

飛騨・世界生活文化センター情報システム維持管理業務実施要領

1 目的

飛騨・世界生活文化センター（以下「センター」という。）に設置又は導入されている情報通信設備、ネットワーク設備、情報セキュリティ設備及び外部のサーバー・サービス等について、適切な保守、運用及び管理を行い、施設運営、催事、施設利用者へのサービス提供等に必要な情報通信環境を安全かつ安定して利用できる状態に維持することを目的とする。

また、情報通信技術及びセキュリティ環境の変化に対応するとともに、障害発生時の早期復旧、情報セキュリティの確保及び災害時等における通信手段の確保に努めるものとする。

2 総則

- (1) 維持管理を行う者は、維持管理の対象となる情報通信設備、ネットワーク、情報セキュリティ、ソフトウェア及び外部サービス等の保守、運用及び管理について、必要な知識及び技能を有する者とする。
- (2) 維持管理を行う者は、本業務により知り得た情報、ネットワーク構成、IP アドレス、認証情報、設定情報その他セキュリティ上重要な情報について適切に管理し、正当な理由なく第三者に開示又は漏えいしてはならない。
- (3) 情報システムの管理責任者を定め、その管理のもとに情報通信設備及びシステムの運用、保守及び管理を行うこと。
- (4) 情報通信設備及びシステムの構成、設定等を変更する場合は、施設運営及び他の設備への影響を十分確認したうえで実施すること。
- (5) 情報通信設備及びシステムに障害又はセキュリティ上の異常が確認された場合は、速やかに状況を確認し、原因の切り分け、応急措置、復旧その他必要な対応を行うこと。
- (6) 情報通信設備の更新、ソフトウェアの更新、サービスの変更その他情報システムに変更を加えた場合は、ネットワーク構成図、機器台帳、設定資料その他関連する技術資料を更新すること。
- (7) 情報通信設備及びシステムの運用にあたっては、必要なセキュリティ対策を講じるとともに、利用目的及び重要度に応じた適切な管理を行うこと。

3 維持管理対象設備等

維持管理の対象は、別表－1 に示す設備、ソフトウェア及び外部サービス等とする。

ただし、別表－1 に記載されていない設備等であっても、センターの情報通信環境の維持に必要な設備、配線、ソフトウェア、契約又はサービス等については、必要に応じて維持管理の対象とする。

- (1) インターネット回線及び回線終端設備 一式
- (2) ルーター、UTM その他ネットワーク境界設備 一式
- (3) スイッチ、メディアコンバーターその他ネットワーク設備 一式
- (4) LAN ケーブル、光ケーブル、情報コンセント、パッチパネルその他通信配線設備 一式
- (5) 無線 LAN 設備 一式
- (6) 無停電電源装置（UPS） 一式
- (7) 管理用端末及び関連ソフトウェア 一式
- (8) ウイルス・マルウェア対策その他情報セキュリティ関連ソフトウェア 一式

- (9) レンタルサーバー、クラウドサービスその他外部サービス 一式
- (10) ドメイン、DNS 及び SSL/TLS 証明書等 一式
- (11) その他情報通信システムの維持管理に必要な設備、ソフトウェア及びサービス 一式

4 維持管理内容

維持管理の内容は、おおむね次のとおりとする。

(1) 管理運用

情報通信設備及びシステムを利用した施設運営、業務及び催事等が安定して実施できるよう、設備、ソフトウェア、ネットワーク及び外部サービス等の管理運用を行う。

① 資源・構成管理

情報通信設備、ソフトウェア及び外部サービス等について、機器構成、設置場所、接続状況、稼働状況、設定状況、バージョン、契約状況、ライセンス、使用期間等を把握し、適切に管理すること。

ネットワーク構成図、IP アドレス、VLAN、SSID、機器設定、通信経路その他維持管理に必要な情報を整理し、変更があった場合は関連資料を更新すること。

② 障害管理

通信障害、機器故障、システム障害その他異常が発生した場合は、ONU 等の回線終端装置、ルーター・UTM、スイッチ、メディアコンバーター、LAN・光配線、無線 LAN アクセスポイント、端末及び外部サービス等について原因の切り分けを行い、早期復旧に努めること。

障害対応にあたっては、必要に応じて通信事業者、機器メーカー、保守事業者、レンタルサーバー事業者その他関係事業者と連携すること。

また、障害の発生日時、対象設備、現象、原因、切り分け内容、応急措置、復旧内容及び再発防止措置等について記録すること。

③ 設備管理

情報通信設備について、温度、湿度、電源、設置状態、配線状態その他機器の安定稼働に必要な環境を確保すること。

機器、配線及び接続部等について異常が確認された場合は、必要な補修、交換又は改善を行うこと。

④ セキュリティ管理

不正アクセス、マルウェア感染、情報漏えいその他情報セキュリティ上の事故を未然に防止するため、UTM、ファイアウォール機能、ウイルス・マルウェア対策ソフトその他必要なセキュリティ機能について適切な設定及び管理を行うこと。

セキュリティ機能、ソフトウェア、ファームウェア等については、提供元から公開される更新情報、脆弱性情報等を必要に応じて確認し、施設運営への影響を考慮したうえで適切な対応を行うこと。

⑤ 性能管理

施設運営及び利用状況に応じ、通信速度、通信量、接続台数、ネットワーク機器の負荷、無線 LAN の利用状況その他必要な項目を確認し、情報通信システムに必要な性能水準を確保すること。

通信量又は接続台数の増加等により性能低下が見込まれる場合は、設定変更、機器増設、構成変更その他必要な改善について検討すること。

⑥ バックアップ・復旧管理

ルーター、UTM、スイッチ、無線 LAN アクセスポイントその他設定情報を有する機器について、障害又は機器交換時の復旧に必要な設定情報を適切に保存すること。

レンタルサーバーその他重要なデータを保存するサービスについては、バックアップ機能及び復旧方法を確認し、障害発生時に必要な復旧が行える状態を確保すること。

(2) 保守

情報通信設備、ソフトウェア又は外部サービス等に障害、不具合又はセキュリティ上の問題が発生した場合は、原因を調査し、必要な復旧、補修、設定変更その他の対応を行う。

また、設備更新、利用環境の変化、情報通信技術の変化等に応じ、必要な設定変更又は機能改善を行う。

① 修理・復旧作業

情報通信設備に障害が発生した場合は、原因を調査し、必要に応じて部品交換、機器交換、配線補修、設定復旧その他必要な措置を行うこと。

② 更新作業

OS、ソフトウェア、ウイルス対策ソフト、ファームウェアその他情報通信システムの運用に必要なソフトウェアについて、必要に応じて更新を行うこと。更新にあたっては、既存設備及びシステムとの互換性並びに施設運営への影響を確認すること。

③ 変更作業

施設利用状況、催事内容、機器更新、回線変更その他運用環境の変化に対応し、ネットワーク、セキュリティ、無線 LAN 等について必要な設定変更を行うこと。

(3) その他

維持管理に必要な技術資料、取扱説明書、設定資料等を収集し、整理・保管すること。

維持管理に必要な管理記録、点検記録、障害記録、設定変更記録、修繕記録等を作成し、適切に保管すること。

必要に応じて機器操作手順、障害対応手順その他運用に必要な資料を作成すること。

5 各システムの管理運用・保守特記事項

情報通信システムを維持管理するため、特に次の事項を実施するものとする。

(1) インターネット回線・ONU 等

- ① インターネット接続及び ONU 等の回線終端設備の稼働状態を確認すること。
- ② 通信障害が発生した場合は、施設内設備と通信事業者側設備との切り分けを行うこと。
- ③ 通信事業者側に障害があると判断される場合は、必要に応じて通信事業者への障害対応依頼を行うこと。

(2) ルーター・UTM

- ① ルーター及び UTM 等の稼働状態を確認し、インターネット及び施設内ネットワークが正常に通信できる状態を維持すること。
- ② ファイアウォール、アクセス制御、VPN、DHCP、DNS 転送その他必要な機能について適切に設定及び管理すること。

- ④ 通信状況、接続数、エラー、警告その他必要な情報を確認し、異常の早期発見に努めること。
- ⑤ 設定変更を行った場合は、その内容を記録するとともに、復旧に必要な設定情報を保存すること。
- ⑥ ファームウェア及びセキュリティ情報を必要に応じて確認し、必要な対応を行うこと。

(3) ネットワーク機器及び通信配線

- ① スイッチ、PoE スイッチ、メディアコンバーター等の稼働状態及び通信状態を確認すること。
- ② LAN ケーブル、光ケーブル、情報コンセント、パッチパネルその他通信配線について、障害発生時には通信経路及び故障箇所の切り分けを行うこと。
- ③ PoE 給電を利用する設備については、通信状態と併せて給電状態を確認すること。

(4) 無線 LAN 設備

- ① 無線 LAN アクセスポイント等の稼働状態、接続状態及び通信状態を確認すること。
- ② 利用状況に応じ、SSID、認証方式、周波数帯、チャンネル、送信出力、接続制限その他必要な設定を適切に管理すること。
- ③ 施設運營業務用、施設利用者用、催事用その他用途の異なるネットワークについては、必要に応じて適切な分離及びアクセス制御を行うこと。
- ④ 多数の端末接続が想定される催事等については、必要に応じて事前に通信環境を確認し、アクセスポイントの増設、配置変更、SSID の設定その他必要な措置を行うこと。
- ⑤ 無線 LAN 設備の設定情報について、障害又は機器交換時の復旧に必要な情報を適切に保存すること。

(5) ウイルス・マルウェア対策

- ① 管理対象端末について、ウイルス・マルウェア対策ソフトが正常に稼働していることを確認すること。
- ② ウイルス定義ファイル、検出エンジンその他必要な情報について、適切に更新される状態を維持すること。
- ③ マルウェア等が検出された場合は、対象端末の隔離、駆除、影響範囲の確認その他必要な措置を行うこと。

(6) UPS

- ① UPS の運転状態、警報及びバッテリー状態等を確認すること。
- ② バッテリーの使用期間及び劣化状態を把握し、必要に応じて計画的な交換を行うこと。
- ③ 停電時に必要な情報通信設備が適切に保護される構成を維持すること。
- ④ UPS の交換又は構成変更を行った場合は、接続設備及び必要容量を確認すること。

(7) レンタルサーバー・外部サービス

- ① Web サイトその他施設が利用するレンタルサーバー及び外部サービスについて、契約及び稼働状況を適切に管理すること。
- ② サーバー容量、データ使用量、バックアップ状況その他サービスの安定運用に必要な項目を確認すること。

- ③ CMS その他 Web サイト運用に使用するソフトウェアについて、必要なセキュリティ対策及び更新を行うこと。
- ④ サービス障害が発生した場合は、施設側の通信環境との切り分けを行い、必要に応じてサービス提供事業者への確認及び復旧依頼を行うこと。

(8) ドメイン・DNS・SSL/TLS 証明書

- ① 施設が使用するドメインについて、登録状況、契約期間及び更新期限を適切に管理し、契約失効等によるサービス停止を防止すること。
- ② DNS について、Web サイトその他利用サービスに必要な設定内容を把握し、変更時には影響範囲を確認したうえで適切に設定すること。
- ③ Web サイトその他暗号化通信を必要とするサービスについて、SSL/TLS 証明書の有効期間及び設定状況を確認し、証明書の期限切れ等によるサービス停止又はセキュリティ低下を防止すること。
- ④ ドメイン、DNS 又は SSL/TLS 証明書の設定を変更した場合は、その内容を記録すること。

(9) 催事等における通信環境

- ① インターネット又は無線 LAN 等を使用する催事については、必要に応じて事前に通信環境及び設備の動作確認を行うこと。
- ② 多数接続、大容量通信、オンライン配信、Web 会議その他通常時と異なる通信利用が想定される場合は、利用内容を確認し、必要に応じてネットワーク構成、アクセスポイント配置、SSID、通信経路等を調整すること。
- ③ 催事中に通信障害が発生した場合は、施設側ネットワーク、利用端末、外部サービス等について原因を切り分け、可能な範囲で通信環境の復旧に努めること。

(10) 災害時等における通信環境

- ① センターが避難所又は広域防災拠点等として使用される場合に備え、必要な情報通信設備の構成及び稼働方法を把握しておくこと。
- ② 災害、停電、通信障害等が発生した場合は、情報通信設備の被害状況及び通信可否を確認すること。
- ③ 通常の通信手段が利用できない場合は、利用可能な設備及び通信手段を確認し、必要に応じて代替手段による通信環境の確保に努めること。

6 細則

- ア 催事等で情報通信設備を使用する場合は、必要に応じて事前に動作及び通信確認を行うこと。
- イ 保守点検等を第三者に委託した場合は、その実施状況及び実施内容を確認し、必要な指示を行うこと。また、完了時には履行内容を確認すること。
- ウ 保守、修繕、設定変更等を行った場合は、必要に応じて報告書、作業記録、設定変更記録、記録写真等を作成し、整理・保管すること。
- エ 修繕又は設備更新を行おうとする場合は、必要に応じて仕様、数量、市場価格、メーカー見積等を確認し、適正な費用の把握に努めること。

- オ 修繕又は設備更新を第三者に実施させた場合は、その実施状況及び実施内容を確認し、必要な指示を行うこと。また、完了時には履行内容を確認すること。
- カ 障害、修繕、設定変更等に関する記録には、日時、対象設備、障害又は作業内容、対応者、原因、対応内容その他維持管理に必要な事項を記載すること。
- キ 予備品及び消耗品については、設備の重要度、故障時の影響、製品寿命及び調達期間等を考慮し、必要に応じて確保すること。
- ク 設備、配線又は設定等に変更を加えた場合は、ネットワーク構成図、機器台帳、IP アドレス管理資料、設定資料その他関連する技術資料を更新すること。
- ケ ルーター、UTM、スイッチ、無線 LAN アクセスポイントその他重要なネットワーク機器の設定情報については、障害又は機器交換時に復旧できるよう適切に保存すること。
- コ 機器、ソフトウェア、ライセンス、ドメイン、SSL/TLS 証明書及び外部サービス等について、更新時期又は契約期限を把握し、計画的な更新を行うこと。
- サ 情報通信設備について、設備の重要度、使用状況、耐用年数、メーカーサポート期間等を考慮した更新計画を作成すること。
- シ 情報セキュリティ上重大な異常又は情報漏えい等が発生し、若しくはそのおそれがある場合は、速やかに管理責任者へ報告し、必要な措置を講じること。

別表－1 情報システム設備等

区分	設備・サービス	主な対象	数量	備考
通信回線	インターネット回線	光回線等	一式	契約情報を含む
回線終端設備	ONU 等	回線終端装置	一式	通信事業者設備を含む
ネットワーク境界設備	ルーター・UTM	ルーティング、FW、VPN、DHCP 等	一式	設定情報を含む
ネットワーク設備	L2/L3 スイッチ	基幹・各所スイッチ	一式	PoE 機器を含む
ネットワーク設備	メディアコンバーター	光・LAN 変換設備	一式	
通信配線設備	LAN ケーブル	幹線・支線・パッチコード等	一式	
通信配線設備	光ケーブル	建物内光幹線等	一式	
通信配線設備	情報コンセント・パッチパネル等	各所通信端末部	一式	
無線 LAN 設備	アクセスポイント	施設内 Wi-Fi 設備	一式	設定情報を含む
無線 LAN 設備	コントローラー等	AP 管理機能	一式	仮想コントローラー等を含む
電源設備	UPS	ネットワーク機器用等	一式	バッテリーを含む
管理端末	管理用 PC 等	ネットワーク管理端末	一式	
セキュリティ	ウイルス・マルウェア対策	管理対象端末	一式	ライセンスを含む
外部サービス	レンタルサーバー	Web サイト等	一式	契約・バックアップを含む
Web 関連	CMS 等	Web サイト管理システム	一式	プラグイン等を含む
ドメイン	独自ドメイン等	Web・メール等	一式	契約・更新管理を含む
DNS	DNS サービス	名前解決設定	一式	設定情報を含む
SSL/TLS	SSL/TLS 証明書	Web サイト等	一式	有効期限管理を含む
その他	その他関連設備等	情報通信環境の維持に必要なもの	一式	必要に応じ対象とする