資料３－２

総務省におけるサイバーセキュリティ施策の取組状況について

2023年12月

総務省サイバーセキュリティ統括官室

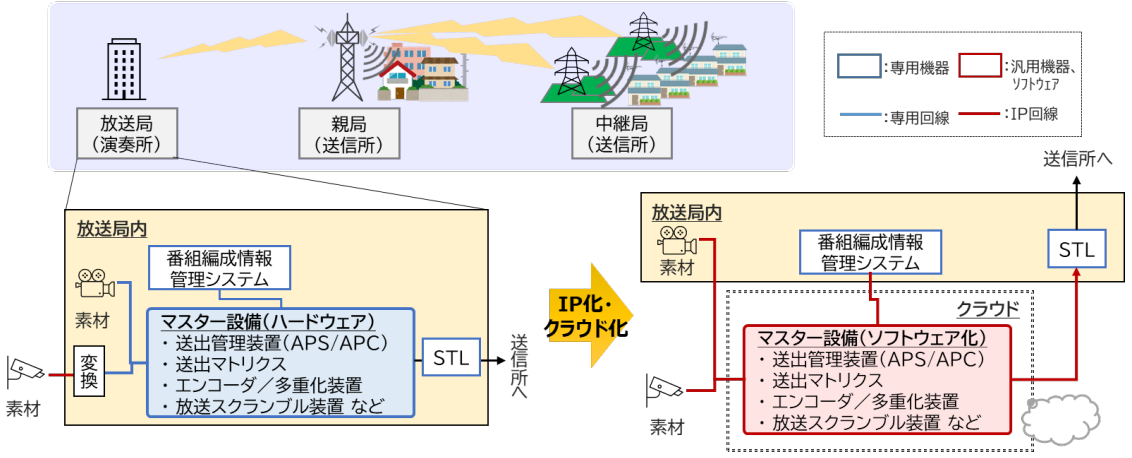
（１）放送設備のIP化に伴う安全・信頼性に関する技術的条件の検討

放送設備のIP化に伴う安全・信頼性に関する技術的条件
（令和５年11月21日　情報通信審議会答申）

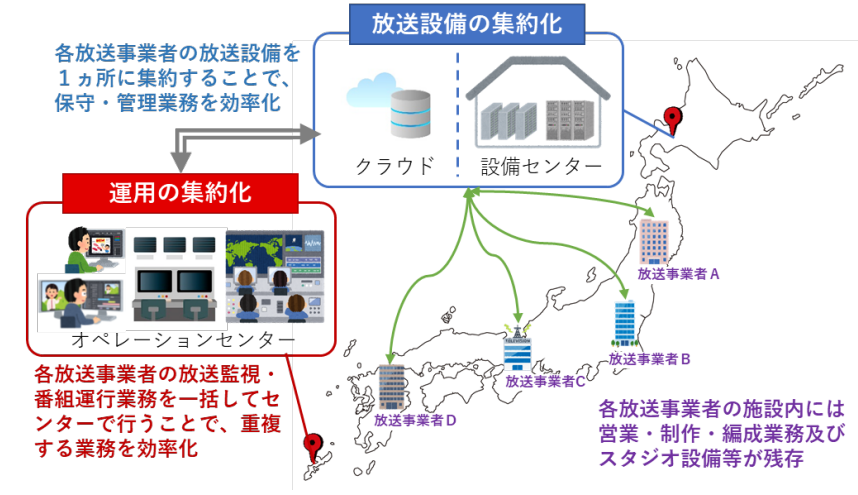
検討の背景・目的

- 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）を中心に放送設備のIP化・クラウド化・集約化が進むものと想定。
- 「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。
- 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、**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**の検討を開始。
  ※情報通信審議会諮問第2031号（H22.12.21）
- 放送設備への実装が実用化段階にあり、放送事業者の導入計画が具体化している**IP化について**、令和５年11月21日、**情報通信審議会から一部答申**。

■ IP化・クラウド化のイメージ



■ 集約化のイメージ



【参考】 マスター設備（番組送出設備）の概要

- マスター設備（番組送出設備）は、放送番組及びCM、並びに時刻・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。
- 法令上は、「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。

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 “

【参考】 マスター設備（番組送出設備）に関する動向

■ 現状と課題

- 現状、オンプレミスのシステムであり、地上基幹放送事業者毎にその社屋等に設置されている。
- 10～15年毎に設備更新が必要であり、更新投資は各地上基幹放送事業者にとって大きな負担となっている。
- 放送以外の分野においては、専用機器から汎用化（IP化）・ソフトウェア化・クラウド化という順に実用化が進んでいるところ、マスター設備についても、**一部の地上基幹放送事業者においてIP化の導入が予定**されている。
- **クラウド化**については、メーカーにおいて、**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。

● 今後の方向性

- 地上デジタルテレビジョン放送のマスター設備について、2028年～2030年頃（令和10年～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、**効率化を図る観点から、マスター設備の集約化・IP化・クラウド化は経営の選択肢**となり得る。(※)
- 集約化に当たっては、放送番組のやり取りが行われており、設備仕様がある程度共通化されている系列局の単位で集約化を図ることが現実的である。例えば衛星放送のプラットフォーム事業者のように、マスター設備を特定の場所に設置し、その運用・維持管理を地上基幹放送事業者以外の事業者が担うことや、クラウドサービスとして提供を受けることが考えられる。
- 集約化の対象エリアは、系列局単位での集約化を前提に、地域ブロックに加え、全国単位も視野に入ると考えられる。
- **集約化・IP化・クラウド化に当たっては、サイバーセキュリティ対策等、安全・信頼性をどのように確保可能かについて検討すべき**である。追加的なコストが発生することとなるが、持続可能な放送の実現のためのコスト削減とサイバーセキュリティ対策等の安全・信頼性確保の両立に向けた道筋を描くことは可能と考えられる。
- 我が国における**クラウド化の実現に向けて、どの程度の可用性を確保すべきかといった検討が必要**と考えられる。
- 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。その際、**放送に求められる可用性を確保するためには、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）できることが重要であることにも留意すべき**である。

（※）出典：「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）より事務局作成

技術的条件の検討経過

- 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化を対象として検討を開始**した。
- クラウド化・集約化に伴う技術的条件の検討については、IP化に伴う技術的条件の検討後に実施することとした。
- 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。
- 検討の過程において、IP化・クラウド化等の技術動向及びニーズが示された**音声放送及び衛星放送についても検討対象として追加**した。
- 技術的条件の具体的な検討は、以下のとおり実施した。

  - 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化等の標準モデルを検討した。
  - 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た。

- 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。

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

- IP化に伴って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**である（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）。

  - 放送本線系の伝送回線の一部が、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（同軸ケーブル）から、IP回線（光ケーブル等）に変更される。
  - 構成装置が、機能ごとに設計された専用機器（ハードウェア）から、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。
  - IP回線及びIP対応機器に置き換わることで、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なる。

- 番組送出設備の設置場所は、**放送事業者の施設内（演奏所内）**であることに変更はない。

□ 放送本線系が外部ネットワークと接続された状態になることで、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ことが必要**

- 従来型の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
- 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も重要な観点であり、具体的な措置内容は、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

□ 番組送出設備の設置場所に変更はないこと等から、**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見直しの必要なし**

番組送出設備のＩＰ化に伴う安全・信頼性に関する技術的条件

＜従来の番組送出設備＞

■ 放送専用規格に対応した専用ハードウェアで構成
■ 各装置は同軸ケーブルにより1対1接続
■ 365日24時間有人管理のマスター室に設置され、室内の専用端末で操作

■ **外部ネットワークから原則隔離された状態で運用**

＜IP化された番組送出設備＞

■ IPに対応した汎用ハードウェアとソフトウェアで構成
■ 各装置はIPに対応したLANケーブル1本で接続
■ 放送事業者のネットワーク(社内LAN等)上の汎用端末からも操作可能

■ **外部ネットワークと接続された状態で運用**

サイバーセキュリティ確保のための新たな措置内容

① 放送本線系に係る不正接続対策等

- ファイアーウォールの設置に加えて、**不正侵入の検知及び当該侵入の遮断**等、不正接続を防止するための措置
- **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、マルウェア感染防止のための措置
- **構成装置のシステム設定等に関する定期的なバックアップの実施**等、早期復旧のための措置

② ソフトウェア点検時の不正プログラム対策

- **定期的なウイルスチェック等、不正プログラムの早期検出のための措置**

③ 規程・手順書等の整備

- **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**、**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

（２）サイバー攻撃に悪用されるおそれのあるIoT機器の調査の継続・拡充のための法改正

国立研究開発法人情報通信研究機構法の一部を改正する等の法律の概要

NICTが行うサイバー攻撃に悪用されるおそれのあるIoT機器の調査について、①令和５年度末に時限を迎えるID・パスワードに脆弱性があるIoT機器の調査を、令和６年度以降も継続的に実施を可能とするとともに、②調査の対象を拡充するための規定を整備する。あわせて、特定通信・放送開発事業実施円滑化法の廃止等を行う。

１．サイバーセキュリティ関連業務の規定の整備

（国立研究開発法人情報通信研究機構法の改正）

①　ID・パスワードに脆弱性があるIoT機器の調査の継続的な実施

○　NICTが令和５年度末までに限り行うこととされているID・パスワードに脆弱性があるIoT機器の調査（特定アクセス行為）を、令和６年度以降も継続的に実施できることとする。

②　調査対象の拡充

○　NICTが行うIoT機器の調査等に係る業務について、その対象を拡充※するとともに、総務大臣が、サイバーセキュリティ戦略本部から意見を聴取した上で、NICTの中長期目標の策定等をする旨を規定する。

※ID・パスワードに脆弱性があるIoT機器に加えて、脆弱性があるファームウェア等を搭載しているIoT機器、既にマルウェアに感染しているIoT機器を新たに対象とする。

２．信用基金の清算及び特定通信・放送開発事業実施円滑化法の廃止等

・国立研究開発法人情報通信研究機構法の改正
・特定通信・放送開発事業実施円滑化法（NICTの業務特例を規定）の廃止

○　NICTの信用基金を清算し、これに伴い、NICTの関連業務及び当該基金に係る業務を規定する特定通信・放送開発事業実施円滑化法を廃止する。

施行期日：令和６年４月１日（一部の規定を除く。）

サイバーセキュリティ関連業務の規定の整備（NOTICE関係）

情報通信研究機構（NICT）法

総務大臣

中長期目標・計画に係る意見聴取

サイバーセキュリティ戦略本部

特定アクセス行為等に係る実施計画認可

中長期目標策定・計画認可

情報通信研究機構（NICT）

【法改正のポイント②】
サイバーセキュリティ対策助言等業務を新設し、サイバー攻撃に悪用されるおそれのあるIoT機器の調査対象を拡充

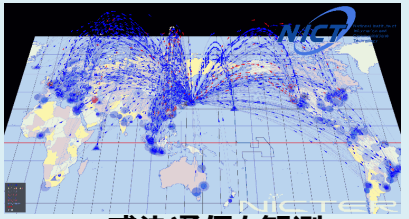
サイバーセキュリティ対策助言等業務

（サイバー攻撃に悪用されるおそれのあるIoT機器を調査し、機器の管理者等に必要な助言及び情報を提供）

ID・パスワードの設定に脆弱性を有する機器

ファームウェアの脆弱性等のID・パスワード以外の脆弱性を有する機器

既にマルウェアに感染している機器



感染通信を観測

令和６年度以降も継続して実施（特定アクセス等実施業務）

NICTの業務として新たに法的に位置づけ

【法改正のポイント①】
サイバー攻撃の最新動向等に応じて機動的に対応するため、特定アクセス等について、総務大臣の認可を受けた実施計画で定めた期間において実施

IoT機器メーカー

電気通信事業者（ISP）

SIer

その他セキュリティ関係者

注意喚起

機器の利用者

利用者からのサイバー攻撃の被害の申告を待つことなくプッシュ型による支援を実施するとともに、様々な関係者との連携により総合的なIoTセキュリティ対策を促進