

放送設備のサイバーセキュリティ確保について



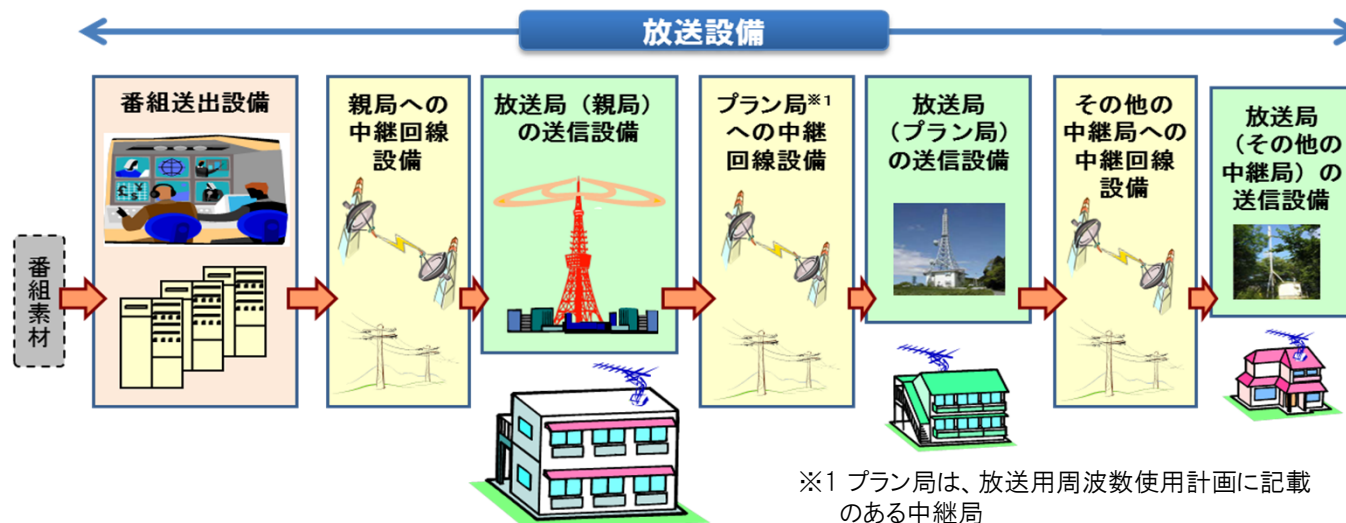
- 放送設備の安全・信頼性の確保については、現行法令において地上デジタルテレビや中波放送といった放送種別ごとに、それらの放送設備の構成等を考慮し、予備機器の配備、故障検出機能の具備、耐震対策、停電対策など、放送設備が満たすべき技術基準を規定。
- 放送設備のサイバーセキュリティの確保については、これまでも放送事業者がそれぞれに対策を行ってきているが、現行法令に技術基準として明文化された規定がない状況。
- 以上を踏まえ、放送設備のサイバーセキュリティの確保に係る規定を技術基準に追加。

○ 技術基準の対象となる放送設備は、地上デジタルテレビ放送の場合、下図のとおり、**番組送出設備**※1、**中継回線設備**※2及び**放送局の送信設備**※3で構成。なお、中波放送、衛星放送及び有線放送等における放送設備もほぼ同じ構成。

※1) 番組の素材を切り替え、映像・音声・文字・データ等の信号の符号化と多重化する設備

※2) 放送局の送信設備まで伝送する設備

※3) 放送波の送信を行う設備

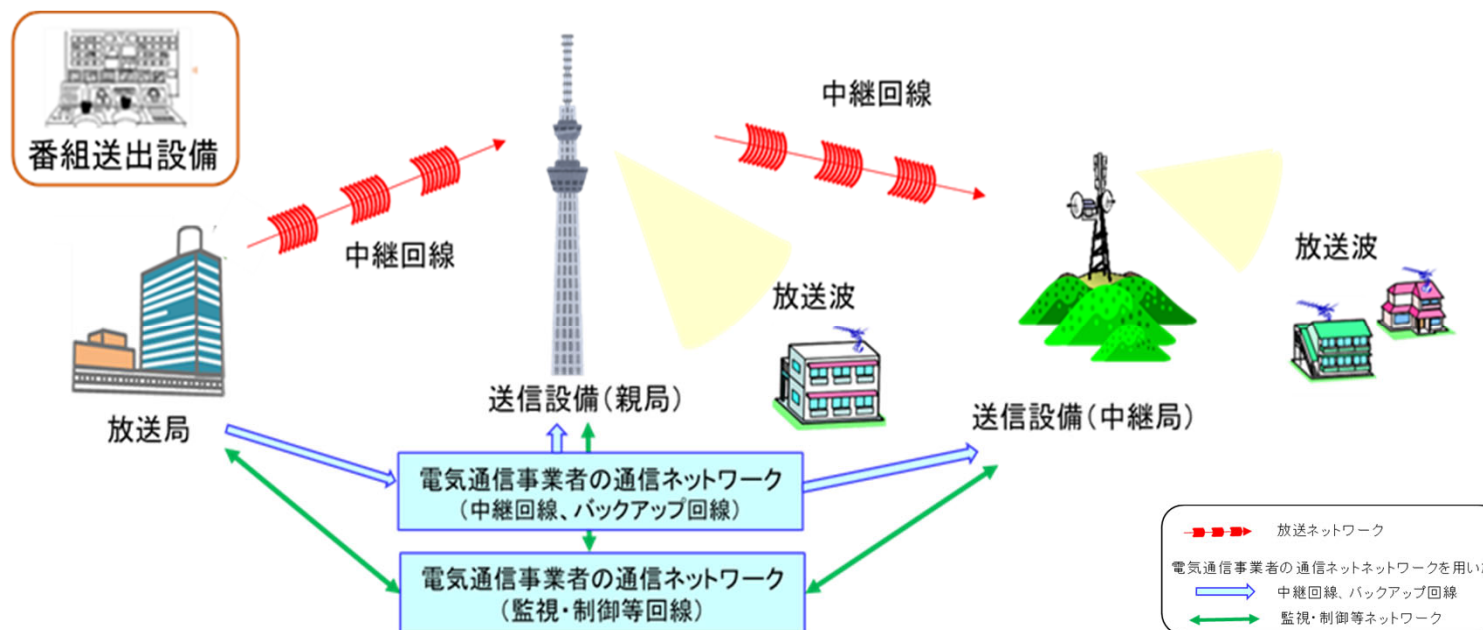


地上デジタルテレビ放送の例

※) 地上放送、衛星放送及び有線放送も、同様の設備構成

放送設備の現状とサイバーセキュリティの確保

- 放送設備及び有線放送設備の構成は、①放送番組を視聴者に届ける放送ネットワーク系統(放送本線系)と②各放送設備の故障検出や設備切替等を行う監視・制御ネットワーク系統(監視・制御系)に大別。
- 放送本線系は、映像や音声伝送のための専用方式による片方向の中継伝送と、直接受信のための放送方式による一対多の片方向の送信で構成されており、外部のネットワークと直接接続されていない。したがって、送信の起点となる箇所について対策を行うことで、効率的・効果的に他のネットワークから分離することが可能。
- 放送本線系の予備回線や監視・制御及び保守等のために電気通信事業者回線を使用する場合は、専用回線の使用、VPN化、ポート制限、ID・パスワードによる使用者の権限・アクセスの管理に加え、その管理に係る規程・マニュアルの整備など、セキュリティの確保のための措置が重要。



放送設備の構成のイメージ (地上デジタル放送の例)

- 放送本線系の入力となる番組送出設備については、その機能を、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隔離すること。
 - 放送本線系内は専用通信方式であるため、その入力となる番組送出設備において分離の措置が必要。また、起点である番組送出設備における措置により、放送本線系内全体の分離が可能となるもの。
- 放送設備に接続される監視・制御回線、保守及びシステム変更時に使用される回線については、第三者がアクセス可能な外部ネットワークからの侵入対策の措置を講じること。
 - 監視・制御用及び保守用回線は、放送設備に付随する設備であり、放送設備と同様の措置が必要。送信所等の設置場所ごとに所要の回線が手当されるが、電気通信回線を使用する場合、分離のための対策の措置が必要。
- 不正プログラムによる被害を防止するため、放送設備の隔離・遮断の措置を講じることに加え、設備の導入時及び運用・保守段階での修理・改修の受入時において、ソフトウェアの点検を行うことによる不正プログラムの感染防止の措置を講じること。
 - 外部ネットワークとの分離はサイバー攻撃対策として有効な対策。しかし、設備の更新や保守・修理機会において更新される機器内に不正プログラムが侵入している可能性があり、受入時の点検措置を行うことが必要。
- 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その実施に係る規程やマニュアルを整備すること。なお、規程やマニュアルの整備にあたり、サイバー事案の発生時の対応策と再発防止策について、事故報告を含めた事後対応を迅速かつ確実に行うこと。
 - サイバーセキュリティの確保には、その対策状態が適切に維持管理されることが必要であり、その実施の状態を確保する組織体制及び規程、マニュアルの整備を行う措置が必要。
- 今回の措置内容に対して、新たな放送サービス、技術革新等の環境変化が生じた際には、その設備形態に応じて、措置とその放送設備の対応について、適宜見直しを図ること。

- 有線放送設備については、技術基準の対象となる設備が地上デジタルテレビ放送等の放送設備とほぼ同じ構成であることから、有線放送設備についても地上デジタルテレビ放送と同様のサイバーセキュリティ確保に係る措置を講じること。
 - ケーブルテレビは、電気通信役務の提供及び有線放送設備を用いた放送を行っており、このうち電気通信役務の提供のために用いる電気通信設備に係るサイバーセキュリティは電気通信事業法によって確保されているため、有線放送設備に関するサイバーセキュリティ確保に係る措置が必要。
- 有線放送設備のうち小規模な設備（引込線数501以上5000以下）についても、大規模な設備（引込線数5001以上）と同様のサイバーセキュリティの確保に関する措置を講じること。
 - 設備の規模に関係なくサイバー攻撃の対象になる恐れがあることから、小規模な設備においてもサイバーセキュリティの確保に係る措置が必要。

(参考) 脅威と対策に係る措置の事例

脅威と対策		措置の事例	
		導入段階	運用・保守段階
不正アクセス	不正行為の影響を限定的にするため通信経路の分離を行うこと、また、不正な通信を防止するため、特定の通信を遮断すること。	<ul style="list-style-type: none"> ・専用線の使用、または敷設 ・第三者がアクセス可能な回線を使用する場合、VPN等ネットワークの閉域化やファイヤーウォールによるアクセス制御、利用者管理 ・ネットワーク監視システムの設置 等 	<ul style="list-style-type: none"> ・リモートアクセス時のアクセス制御及び利用者管理 ・利用状況の監視 ・ネットワークの監視 ・外部記録メディア等媒体接続の管理 ・ログの蓄積と管理 等
		<ul style="list-style-type: none"> ・設置時に導入される放送設備、付属設備及びソフトウェア等の受入時の点検等 	<ul style="list-style-type: none"> ・保守・修理・改修において持ち込まれる機器、ソフトウェア等の受入時の点検 ・外部記録メディア等媒体接続の管理等
管理	必要な機器のみによって必要なサービスのみを提供するようシステムの構成及び稼働状況の管理を行うこと	<ul style="list-style-type: none"> ・設定情報のドキュメント化 ・システムのバージョン管理、更新ルールの策定 等 	<ul style="list-style-type: none"> ・設定情報の更新管理 ・更新ルールの徹底と適切な更新等の実施 等
		<ul style="list-style-type: none"> ・インシデント対応の明確化 等 	<ul style="list-style-type: none"> ・インシデント発生時の対応と再発防止等
インシデント対応	障害時の迅速な復旧を行うこと。また、その後の再発防止に資すること。	<ul style="list-style-type: none"> ・インシデント対応の明確化 等 	<ul style="list-style-type: none"> ・インシデント発生時の対応と再発防止等

- 放送法第121条等において、放送設備の技術基準への適合を義務付け。
- 技術基準は、その発生を未然に防止するための措置及び発生した際の復旧を目指した措置として、設備故障、自然災害、停電その他、計12項目の措置事項を省令(放送法施行規則)で規定。
- 今般、これに、サイバーセキュリティの確保に係る規定を新たに追加。

① 予備機器等

② 故障検出

③ 試験機器及び応急復旧 機材の配備

④ 機能確認

⑤ 誘導対策 (アンテナからの電磁誘導影響への対策)

⑥ 耐震対策

⑦ 対雷対策

⑧ 防火対策

⑨ 屋外設備

⑩ 収容する建築物

⑪ 停電対策

⑫ 宇宙線対策

・ サイバーセキュリティの確保

【新規追加】