富山エフエム放送株式会社

放送設備等サイバーセキュリティ対策規程

第１条（目的）

この規程は、当社の情報セキュリティ対策についての基本的事項を示すものであり、社外および社内からのサイバー攻撃等によるデータ・プログラムの漏洩、破壊、改竄および通信ネットワークを経由した不正侵入等の脅威に対して、放送設備全体の正常な運用および保全ならびに情報資産の防護を目的とする。

第２条（適用範囲）

この規程は、放送局舎、送信局舎、中継回線設備、自動放送システムおよび営放システム、事務処理システムに係る業務処理に適用する。

第３条（用語の定義）

用語の定義は次のとおりとする。

(1)「放送局舎」とは、演奏所、番組送出設備、音声調整装置等の放送設備を有する施設をいう。

(2)「送信局舎」とは、「親局」「中継局」等の送信設備を有する施設をいう。

(3)「自動放送システム」とは、番組およびＣＭ放送の電波を自動発信する仕組み全体をいう。

(4)「営放システム」とは、番組放送スケジュール、ＣＭ放送を管理する仕組み全体をいう。

(5)「事務処理システム」とは、情報処理機器を使用して事務処理するための仕組み全体をいう。

(6)「システム」とは、営放システムおよび事務処理システムを総称し、情報処理機器、プログラム、通信ネットワークおよびそれらにより提供される機能全体をいう。

(7)「情報」とは、営放システムおよび事務処理システムに電磁的に記録されたデータを言う。

(8)「通信ネットワーク」とは、システムにおいて使用する通信線、通信装置、通信制御プログラムおよびそれらに提供される機能をいう。

(9)「情報資産」とは、「システム」および「情報」をいう。

(10)「情報セキュリティ」とは、情報資産の機密性、完全性および可用性を維持することを言う。

ａ「機密性」とは、許可されていない者が情報資産にアクセスできないよう制限することをいう。

ｂ「完全性」とは、情報およびシステムによる情報の処理結果が完全である状態をいう。

ｃ「可用性」とは、許可された者が必要な時に情報資産にアクセスできるようにすることをいう。

(11)「サイバー攻撃等」とは、情報資産に対する電子的攻撃および情報資産の不適切な取り扱いなどをいう。

(12)「不正アクセス」とは、許可されていない者が情報資産へのアクセスを行うことをいう。

(13)「セキュリティ事故」とは、サイバー攻撃等により事業運営に支障となる事故をいう。

(14)「利用者」とは、当社の情報資産を利用する者をいう。
(15)「情報資産を所管する組織の長」とは、各部長および東京支社長をいう。

第４条（情報セキュリティに関する基本的な考え方）

情報セキュリティに関する基本的な考え方は次のとおりとする。
(1)情報セキュリティ水準の維持・向上を継続して行える体制を確立する。
(2)情報資産への攻撃を遮断する防護策を実施する。
(3)万が一の攻撃を想定した緊急時の対応を定め、迅速な復旧と再発防止に備える。
(4)情報セキュリティに関する全社員の意識の高揚をはかる。

第５条（情報セキュリティ統括責任者）

情報資産は、常務取締役が情報セキュリティ統括責任者として、防護すべき情報資産を特定し、状況の把握および指導等を行う。
２　各情報資産について、具体的な対策の実施と管理を行うため、情報セキュリティ管理者を定める。
３　各組織の長が所管する情報資産は次のとおりとする。
(1)総務部長・・・・・総務部が所管する情報資産
(2)放送部長・・・・・放送部が所管する情報資産
(3)営業部長・・・・・営業部が所管する情報資産
(3)東京支社長・・・・東京支社が所管する情報資産

第６条（情報セキュリティ対策）

情報セキュリティ統括責任者は、情報資産の重要度に応じて以下の対策を適切に実施し、セキュリティ事故の発生の防止に努める。
(1)物理的セキュリティ対策
a.放送局舎への入館は、事前登録したカードキーで管理し、関係者以外が容易に立入りできないよう、必要な措置を講ずること。
b.マスター室への入室には、電子的認証等で入室制限を行うこと。
c.送信局舎等、電子的認証等が不可能な施設は、施錠し管理する措置を講ずること。
(2)システム構成面に関する対策
システムを社内外の他のシステムと切り離すことを基本とし、必要により継続する場合は、接続点を極力少なくするとともに、必要な通信だけに限定し、不正進入等を防止する仕組みを講じる。
(3)情報資産の設置場所に関する対策
不正な立入による損傷および妨害等から情報資産を防護するため、警備および施錠等の必要な対策を実施する。
(4)システム利用面に関する対策

利用者が次の事項を守り、正しくシステムを利用しているかを管理する。また、情報セキュリティの重要性を認識し、適切な利用が守られるよう教育周知する。

ａ他の者の権利を侵害しない。

ｂ法令に違反する行為およびその恐れのある行為を行わない。

ｃ公序良俗に反する行為および業務目的以外の利用行為を行わない。

ｄデータの改竄および当社業務に支障を与える恐れのある工作などを行わない。

ｅ不正アクセスおよびそれを助長する行為を行わない。

ｆ利用者ＩＤおよびパスワードが他人に不正使用されないよう厳重に管理する。

⑸情報保管・管理に関する対策

情報を厳重に保管および管理するとともに、第三者に不正使用されないよう適性な防護策を講じる。

⑹通信ネットワークを通じたアクセスに関する対策

通信ネットワークを通じたアクセスについて、許可されていない者がその情報資産にアクセスすることを制限するための用件を明確にし、それを確実にシステムに組み入れる。

⑺外部委託に関する対策

情報資産の開発、運用および保守を外部委託する場合、情報資産に対するリスクを考慮した上で、再委託を含むすべての委託先の安全性を確認する。また、委託先とは情報セキュリティに関する事項を契約事項として定め、その状況を定期的に確認すること。

⑻コンピュータ・ウィルス等に関する対策

情報セキュリティに関する情報収集を継続的に行い、コンピュータ・ウィルスやセキュリティ・ホール等への対策を実施する。

第７条（緊急時対応）

情報セキュリティ統括責任者は、重要な情報資産について、予めセキュリティ事故の発生を想定した緊急時対応計画を定め、緊急時にはこれに従い、迅速に体制を確立し、早期復旧と再発防止に努める。

重要インフラサービス障害・システム不具合等（法令等報告対象の事象等）は北陸総合通信局へ、障害・攻撃情報等（予兆・ヒヤリハット等（法令等報告対象外の事象））は放送セプター事務局へ報告を行う。

第８条（評価・見直し）

情報セキュリティ統括責任者は、定期的に情報セキュリティの状況を評価し、必要に応じて、さらなる対策および改善を実施する。

平成１８年６月１日制定

令和５年４月１日改正