札幌市議会本会議及び特別委員会等映像配信業務仕様書

1　総則

⑴　委託業務名

札幌市議会本会議及び特別委員会等映像配信業務

⑵　目的

札幌市議会の本会議、予算・決算・議案審査特別委員会、調査特別委員会、公聴会及び聴聞会等（以下「会議」という。）の審議状況を、インターネット上で生中継（以下「ライブ配信」という。）及び録画映像の公開（以下「VOD配信」という。）をし、広く議会情報を配信することを目的とする。

なお、この仕様書に定めのない事項については、委託者、受託者間で別途協議を行い決定する。

⑶　履行場所

ア　札幌市役所本庁舎18階　調音室（以下「調音室」という。）

イ　札幌市役所本庁舎16階　第一特別委員会会議室

ウ　札幌市役所本庁舎18階　第二特別委員会会議室（以下、上記イと合わせ「第一・第二特別委員会会議室」という。）

⑷　業務内容

ア　会議の審議状況のインターネットによるライブ配信及びVOD配信の実施並びに運用管理。

イ　配信に必要となる機器の設置、管理及び保守。

ウ　ライブ配信及びVOD配信用のホームページの作成及び運用管理業務。

エ　VOD配信のための編集作業。

オ　そのほか上記業務に付随する業務。詳細は、別紙「札幌市議会本会議及び特別委員会等映像配信業務実施要領」のとおり。

⑸　特記事項

ア　映像配信及び運用管理の詳細な実施内容については、別途協議するものとする。

イ　映像配信の円滑な運用のために委託者を支援するとともに、調査依頼、資料請求等に対して、迅速に対応すること。

ウ　委託業務の履行に伴い機器構成図、システム構成図、運用マニュアル等を作成すること。

エ　映像等に係る著作権及び委託業務の履行に伴い発生する成果物は委託者に帰属するものとする。

オ　映像配信の運用に当たって必要な機器・機材・回線及びソフトウェア等の映像配信機器は委託者に帰属しないものとする。

カ　本業務の実施に当たり、契約締結後速やかに業務スケジュール（役務履行計画書）を提出すること。

2　一般仕様

⑴　法令、規定、基準の遵守

業務の実施に伴い、適用を受ける法令、規定、基準、指針等については、これを遵守し、遺漏のないようにすること。

⑵　一般管理

受託者は、業務の実施に当たってデータの漏えい、データの滅失、事故等の予防に十分留意し、業務の信頼性、安全性の確保に努めなければならない。

⑶　業務責任者

受託者は受託業務の業務責任者及び代行する者を置くこと。

業務責任者は、業務実施中に業務従事者を指揮し、委託者の担当者と連絡を密にし、遺漏のないように努めること。また、業務責任者及び業務従事者は、業務を遂行するために要求される十分な知識及び技能を備えていること。

3　履行期間

契約締結日から令和12年6月30日まで

4　映像配信実施時期

⑴　ライブ配信

令和8年7月1日から令和12年6月30日までに開催される会議

⑵　VOD配信

令和8年7月1日から令和12年6月30日まで

5　注意事項

⑴　入札参加者は、本仕様書を熟読の上、入札に参加すること。また、落札者は、本仕様書の全ての事項に対し、責任を持って完全に契約を履行すること。

⑵　本業務に係る一切の経費は、委託料に含むこと。

⑶　受託者は業務上知り得た秘密を第三者に開示又は漏えいしてはならない。

⑷　受託者は、本業務の全部又は一部を第三者に委託（以下「再委託」という。）してはならない。ただし、主要でない業務の一部であって、業務の性質上特に委託者がやむを得ないと認めた場合に限り、あらかじめ書面により委託者に申請し、その承諾を得て再委託することができる。この場合、受託者は、再委託先に対しても本契約及び仕様書と同等の義務を負わせ、適切に管理・監督しなければならない。また、受託者は、再委託先が本業務の履行に関して行った全ての行為及びその結果について、委託者に対し一切の責任を負うものとする。

札幌市議会本会議及び特別委員会等映像配信業務　実施要領

1　運用形態

⑴　本業務は、受託者が委託者の指示を受け、会議の審議状況を、インターネット経由でライブ配信及びVOD配信を行うとともに、その運用管理並びに映像配信に係る機器の管理及び保守を行うものである。

⑵　映像配信の運用に当たって必要な機器・機材・回線及びソフトウェア等（以下「映像配信機器」という。）については、受託者が調達及び設置し、受託者が運用管理を行うこと。なお、この業務はASPサービスとして業務委託する。

⑶　会議中のカメラ及びテロップの操作は委託者が行う。

⑷　受託者は、ライブ配信の視聴やVODコンテンツの検索及び視聴が簡単にできる議会映像配信専用サイト（以下「配信サイト」という。）を提供すること。

⑸　本業務で提供される映像及び配信サイトは、一般に広く使用されているWindows、MacOS、iOS、Android等の端末上の主要なブラウザで利用及び視聴できること。ただし、すべてのバージョン等での動作の保証を求めるものではない。

⑹　映像はストリーミング配信とすること。

⑺　受託者は、一般視聴者がライブ配信、VOD配信を視聴した件数を集計し、その結果について委託者が専用のサイトからいつでも閲覧できるようにすること。

⑻　受託者は、障害などが発生した際には速やかに復旧し、以降の運用に支障が出ないように対策を施すこと。

2　運用に関する要件

⑴　業務を実施するに当たり、受託者は業務に精通した業務責任者及び代行を選任し、その旨を委託者に届け出なければならない。また、業務責任者及び代行に変更が生じた際も同様とする。

⑵　受託者は議会の運営及び映像配信業務に精通している複数の要員で組織されたサポート窓口を設けていること。このサポート窓口は常設されており、定例会時期以外でも受け付け可能であること。また、この中から担当者を選任した際はその旨を委託者に届け出るものとし、変更が生じた際も同様とする。

⑶　受託者は、配信の停止や機器の故障等の緊急事態に備え、委託者からの要請後２時間以内に現場に到着し、復旧作業を開始できる業務従事者を選任し、委託者に届け出ること。また、業務従事者に変更が生じた際も同様とする。

⑷　サービスの利用環境の最適化を図るため、常にサービス監視・安定したサービス運用・使用状況の確認等で確実なサービスを提供すること。

⑸　各定例会及び臨時会前には、受託者による映像配信に関する一連の動作確認を行い、確認結果報告書により委託者に報告すること。日程及び確認方法については事前に委託者の承諾を得ること。なお、動作確認には、本市イントラネットへの映像及び音声出力に関する確認を含むものとする。

⑹　受託者は委託者側に設置するエンコードシステムの状態確認、変更などを配信センターから操作が可能であること。

⑺　会議が開催される当日の開会前に、ライブ配信の稼働状況及び委託者側エンコードシステムとの通信確認を行うこと。

⑻　設備メンテナンスなどでサービスの停止を行う場合にはあらかじめ委託者に連絡

の上行うこと。

⑼　視聴者から映像配信について問い合わせ等があった場合、受託者は委託者の回答等の支援を行うこと。

⑽　会議終了後の翌日から起算して15営業日以内に、会議の開始から終了までの全体映像のファイルのほか、公開されているシーン単位にカット編集されている映像ファイルを、会議毎にmp4形式でDVD等に格納して、各1部を提出すること。

3　ライブ配信に関する要件

映像配信機器の設置場所によって要件が異なる。各設置場所の要件は以下のとおり。

⑴　調音室（対象会議：本会議、公聴会及び聴聞会）

ア　委託者が設置した本会議映像配信機器からの映像及び音声をソースとして、インターネットへ以下のライブ配信を行うための環境を整えること。

(ｱ)　通常ライブ配信

委託者提供の映像・音声を特段の加工なく配信する形態

(ｲ)　字幕付ライブ配信

委託者提供の映像・音声を元に、映像中に字幕を構成する機器（ライブ字幕生成機器）をもって構成した映像と音声を配信する形態

イ　ライブ字幕生成機器は、オンプレミス型の機器を導入すること。

⑵　第一・第二特別委員会会議室（対象会議：予算・決算・議案審査特別委員会及び調査特別委員会）

ア　受託者が設置するカメラからの映像及び既設音響機器からの音声をソースとして、インターネットへライブ配信するための環境を整えること。

イ　当該両会議室では同日同時刻から委員会が同時開催される可能性があるため、双方の審議状況を同時に配信できること。なお、散会時刻はそれぞれ異なるので、適宜対応すること。

ウ　映像に表示されるテロップは、会議名、委員名・会派名・市長名等を事前に登録でき、カメラ操作時のワンアクション操作に連動して表示できること。詳細は、別紙１「テロップ例」のとおり。

エ　会議の開会前、休憩中及び閉会後は、静止画とテロップのみを表示した映像を配信し、音声は無音にすること。

オ　庁内イントラネットへのライブ配信も行うため、第一・第二特別委員会会議室の各室の映像音声を既設庁内配信設備へ提供すること。また16階と18階の各室から14階の庁内配信設備までのケーブル敷設も実施すること。

カ　ライブ配信時の障害回避のため、受託者が設置するHDDレコーダーを用いて、エンコード前の映像及び音声のバックアップ作業を行うこと。

⑶　共通事項

ア　開催予定日については、会期日程が決定次第、速やかに委託者から受託者に通知する。

イ　会議の開会から閉会までの模様を全て配信すること。

ウ　契約期間中の配信見込日数、総見込時間等は別紙２のとおり。なお、あくまでも見込数値であり、増減する可能性があることに留意すること。

エ　ライブ配信のビットレートは500Kbps程度以上とすること。

オ　ライブ配信時には、配信サイトのトップページに会議名及び配信が開始されている旨を表示すること。

カ　ライブ配信と同時にエンコードシステムに配信映像が保存され、同時に配信センター側にも同じ配信映像が保存されること。

キ　委託者は必要に応じて、受託者側のライブ配信サービスをいつでも使用できること。

4　字幕なしVOD配信に関する要件

⑴　ライブ配信により保存された映像を利用し、委託者が指定するコンテンツ構成に基づき映像の編集作業を行い、当該会議終了後の翌日から起算して５営業日までにVOD配信が可能な状態とすること。

⑵　映像の編集作業は、３．⑶．カによって保存された映像を利用すること。

⑶　当該VOD配信のビットレートは係るライブ配信と同程度とすること。

⑷　開会前、休憩中及び閉会後の映像はカット編集すること。

⑸　発言訂正、テロップの誤表示及びテロップ追加の必要が生じた場合は、委託者の指示に基づき当該部分の変更等を随時行うこと。

⑹　当該VOD配信の公開前にサイトと映像を確認するため、配信サイトと同じ機能の事前公開サイトを用意し、委託者による公開前確認を受け、承諾を得た後に公開すること。なお、事前公開サイトはIDとパスワードにより保護し、委託者のPC等にて公開前確認ができるようにすること。

⑺　当該VOD配信は当該会議終了後から２年間公開されること。公開期間が終了した映像ファイルは公開終了後１年間保存し、保存期間が終了した映像ファイルは速やかに消去すること。

⑻　令和８年７月１日からVOD配信を実施する過去２年分の映像については、委託者が、シーン単位にカット編集されている映像ファイルをmp4形式にて提供する。また、配信に必要な資料等も併せて提供する。

⑼　設備メンテナンス等でサービスを停止する場合を除き24時間配信すること。

5　字幕ありVOD配信に関する要件

⑴　ライブ配信により保存された映像を利用し、開会前及び閉会後をカット編集し、当該会議終了後の翌日から起算して５営業日までにVOD配信が可能な状態とすること。

⑵　映像の編集作業は、３．⑶．カによって保存された映像を利用すること。

⑶　当該VOD配信のビットレートは係るライブ配信と同程度とすること。

⑷　発言訂正、テロップの字幕内容等に起因する映像修正は指示しないが、一般公開については委託者の指示により実施すること。

⑸　当該VOD配信の公開前にサイトと映像を確認するため、配信サイトと同じ機能の事前公開サイトを用意し、委託者による公開前確認を受け、承諾を得た後に公開すること。なお、事前公開サイトはIDとパスワードにより保護し、委託者のPC等にて公開前確認ができるようにすること。

⑹　当該VOD配信は当該会議終了後から委託者から公開終了の指示があるまでの間、公開されること。公開期間が終了した映像ファイルは公開終了後１年間保存し、保存期間が終了した映像ファイルは速やかに消去すること。

⑺　設備メンテナンス等でサービスを停止する場合を除き24時間配信すること。

6　映像配信機器に関する要件

⑴　本業務に要する映像配信機器は全て受託者が用意するものとし、機器構成及びインターネット通信環境は、画像・音声の品質を確保するための十分な機能を備えていること。

⑵　本業務で使用する映像配信機器は十分な稼働実績を有しているなど高い信頼性を有する製品を使用し、それらを構成した状態でシステムとして不具合なく作動するとともに、障害が発生した場合は迅速に対応できるものであること。

⑶　使用する映像配信機器は開発メーカーの製品サポート期間内であること。

⑷　ソフトウェアは事前に委託者に画面展開及び操作方法等を提示し、承諾を得ること。

⑸　OSのサポート期間終了、技術革新の進展及び配信環境の変化等に応じて、適宜、OS及びソフトウェアのアップデートを無償で行うこと。

⑹　本業務に使用する映像配信機器のうち下記のものについては、次に掲げる各仕様を満たすものであること。

ア　調音室（対象会議：本会議、公聴会及び聴聞会）

(ｱ)　エンコードシステム（調音室内）

a　調音室内に２式設置すること。内１式は通常ライブ配信用とし、もう１式は字幕付ライブ配信用とすること。

b　マウス、キーボード、モニター等、必要な機器が付属していること。

c　配信用エンコードシステムにPCを利用する場合、搭載OSは「Microsoft Windows 11pro」とすること。

(ｲ)　無停電電源装置（調音室内）

a　調音室内に１台設置すること。

b　設置する映像配信機器全体を補う無停電電源装置を設置すること。

c　無停電電源装置単体で遠隔からの配信機器類の電源状況把握が可能であること。

(ｳ)　ライブ字幕生成機器（調音室内）

a　調音室に1式設置すること。

b　オンプレミス型であって、かつ、インターネット接続を必要としないシステムであること。

c　人名や地名などの用語の辞書登録機能を有すること。また、禁止用語の登録も可能であること。

d　ふりがな付与機能を有すること。

イ　第一・第二特別委員会会議室（対象会議：予算・決算・議案審査特別委員会及び調査特別委員会）

(ｱ)　エンコードシステム（第一・第二特別委員会会議室内）

a　第一特別委員会会議室に１式、第二特別委員会会議室に１式の合計２式を設置すること。

b　マウス、キーボード、モニター等、必要な機器が付属していること。

c　カメラテロップ挿入機器にPCを利用する場合、搭載OSは「Microsoft Windows 11」又は「Microsoft Windows 11 IoT」とすること。

(ｲ)　カメラ制御PC（第一・第二特別委員会会議室内）

a　第一特別委員会会議室に１台、第二特別委員会会議室に１台の合計２台を設

置すること。
b　デスクトップ型のPCであること。
c　マウス、キーボード、モニター等、必要な機器が付属していること。
d　モニターのサイズは23インチ程度の大きさとすること。
e　搭載OSは「Microsoft Windows 11」又は「Microsoft Windows 11 IoT」とすること。
f　既設音響機器との接続は音声入力のみとし、機器の共有、操作の連動は行わないこと。
g　カメラ位置は、事前にプリセットの保存が可能なこと。
h　テロップは、別紙１「テロップ例」の表示等を事前に登録可能なこと。
i　操作画面には、委員長席、委員席及び説明員席等、事前に設定した会議室のレイアウトが表示されていることに加え、３台のカメラ映像と送出しているカメラ映像（テロップ付き）が同時に表示可能なこと。
j　操作画面上に事前に設定したボタンをクリックすることで、カメラの切り替え、カメラプリセットの呼び出し及びテロップ表示が同時に可能なこと。また、8つのカメラプリセットを登録及び呼び出しが可能なこと。
k　操作画面上の３台の各カメラ映像をボタンで、カメラの切り替え及びカメラのパン・チルト・ズーム操作が可能なこと。
l　カメラの切り替えの際は、映像がスムーズに切り替わること。
m　配信中であっても、キーボード操作により任意の文章を表示することが可能なこと。
n　テロップは「議案」「氏名」「メッセージ」の３種類を登録可能であること。また、「メッセージ」については、テロップとして表示させる文章が長い場合には、横書きでスクロール表示ができること。
o　議案、氏名、メッセージのデータはインポート、エクスポートができること。
p　カメラ操作のログ情報を収集し、発言順序が分かるタイムシートをテキスト（CSV）形式にて自動生成すること。タイムシートには日付、時間、発言者（開会、閉会及び休憩を含む。）の情報を出力すること。
q　開会操作と同時に、６．⑹．イ.(ｳ)の録画機器が自動で録画を開始し、会議終了操作時には自動で停止することが可能なこと。
r　６．⑹．イ.(ｳ)の録画機器の残量が少なくなった場合は、アラートを表示すること。
s　操作画面はカラーユニバーサルデザイン認証を取得していること。

(ｳ)　HDDレコーダー（第一・第二特別委員会会議室内）

【参考機器：DMR-T5000UR】

a　第一特別委員会会議室に１台、第二特別委員会会議室に１台の合計２台を設置すること。
b　１TB以上のHDDが内蔵されていること。
c　録画メディアはDVD-R、DVD-RW、BD-R、BD-REが対応できること。
d　レコーダーの操作状況を把握するため、モニターを設置すること。モニターのサイズは７～10インチ程度とする。なお、モニターは、エンコード用のPCのモニターと兼用できる場合は付属しないことができる。

㈡　カメラ（第一・第二特別委員会会議室内）

【参考機器：AW-UE80W】

a　第一特別委員会会議室に３台、第二特別委員会会議室に３台の合計６台を設置すること。

b　天井に取り付けること（落ちないように補強すること）。

c　解像度はフルHD以上であること。

d　水平解像度は、カラー1000TV本以上であること。

e　ズームは、光学24倍以上（超解像ズーム等によりHD時30倍以上となること）であること。

f　最低被写体照度は、３ルクス以下であること。

g　回転範囲は、水平350度（-175～+175度）、垂直120度（-30～+90度）以上であること。

h　最大回転速度は、水平180度／秒、垂直180度／秒以上であること。

i　フォーカスは、フルタイムオートフォーカスであること。

j　映像出力は、HD/SD-SDI方式であること。また、RS422ケーブルや100BASE-TXによりカメラ制御が可能なこと。

k　重量は、2.0キログラム程度であること。

l　プリセット数は、対象となる席の数だけ可能なこと（ソフトウェアでの対応可）。

㈢　無停電電源装置（第一・第二特別委員会会議室内）

a　第一特別委員会会議室に１台、第二特別委員会会議室に１台の合計２台を設置すること。

b　配信システム全体を補う無停電電源装置を設置すること。

c　無停電電源装置単体で遠隔からの配信機器類の電源状況把握が可能であること。

⑺　受託者の配信センターと委託者側設置機器等を接続するルーターは受託者が設置すること。

⑻　設置する機器類の電源は一括管理できること。

⑼　設置する機器類を収納するデスク型ラック等を用意すること。なお、デスク型ラック等の規格及び設置場所については、委託者と協議の上決定すること。

⑽　その他、本業務を実施するために必要な機器等を設置すること。

⑾　受託者は適宜、機器等の保守・点検を行うこと。

7　配信サイトに関する要件

⑴　受託者は、配信サイトのデザイン、画像、色合いに関して、委託者の意向を反映して作成すること。

⑵　札幌市議会ホームページに掲載するためのリンクバナー（460×60ピクセル）を１種類作成すること。また、配信サイト上に札幌市議会ホームページへの再リンクを掲載すること。

⑶　PC、スマートフォン等のデバイスを自動的に検出し、最適なユーザーインターフェイスを視聴者に意識させずに表示させること。

⑷　映像は、HTML5フォーマットで配信すること。

⑸　映像の解像度は640×360以上であること。又プレイヤーサイズも同様以上である

こと。

⑹　配信のボタンは字幕なしの通常配信用と字幕入り映像の配信用ボタンを準備し視聴者を誘導すること。

⑺　VOD配信の再生画面では、シークバーを操作することで任意の位置から視聴できることとし、タイム表示（現在／全体）を付けること。また、0.5・1・1.25・1.5・2倍速の再生スピードコントロール機能を有すること。

⑻　映像については、利用者が安易に保存できないようにすること。

⑼　映像を再生するページには、映像とともに質問者名、議題、質問項目等が表示されること。

⑽　視聴者がVODコンテンツを検索する場合には、会議名称、案件名、会派名、議員名で検索でき、文字列による検索機能を持つこと。また、検索結果の表示は、該当箇所が確認できるように色付け等の強調表示ができること。

⑾　検索結果の一覧画面には当該議員の顔写真の表示が可能なこと。

⑿　議員名検索結果等の画面に対して議員のホームページやブログなどの外部サイトからのリンクを許し、閲覧ができること。

⒀　ユニバーサルデザインを十分考慮し、ウェブアクセシビリティが確保された画面デザインであること。また、可能な限り日本工業規格JIS X 8341-3:2016の適合レベルAA（国際規格ではWCAG 2.0と一致）に準拠するものとなるよう努めること。

⒁　音声読み上げソフトや音声ブラウザの利便性を考慮し、ページの構成にフレーム機能及びプルダウン機能は使用しないこと。

⒂　受託者は配信サイトの細部のデザインや色の変更等に関して、契約期間中は委託者の意向を受け無償で対応すること。

8　アクセス報告に関する要件

⑴　受託者は視聴者からのアクセス管理を行い、アクセス数を集計表示できる委託者専用サイトを提供すること。会議毎に任意の年、月及び集計種別を選択することで24時間以前のアクセス数を集計表示すること。

⑵　委託者専用サイトはID、パスワードの認証を必要とすること。

⑶　ライブ配信のアクセス集計表は各時間帯別、主なOS別のアクセス数を月間の日毎に集計すること。

⑷　VOD配信のアクセス集計表は各時間帯別、VODコンテンツ別、議員名別、主なOS別のアクセス数を月間の日毎に集計すること。

⑸　サイトに表示された集計表は同じ構成でCSVファイルとしてダウンロードでき、EXCEL等の表計算ソフトに読み込むことができること。

9　ネットワークに関する要件

⑴　ライブ配信、VOD配信のネットワーク及び配信設備は同時に5,000ユーザ程度の視聴が可能なこと。

⑵　本業務に基づいて設置する機器については、３.⑵.オに記載の庁内イントラネットへのライブ配信を行うための接続を除き、市のネットワークに接続してはならない。

⑶　委託者側に設置するルーターのアクセス回線は、委託者が提供する光回線（フレッツ光ネクスト（ファミリー・ギガラインタイプ））を用いること。なお、委託

者が提供する光回線は本会議と委員会を合わせて１系統とする。配信センターと委託者側ネットワークの接続においては、インターネットを経由しない閉域網 VPN を用いること。

⑷　配信センターは地理的冗長性を考慮し、異なる地域に設置すること。

⑸　配信センターはインターネットへの配信に CDN を使用すること。

⑹　光回線の回線基本料については委託者負担とする。また、閉域網 VPN の費用は受託者負担とする。

⑺　その他、映像配信設定に関して必要な情報は、委託者及び市情報システム部が協議し提供するため、受託者はその情報を基に映像配信に係る設定を行うこと。

10　セキュリティに関する要件

業務の遂行に当たって、受託者は、委託者の指示の下、札幌市情報セキュリティポリシーに定める内容を遵守すること。詳細は別紙３「受託者に求める情報セキュリティ対策等」のとおり。

11　障害対応に関する要件

⑴　障害の発生については、委託者又は受託者が発見し次第、受託者又は委託者に通知し、受託者が機器の修繕・交換等必要な対応を迅速に行うとともに、障害対応中である旨を配信サイトに表示すること。また、障害を回復した後、障害の内容とその原因、対応状況等を委託者に報告すること。

⑵　会議開催日の障害発生時には、委託者の求めに応じて直ちに現場に急行し、復旧作業内容について委託者と協議し、委託者の了承を得てから作業を開始すること。また、障害対応中である旨を配信サイトに表示すること。

⑶　障害発生時は連絡から２時間以内に駆け付け対応すること。

12　工事

⑴　工事（映像配信機器設置等を含む。以下同じ。）が実施可能な期間は令和８年６月中旬から令和８年７月上旬までの予定であるが、詳細な日程については別途協議するものとする。

⑵　必要に応じて、委託者及び関係部局と協議を行うこと。

⑶　調音室は、令和８年６月 30 日までに工事を完了させ、令和８年７月１日から配信が可能な状態とすること。

⑷　第一・第二特別委員会会議室は、いずれか１室の工事を令和８年６月 30 日までに完了させ、令和８年７月１日から配信が可能な状態とすること。また、もう１室も令和８年７月 15 日までに工事を完了させること。なお、第一・第二特別委員会会議室は、同時に両会議室が使用不可とならないように工事を行うこと。

⑸　各機器等の搬入に当たっては、既存施設部分、工事目的物の施工済み部分等について、損傷しないよう適切な養生を行うこととし、損害を与えた場合は、受託者の責任において修復すること。加えて、導入した機器については、転倒防止、落下防止措置をすること。

⑹　機器設置、接続終了後は、各機器が仕様書記載の要件を満たすよう調整し、問題がないことを確認すること。

13　環境への配慮

本業務においては、本市の環境マネジメントシステムに準じ、環境負荷低減に努めること。

⑴　電気、水道、油、ガス等の使用に当たっては、極力節約に努めること。

⑵　ごみ減量及びリサイクルに努めること。

⑶　両面コピーの徹底やミスコピーを減らすことで、紙の使用量を減らすよう努めること。

⑷　自動車等を使用する場合は、できるだけ環境負荷の少ない車両を使用し、アイドリングストップの実施など環境に配慮した運転を心がけること。

⑸　業務に係る用品等は、札幌市グリーン購入ガイドラインに従い、極力ガイドライン指定品を使用すること。

⑹　業務に関わる従業員に対し、札幌市環境方針の理解及び業務と環境の関連について自覚を持つよう周知すること。

⑺　特定業務（設備機器の運転管理、毒物又は劇物の取扱い、特別管理産業廃棄物の保管又は処理業務）に従事する者は、それを遂行するために要求される十分な知識及び技能を備えていること。

14　その他

⑴　映像配信を安定的に運用するため、委託者に対し、映像配信機器の操作方法等について一連の研修会を実施すること。

⑵　契約満了時には、映像配信機器を撤去すること。ただし、双方の合意がある場合は、機器の一部を撤去の対象外とする。なお、撤去に係る詳細な日程については別途協議するものとする。

⑶　業務の履行において不明な点が発生した場合、又は仕様書に定めのない事項については委託者、受託者間で別途協議を行い決定する。

⑷　業務の履行に当たり、既存機器との調整が必要な場合については、既存機器の保守・管理業者と十分な連携を図ること。

テロップ例

【開会前の表示】

令和８年
第二部決算特別委員会

会議は 10 時 00 分開会予定です

委員会室の静止画を流す。音声は流さない

【開会中　委員長】

令和８年第二部決算特別委員会（○○局）

（委員長）
○川　×子

開会中は、画面上部に会議名、画面下部に発言者を表示する。
委員長は、氏名の上に役職名を加える。

【開会中　質問】

令和８年第二部決算特別委員会（○○局）

（●●党）
○山　×男

質問者は、氏名の上に会派名を加える。

【開会中　答弁】

令和８年第二部決算特別委員会（○○局）

当局

答弁者は、氏名等を表示しない。

【休憩中①】

（ただいま休憩中です）

画面背景は静止画。音声は流さない。

【休憩中②】

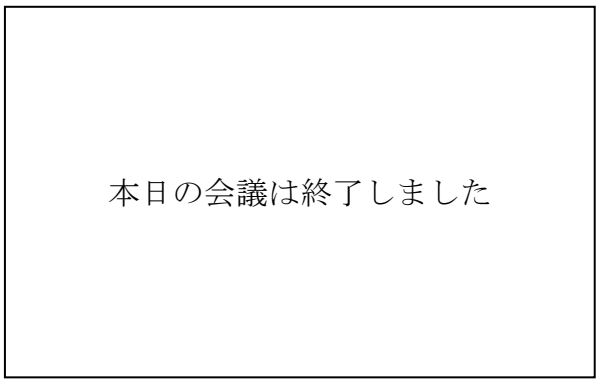
○時○分から再開いたします

（ただいま休憩中です）

再開時刻決定後、再開時刻を追加で表示する。

テロップ例

【閉会後】



画面背景は静止画。音声は流さない。

各年度におけるライブ配信に係る中継見込み日数及び総見込時間等

※過去の実績を元に算出しているため、実際の日数や時間等は見込みと大幅に変動する場合がある。

１　本会議

⑴　想定される中継

議　　会	第26期		第27期															
	８年		９年					10年				11年				12年		
	３定	４定	１定	１臨	２定	３定	４定	１定	２定	３定	４定	１定	２定	３定	４定	１定	２定	
中継の有無	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	

※臨時会が追加される場合がある。

⑵　中継見込み日数、質問者数及び時間

年　度	年　　月　　日	日　数	質問者数	時　間
8	令和８年７月１日～令和９年３月31日	23	42	48:23
9	令和９年４月１日～令和10年３月31日	23	48	50:57
10	令和10年４月１日～令和11年３月31日	30	51	61:07
11	令和11年４月１日～令和12年３月31日	30	51	61:07
12	令和12年４月１日～令和12年６月30日	5	9	9:21
合　　計		111	201	230:55

２　予算・決算・議案審査特別委員会

⑴　想定される中継

議　　会	第26期				第27期											
	８年		９年				10年				11年				12年	
	３定	４定	１定	２定	３定	４定	１定	２定	３定	４定	１定	２定	３定	４定	１定	２定
中継の有無	○		○	○	○		○		○		○		○		○	

⑵　中継見込み日数、質問者数及び時間

年　度	年　　月　　日	日　数	質問者数	時　間
8	令和８年７月１日～令和９年３月31日	15	338	89:31
9	令和９年４月１日～令和10年３月31日	24	491	127:21
10	令和10年４月１日～令和11年３月31日	19	405	112:16
11	令和11年４月１日～令和12年３月31日	19	405	112:16
12	令和12年４月１日～令和12年６月30日	－	－	－
合　　計		77	1,639	441:24

３　調査特別委員会

⑴　想定される中継

契約期間中の全期間、随時開催される。

⑵　中継見込み日数、質問者数及び時間

年　度	年　　月　　日	日　数	質問者数	時　間
8	令和８年７月１日～令和９年３月31日	11	48	13:33
9	令和９年４月１日～令和10年３月31日	14	66	18:02
10	令和10年４月１日～令和11年３月31日	14	66	18:02
11	令和11年４月１日～令和12年３月31日	14	66	18:02
12	令和12年４月１日～令和12年６月30日	4	19	4:28
合　　計		57	265	72:07

別紙３

受託者に求める情報セキュリティ対策等

本業務の履行に当たっては、本市の情報セキュリティポリシーに沿って、原則として、以下に規定する内容に従いセキュリティ対策を行うこと。ただし、対応できないものについては、他の手段による対策等によることを認める場合がある。

１．基本的事項

⑴　情報セキュリティを確保するための体制の整備

・受託者は、本業務の情報セキュリティ責任者、技術担当窓口、作業員及び作業場所を定め、委託者へ報告すること。また、これらを変更する場合も報告すること。

・従業者に対する情報セキュリティ教育を実施すること。

・情報システムに本市の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、本市と委託事業者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

・本市の求めに応じ、委託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格（情報処理安全確保支援士等）・研修実績等）・実績及び国籍に関する情報を提供すること。

⑵　取り扱う情報資産の秘密保持等

・受託者は、本業務で知り得た情報の機密性を確保し、目的外利用及び必要以上の複製・配布を禁止する。この義務は契約終了後も継続するものとする。

・委託業務終了時には、本市の情報資産を適切に廃棄すること。

⑶　情報セキュリティインシデントが発生した場合の対処

・情報セキュリティインシデントが発生した場合は速やかに委託者へ報告し、被害拡大防止の措置を講じること。また、事実関係の調査や再発防止策の検討、必要に応じた公表に協力すること。

・不正アクセス、サービス不能攻撃、不正プログラムの感染等、短時間で被害が拡大する情報セキュリティインシデントについては、委託先において緊急時対策を行うこと。

⑷　製品のサポート期間への対応

・本業務に導入する機器およびソフトウェアは、次期システム更改時期までメーカーのサポート（パッチ提供等）が継続されると見込まれる製品を選定すること。

⑸　情報セキュリティ対策の履行状況の報告・監査等

・受託者は、本業務の情報セキュリティ対策の履行状況について、定期的に報告すること。

・委託者は、受託者の情報セキュリティ対策の履行状況を確認するため、必要に応じて、実地検査等による情報セキュリティ監査を実施できるものとする。受託者はこれに協力すること。

・受託者の情報セキュリティ対策の履行が不十分であると認められる場合、委託者は、受託者と協議した上で、業務の一時中断や損害賠償など、必要な措置をとらせることができるものとする。

⑹　委託者および受託者双方の責任の範囲

・本業務の遂行における委託者および受託者双方の責任の範囲については、次のとおりとする。

委託者…コンテンツの内容・権利に関する責任（例：配信映像の編集・公開の判断等）

受託者…システムの運用・セキュリティに関する責任（例：不正アクセス対策、データの管理、システム稼働の維持。）

⑺　再委託に関する事項

・受託者が業務の一部を再委託する場合には、委託者の事前承諾を要する。また、受託者は再委託先に対しても本契約と同等の義務を負わせ、適切に管理、監督する責任を負う。

２．本業務で求める情報セキュリティ技術対策基準

⑴　物理的技術対策

①　各区域における施錠

【入退室管理システムによる施錠】

・管理区域は、IC カード等を利用した入退室管理システムを設置し、電子錠により施錠を行う。

【鍵による施錠】

・管理区域及び業務区域は、室、区域又はサーバラック等に鍵で施錠を行う。

区　域	内　容	本業務での想定される区域（例）
管理区域	情報資産を取り扱う情報システムのデータベース及びサーバ等を設置し、運用する施設、室及び区域であり、情報システムの運用、開発保守等の担当者のみが入退室でき、入退室管理及び施錠可能な区域	配信センター（ASP サーバ）
業務区域	事務室等、業務を行う部屋をいい、パソコン等を管理運用及び保管する区域	受託者のオフィス 調音室、第１・第２特別委員会会議室
一般区域	その他、不特定多数の者が通行し、入退出することが可能な区域	―

②　管理区域における入退室管理

【入退室管理システム】

・IC カード等による電子錠の開閉及び入退室記録が収集可能な入退室管理システムを導入し、区域への入退室日時及び入退室者の記録を管理する。

【有人又は監視カメラによる監視】

・入退室管理と組み合わせ、本市職員や警備員を配置することによる有人監視又は監視カメラによる監視を行い、区域への入退室者の本人性確認又は映像の記録及び監視を行う。

【入退室記録の管理】

・入退室記録は１年間、映像記録は３ヶ月間保存し管理を行う。

③　無停電電源装置の設置

・配信システムを構成するサーバおよびネットワーク機器には、停電時に機器を安全に停止させるために十分な電力を供給できる無停電電源装置を設置する。

④　設置する機器の耐震対策

【ラック等】

・震度６弱でも耐えうるように、ラック等と床面又は壁面をアンカーボルト、固定金具等を利用し固定する。また、キャスター付ラックの場合で、金具等による固定が困難な場合は、金具等により固定できるまでの当面の間、キャスターをゴム製ストッパ等で固定すること。

【ラックマウント型機器】

・関係事業者の専用ラックや汎用型ラックへ搭載可能なサーバ、ネットワーク機器等は、固定金具でラックに固定する。

⑤　ケーブル配線

・ケーブル配線について、下記の表に基づき保護しなければならない。

	管理区域における配線	業務区域における配線
通信ケーブル	床下又はケーブルラック等による保護。	床下又はプロテクタにより保護。
ＨＵＢ	ラック等へ設置。	施錠可能なキャビネットに入れるか、机下等容易に関係者以外の手に触れることができない場所へ設置。
ＬＡＮケーブル	床下又はケーブルラック等による保護。床からの立ち上げ部分をダクト等で保護。	床下又はプロテクタにより保護。十分に余長をとり、机下でまるめておく。
識別タグ及びラベル表示	関係者以外が判別できない表示内容として、各ケーブルの両端又はモジュラに取り付ける。	関係者以外が判別できない表示内容として、各ケーブルの両端又はモジュラに取り付ける。ただしネットワーク情報は表示しない。ＨＵＢへラベルを取り付ける。

※【識別タグ、ラベルの取り付けについて】使用するケーブル、ＨＵＢ及びモジュラには、故障時の切り分け又は保守作業上、関係者のみが識別可能なタグ又はラベルを取り付ける。タグ、ラベルの表示内容には、ＩＰアドレス、コンピュータ名等ネットワークに関する情報を表示してはいけない。なお、表記方法については、受託者の決定後に別途指示する。

・管理区域及び業務区域内に敷設するＬＡＮケーブルは、下記表の基準を満たすものを使用しなければならない。

品名	基準内容
ケーブル	・ツイストペアケーブルは、規格カテゴリ５ｅ～６ａ以上のＵＴＰケーブルを使用 ・光ケーブルは、接続する距離に応じて使用し、タグを取り付ける ・色は濃緑色・橙色・白色以外を使用（加えて、各ケーブル同士の区別がつくように色を選定）
コネクタ	・ＵＴＰケーブルには、ケーブル規格に準拠したコネクタを使用 ・光ケーブルには、接続する機器に対応したコネクタを使用

⑵　ネットワーク構築における技術対策

①　ネットワーク構築時の制限事項

【ＬＡＮケーブルの制限長】

・ＵＴＰケーブルの制限長は、使用するケーブルの規格カテゴリにおいて定められた長さとする。１００ｍを超える場合は、ＨＵＢによるカスケード接続又は光ケーブルを使用する。

・光ケーブルは規格により制限長が異なり、接続する距離に応じてシングルモードケーブル又はマルチモードケーブルを適切に使用する。

【ＨＵＢ同士のカスケード接続】

・ＨＵＢ同士によるカスケード接続は、遅延時間等を考慮して適切に対処すること。

②　ネットワーク接続における対策

・ネットワーク構築においては、以下の機能を利用し外部からの不正アクセスや破壊行為を防止しなければならない。

【ルータ】

・ネットワーク経路制御（ルーティング情報の設定）

※ルータが１対１のような小規模ネットワークの場合は、リモート側ルータにデフォルトルートとしてサーバ側の１経路のみの設定を行う。

・ＩＰフィルタリング機能（アクセスリストの設定）

⑶　システム開発・構築における技術対策

①　ＩＤ及びパスワードの使用

・ＩＤ及びパスワードの使用にあたり、次の制限事項を遵守しなければならない。

制限事項	制限内容
ＩＤの使用制限	・“administrator”、”guest”、”root”は使用制限
推測されにくいパスワードの設定	・英数字記号混在８桁以上、当人の関連情報からは推測できないなどの条件を満たす、推測されにくいパスワードを設定（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）

※サーバの管理者パスワードは、他のサーバや端末、他のアカウント等のパスワードと同一にしてはならない。

【パスワードの使いまわしの禁止】

・ビルトインアカウントを含む全てのアカウントにおいて、パスワードは他のサーバや端末、他のアカウント等のパスワードと同一にしてはならない。

【推測されにくいパスワードの設定】

・パスワードは、以下の条件を満たす推測されにくいものを設定すること。

◦英数字記号を混在させ８桁以上であること（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）

◦過去に漏えいしたパスワードではないこと

◦当人の関連情報（名前、電話番号、生年月日等）からは推測できないこと

◦英単語など、辞書に含まれる文字列をそのまま使用していないこと

◦同じ文字の繰り返しやわかりやすい並びの文字列ではないこと

【共用ＩＤ等のパスワード変更】

・利用者ごとにＩＤの付与及びパスワードの設定ができない、共用ＩＤや特権者用ＩＤの利用者に異動、退職があった場合は、パスワードを変更すること。

②　利用者グループ及びアクセス権の設定

・情報システムへのアクセスについて、受託者は自社の従業者に対して、以下の利用者グループ及びアクセス権を設定しなければならない。

・また、特権を持つ主体の認証情報については、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じなければならない。

【利用者グループの設定】

・特権者権限グループ

特権者権限は、情報システムに関わるすべての操作が可能であることから、システム管理責任者、システム管理者(正・副)等、必要最小限の利用者を設定する。

・運用保守権限グループ

運用保守権限は、情報システムの運用保守業務担当者を設定する。

・一般利用者権限グループ

一般利用者権限は、業務処理の実行又は参照及び閲覧する利用者を設定する。

【アクセス権の設定】

・特権者権限グループのアクセス権

オペレーティングシステム及び業務用プログラムへのアクセス等、情報システムに関わるすべての操作に対しての権限を設定する。

・運用保守権限グループのアクセス権

オペレーティングシステムでの運用管理業務に関わるフォルダ、ディレクトリへのアクセス権、業務用プログラムへのアクセス権及び業務用フォルダ、ディレクトリへのアクセス権を設定する。

・一般利用者権限グループのアクセス権

業務用プログラムへのアクセス権及び業務用フォルダ、ディレクトリへのアクセス権を設定する。

【特権を付与されたIDの管理】

・悪意ある第三者等によって窃取された際の被害を最小化するための措置即時にアクセスを遮断する、特権ID利用のためのパスワードを直ちに変更する等により、特権を付与されたIDが窃取された際の被害を最小化するための措置を講じること。

・内部からの不正操作や誤操作を防止するための措置特権を付与されたIDを使用した際の操作ログを取得する、特権を付与されたIDの利用に対する承認ワークフローを準備する等により、不正操作や誤操作を防止するための措置を講じること。

③　認証機能

【認証機能】

・情報システムには、知識情報（ID及びパスワードなど）、所持情報（ICカードなど）、生体情報（指紋認証など）のいずれかの手段による認証手段を備えること。

・ただし、外部ネットワークから内部通信回線へ接続した機器に対してリモートメンテナンスを行う場合は、２つ以上の認証手段を用いた多要素認証を利用すること。

【ＩＤの管理】

・ＩＤについては、所属するグループ、利用者名等をＩＤ管理台帳等によって管理すること。

・原則として、１つのＩＤを複数人で共用しないこと。システムの制約等によりやむを得ずＩＤを共用する必要がある場合は、ＩＤ管理台帳により利用者、使用日、使用開始時刻及び使用終了時刻等を記録しなければならない。また、共用ＩＤの利用者に異動・退職があった場合は、パスワードを変更すること。

【セッションタイムアウト時間の設定】

・一定時間作業を行わない場合等に、スクリーンセーバー等によりパソコンや機器等の画面をロックし、再認証を要求すること。パソコンや機器等で設定が困難な場合には、離席時には必ず画面ロックを行うこと。

④　暗号技術の利用

・配信センターと委託者側ネットワークの接続においては、インターネットを経由しない閉域網VPNを用いて通信データの暗号化対策を行うこと。

⑤　無線ＬＡＮの使用

・無線ＬＡＮを利用する場合は、以下の技術を利用しなければならない。

【利用端末の認証】

・アクセスポイント側、無線ＬＡＮ端末側にＳＳＩＤを設定し、利用端末の認証を行う。また、アクセスポイント側でＡＮＹ接続拒否の設定を行い、不正アクセスを防止する。ＳＳＩＤは、外部の者から推測しにくいＩＤにすることとし、一般的な名前やデフォルトの名前は使用しないこと。

【暗号化】

・共通の暗号化キーであるＷＰＡ３方式若しくはＷＰＡ２方式を利用し、アクセスポイントと無線ＬＡＮ端末間のデータを暗号化する。また認証の際に設定する文字数は、２１文字以上とする。

⑥　外部記憶媒体の利用

・本市の情報資産について、原則として、USB メモリ等の電磁的記憶媒体による端末からの情報持ち出しを行わないこと。例外的に USB メモリ等の電磁的記憶媒体を使用する場合は、以下の対策を講じること。

【ハードウェア暗号化機能の利用】（ＵＳＢメモリ利用の場合）

・ＵＳＢメモリに情報資産を保存する場合は、ハードウェア暗号化機能がついた製品を利用する。

【不正プログラム対策機能の利用】（ＵＳＢメモリ利用の場合）

・ＵＳＢメモリに情報資産を保存する場合は、不正プログラム対策機能がついた製品を利用する。

【保存データの暗号化】

・ＵＳＢメモリ以外の外部記憶媒体に情報資産を保存し、業務区域以外に持ち出す場合は、保存データの暗号化を行う。ただし、システム上暗号化が困難な場合は、専用のかぎ付ケースを使用するなどの対策を実施すること。

【その他対策】

・端末には利用許可された媒体のみ接続可能とすること。

・利用媒体は、全て管理し利用履歴を残せること。

⑦　サーバの利用

・サーバを導入する場合、以下の項目を考慮して運用しなければならない。

【ウイルス対策ソフトの利用】

・サーバの不正プログラム感染を防ぐため、ウイルス対策ソフトを導入しなければならない。

【最新パターンファイルの取得】

・最新パターンファイルを取得し、サーバにインストールしなければならない。

【バグフィックスされた修正プログラムの適用】

・サーバへの影響を考慮し、必要に応じて OS 等の修正プログラムを適用する。

【無停電電源装置の選定、設置】

・無停電電源装置を設置しなければならない。

【耐震対策】

・専用ラックや汎用型ラックへ搭載可能なサーバは、固定金具でラックに固定する。タワー型サーバについては、転倒防止用ベルト又は簡易な耐震用具を使用し、ラック、什器又はデスク等に固定する。

【管理者の限定】

・管理者権限の範囲は最小限とし、必要な職員又は受託者の作業員のみにIDを付与しなければならない。また、当該IDが不要となった場合には、速やかにIDを削除しなければならない。IDが削除できない場合は、速やかにパスワードを変更しなければならない。

【アクセス権の設定】

・サーバに対するアクセス権限は、当該サーバに格納された情報の利用が必要な者に限定して設定しなければならない。また、必要に応じてフォルダごとにアクセス権設定をしなければならない。

【アクセス記録の保管】

・サーバへのアクセス状況を記録し、管理しなければならない。

【運用限界の適切な管理】

・OS等のサポート期限及びハードウェアの部品供給が終了する前に計画的に更新作業を行わなければならない。

⑧　Ｗｅｂサーバ等に対する対策

・Webサーバ等をインターネット上へ公開する場合は、次のとおりセキュリティ対策を実施しなければならない。

【ファイアウォールの設置】

・内部ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

【Webアプリケーション、プラットフォームの監視、脆弱性対策】

・インターネット上に公開する情報システム、ホームページ等の構築、改修又は運用を行う場合は、原則としてWAF、IDS、IPS等を利用しなければならない。

・WAF、IDS、IPS等による対策が行われていない場合は、Webアプリケーション診断及びネットワーク診断（プラットフォーム診断）を年１回以上実施して、脆弱性を把握し、早期に対策を行うこと。

【電子証明書による認証の対策、通信データの暗号化】

・インターネットを介して転送される情報の盗聴及び改ざんを防止するために、全ての情報に対する暗号化及び電子証明書による認証の対策を講じなければならない。

【Webサーバで利用する機能の制限】

・脆弱性が存在する可能性が増大することを防止するために、Webサーバが備える機能のうち、必要な機能のみを利用しなければならない。

【Webサーバ上へ保管する情報の選定】

・Webサーバからの不用意な情報漏えいを防止するために、Webサーバ上には非公開の情報は保管しないなど必要な措置を講じなければならない。

【Webコンテンツの編集作業を行う主体の限定】

・Webコンテンツに起因する情報漏えいを防止するために、Webコンテンツの編集作業を行う主体を限定しなければならない。

【運用基準の策定】

・情報システムの運用に関し、必要な事項を定めた運用基準を策定しなければならない。

例：運用時連絡先や営業時間に関する項目、サービス（事業）変更・終了時の事前告知及び問い合わせ先に関する項目サービス提供時間等に関する項目、サービス稼働状況の監視に関する項目、ID 及びパスワードの盗難によるなりすましへの対策など

【ドメインの管理】

・独自に取得したドメインの運用を停止する場合は、第三者に再取得され元の Web サイトへのアクセスを利用し、詐欺サイト等へ誘導されることのないようドメインを一定期間保持する。

【外部ホームページ等の運用】

・保守体制図を作成し、緊急時の連絡先を明らかにしなければならない。

⑨　ＩＰｖ６への対応

【ＩＰｖ４及びＩＰｖ６の両対応】

ＩＰｖ４とＩＰｖ６のその両方に対応すること。

⑷　不正プログラム対策

①　ウイルス対策ソフトウェア等による対策

・ウイルス対策ソフトウェアは、Ｗｉｎｄｏｗｓ系に限らず、各システムに対応した対策ソフトウェア等を適用する。また、単体パソコン及び独自ネットワーク上のパソコン等についても、適切に対策すること。さらに、仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。

【ウイルス対策ソフトウェアの導入】

・各システムで利用しているサーバ等、端末及びモバイル端末に対応したウイルス対策ソフトウェアを導入する。

【ウイルスチェック】

・「ウイルス感染の疑いがある場合」、「システムに重大な損害を与えるウイルスの脅威が発生した場合」は、直ちに該当端末をネットワークから切り離すとともに、ハードディスクドライブのフルスキャンによるウイルスチェックを実施する。それ以外の場合は、各システムの運用状況を考慮した上で、定期的にハードディスクドライブのフルスキャンによるウイルスチェックを実施する。

【最新パターンファイルの取得】

・ウイルス対策ソフトウェアのパターンファイルを常に最新の状態を保つために、最新のパターンファイルを取得し、インストールする。

②　修正プログラムの適用

【バグフィックスされた修正プログラムの適用】

・サーバ等や通信機器、業務アプリケーション及び端末に、関係事業者等から提供される修正プログラムを、可能な限り事前に動作検証を行い、情報システムへの影響を考慮した上で、必要に応じて適用する。

・また、運用している情報システムに導入されているソフトウェアについて、脆弱性の情報を収集し、脆弱性が発見された場合には速やかに対策を講じる必要がある。

⑸　システム運用における技術対策

①　アクセス状況等の記録

・情報システム、外部ホームページ及びファイルサーバ等を運用する場合は、アクセス状況を記録し、管理しなければならない。なお、保存期間は、原則として最低１年間とする。

【アクセス状況等記録の収集】

収集する情報は、以下の項目を参考に必要なものを協議する。

◦利用端末…アクセスした端末名又はＩＰアドレス

◦ＩＤ…アクセスしたＩＤ

◦ログオン及びログオフの日時…ログオン及びログオフした日時

◦アクセスの成否…フォルダ、ファイルへのアクセス状況（成功・失敗）

◦アクセスした情報…アクセスしたフォルダ名又はファイル名

◦操作内容…利用者が操作した内容（閲覧、作成、更新、削除等）

【ログの収集】

・一般的なログの収集については、「いつ」「誰が」「何を」したかを一意に特定できることを原則とする。Web サーバの場合は、庁外の IP からアクセスされたログを収集し、ファイルサーバの場合は、端末と操作内容(閲覧、上書き、削除等)を識別できるログを収集する。

【アクセス状況等記録の管理】

・収集した情報は、開示請求やセキュリティ事故、システム障害時の追跡・形跡調査等に必要な記録となることから、厳重な管理及び保管をしなければならない。保管場所は、施錠可能なキャビネット、アクセス制限を施したフォルダや外部媒体等とする。

【アクセス状況等記録の報告】

・不正アクセス等が認められた場合などは、受託者が提供可能な情報の範囲について別途協議のうえ、遅滞なく報告すること。【時計の同期】

・収集する情報の記録の正確性を保障するために、定期的にコンピュータの時計をシステム又は手動により標準時間に合わせるよう補正する。

【情報システムの監視機能】

・管理する情報システム及びネットワークの稼働状況を監視し、障害等の早期発見に努めなければならない。また、安定稼働を確保するための適切な運用保守を行わなければならない。監視の対象やイベントとしては以下が考えられるが、新たな脅威の出現、運用の状況等により、定期的に見直すことが必要である。

◦サーバ装置上での情報セキュリティインシデントの発生を監視する必要がある場合は、当該サーバ装置

◦内部通信回線と外部の通信回線との間及び内部通信回線内で送受信される通信内容

◦重要情報を取り扱う情報システムについて、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線

◦C&C サーバ等への不正な通信

②　情報システム利用に関わる制限事項

【複数ネットワーク接続の禁止】

・ネットワークインタフェースカードの複数搭載、モバイルカードの搭載、ＵＴＰケーブルの接続替えなど、利用端末を複数のネットワークに接続することを禁止する。

③　オペレーティングシステム・ソフトウェア等の制限及び維持、運用

・情報システムで使用するオペレーティングシステム・ソフトウェア等について、関係事業者からの提供期間終了等によるサポート終了のものを使用せず、最新のオペレーティングシステム・ソフトウェア等を選定する。尚、オペレーティングシステム・ソフトウェア等の導入にあたっては、導入するシステムの動作が安定且つ正常に動作することを十分検証した上で行うこと。

【オペレーティングシステム・ソフトウェア等の維持、運用】

・利用しているオペレーティングシステム・ソフトウェア等について、常に最新の状態を保持するために、関係事業者から提供される情報や修正プログラムを適切に判断し処置しなければならない。 オペレーティングシステム以外でも.NET Framework、Java SE 等のミドルウェア、テキストエディタ、PDF ビューア等のソフトウェアについても適切に運用すること。

【システム構築におけるオペレーティングシステム等サポート期限の確認】

システムの構築、更新及び改修を行う場合は、使用するオペレーティングシステム・ソフトウェア等のサポート終了予定日を確認し、使用予定期間中にサポートが終了することがないものを選定しなければならない。

④　情報資産の消去

・受託者は、本業務の遂行にあたり本市から預託されたデータ、及び本業務の過程で生成された録画映像データ等について、業務終了時または本市が指示した際には、速やかに消去しなければならない。

・消去にあたっては、単なるファイル削除（ゴミ箱への移動等）に留めず、専用のデータ消去ソフトウェアによる上書き消去、またはクラウドサービス上の管理者権限による完全削除機能（パージ機能）等を用い、復元不可能な措置を講じること。

・データの保存先が受託者の契約する外部クラウドサービス（プラットフォーム）である場合は、当該サービスにおいてバックアップデータを含め、物理的・論理的にデータが残存しない仕様であることを確認し、その結果を本市に報告すること。

・受託者は、消去完了後、速やかにデータ消去証明を本市に提出すること。

⑤　特定用途機器のセキュリティ管理

・特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵している「特定用途機器」については、次のとおり取り扱う。

◦認証情報を初期設定から変更した上で、適切に管理する。

◦特定用途機器にアクセスする主体に応じて必要な権限を割り当て、管理する。

◦特定用途機器が備える機能のうち利用しない機能を停止する。

◦インターネットと通信を行う必要のない特定用途機器については、当該特定用途機器をインターネットやインターネットに接続している情報システムに接続しない。

◦特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。

◦特定用途機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる。

◦特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視する。

◦特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されている全ての情報を抹消又は再利用できないようにする。