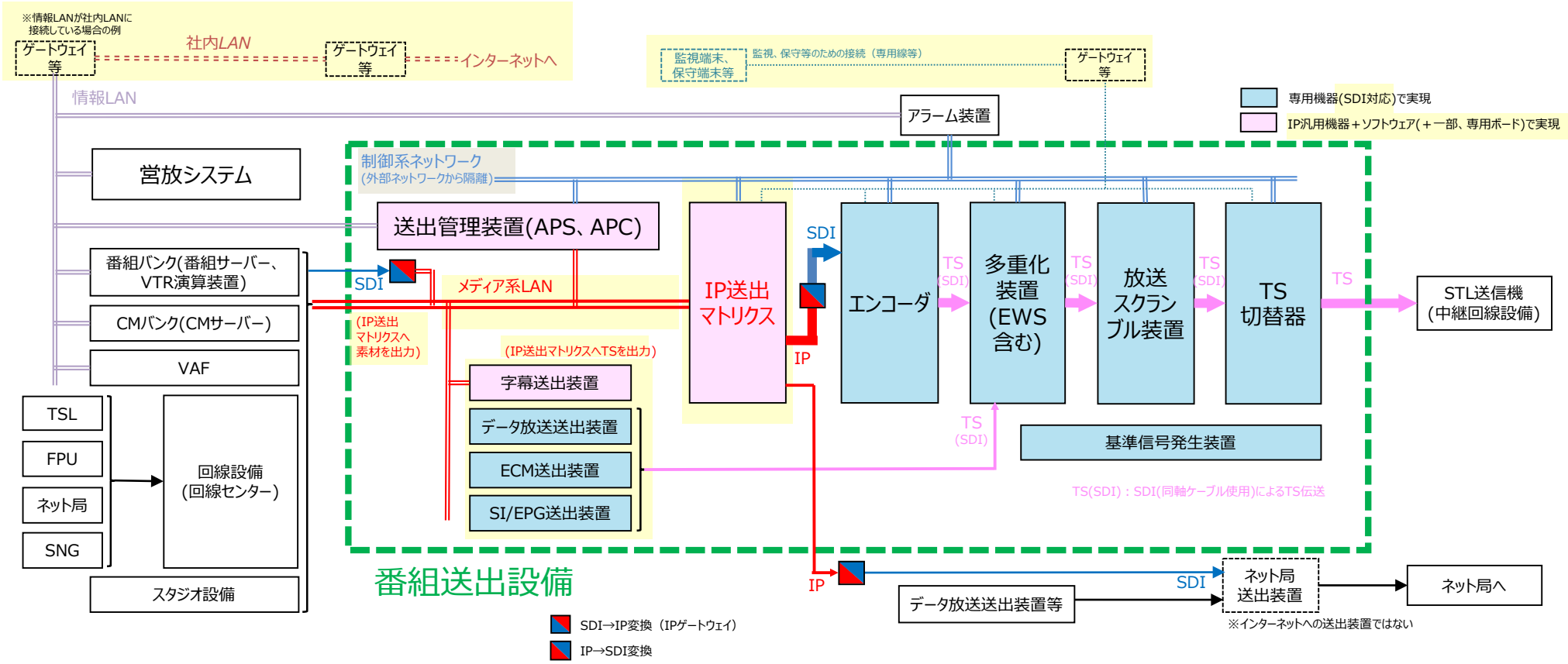
- 本線信号を**SDI**で伝送し、送信機へ送出する**従来型のマスター**
- 放送事業者の**施設内に設置（オンプレミス）**
- 本線系（映像／音声信号を伝送する基幹回線）を構成するSDI回線は、**外部ネットワークから隔離**
- 構成機器の多くは、SDIに対応した**専用機器**で構成



IPマスターの標準モデル（案）※1

※1 地上デジタルテレビジョン放送を想定した標準モデル（案）

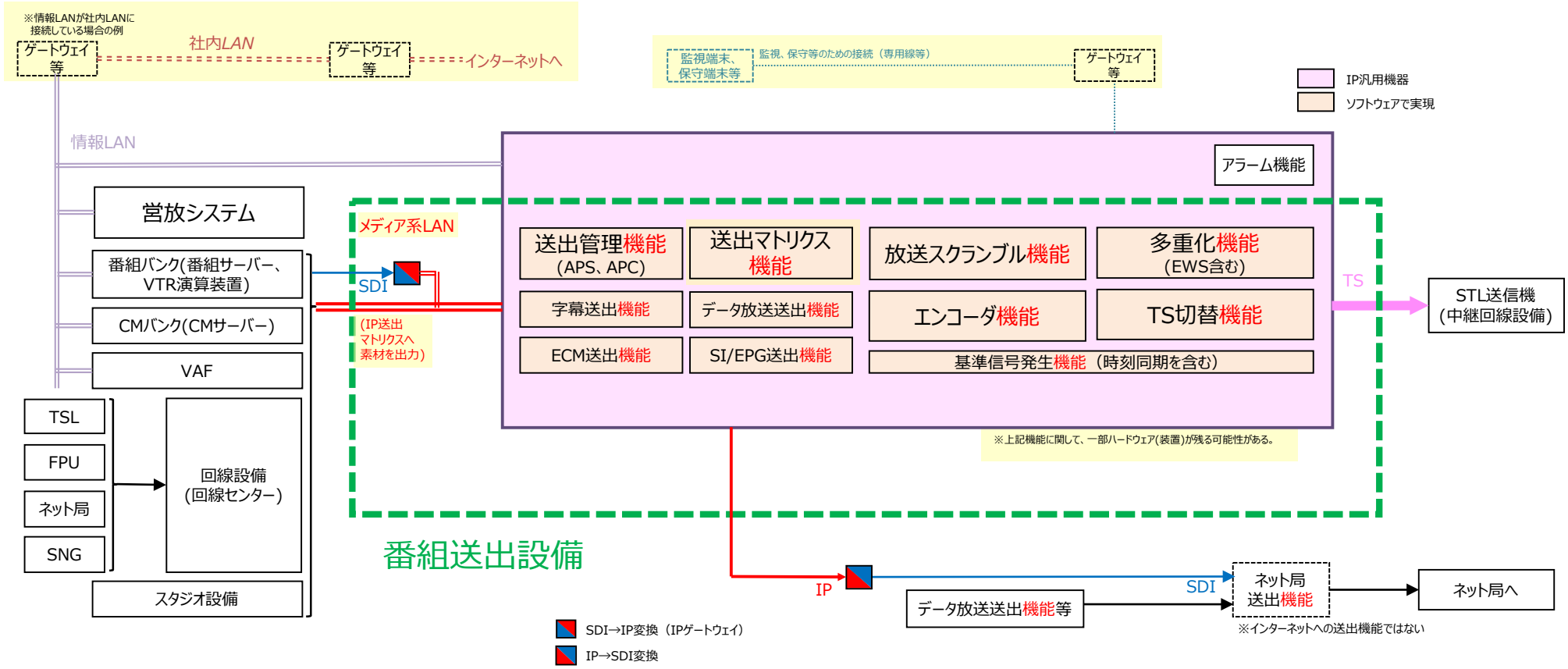
- 本線信号をIPで伝送し、送信機へ送出する**新型のマスター**
- 放送事業者の**施設内に設置（オンプレミス）**
- 本線系を構成するIP回線（図中の「メディア系LAN」）は、**外部ネットワーク接続の考慮**が必要
- **主としてエンコーダへの入力までの機器**を、IPに対応した**汎用機器及びソフトウェア**で構成
  （性能を満たせない一部機能は、専用ボード等で実現）



ソフトマスターの標準モデル（案）※1

※1 地上デジタルテレビジョン放送を想定した標準モデル（案）

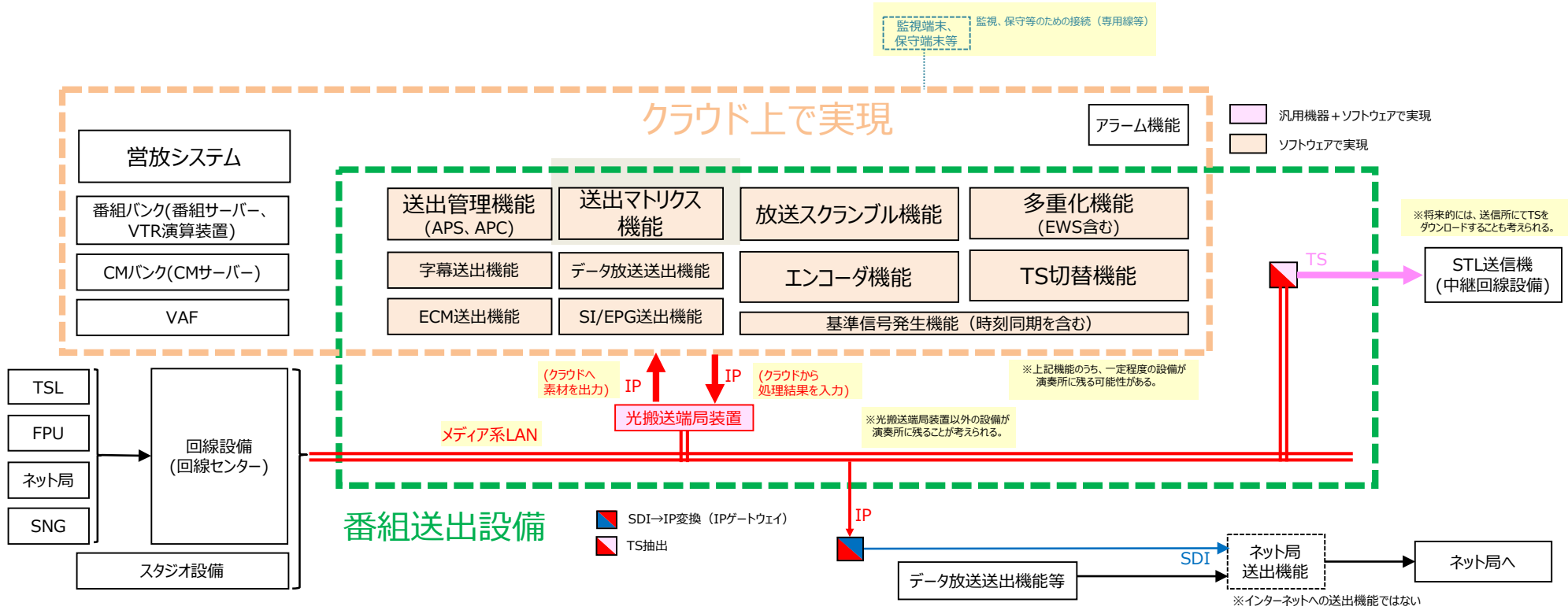
- 本線信号をIPで伝送し、送信機へ送出する**将来実現されるマスター**
- 放送事業者の**施設内に設置（オンプレミス）**
- 本線系を構成するIP回線（図中の「メディア系LAN」）は、**外部ネットワークに接続**
- 構成機器のすべてを、IPに対応した**汎用機器及びソフトウェア**で構成
- 性能や機能要件、システム安定性等の観点から、**一部ハードウェア（装置）が残る可能性**がある



クラウドマスターの標準モデル（案）※1

※1 地上デジタルテレビジョン放送を想定した標準モデル（案）

- 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、放送事業者の施設内には一部機器だけが残存
- クラウドと接続するIP回線（図中の「メディア系LAN」）は、**外部ネットワークに接続**
- 番組送出に関するすべての機能を**クラウド上のリソース及びソフトウェア**で実現



【参考】各マスターシステムの特徴（コメント反映）

比較項目	オンプレミス			クラウド	
	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	不用	不用
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、サーバー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、サーバー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化による外部ネットワークとの接続により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	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
セキュリティインシデントの対応	放送継続のため、該当機器の切り離しは困難(予備系への切替等で対応)	放送継続のため、該当機器の切り離しは困難(予備系への切替等で対応)	放送継続のため、該当機器の切り離しは困難(予備系への切替等で対応)	環境複製が容易なため、該当機能を切り離しての放送継続が可能	環境複製が容易なため、該当機能を切り離しての放送継続が可能

放送設備安全信頼性検討作業班第１回会合資料（日本電気：田中構成員）に基づく

IP化に伴う安全・信頼性に関する技術的条件

技術的条件に対する構成員からのコメント等（1）

■ 検討対象の放送設備

- 「番組送出設備」に限定して検討することが妥当である。
- 検討対象を広範囲にするのではなく、放送設備の中でも特に重要な設備に限定するのがよい。
- 入口／出口対策及び内部対策によるセキュリティ確保についても留意する必要がある。

■ IP化に伴う設備等の変更点

- 外部ネットワークとの接続に関して、従来どおり原則として隔離するか、常時接続かは、経済性や安全性を考慮しての選択になると考える。
- 外部ネットワークとは、番組送出設備外のネットワークのことか、演奏所(局)外のネットワークのことかを確認したい。前者であれば、スタジオ設備や回線設備も今後IP化されるので常時接続が考えられ、後者であれば、常時接続されないシステム構成になると考える。
- 外部ネットワークとの接続については、IPマスターでも必要以上にオープンにはせず、現行SDIマスターと同様に原則として隔離することになると考える。他は事務局資料の記載事項に過不足はない。
- 「外部ネットワークと（常時）接続」という記載があるが、番組送出設備の可用性を担保するためにIP化した場合でも外部ネットワークから隔離するという対策が可能と考える。
- マスター設備は原則として外部ネットワークと隔離し、それに適したサイバーセキュリティ対策を検討する必要があると考える。
- IPマスターは未導入のため、IP化に伴う設備等の変更点を現段階で決めるのは困難である。
- ラジオにも適用可能だと考えるが、「SDI回線」については「ベースバンド」と記載するのがよいと考える。

技術的条件に対する構成員からのコメント等（2）

■ IP化に伴うサイバーセキュリティ脅威

- 専用OSや専用ボード、チップで構成される専用機器から、LINUXやWindowsといった汎用OSや市販のボード、チップで構成される汎用機器への移行、IPプロトコルと技術的互換性のないSDIから、**外部ネットワークと同じプロトコルのIPベースへの移行により、ハード／ネットワーク両面でセキュリティ脅威が各段に増大する**と考える。
- 番組送出設備の信号がSDIからIP化されたとしても、外部ネットワーク接続の扱いによって脅威や対策は異なり、**外部ネットワークと接続する場合は、境界点における不正アクセス対策、汎用機器やソフトウエアの脆弱性対策をどう考えるかが重要な課題となる**。
- 外部ネットワークとの接続等によるサイバーセキュリティ脅威の増大への対応として「境界防御型からゼロトラスト型、サイバーレジリエンスへの転換」とあるのは、確かにサイバーセキュリティ対策の方向性としては最新の方向性と一致しているが、**番組送出設備に限定するのであれば、過大な対応となることが懸念されるため、境界型防御の強化から検討することが現実的である**と考える。
- **現行の番組送出設備は外部ネットワークから隔離するための措置が取られているので、IP化されたとしても、同様の措置を取ることで脅威は回避できる**と考える。
- **マスター設備は原則として外部ネットワークと隔離し、それに適したサイバーセキュリティ対策を検討する必要がある**と考える。
- クラウド事業者のセキュリティ対策が、どこまで開示されるかが気になる。

技術的条件に対する構成員からのコメント等（3）

■ サイバーセキュリティの確保に関する措置内容

- **現行の規定で必要な措置が網羅されていることから、見直しの必要はない**と考える。
- サイバーセキュリティ対策は非常に重要と考えているが、見方によっては、**新たに基準を付け加えなくても現状の基準が包含しており、対応できるところもある**と考える。
- **現行に記載されている措置内容においてカバーできる**と考える。
- **必要な措置内容は記載されているので、確認作業でよい**と考える。
- **従来の外部ネットワークとの隔離等、境界防御型の対策でサイバーセキュリティ対策を取ることも可能である**が、**ゼロトラスト型、サイバーレジリエンスへの転換等の図る場合は見直す必要がある**と考える。
- 外部ネットワークとの接続等によるサイバーセキュリティ脅威の増大への対応として、「境界防御型からゼロトラスト型、サイバーレジリエンスへの転換」と記載されているが、**高い可用性が求められる番組送出設備においてゼロトラスト型のサイバーセキュリティ対策を行う場合、境界防御型と比較して対策にかかる費用負担が増加する懸念がある**。ゼロトラスト型のサイバーセキュリティ対策が有効であることに異論はないが、**番組送出設備においては、放送事業者が可用性の担保と経済合理性を両立するために、境界防御型の対策をとることも可能であり、現実的・合理的な場合がある**と考えられる。そのような可能性も視野に入れて、技術的条件の検討を行うべきと考える。
- 例えば、**欧州におけるEBU R143（Cybersecurity for media vendor systems, software & services）等を参考に、設備の動作の担保やコスト等を踏まえた措置内容を検討するのがよい**と考える。

技術的条件に対する構成員からのコメント等（4）

■ サイバーセキュリティ以外の措置項目

- **現行の規定を見直す必要はない**と考える。

■ その他

- 放送設備のサイバーセキュリティ確保は有意義な取り組みであり、本作業班で番組送出設備のIP化等を見据えた検討を行うことは重要であると考えている。
- 標準モデルを基に、設備のどのポイントに、どのような目的で、どのような攻撃を行う攻撃者を想定すべきかを「実際の設備の現状に沿って」検討し、どのような対策が必要かを検討することができる。「実際の設備の現状に沿って」については、これらの設備を構成する機器やネットワーク、利用者、データの実態に応じて現実的な脅威の有無や度合を検討すべきである。**従来から行われているSDIマスターにおける脅威分析をベースにIPマスターへの移行により生じる差異を中心に検討する方が効率的である**。
- **厳しい技術基準を課して先進的なICTサービスの利用を制限する方向ではなく、今後、放送事業者がIP・クラウド化を選択した場合に、安心かつ円滑に導入できるようにするための技術基準策定を念頭に検討を進めるべき**と考える。

IP化に伴う安全・信頼性に関する技術的条件の見直しの論点（コメント反映）

- 検討対象の放送設備：IP化に伴い変更が生じる番組送出設備

- IP化に伴う番組送出設備の変更点：
  - 放送本線系の伝送回線：SDI回線 → IP回線
  - 構成装置：専用機器（ハードウェア） → IP対応の汎用機器（ハードウェア）＋ソフトウェア

    ※ IP化への移行過程において既存の専用機器を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⇔SDI変換が必要となる。
  - 外部ネットワークとの接続：原則として隔離 → 原則として隔離 または（常時）接続

    ※ 従来どおり「原則として隔離」するか、または「（常時）接続」するかは、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。
  - 設置場所：放送事業者の施設内（オンプレミス）【変更なし】

□ **外部ネットワークから原則として隔離する場合は、従来の措置内容を踏襲**

□ **外部ネットワークと接続する場合は、サイバー脅威に対応した新たな措置内容を適用**

- ➢ 境界防御の強化、ゼロトラスト型及びサイバーレジリエンスへの転換
- ➢ マスター設備に求められる可用性の担保と経済合理性の両立

□ サイバーセキュリティ以外の措置項目の見直しは不要

【参考】マスター設備に対するセキュリティ脅威と対策

● IP化及びソフト化により一般的なIT機器と同様の脅威が増大し、クラウド化により外部要因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。

脅威			脅威の有無 ○：有　○※：有（汎用機器化により攻撃機会増加）				対策例（青文字：クラウド固有事項の対策例）
分類		内容	SDIマスター	IPマスター	ソフトマスター	クラウドマスター	
改ざん	A	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
	B	マルウェア感染（本線系IPネットワーク）		○	○	○	・アプリケーションホワイトリストの導入 ・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 ・クラウド環境の場合は、感染環境を分離し複製から容易に復旧可能
	C	マルウェア感染（情報系IPネットワーク）	○	○	○	○	・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
特権昇格	D	汎用機器のソフトウェア（アプリ、ミドル、OS）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
物理的な脅威	E	放送機器の障害	○	○	○	○	・放送機器の冗長化 ・クラウド環境の場合は環境複製により対策容易
	F	ネットワークの障害	○	○	○	○	・ネットワーク分離による影響の低減およびネットワークの冗長化 ・クラウド環境の場合はマルチリージョン、マルチA-Z等により対策容易
	G	仮想化基盤の障害 （オンプレ環境では仮想化を行う場合）			○	○	・オンプレ環境の場合は仮想化基盤の冗長化 ・クラウド環境の場合は、稼働環境の複製により対策容易
	H	クラウド基盤の障害				○	・マルチリージョン、マルチA-Z、マルチクラウド、バックアップシステム整備等による冗長化
	I	クラウド基盤とSTL間の回線障害				○	・クラウド基盤ーSTL間の回線冗長化
否認	J	運用者の虚偽報告	○	○	○	○	・入室制限など利用者の制限・明確化 ・ログの管理
	K	システム混在による他システムの誤操作 （オンプレ環境では仮想化を行う場合）			○	○	・操作者がアクセスできるシステムと操作の権限を管理 ・ログの管理
サービス拒否	L	マルウェア感染等による内部からのDoS攻撃	○	○	○	○	・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
	M	本線系IPネットワークからのDoS攻撃		○	○	○	
	N	外部からのDoS攻撃				○	・放送局とクラウド間を専用線で接続しアクセスを制限 ・クラウド基盤のセキュリティサービスを利用し対策 （ID管理、多要素認証、不許可通信の拒否 など）
なりすまし	O	外部からの不正アクセス				○	

放送設備安全信頼性検討作業班第１回会合資料（日本電気：田中構成員）に基づく

【参考】IP化・クラウド化等に伴う安全・信頼性に関する課題や問題意識

- クローズド環境での境界防御型での対策がこれまでの主流であったが、IP化やクラウド化を考慮すると、境界防御型からゼロトラスト型への転換が必要となる。

ゼロトラスト型での検討事例

- マスターシステムに対してリソースの追加が容易となるため、**IPリソースの認証及び管理が重要**となる。
- クラウド利用やソフトウェア化が推進する事により、従来は放送局内で実施していた番組・CMコンテンツの検尺及びプレビュー作業が放送局外で行うことができるため、**コンテンツ流出の対策が重要**となる。
- ロケーションフリーの環境での業務が可能となるため、従来の入退出管理に加え、**設備に対するアクセス管理が重要**となる。
- 外部からの不審なアクセスの**侵入検知（IDS）及び防止（IPS）する仕組みが重要**となる。

放送設備安全信頼性検討作業班第１回会合資料（東芝インフラシステムズ：三腰構成員）に基づく

安全・信頼性に関する具体的な措置内容（サイバーセキュリティ関連①）

■ サイバーセキュリティの確保

放送法関係審査基準　別添１の１(13)

基幹放送設備に係るサイバーセキュリティの確保に当たっては、次の措置が講じられていること（規則第115条の２関係）。

- 放送本線系入力となる番組送出設備について、外部ネットワークから隔離するための次の措置又はこれと同等と認められる措置
  - 原則として、第三者が接続可能な外部ネットワークとの接続を行わない措置
  - やむを得ず接続を行う場合には、ファイアーウォール（ネットワークの通信において、送信元アイ・ピー・アドレス等を基に、その通信をさせるかどうかを判断し、許可する又は拒否する仕組みをいう。）の設置又は不正接続対策等の措置
- 放送設備に接続される監視・制御及び保守に使用される回線について、外部ネットワークからの不正接続対策を行うための次の措置又はこれと同等と認められる措置
  - 専用回線又はVPN回線（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。）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及びパスワードにより権限を有する者だけが接続できるようにする措置
  - 未使用時は回線を通じた接続を遮断する等の措置
- 設備の導入時及び運用・保守時におけるソフトウェアの点検について、不正プログラムによる被害を防止するため、放送設備のネットワークからの分離・遮断の措置及び不正プログラムの感染防止の措置

安全・信頼性に関する具体的な措置内容（サイバーセキュリティ関連②）

■ サイバーセキュリティの確保（続き）

放送法関係審査基準　別添１の１⑬

- 放送設備に対する物理的なアクセス管理について、機密性が適切に配慮されるための次の措置又はこれと同等と認められる措置
  - 番組送出設備に対しIDカード、テンキー錠又は有人による入退室の管理等を行う措置及び監視・制御回線、保守回線に係る機器の設置場所に対し公衆が容易に立ち入ることができないよう施錠その他の必要な措置
  - 外部記録メディア等を介した不正プログラムへの感染防止の措置
- 放送設備の運用・保守に際して、業務を確実に実施するための組織体制の構築及び業務の実施に係る規程若しくは手順書の整備に関する次の措置又はこれと同等と認められる措置
  - サイバー事案の発生時の対応策及び再発防止策について、事故報告を含む事後対応を迅速かつ確実に実施するための規程又は手順書を整備する措置
  - サイバー事案が発生した場合の連絡先の整備及び報告実施等の手順書化、放送設備のソフトウェアの更新等設備の運用・保守等について、実施方法を定める規程又は手順書を整備する措置