

サイバーセキュリティ確保に係るガイドライン(HP)

一般社団法人日本コミュニティ放送協会

## まえがき

コミュニティ放送は、ネットメディア時代を迎えている現在でも、住民に最も身近で、地域に密着した地上基幹放送であり、平常時は、住民に対し生活情報や行政情報等を提供し、地域の活性化、振興に寄与し、非常・災害時には、地域の生命線として情報の収集・伝達の重要な役割を担い、頻発する様々な自然災害、大地震・津波への警戒体制が見直される中、期待と重要性は一層高まっています。

そこで、放送・送信関連設備のハード面とソフト面の安全・信頼性を確保し、継続した放送番組を安定して届けるべく努力を重ねています。一段と進化するインターネット社会、増加が予測されるサイバー攻撃に対応した「サイバーセキュリティの確保」は重要課題であり、今般、日本コミュニティ放送協会では、人為的・意図的な障害、サイバー攻撃等に備えるため、コミュニティ放送業界全体に共通する「サイバーセキュリティの確保」の考え方をガイドラインとして整理しました。

## 規 定

放送・送信設備に対し放送法施行規則第 115 条の 2 の規定に基づく措置を講じ、サイバーセキュリティ確保を目的とした規定を作成する。

## 対 象

大凡、次の設備、施設を対象とするものである。

- 1)放送局舎・・・屋内放送設備の概要：演奏所、番組送出設備、音声調整装置、ステレオ変調装置
- 2)中継回線設備・・・電気通信設備の概要：STL(演奏所→主送信所=親局への伝送路)・TTL(主送信所=親局→中継局、中継局→中継局)
- 3)送信局舎・・・屋内送信設備の概要：送信装置、電源設備(UPS等予備電源を含む)  
屋外送信設備の概要：給電線、空中線、空中線柱等

### 防護措置

1. 放送設備等を収容し、又は設置する建物(放送局舎)は、建物内に関係者以外が容易に立入り、又は容易に放送設備に触れる事ができないよう、施錠その他必要な措置が講じられていること。
2. 送信設備を収容し、又は設置する建物(送信局舎)及び給電線、空中線等の屋外工作物は、建物、屋外工作物に関係者以外が容易に立入り、又は関係者以外が容易に送信設備に触れる事ができないよう、施錠その他必要な措置が講じられていること。
3. 番組中継用固定局の代替等として電気通信サービスを利用する場合の有線施設についても、できる限り上記に準じた措置が講じられるよう、要請等を行うこと。

### 防護措置(設備)

1. 放送局舎の演奏所(スタジオ)、番組中継用固定局の代替等(サテライトスタジオ)、番組送出設備を設置する場所には関係者以外が容易に立入り、又は容易に番組送出設備等に触れる事ができないよう、必要な措置が講じられていること。
2. 放送本線系入力となる番組送出設備はその機能を、インターネットなど第三者がアクセス可能なネットワークから隔離するような措置が講じられていること。
3. APS の保守及びシステム変更時に使用される回線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が講じられていること
4. 緊急割込放送装置はその機能を、インターネットなど第三者がアクセス可能なネットワークから隔離するような措置が講じられていること。
5. 外部記録メディア等媒体接続による不正対策が講じられていること。
6. 放送用伝送路(STL・TTL)として使用される中継回線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が講じられていること。
7. 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をすること。

## 管理体制

1. サイバーインシデント発生時の対応が講じられていること。
2. 放送設備(番組送出設備)に係わるソフトウェアバージョンアップ等システム変更の実施方法を定めるマニュアルの策定
3. 保守事業者との窓口を明確にするとともに、連絡体制を整備すること。
4. 事務系で使用するデバイス(PC)は不正侵入対策を講じること。
5. 業務に使用する外部記録メディア(USB)は業務専用とし外部への持出を禁止する対策を講じること。
6. 不正プログラムによる被害を防止するため放送設備の導入時及び運用・保守段階での修理改修時にソフトウェアの点検を行う。

## 解 説

### 1. 「対象」について

大凡、次の設備、施設を対象とするものである。

番組送出設備（演奏所、送出マトリクス、音声調整装置、ステレオ変調装置）

中継回線設備（STL・TTL・マイクロ波利用無線設備）

放送局の送信設備（送信装置、給電線、空中線、電源設備等）

これらを収容、支持等する建物及び工作物

### 2. 「サイバーセキュリティの確保」について

サイバー攻撃とはコンピュータシステムやネットワークに悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うこと

マルウェアとはセキュリティ上の被害を及ぼすウイルス、スパイウェア・ポットなど

主な感染経路は WEB 閲覧・メール・ファイル共有ソフト・USB メモリー

### 3. 「サイマル放送設備」について

サイマル放送用設備は通信設備であり放送設備として扱われないが、当然のことながらサイバーセキュリティ対策が講じられている必要がある。

サイバーセキュリティ確保ガイドライン

令和2年3月2日(第1版策定)

一般社団法人 日本コミュニティ放送協会

JCBA 総合検討委員会 技術部門