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
地上デジタル放送方式高度化作業班（第16回）資料

デ高作16－3

放送設備のIP化・クラウド化の技術動向等の調査結果について

三菱総合研究所

デジタル・イノベーション本部

ICTインフラ戦略グループ

2022/6/22

総務省（令和3年度）「放送サービス高度化に伴う放送設備のIP化・クラウド化の技術動向等に関する調査検討」より

目次

（1）放送設備のIP化・クラウド化

マスターシステムの定義

- マスターとは、製作された番組・CMの映像音声データ、時刻や天気予報、データ放送など、放送に付帯するデータを集約し、放送時間に合わせて順番通り、確実に送信機に送出することを目的とするシステムである。

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

放送局にとっての”心臓部“

マスターシステムの役割

放送機器メーカー 提供資料より作成

クラウドサービスの定義

- クラウドとは、ネットワークを経由して必要に応じてサービスを利用できる仕組みであり、ユーザーが大規模なインフラやソフトウェアを設置しなくても、求めた機能を利用できる。
- これらの仕組みを用いた提供されるサービスがクラウドサービスと呼ばれる。

パブリッククラウド（Public Cloud）

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。
主なサービス：Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP）、Salesforce.com　など

プライベートクラウド（Private Cloud）

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。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。

- オンプレミス型：自社内でクラウド環境を構築して提供する
- ホスティング型：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

上記2つのプライベートクラウドは、どちらも専有のクラウド環境として機能する。特徴として、「オンプレミス型」では独自のカスタマイズや管理が可能であり、「ホスティング型」は導入・管理・運用の一部を事業者が代行するのが一般的となる。

以降の説明では、プライベートクラウド＝「ホスティング型」として扱う。

放送機器メーカー 提供資料より作成

放送設備におけるIP化・クラウド化の過程

- 放送設備のクラウド化は、放送設備における構成品のIP化・ソフト化と、オンプレミスからクラウドサービスへ環境を変化（クラウドリフト）させることで実現される。

オンプレミス

SDIマスターシステム
- 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化

IPマスターシステム
- 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

ソフト化

ソフトマスターシステム
- 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

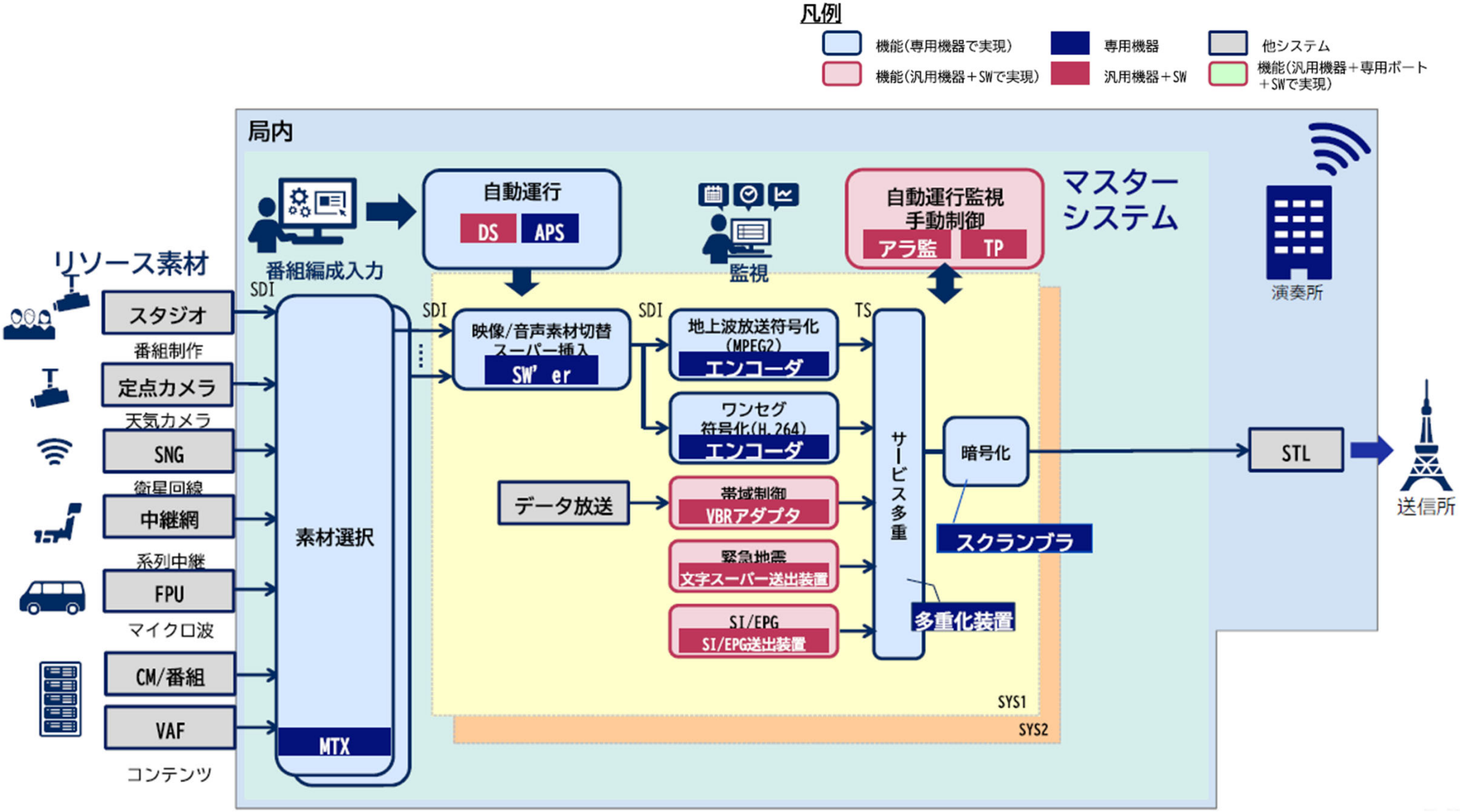
クラウドリフト

クラウド

クラウドマスターシステム
- 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

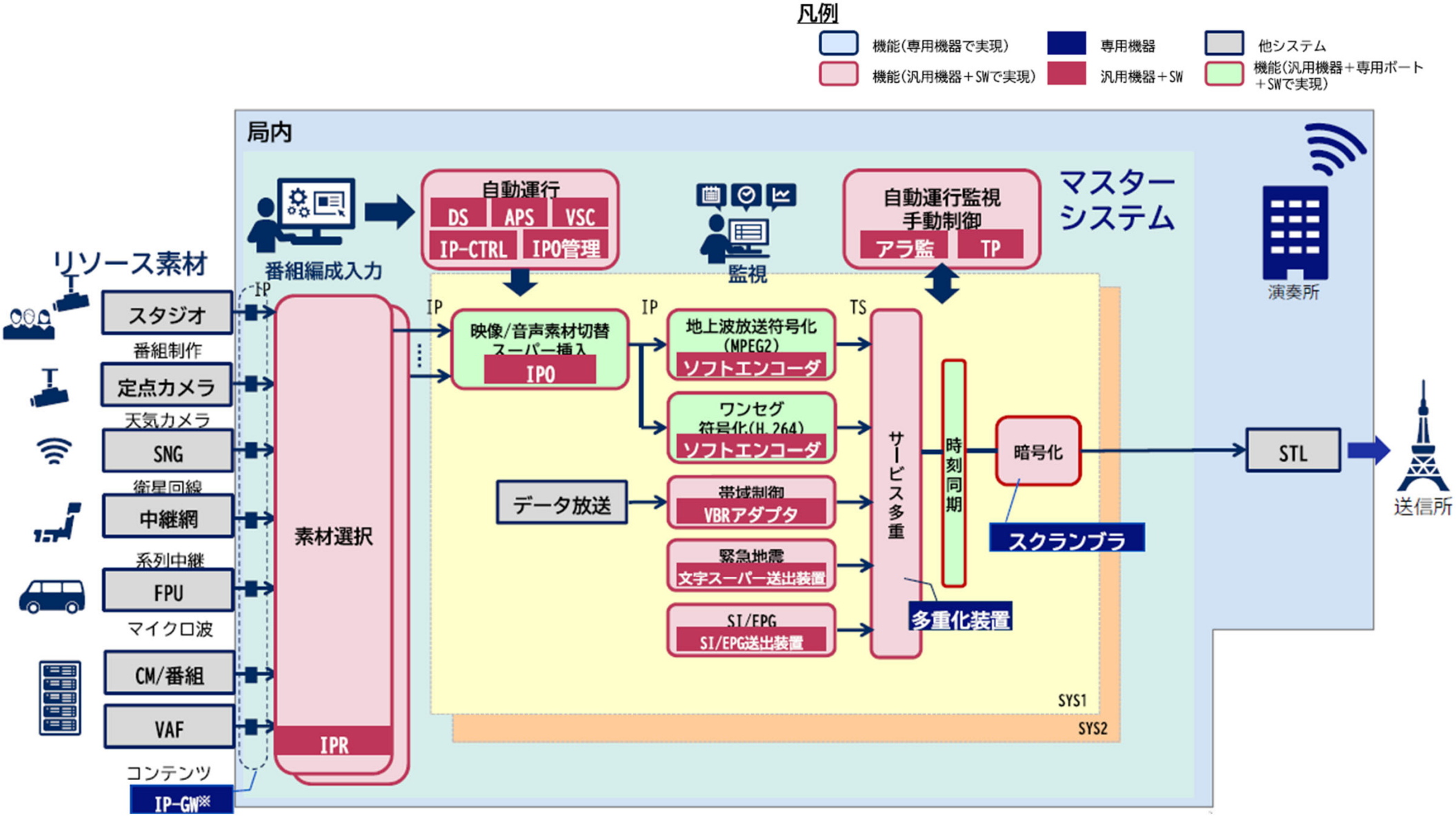
放送機器メーカー 提供資料より作成

SDIマスターシステムの機能ブロック図



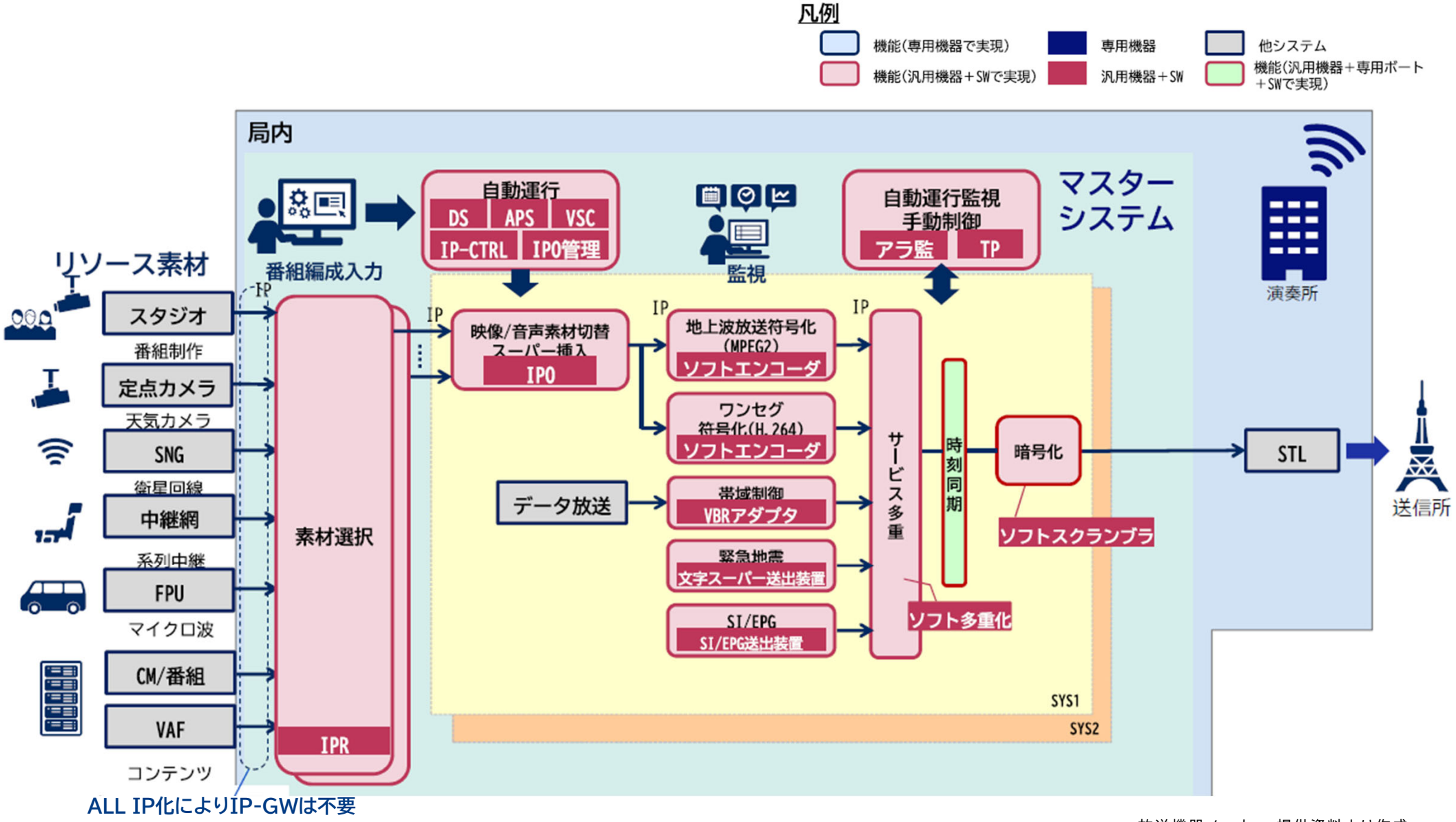
放送機器メーカー 提供資料より作成

IPマスターシステムの機能ブロック図



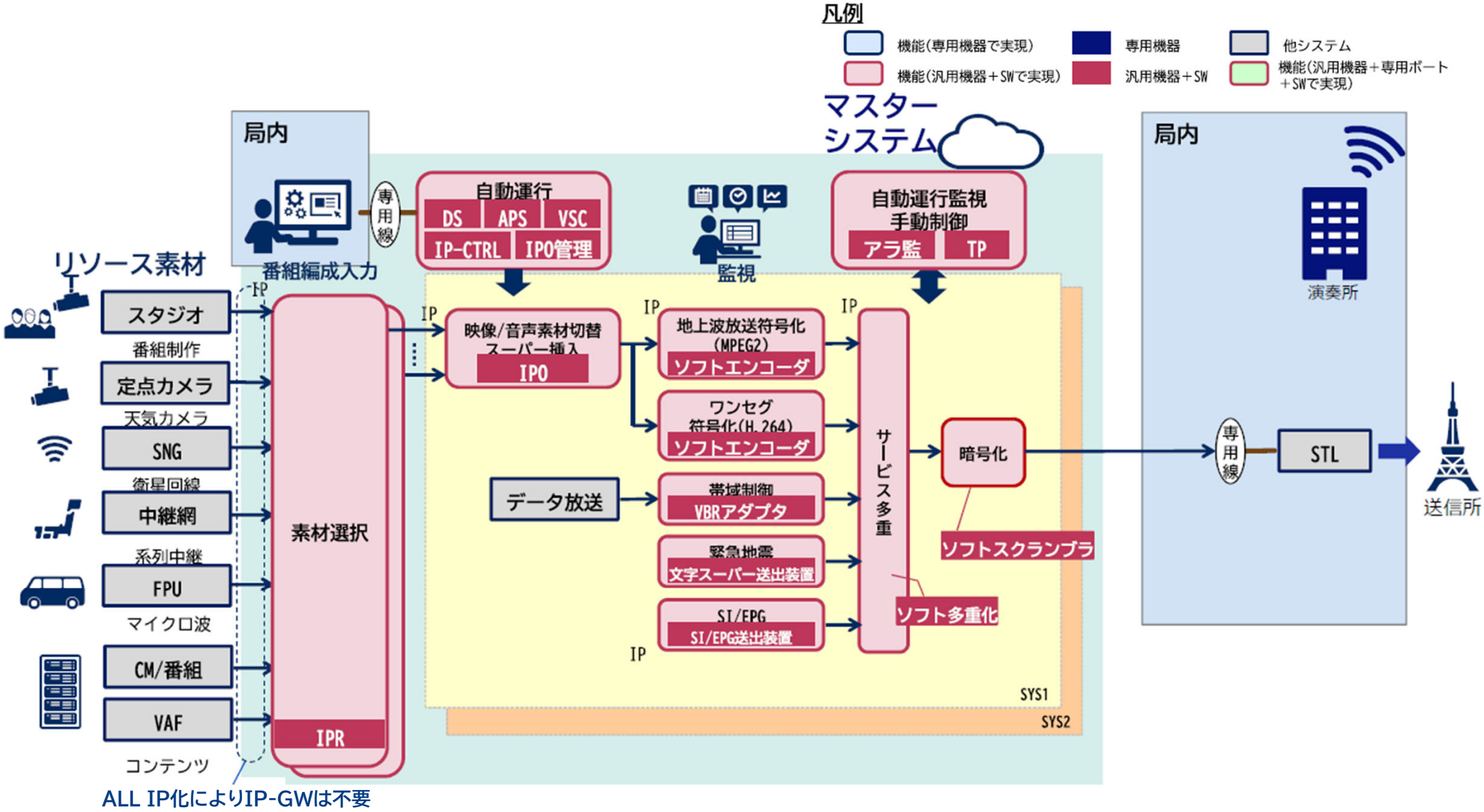
放送機器メーカー 提供資料より作成

ソフトマスターシステムの機能ブロック図



放送機器メーカー 提供資料より作成

クラウドマスターシステムの機能ブロック図



放送機器メーカー 提供資料より作成

放送設備のIP化・クラウド化におけるメリット・デメリット

	IP化・クラウド化のメリット	IP化・クラウド化のデメリット・課題
IP化	• 汎用機器の利用による調達期間が短縮 • IP関連機器の導入による高い機能拡張性 • （IP機器に限定）機器増減などに対する高い拡張性	• NW揺らぎを考慮した設計が必要 • 外部NWとの接続増によるセキュリティ脅威の増大（下記は脅威例） ➢ マルウェア感染 ➢ 本線IPネットワークからのDoS攻撃　など
ソフト化	• オーバーホール費用の削減 • 汎用機器の幅広い利用による調達期間の短縮 • 汎用機器の幅広い利用による高い機能拡張性 • 機器増減などに対する高い拡張性	• 汎用機器のアーキテクチャを考慮した設計が必要 • 汎用機器の増加に伴うセキュリティ脅威の増大 • 仮想化やシステム混在による複雑化、および複雑化に伴う誤操作の増加
クラウド化	• 放送設備の経費計上となり費用が平準化、設備投資からの脱却が可能 • 運用・保守をクラウド事業者に委託することが可能 • オンプレ設備がないことで、保守費用・業務が軽減 • アカウント登録後すぐに利用可能（但し、プライベートクラウドでは機器導入のリードタイムが必要な場合がある） • クラウド上に実装された機器の高い変更容易性 • リソースを動的に確保可能 • 迅速なスケールアウト/スケールインが可能 • 複数のデータセンターで提供されることによる高い災害耐性 • 環境複製が容易なため、セキュリティインシデントが発生した際も、該当機能を切り離して放送の継続が可能 • クラウドから直接送信所、中継所に伝送できればSTL、TTLが不要 • システムの共通化が容易であり、系列局や県域をひとまとめとした、放送設備の集約が可能（→センター化） **プライベートクラウド（ホスティング型）** • パブリッククラウドより占有化しやすく拡張も容易 **パブリッククラウド** • プライベートクラウドよりサーバ台数の増減やスペック変更が迅速かつ容易	• クラウド回線接続による遅延を考慮した設計が必要 • クラウドダウン時の予備として、マルチクラウドまたはオンプレが必要 • IP/TS変換機を保有していない事業者は、SDI変換後、TS変換して送信所へ伝送が必要 • セキュリティ脅威増大への対応 ✓ クラウド基盤の障害 ✓ クラウド基盤との回線障害 ✓ 外部からの不正アクセス（なりすまし） ✓ 外部からのDoS攻撃　など **プライベートクラウド（ホスティング型）** • 災害耐性を上げるため、複数のデータセンターを分散する必要あり **パブリッククラウド** • 可用性がクラウドのSLAに依存 • 災害発生時の放送継続のため、BCPオンプレミスの設置が必要 • 一部情報開示不可などの制限事項がある

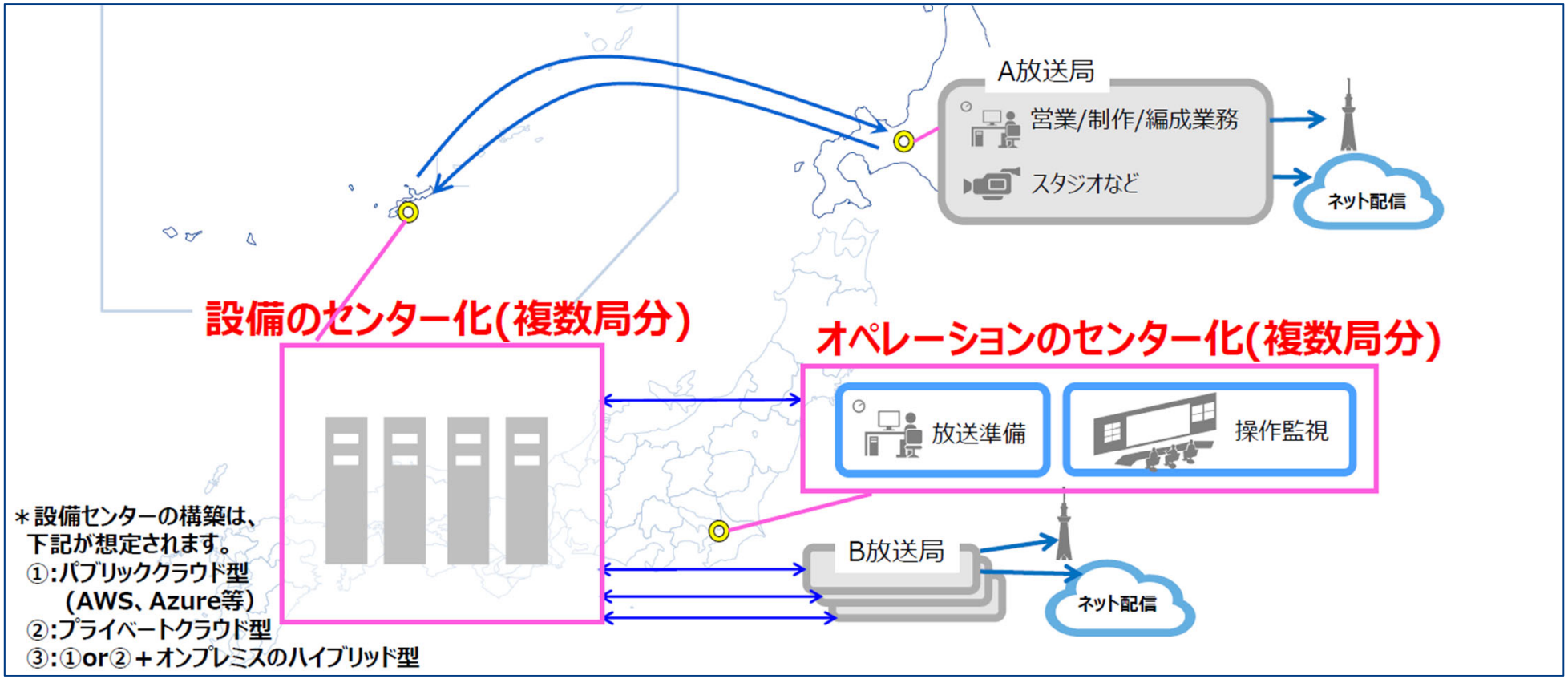
放送機器メーカー 提供資料等より作成

（2）放送設備の集約（センター化）

放送設備のセンター化の概要

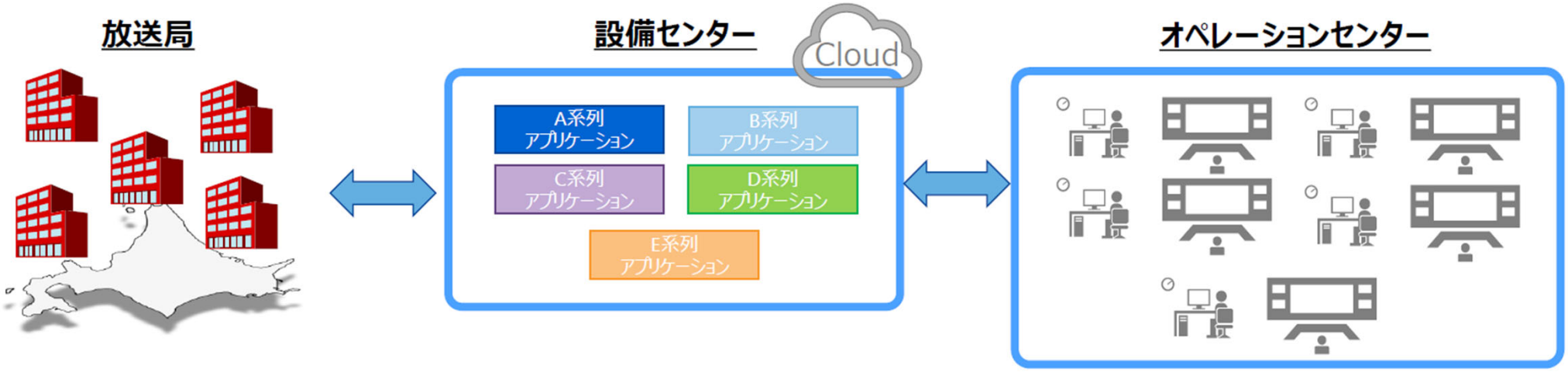
IP化・クラウド化により、NWを介して放送設備を集約（センター化）することが可能となる。
センター化は、二つの要素で構成される。

- 設備のセンター化：各局設備を1ケ所に集約する事で、各放送局が保有管理する設備を極小化する。
- オペレーションのセンター化：各局の監視業務や放送準備業務を一括してセンターで行い、重複する業務を効率化する。



放送機器メーカー 提供資料より作成

放送設備のセンター化の構成イメージ【1.県域集約（系列横断）】

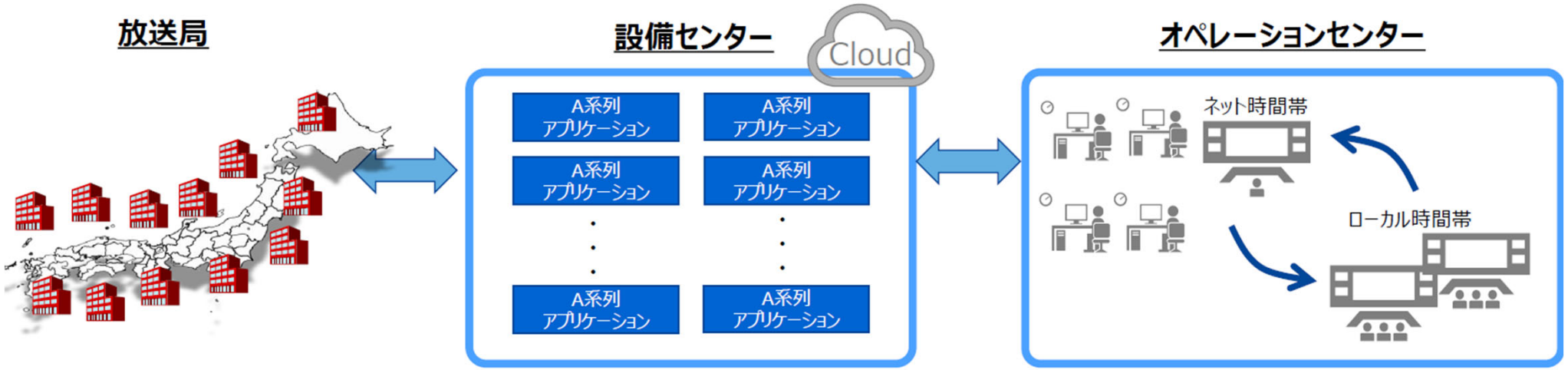


設備センター
- コンピューターリソースの共有が可能である。
- 地域固有の情報設備（気象情報・自治体連携）が共通化が可能である。
- アプリケーションやシステム構成が系列毎に異なり、個々の要求仕様への対応が必要となる。

オペレーションセンター
- 運用の違いにより、集約効果は大きく得られない。
- 編成の違いによる監視時間の差分や、ネット番組の違い、系列毎の特番編成などの運用差分により、オペレーターがそれぞれ必要となる。
- 放送するコンテンツも異なるため、番組・CM・提供の事前準備業務などについて、共通化を図れる範囲が少ない。

放送機器メーカー 提供資料より作成

放送設備のセンター化の構成イメージ【2.系列集約（全国または地方ブロック単位）】

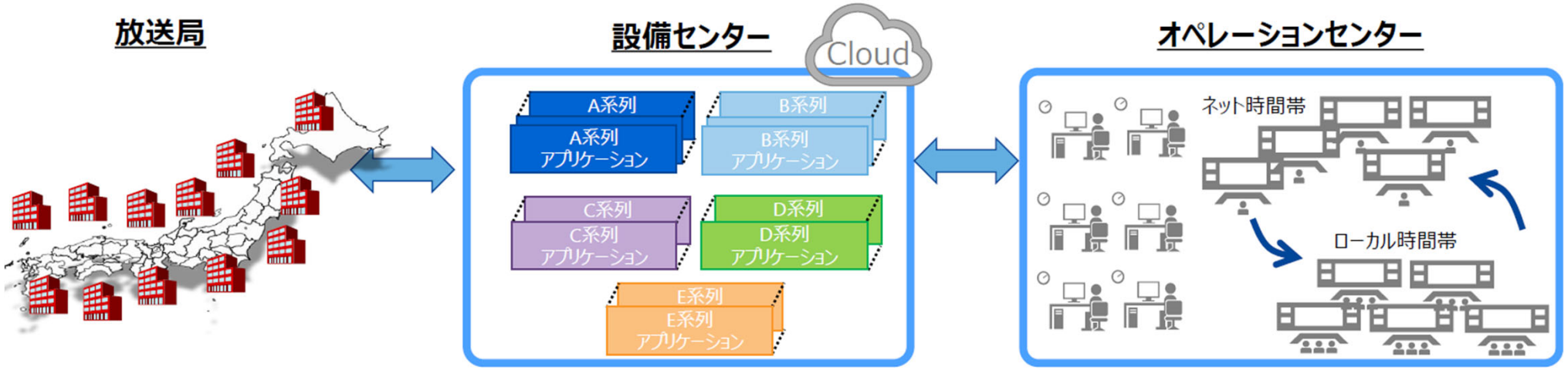


設備センター
- コンピューターリソースの共有が可能である。
- アプリケーションやシステム構成の類似性が高く、仕様の共有化が可能となる。

オペレーションセンター
- 編成が同じ時間帯も多く、監視業務については大きな集約効果が見込める。
- 放送するコンテンツは共有する部分が多いため、番組・CM・提供の事前準備業務など共通化を可能となる。
- 天気や速報スーパーなどの地域性のあるオペレーションについて、共通化の範囲を決めるなどの考慮が必要となる。

放送機器メーカー 提供資料より作成

放送設備のセンター化の構成イメージ【3.全事業者集約】



設備センター
- 集約効果を最大限に発揮でき、リソース分配の最適化が可能となる。
- アプリケーションやシステム構成が系列毎に異なり、個々に要求仕様への対応が必要となる。

オペレーションセンター
- 「2.系列集約」と比較すると運用の違いにより集約効果は大きく得られない。
- 編成の違いによる監視時間の差分や、ネット番組の違い、系列毎の特番編成などの運用差分により、オペレーターがそれぞれ必要となる。
- 放送するコンテンツも異なるため、番組・CM・提供の事前準備業務などについて、共通化を図れる範囲が少ない。
- 天気や速報スーパーなどの地域性のあるオペレーションについて、共通化の範囲を決めるなどの考慮が必要となる。

放送機器メーカー 提供資料より作成

放送設備のセンター化のメリット・デメリット

センター化のメリット

【設備のセンター化】
- 設備を共通化することで、各放送局における一部設備の設置が不要となり、設備規模の圧縮に一定の効果が期待（但し、集約側に更新用を含む設備設置スペースおよび電源・空調の確保が必要）
- アプリケーション開発の実装プラットフォームなど、ソフトウェアについても集約を行うことで、各局で必要となっていたプラットフォーム構築に係るコストの削減
- システムの複製化が容易であり、系列局への展開など、同じ用途のシステムに対して開発要素なくそのまま横展開が可能

【オペレーションのセンター化】
- 各放送局における一部オペレーションが不要になることによる各放送局のコスト削減効果
- 高スキル者の集中配置など、効率的な運用体制の再構築に一定の効果が期待（但し、効果の度合いは放送サービスに応じた非常時含む運用規定による）

センター化のデメリット・課題

【設備のセンター化】
- 設備利用の関係者増加による設備更新の調整難易度の向上
- 遅延にシビアな生放送や緊急地震速報などに対応するため、関連する一部放送設備を自局に設置する等、回線コスト低減の工夫が必要
- 高い集約により、大規模災害等による機能停止時の影響拡大
- 高い集約により、DoS攻撃等のサイバー攻撃による機能停止時の影響拡大（Single Point of Failure）

【オペレーションのセンター化】
- センターにおけるオペレーション作業集中による高負荷
- 系列局における異なるタイミングでのオペレーションへの個別対応
- 映像素材のセンターへの集中による高い回線負荷（素材のやり取りに圧縮信号を用いる、あるいはオンプレミスを含む放送設備全体の設計など、別途検討が必要）
- 編成や報道部門との正確な連携について集約度に応じた仕組み作りが必要
- システム操作・監視機能等の高度化への対応が必要

県域集約（系列横断）	【設備のセンター化】 • 地域固有の情報設備（気象情報など）の共通化が可能 【オペレーションのセンター化】 • 一部の業務について共通化が可能	【設備のセンター化】 • アプリケーションやシステム構成が系列ごとに異なるため、別途対応が必要 【オペレーションのセンター化】 • 放送局ごとにオペレーションの差異があるため、集約効果が限定的 • 編成の違い、系列毎の特番編成等の差分があるため共通化は限定的
系列集約	【設備のセンター化】 • アプリケーションやシステム構成の類似性があり、高い共通化が期待 【オペレーションのセンター化】 • 編成が類似する部分も多く、監視業務については高い集約化が期待 • コンテンツの共通部分も多く、高い業務共通化が期待	【設備のセンター化】 • 同じ系列の場合でも、異なるアプリケーションやシステム構成があれば個別に対応が必要 【オペレーションのセンター化】 • 同じ系列の場合でも、オペレーションの差異がある場合は、別途対応が必要
全事業者集約	【設備のセンター化】 • 集約効果を最大限に発揮でき、リソース配分の最適化が可能 【オペレーションのセンター化】 • 一部の業務について共通化が可能	【設備のセンター化】 • アプリケーションやシステム構成が系列ごとに異なるため、別途対応が必要 【オペレーションのセンター化】 • 放送局ごとにオペレーションの差異があるため、集約効果が限定的 • 編成の違い、系列毎の特番編成等の差分があるため共通化は限定的

放送機器メーカー 提供資料等より作成

（3）セキュリティに係る脅威と対策

重要インフラに対するサイバー攻撃の動向

- 経済的/政治的に価値あるシステムとして、重要インフラ※1や産業制御システムが狙われる事例が多数あり、攻撃者による周到な準備と継続的で執拗な活動を通した攻撃が行われる。

重要インフラ・産業制御システムに関連する攻撃事例

年	国	企業・施設等	概要
2010年	イラン	イラン核燃料施設	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、破壊目的であり、USBメモリ経由で持ち込み感染
2015年	ウクライナ	発電所	サイバー攻撃により変電所の遮断機切断、最大6時間停電、22万人以上に影響（妨害目的）
2016年	ウクライナ	発電所	サイバー攻撃により変電所の遮断機切断、1時間強の停電（妨害目的）
2017年	150ヶ国	-	150か国30万台以上（国内600か所以上）が自動感染拡大機能を持つワーム型であるランサムウェア（WannaCry）に感染
2018年	台湾	TSMC	感染端末の持ち込みにより、世界的半導体企業TSMCの工場NWにランサムウェアWannaCryが侵入、3日間生産停止による損害額は最大190億円
2019年	ノルウェー	ノルスク・ハイドロ	アルミ最大手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感染. 世界40か国170か所のオフィスや工場のコンピュータが感染. 被害額は約65-77億円と見積もり。支払い拒否と積極的情報公開によって対応
2020年	米国	ソーラーウインズ	システム管理ツールの開発会社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含）が連鎖的に攻撃を受けており、被害の全容は未だ不明。（サプライチェーン攻撃）
2021年	米国	コロニアル・パイプライン	米大手パイプライン会社がランサムウェア攻撃（※2）で5日間操業停止、4.8億円の身代金支払い（二重脅迫、RaaS）

※1 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分野に位置づけられる
※2 マルウェアの一種であり、組織に侵入後、内部情報の持ち出しおよび暗号化を行い、暗号化の解除と引き換えに身代金を要求する。

有識者 提供資料より作成

重要インフラに対するサイバー攻撃の動向【放送事業者への攻撃事例】

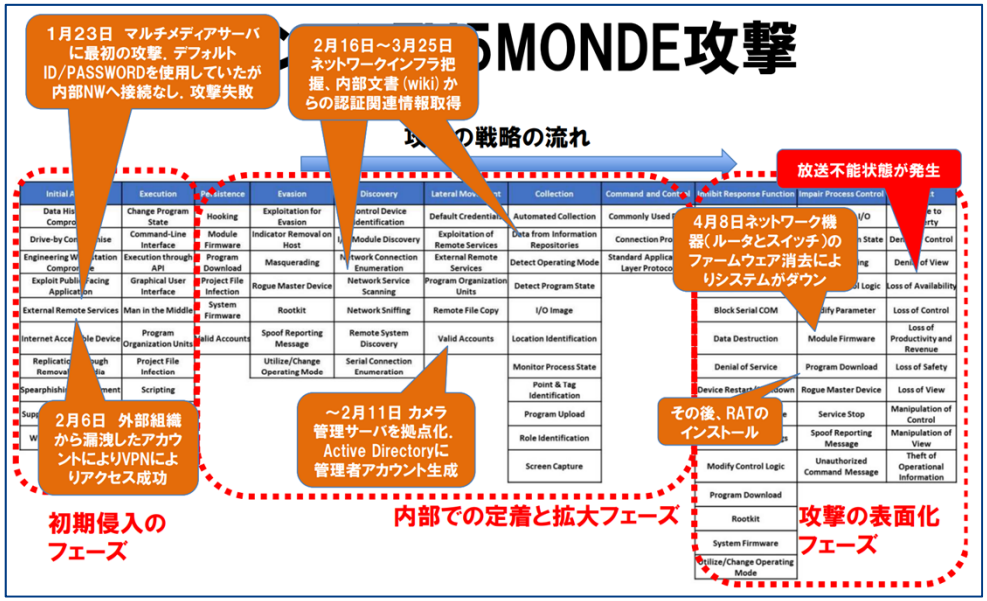
- 重要インフラの一つとして、影響力の大きい放送システムに対するサイバー攻撃事例・被害も確認されており、サイバーセキュリティ対策は「コスト」ではなく、「必要な投資」とみなすべきである。

Sinclair Broadcast Group（米国）

- 米国放送局運営最大手Sinclair Broadcast Groupは、2021年10月18日にランサムウェア攻撃を受けたことを発表。
- 同グループへのサイバー攻撃により、サーバーの一部が暗号化、ネットワークは遮断状態となり、複数のテレビ局が放送停止に追い込まれた。傘下の複数のテレビ局では、朝のニュース番組やNFLゲームのライブ放送ができない状態となった。
- 同社の第4四半期の業績によれば、同サイバー攻撃により、6,300万ﾄﾞﾙ（約73億円）の広告収入減、対策のため1,100万ﾄﾞﾙ（約13億円）の費用増につながった。
- 一部は保険で賄うが、2，400万ﾄﾞﾙ（約28億円）の純減は回収不可と推定している。

TV5MONDE（仏国）

- 2015年4月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）の12チャンネルがサイバー攻撃により18時間放送不能。
- 同時に同社のSNSアカウントが乗っ取られISのプロパガンダメッセージが表示されたため、当初はISによる攻撃の可能性が疑われた。

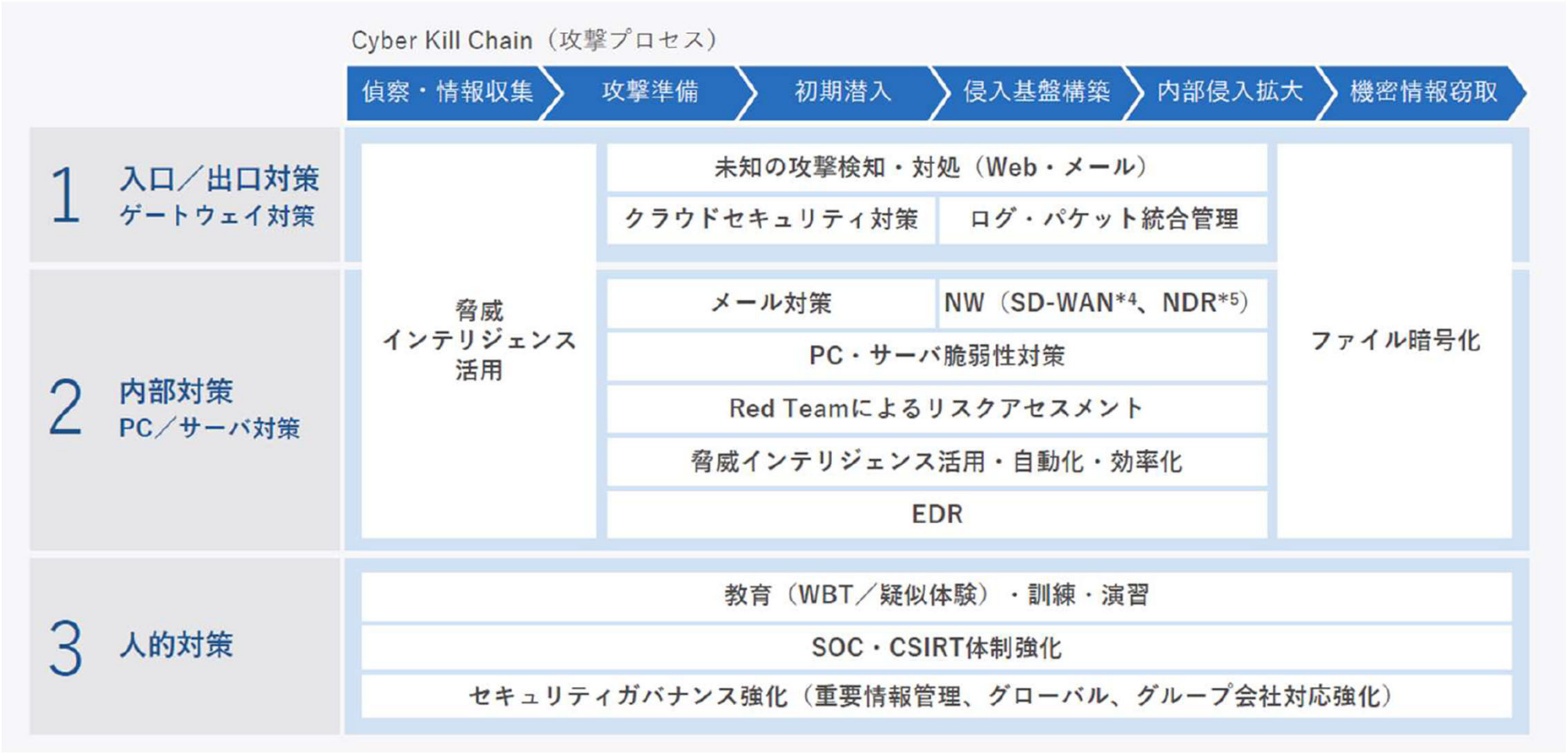


MITRE ATT&CKによる整理

有識者 提供資料等より作成

放送局におけるセキュリティガバナンスの強化

- 放送局におけるセキュリティは、攻撃プロセス（Cyber Kill Chain）を踏まえたサイバーセキュリティ対策を実施し、放送局全体のセキュリティガバナンス強化を行うことが求められる。



グローバルサイバー攻撃対策の全体像

放送機器メーカー 提供資料より作成

システム開発におけるセキュリティ対策

- サイバーセキュリティ対策は、放送設備の導入検討段階からセキュリティ対策を考慮に入れる「セキュリティバイ・デザイン」の設計思想に基づき、セキュアなシステム開発・運用を進めることが重要となる。

放送設備の開発から運用における設計プロセス

放送機器メーカー 提供資料より作成

放送機器におけるサイバーセキュリティ対策

- 放送機器のIP化は不可避な流れであることを前提とし、従来の組込みネットワーク機器と同様、放送機器のサイバーセキュリティ対策も検討を進める必要がある。

● 放送機器のIP化は不可避な流れ

- ✓ 従来の組込みネットワーク機器と同様にサイバー攻撃の脅威に備える必要がある

● 放送機器の設置・運用方法のマニュアル化は必須

- ✓ ネットワークの疎通確認ができたら完了！ではない！
- ✓ グローバルIPアドレスの直付けは極力避ける（治安の悪い街に機器を放置するのと同じ）
- ✓ ゲートウェイ（セキュリティ）機器の内側のプライベートネットワークに設置する
- ✓ 不要なポート/サービスを無効化する（つなげる前にopen portを確認）
- ✓ 機器のファームウェアを常に最新に保つ（久しぶりに使う機器は特に注意）
- ✓ ID/Passwordはデフォルトのものから必ず変更（推測困難なPasswordに）
- ✓ 自組織で運用している機器をリストアップ（資産管理はセキュリティの第一歩）
- ✓ 機器の脆弱性情報等を常にウォッチ（重大な脆弱性は数時間で攻撃が始まる）
- ✓ インシデント対応プロセスの明確化（それでもインシデントは起こるもの）　　etc., etc…

● セキュリティエンジニアを組織で雇う・育てるのが一番の安上がり

放送機器におけるサイバーセキュリティ対策への提言

情報通信研究機構　提供資料より作成

未来を問い続け、変革を先駆ける

MRI 三菱総合研究所