

株式会社エフエム大阪 情報セキュリティポリシー

策定：2003年10月1日

最終更新日：2023年11月1日

情報セキュリティ基本方針

1.はじめに

株式会社エフエム大阪(以下当社という)は、音声メディアに加え、タイムテーブルなど紙媒体から情報技術を利用した情報発信に力点がおかれ、放送の付加価値を高めている。

また、当社の扱っている各種情報がネットワーク上で扱われることが当然のこととなりコンピュータネットワークの導入による業務効率改善やインターネットを利用したビジネスチャンスの拡大も期待されるところである。

しかしながら情報技術においては、情報の発信・収集、蓄積などにおいて高い利便性を有する反面、常にリスクを抱えている。主なものとしてウイルス等による攻撃や不正アクセスによる情報漏えいや、情報の改ざん・破壊活動などがあるが、それらによる被害は全世界においても甚大なものとなりつつある。

また、被害を受ける立場だけでなく、故意や不用意な操作などによって対外的に大きな損害を与える可能性もある。

ひとたび問題が発生すると、経営上の損失だけでなく、損害賠償や社会的信用の失墜につながりかねない事態となる恐れがある。コンピュータやネットワークのセキュリティを確保することは、大きな課題であり、具体的に被害を防止するための対策や、情報発信サイドである当社から問題を発生させないための行動指針を策定し、これをもって当社の情報セキュリティ基本方針を定め、社会の負託に応えるものとする。

2. 情報セキュリティに関する宣言

(1) 社内体制および情報セキュリティポリシーの整備

当社は、セキュリティの維持及び改善のために必要な管理体制を整備し、必要な情報セキュリティ対策を社内の正式な規則として定めます。

(2) リーダーシップにおける責任および継続的改善

当社の経営者は、本方針の遵守により、当社及び関係する皆様の情報資産が適切に管理されるよう主導します。

(3) 法令、契約上の要求事項の遵守

当社の従業員は、事業活動で利用する情報資産に関連する法令、規制、規範及び関係する皆様との契約上のセキュリティ要求事項を遵守します。

（４）従業員の取組み

当社の従業員は、情報セキュリティの維持及び改善のために必要とされ知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

（５）違反及び事故への対応

当社は、情報セキュリティに関わる法令、規制、規範及びお客様との契約に関わる違反及び情報セキュリティ事故への対応のための体制を整備し、違反及び事故の影響を低減します。

株式会社エフエム大阪

情報セキュリティポリシー

1. 適用範囲

本情報セキュリティポリシーの適用範囲を次のとおりとする。

(1) 情報

- ・ 当社で運用するコンピュータシステム内の磁気、光等の記録媒体に記録されている情報
- ・ 当社で運用する磁気や光などの外部媒体および紙等の印刷された情報、会議などの録音情報
- ・ その他経営に資する情報の一切

(2) 情報システム

- ・ 当社の情報システムを構成するハードウェアおよびソフトウェアに関する全般
- ・ 当社で運用するコンピュータシステムを管理・運用する組織と人員
- ・ 当社で運用する情報システムを設置している建物やサポートしている設備など

(3) 人員

- ・ 役員、社員、嘱託員、派遣社員、パート・アルバイトなど雇用形態や契約形態を問わず当社業務に従事するすべての人
- ・ 業務を外部委託する場合は、別に定める機密保持契約の締結をもって、情報のセキュリティを確保すること。

(4) 個人情報保護

- ・ 個人情報保護については、本情報セキュリティポリシーの範囲外とし、別途定める個人情報保護規程によるものとする。

2. 情報セキュリティマネジメント体制

(1) 情報セキュリティのための組織

① 委員会

情報セキュリティ対策活動を推進するための組織として、「情報セキュリティ委員会」を設置し、必要に応じ委員会を開催する。委員会の構成は、委員長および数名の委員から構成する。委員長は社長が任命し、委員は常務会で決定する。

情報セキュリティ委員会は、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有、情報漏洩事故等のインシデントが発生した場合の対策、再発防止策の策定とその実施を行う。

② 情報セキュリティの責任体制

情報セキュリティに関する責任者を以下のように定める。

情報セキュリティ責任者 (情報セキュリティ全般の責任者)	情報セキュリティ委員会委員長
---------------------------------	----------------

情報セキュリティ部門責任者 (当該情報システムを運用・保有する部門の責任者)	各部長
システム管理者・教育責任者・監査・点検責任者	総務部長

情報セキュリティ責任者及び情報セキュリティ部門責任者は、本情報セキュリティポリシーが適用される情報・情報システムの管理・運用に責任を持ち、管理監督を行う。

③ 情報セキュリティへの取り組みの監査・点検

【社内監査】

監査・点検責任者は定期的に本情報セキュリティポリシーの実施状況について、点検を行い、点検結果を情報セキュリティ委員会へ報告しなければならない。

情報セキュリティ委員会は、報告に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。

- ・ 情報セキュリティポリシーが有効に実施されていない場合、その原因の特定と改善
- ・ 情報セキュリティポリシーに定められたルールが、新たな脅威に対する対策として有効でない場合は、情報セキュリティポリシーの改訂
- ・ 情報セキュリティポリシーに定められたルールが、関連法令や取引先の情報セキュリティに対する要求を満たしていない場合は、情報セキュリティポリシーの改訂

【外部監査】

監査・点検責任者は必要に応じ、社外監査機関にセキュリティ評価を依頼することができ、安全性を確保しなければならない。

(2) 情報セキュリティに関する人的対策

【取締役及び従業員の責務】

取締役及び従業員は、以下を遵守する。

- ・ 取締役及び従業員は、当社が秘密として管理する情報及びその複製物の一切を許可されていない組織、人に提供してはならない。
- ・ 取締役及び従業員は、当社の情報セキュリティポリシー及び関連規程を遵守する。

【周知と情報セキュリティ教育】

教育責任者は、情報セキュリティポリシー確保のため、必要とする情報を社員・スタッフに周知しなければならない。また社員に対し定期的に教育を行うこととする。教育内容は別に定める。

3. 管理規定

(1) 対象システム

本情報セキュリティポリシーで管理する具体的システムは以下のものとする。これ以外の機器・システムについては、本情報セキュリティポリシーに準拠した形で、運用部門で管理を行うこととし、その責任者は運用部門の部門長（部長）とする。

【対象システム名称】

- ① 会計システム、給与システム、電子伝票システム
- ② 放送系システム（ABM システム（EDPS・DAW 等）、マスターシステム、送信システム等の放送本線に関する設備）
放送系システムについては、他のシステムとは繋がずクロードなシステムを基本とする。ただし、他システムやインターネットとの連携が必要な部分では、ルーターやゲートウェイなどのネットワーク機器でセキュリティ上の安全性を確保する。
- ③ 一般系社内 LAN システム（サーバー、クライアント PC を含む）
- ④ スタッフ系社内 LAN システム
社内 LAN システムについては、外部との接続部や他システムとの接続部にルーターやゲートウェイ、ファイヤーウォールなどのセキュリティを確保するネットワーク機器を導入し、セキュリティ上の安全性を確保する。
- ⑤ 一般 OA 機器
- ⑥ その他通信システム
- ⑦ スタジオ・社屋等の構築物
- ⑧ 入室管理設備・監視機器

(2) 管理規定

以下の管理規定については別途定める。

- ① 情報資産管理規定
- ② ウイルス対策規定
- ③ クライアント PC の取扱規定
- ④ ネットワーク利用規定
- ⑤ インターネット利用規定
- ⑥ メール利用規定
- ⑦ 設備等管理規定
- ⑧ アウトソーシング管理規定
- ⑨ 情報セキュリティインシデント対応規定
- ⑩ 放送系システム管理規定

4. 情報セキュリティ確保のための予算措置

情報セキュリティ確保のために必要な予算は、原則として総務部の予算とする。

5. 罰則

当規定で定めるものを過失または故意で会社に損失を与えた場合は、就業規則に定める賞罰委員会および懲戒規定により懲戒する。

附則

この規定は 2003 年 10 月 1 日より施行する。

① 情報資産管理規定

【情報資産の管理責任者】

情報資産の管理責任者は、当該情報資産を保有する部門長とする。

【情報資産の利用者】

情報資産の利用は管理責任者の許可を得て行うこと。

【情報資産の社外持ち出し】

情報資産を社外に持ち出す場合には、以下を実施すること。

- ・ 所属部門長の許可を得る。
- ・ 情報機器やデータを持ち出す場合は、データの暗号化や、セキュリティロックを設定し、第三者がデータを参照できないように設定する。
- ・ 屋外でネットワークへ接続して情報資産を送受信する場合は、情報セキュリティ上安全な方法（例えば暗号化通信など）で行う。
- ・ 携行中は常に監視可能な距離を保つ。

【退社（退職）時の情報資産の扱い】

退社（退職）時には、秘密保持契約などを交わし在職中に得た情報を第三者に漏洩・提供しないこととする。

【情報資産の送信】

- ・ 情報資産を送信する場合は、利用するサービスの情報セキュリティ方針が、当社の情報セキュリティポリシー以上の厳重なセキュリティを確保していることを確認して利用すること。

【媒体の処分】

重要情報・機密情報の情報資産を廃棄する場合は、以下の処分を行うこと。

- ・ 書類・フィルムなどは細断・溶解・焼却処分とする。
- ・ 電子媒体（USB メモリ・HDD・CD・DVD など）は破壊・細断・完全消去とする。

【媒体の再利用】

重要情報・機密情報の情報資産を保存した媒体を再利用する場合は、以下の処分を行うこと。

- ・ 書類については裏紙再利用禁止。
- ・ 電子媒体（USB メモリ・HDD・CD・DVD など）は完全消去後再利用する。

【バックアップ】

- 情報システムの運用者は自部門が運用するシステムのデータのバックアップを定期的
に取得する。バックアップに利用した機器及び媒体の取り扱いは、セキュリティに厳
重に注意して行うこと。
- クラウドサービスを利用し、外部のサーバーにバックアップを保存する場合は、サー
ビス提供者のサービス利用約款、情報セキュリティ方針が、当社の情報セキュリティ
ポリシー以上の厳重なセキュリティを確保していることを確認し利用すること。

② ウイルス対策規定

コンピュータウイルス対策のため、次の事項を遵守すること。

- ・ パソコン・スマートフォン・タブレットなどを利用する場合は、ウイルス対策ソフトウェアの利用すること。
- ・ 社用パソコンなどについては、会社で推奨するウイルス対策ソフトを導入し使用すること。
- ・ ネットワーク経由で入手するファイルは、ウイルス対策ソフトウェアの自動検知機能を有効にしてウイルス検知を実施すること。
- ・ 電子媒体を用いてファイルの受け渡しを行う場合は、媒体内のファイルにウイルス検知を実施すること。
- ・ ウイルス対策ソフトウェアの定義ファイルを随時更新する。持ち出し用ノートパソコンは利用時に定義ファイルの更新を確認すること。定義ファイルの更新は基本的に自動的に行われる。
- ・ 当社が管理するパソコン及びサーバー以外の機器を社内 LAN に接続することを基本的に禁止する。業務上必要な場合は、情報セキュリティ管理者（または部門管理者、システム管理者）の許可を得たうえで、当該機器にウイルス対策ソフトウェアが導入されており、当該機器にウイルスが検知されないことを確認してから接続する。
 - 当社管理以外のパソコン等の管理責任者は、その使用者（及び使用者を管理監督する者）とする。
 - 当社管理以外のパソコン等の設定管理（ネットワーク設定等）はその使用者が行うこと。
- ・ 教育責任者は、適宜ウイルスに関する情報を収集し、重大な被害を与えるウイルスに対しては、対応策及び対応に必要な情報を社内に公開及び通知する。従業員は、感染防止策が通知された場合は、速やかに実施完了すること。
- ・ 知見のない人からのメールや怪しいメールは絶対開かず削除すること。また添付ファイル付きメールや画像付きメール、リンク付きメール等は特に注意すること。
- ・ OS や各種アプリケーションソフトウェアのセキュリティホールを塞ぐため、最新のバージョンにアップデートを行うこと。
- ・ 万一ウイルス等に感染が判明した場合(警報が出る等)むやみな操作は絶対にせず、システム管理者に連絡をすること。また、見慣れないメッセージが出る、頻繁にアプリケーションがハングアップする、システムの電源が落ちるなど、異常と感じた場合もシステム管理者に連絡をすること。

③ クライアント PC 取扱規定

当社が配布したクライアントパソコン(以下 PC)の取扱について規定する。

【一般的利用】

- ・ 自己が使用する PC は、自己の責任において管理しなければならない。
落下、水濡れなど取扱いには十分に注意を払い、退社時には盗難防止のため必要な措置をとること。PC を社外に持ち出す場合はパスワードを設定し、万一置き忘れなどでも情報が漏れないようにすること。
- ・ 個人使用のパソコンは原則として社内 LAN に接続してはならない。
社内 LAN システムは IP アドレスによる管理を行っているため、無断で接続した場合には、社内 LAN システムが停止するなど業務に多大な影響をもたらす。業務上必要な場合は、情報セキュリティ管理者（または部門管理者、システム管理者）の許可を得たうえで、当該機器にウイルス対策ソフトウェアが導入されており、当該機器にウイルスが検知されないことを確認してから接続する。
- ・ 勤務時間内において、PC を業務に関係のないことで使用をしてはならない。
- ・ データ破壊を防ぐため PC の電源の ON/OFF は決められた手順で行い、バッテリーは常に充電しておくこと。
- ・ PC は故障や不用意な操作で簡単にデータの消滅やエラーが発生する。定期的に USB メモリなどの電子媒体にバックアップしておくこと。
- ・ パスワードの設定を行うこと。
- ・ 長時間の離席の場合は情報漏えい対策のため、電源を OFF すること。
- ・ プリンタは「通常使うプリンタを指定」しておき、頻繁に印刷先を変えないこと。
時として重要な情報が思わぬプリンタに放置され、情報漏洩につながる。またプリンタに印刷物を放置しない。

【ソフトウェア】

- ・ 業務に利用するパソコンには、システム管理者（又は部門長）が指定した標準的ソフトウェアを導入する。この標準的ソフトウェア以外のソフトウェアを導入する場合は、システム管理者の許可を得たうえで導入する。
- ・ 業務に利用するパソコンでは、最適なセキュリティを確保するため、OS やアプリケーションのアップデートを自動的に行うように設定し、適宜ソフトウェアの更新を行う事。
- ・ 業務に不要なシステムユーティリティやソフトウェアを利用しない。
特に、以下のソフトウェアについては利用を禁止する。
 - インターネット上で、不特定多数のコンピュータ間でファイルをやりとりできるソフトウェア（ファイル共有ソフト）。
 - 不審なベンダーが提供するソフトウェア。
 - 正規ライセンスを取得していないソフトウェア。

- ※ 当社が配布したクライアント PC 以外の PC 機器（スマートフォン、タブレット等を含む）の管理責任者はその使用者（及び使用者を管理監督する者）とする。その PC 機器の設定（ネットワーク設定等）は、その使用者が行うこと。

④ ネットワーク利用規定

【ネットワーク（LAN）】

当社にはコンピューターネットワーク（LAN）として以下の系統が存在する。下記（１）（２）はインターネットに接続されているが、それ以外は、クローズドな LAN 構成となっている。

※（１）（２）の LAN については、一部 WIFI 化されている場所もある

（１）一般系社内 LAN システム

LAN ケーブルは水色。IP アドレスで管理。FM 大阪固有 IP アドレスで外部に接続。基本的に社員、常駐スタッフが使用する LAN。プリンタ、複合機あり。電子伝票システムなどにも接続されている。

（２）スタッフ系 LAN システム

LAN ケーブルはピンク又は水色に赤丸札。スタジオエリアなどに設置。FM 大阪固有 IP アドレスで外部に接続。IP アドレスは DHCP による自動取得。Wifi 無線 LAN にも対応（SSID：EtrackStudioNetwork2、EtrackStudioNetwork3）。プリンタあり。

（３）EDPS 系 LAN

LAN ケーブルは赤。IP アドレスで管理。EDPS システム専用の LAN で他の機器・システムは使用不可。

（４）DAW 系 LAN

LAN ケーブルは緑。IP アドレスで管理。DAW システム専用の LAN で他の機器・システムは使用不可。

（５）APC（APS）系 LAN

LAN ケーブルはオレンジ又は茶色。放送の基幹であるマスター APC（APS）システム専用の LAN。IP アドレスで管理。APC（APS）システム専用の LAN で他の機器・システムは使用不可。

（６）DAF 系 LAN

LAN ケーブルは黄色。DAF システム専用の LAN。IP アドレスで管理。DAF システム専用の LAN で他の機器・システムは使用不可。

（７）JFN 情報ネット系 LAN

LAN ケーブルは紫またはオレンジ。JFN 情報ネットシステム専用の LAN。IP アドレスで管理。JFN 情報ネットシステム専用の LAN で他の機器・システムは使用不可。

（８）その他

上記（１）～（７）以外の LAN 系統については、システム管理者の許可を得て部門長や従業員が私的に敷設・利用を行っている LAN である。これら LAN については、その敷設・利用者が責任をもって管理運営することとする。

【ネットワーク接続】

- ログイン ID とパスワード(PW)はシステム管理者が発行する。与えられた ID 以外からログインしてはならない。
- PW は基本的に変更しないこと。変更する場合は保守必要性の観点から、管理部門に届け出ること。また、PW は手帳などに控え、間違っても PC の周辺に貼り付けたりしないこと。
- 必要に応じ、社内 LAN 環境の改善のために個々の部門でネットワークを構成する必要がある場合は、システム管理者に相談すること。この場合のネットワーク管理は敷設部門の管轄とする。
- 社内 LAN の一部が WIFI 化されているが、その WIFI に接続する場合の WEP キーなどは、社内関係者以外に漏らさないように注意すること。

⑤ インターネット利用規定

インターネットを利用する際には以下を遵守する。

【ウェブ閲覧】

業務でウェブ閲覧を行う場合は以下に注意する。

- ・ 公序良俗に反するサイトへのアクセスをしない。
- ・ 不審なサイトへのアクセス及び社用メールアドレス登録をしない。
- ・ 業務上、個人情報(メールアドレス、氏名、所属等)を入力する場合は、通信の暗号化、接続先の実在性等を十分に確認したうえで行う。
- ・ 信頼できるサイトから署名付きのモバイルコードをダウンロードする場合を除き、モバイルコード(クライアントパソコン側で動作するプログラム)を実行しない。

【オンラインサービス】

インターネットで提供されているサービスを業務で利用する場合は、以下に注意する。

- ・ インターネットバンキングを利用する際には、当該銀行が提供する専用アプリケーションソフトをなるべく用いる。
- ・ 電子決済を利用する際には、SSL/TLS による通信暗号化を採用しているサイトを利用する。
- ・ 電子メールに記載されているリンクや、他のウェブサイト等に設置されているリンクは、偽サイトへの誘導である可能性があるためアクセスしない。
- ・ オンラインストレージに情報資産を保存する場合は、システムの安全性や情報漏えいなどのリスクに十分注意する。
- ・ オンラインストレージにメールアドレスの登録が必要な場合は社用メールアドレスを登録する。
- ・ セキュリティポリシーを公表していないサービスの利用は禁止する。
- ・ 不審なベンダーが提供しているサービスの利用を禁止する。

【SNS の利用】

- ・ 当社の業務の秘密に関わる情報の書き込みは行わない。
- ・ 取引先等関係先と SNS 上で私的に交流する場合、双方の立場をわきまえ、社会人として良識の範囲で交流する。
- ・ SNS 用のアプリケーションが提供するセキュリティ設定を行い、アカウントの乗っ取りやなりすましに注意する。
- ・ 使用するパソコン、スマートフォン、タブレット上のデータ、写真、位置情報が、予期せず公開される可能性のあることに注意する。

⑥ メール利用規定

電子メールを利用する際には以下を実施すること。

- ・ メールアドレス漏えい防止のため同報メール（外部の多数相手に同時に送信する場合）を送信する場合は、宛先（TO）に自分自身のアドレスを入力し、BCCで複数相手のアドレスを指定する。
 - ☆ CC又は宛先（TO）に複数アドレスを指定すると、送信相手に複数全員のアドレスが通知され、個人情報の漏えいになります。
- ・ 傍受による漏えい防止のため情報資産を送信する場合は、可能な限りメール本文ではなく添付ファイルに記載し、できるだけファイルを暗号化して送信する。
 - ☆ 添付ファイル暗号化は例えばパスワード保護の設定又はパスワード付きのZIPファイルにする。
- ・ 標的型攻撃メール等によるウイルス感染を防止するため、知見のない人からのメールや怪しいメールは絶対開かずに削除すること。また添付ファイル付きメールや画像付きメール、リンク付きメール等は特に注意すること。

⑦ 設備等管理規定

放送設備、ネットワーク設備など中枢システムを防犯のため、次の事項を遵守すること。

- ・ 本社正面玄関は基本的に施錠されている。このため、入館時には、当社発行の ID カードにて入場すること。当社社員以外のスタッフについては入館用 ID カード発行申請を行い ID カードを使用して入館するか、担当従業員を受付前の電話機にて呼び出して入館すること。
- ・ 社内においては必ず ID カードを携行し、常に身分を表示しなければならない。ID カードの紛失や身分喪失の場合は速やかに総務へ届けなければならない。
- ・ サーバなどが設置されている機械・ラック室は、入室制限を行っている。必ず技術担当者に入室の許可をとること。
- ・ 送信所、中継所などの電子的施錠が困難な設備においては、施錠し管理を行っている。これら設備に入場する必要がある場合は、必ず技術担当者が帯同すること。
- ・ 営業時間外の総務部は電気錠が施錠されており、無断で入室すると警報が発し、防災センターに届くので不用意に入室しないこと。
- ・ 社内は監視カメラが多数設置されており、常時録画されている。不審な事象と判断した場合は、警察への通報をする場合がある。
- ・ 玄関をはじめとして、非常警報ボタンが各所に設置されている。警報鳴動時は警察へ通報する場合がある。

⑧ アウトソーシング管理規定

【委託先の評価（クラウドサービスの利用を除く）】

情報資産の処理あるいは授受を伴う業務を外部の組織に委託する場合は、委託先の情報セキュリティ管理について、下記の項目について適切に評価し委託の可否を判断すること。

- ・社内管理体制が適切であるかどうか
- ・従業員の監督が適切であるかどうか
- ・情報機器・媒体の取扱いが適切であるかどうか
- ・サーバー・パソコン等の管理が適切であるかどうか

【委託契約の締結】

委託契約書には、下記に関する事項を明記する。

- ◇ 当社の社外秘又は極秘の情報資産及び個人情報の守秘義務
- ◇ 再委託についての事項
- ◇ 事故時の責任分担についての事項
- ◇ 委託業務終了時の当社が提供した情報資産及び個人情報の返却又は廃棄、消去についての事項
- ◇ 情報セキュリティ対策の実施状況に関する監査の方法とその権限
- ◇ 契約内容が遵守されない場合の措置
- ◇ 事故発生時の報告方法

【再委託】

当社が委託する業務を、委託先が他の組織又は個人に再委託する場合には、事前に書面による報告を委託先に求める。

⑨ 情報セキュリティインシデント対応規定

情報セキュリティに関するインシデント等の発生時には、部門責任者は速やかに情報セキュリティ責任者に連絡する。情報セキュリティ責任者は、情報セキュリティ委員会を速やかに招集し、以下の対応に当たる。

- ・ 事実関係の調査
- ・ 影響範囲の特定
- ・ 影響を受ける対象への報告連絡
- ・ 総務省への報告連絡
- ・ 原因の究明
- ・ 再発防止策の立案・実施と公表

⑩ 放送系システム管理規定

放送系システム（ここで放送系システムとは、ABM システム（EDPS・DAW 等）やスタジオ設備を除く、マスターシステム、送信システム等の放送法施行規則第 115 条の 2 で規定される、番組送出設備、中継回線設備、送信設備等の放送設備を指す）についての管理を規定する。

【本項の目的】

本項の目的は、放送・送信設備が適切に維持管理されるように放送法施行規則第 115 条の 2 で規定に基づく措置を講じ、サイバーセキュリティを確保することを目的とする。

【用語】

・サイバーセキュリティ

ここでは、サイバー攻撃を検知、防止、攻撃に対応することにより情報を保護するプロセスの事をいう。

・インシデント

ここでは、リスクが発現・現実化した事象の事をいい、具体的には不正アクセス、マルウェアやウイルス感染等のサイバー攻撃を起因とした放送停止を指す。

【対象範囲】

・演奏所（所在地：大阪市浪速区湊町 1-3-1 FM 大阪本社）

番組送出設備（マスター APS システム、DAF システム）

・中継回線設備

STL/TSL 設備

・送信所（所在地：大東市北条 2377）

変調器、音声調整装置、送信設備

・中継所（所在地：大阪府豊能郡能勢町野間西山）

受信設備・送信設備

【対策】

- ・ サイバーセキュリティ対策として、放送本線系システムの外部ネットワークからの隔離を行う。
 - 放送本線系のシステムは他のシステムとは繋がずクローズドなシステムを基本とする。ただし、他システムやインターネットとの連携が必要な部分では、ルーターやゲートウェイなどのネットワーク機器で不正接続対策措置を図ることを基本とする。
 - 接続する回線は、専用回線や VPN 回線を使用し、ポート番号や IP アドレスによる接続制限や、ID/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。
 - 不要時には未接続とするようタイムアウト値を設定する。
- ・ 設備の導入時及び保守時における不正プログラム感染防止措置をとる。
 - 設備の導入・保守・点検時等においては、ウイルス検出ソフトなどによりソフトウェアの点検を行い不正プログラムの感染防止を確認する。

- 外部記録メディアを介した不正プログラムへの感染防止策として、放送設備にこれら記録メディアを接続する際には、ウイルス検出ソフトなどで感染防止対策をされた端末に接続することとする。
- 外部記録メディアとしては、USB メモリはなるべく使用せず、SD カードを基本とする。
- ・ 放送設備に対する物理的なアクセス管理として、技術部技術室及びマスター室（ラック室を含む）は基本的に施錠し、その入退室においては、開錠権限を持つ ID カード保持者の入室を基本とし、その他の人員は技術部員及びマスター担当者の許可を得て入室することとする。送信所、中継所などの電子的施錠が困難な設備においては、施錠し管理を行っている。これら設備に入場する必要がある場合は、必ず技術担当者が帯同すること。
- ・ 放送設備のソフトウェアのアップデートについては、クローズドなシステム構成を基本とするため、不具合対応の場合以外では行わない。不具合対応としてのソフトウェアアップデートについては、システムベンダーとそのソフトウェアの安全信頼性について確実な打ち合わせを行い、実施する。
- ・ 放送設備のセキュリティ対策として、ネットワーク機器、サーバー、クライアント PC 等ではログを適切に取得する。インシデント発生時にはログ解析を行うとともに原因究明、その再発防止策に活かすこととする。

【サイバー事案発生時の事故報告に関する連絡先・報告手順】

基本的には「⑨情報セキュリティインシデント対応規定」に基づき対応を行うが、放送システムに関するサイバー事案発生時には、以下のように対応を行うこととする。

※体制

放送系システムに関するサイバーセキュリティを実施する体制は、本情報セキュリティポリシーに記載の「情報セキュリティマネジメント体制」に基づくものとする。ただし、放送システムに関する部門責任者は技術部長とする。

※報告手順

放送システムに関するインシデントが発生した場合には、
《事象発見者➡技術部長➡情報セキュリティ責任者（情報セキュリティ委員長）》
というフローで報告を行う。

この時、

- ✧ 情報セキュリティ責任者は、状況に応じ各部門の部門責任者に連絡を行う。
- ✧ 技術部長（又は情報セキュリティ責任者）は、総務省（近畿総合通信局）へインシデント発生の報告を行う。

※原因の解明と復旧

部門責任者である技術部長は、インシデントの状況を把握し、原因の追求及び復旧作業を行う。

※復旧後の報告・再発防止策

インシデント復旧後には速やかに関係機関（総務省を含む）に報告を行い、情報セキュリティ委員会を開催し、再発防止策を検討し対策を行う。