リモートメンテナンス導入ガイドライン

令和３年（2021）４月１日

苫小牧市総務部ＩＣＴ推進室

第 1.1 版

目　次

は じ め に

本ガイドラインの目的

本ガイドラインは、苫小牧市情報システムの導入において、自庁舎導入サーバ(オンプレミス)及びデータセンター導入サーバ(ハウジング・専用ホスティング)への導入事業者が定期的保守メンテナンスや障害・故障での復旧作業において、遠隔地からの専用回線を利用したリモートアクセスによる保守サービスを提供する場合、安全に行われる事を目的とし、苫小牧市（以下、本市）が策定する「苫小牧市情報セキュリティ対策基準に関する要綱」「苫小牧市リモートメンテナンスの許可等に関する要領」に準じて策定している。

情報システム技術の変化、情報セキュリティ脅威の評価見直しにて基準とする要綱・要領の改訂やガイドラインの見直しが必要となった場合には改定するものとする。

また、本ガイドラインに定めのない事項や、本ガイドラインに沿った対応が困難である場合は、双方協議の上、対応を決定するものとする。

《用語集》

・統括情報セキュリティ責任者	本市ＩＣＴ推進委員会の副委員長を、ＣＩＳＯ直属の統括情報セキュリティ責任者とする。
・情報セキュリティ責任者	主たる情報システムを所管する課が所属する部長を、情報セキュリティ責任者とする。
・統括情報セキュリティ管理者	総務部ＩＣＴ推進室長とし、本市すべての情報セキュリティ対策に関する管理権限及び統括管理責任を有し、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導を行う権限を有する。
・情報セキュリティ管理者	情報システムの担当課長等を情報セキュリティ管理者とする。その担当課の情報セキュリティに関する権限及び責任を有する。
・情報システム担当者	情報セキュリティ管理者の指示等に従い、所管する情報システムに係る情報セキュリティ実施手順に従い運用を行う。
・保守事業者	システムの保守及び運用業務を受託している事業者をいう。システムの保守及び再委託を行う場合、その再委託者の委託する作業及びセキュリティに関する管理責任を伴う。
・再委託者	保守事業者から保守及び運用業務の一部の再委託を受けた者をいう。
・データセンター事業者	本市からの指定を受け、市導入システムが稼働するサーバ(ハウジング・専用ホスティング)データセンター事業を請け負う事業者をいう。
・アクセス制御	情報セキュリティにおいて、資源へのアクセス認証及びネットワークの経路制御・疎通制御を示す。
・アクセスログ	リモートアクセス保守サービスにおいて、ネットワーク接続・切断及びその保守での操作先・保守操作のログを示す。
・セキュリティアクシデント	情報セキュリティ事故(漏洩・盗難)事件(消滅・破壊)が発生した現象
・セキュリティインシデント	情報セキュリティリスク(ヒヤリハット含む)、ルール違反が発生・発覚した現象

第１章　適用範囲

本ガイドラインの各適用範囲を次に示す。

１.事業者の適用範囲

(1).情報システム導入事業者

情報システムの導入(契約)事業者を主体とするシステム保守事業者及びその再委託された再委託者を適用事業者の範囲とする。

(2).ハードウェア保守事業者(CE)の利用範囲外

情報システム導入事業者及びホスティング契約先のハードウェア保守事業者(CE)のハードウェアメンテナンス及び機器故障の保守サービスはリモートアクセス保守として適さない為、適用範囲から除外する。

(3).利用サービスプロバイダー(クラウド・ASP)の適用範囲外

クラウド利用サービス・ASP(アプリケーション・サービス・プロバイダー)が提供するソフトウェア保守に関しては、その利用サービスを提供する事業者の管轄として、適用範囲外する。

2.環境の適用範囲

(1).自庁導入システムの適用範囲

苫小牧市が利用するデータセンターにてハウジングサービス及び専用ホスティングサービスを利用する場合、その管理契約及びデータセンターのリモートアクセス監視サービスに基づき、情報システム担当者からの申請指示を前提とする場合に限り、適用範囲とする。

(2).外部環境ポリシー適用範囲

接続元となる事業者側の外部環境ポリシーとして、第 3 章.リモートサービス環境のセキュリティガイドラインに適合する場合に限り、適用範囲とする。

3.契約形態適用範囲

(1).本市自己導入契約(リース含む)の場合

情報システムを自己導入として契約(リース含む)し、保守メンテナンスを契約行為として行う場合、適用範囲とする。

但し、共同利用での保守契約等にて不特定多数への共有環境への保守サービスの場合、接続先のポリシーを特約出来ない為、契約形態適用の利用範囲から除外とする。

(2).利用料サービスに保守メンテナンスを含む契約の場合

情報システム導入環境が、自庁導入システムの適用範囲であり、そのリモート保守が接続先のポリシーを確約できる場合に限り、適用範囲とする。

但し、利用サービスの環境がクラウド・ASP のプロバイダー環境となる場合は、サービス提供契約するプロバイダーの管轄となるため、適用範囲外とする。

第 2 章　リモートアクセス保守サービスセキュリティ

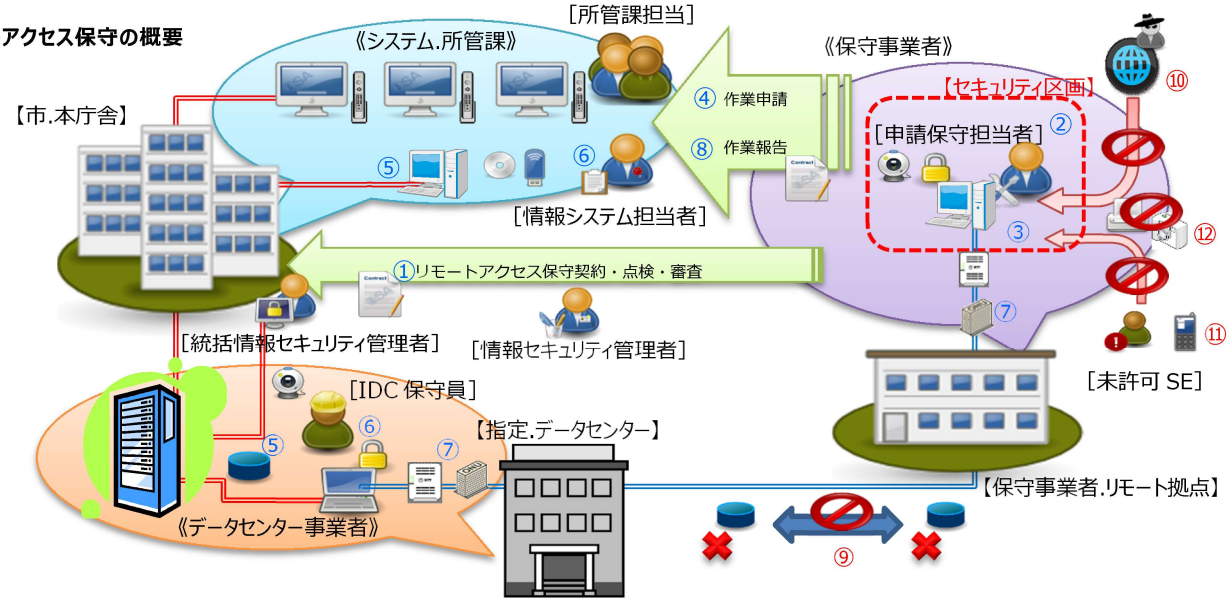
リモートアクセス保守サービスを行うにあたり、そのサービス契約を行う前提事項とリスクアセスメント、保守契約を行う上での契約合意事項を次に示す。

1 .リモートアクセス保守サービスの概要(導入基準)

(1).リモートアクセス保守の概要

リモートアクセス保守は、対障害保守性、保守費用の軽減などを導入の目的とするが、セキュリティリスクを配慮し、導入基準を以下の基本要件、環境要件が満たされている事を条件として、予め申請・協議・許可の上、統括情報セキュリティ管理者が認めた環境からの接続を行う事ができるものとする。

図 1.リモートアクセス保守の概要



《事前準備》　①.リモートアクセス保守サービスの契約 → 仕様の点検・審査
(保守事業者→情報セキュリティ管理者→統括セキュリティ管理者)
②.セキュリティ区画の整備・確認 → 点検・視察・定期監査
③.リモート保守環境(デバイス)の設置→ネットワーク網・通信機器・ネットワークルート・PC・ソフトウェア整備

《保守手順》　④.リモート保守申請(情報システム担当者が内容を確認し作業許諾)
⑤.適用モジュール等資産がある場合は、事前送付にて市.I-O 端末経由にて所管課が指定場所に事前適用後作業
⑥.リモート保守端末 ON(情報システム担当者がリモートで電源ロック解除)、又は IDC 保守員に依頼
⑦.リモート保守回線にてセッション開設し、リモート保守端末にログイン(二要素認証)※.保守端末を踏み台とする事
⑧.作業終了後、リモート回線の切断と端末の電源 OFF→作業結果の書面での報告(情報システム担当者受理)

《禁止事項》　⑨.リモート回線を介してのデータ(ファイル・ログ)の送受信を禁止する。
⑩.リモート回線・リモート保守端末は専用設備として、社内ネットワーク及びインターネット網からは完全分離とする。
⑪.セキュリティ区画は、入退室監理・24h カメラ録画等監視可能な環境とする。また、携帯他カメラなどの持込及び作業者以外入退を禁止する。
⑫.リモート回線操作画面の写真撮影及びプリントアウトは禁止する。

(2).リモートアクセス保守の必要性

リモートアクセス保守サービスにより、本市情報システム管理維持及び導入保守事業者側も様々なメリットを得ることが出来る。但し外部からのネットワーク接続を行う事による脅威も発生する事から、まず導入システムがリモートアクセス保守の必要性の要件に該当するかを判断の上、苫小牧市が制定する「苫小牧市情報セキュリティ対策基準に関する要綱」を担保したサービスの導入が必要である。

表 1.リモートアクセス保守必要性の基本要件(苫小牧市リモートメンテナンスの許可等に関する要領　別表１より一部抜粋)

項目	内容	左記解説
1.基本要件	1).保守事業者が遠隔地（市外）であること	障害・メンテナンス保守に関する対応での利用を目的とする(導入時、システム開発などの作業主体でのリモートアセスは用途として除外する) 契約での拠点サービスは SLA を保証すること。
	2).保守対応が迅速化されること	障害時のダウンタイムの大幅短縮 確認・調査対応のレスポンスの向上 本市システム担当職員の立会等作業負担の低減
	3).保守に係る経費が抑えられること	保守経費の削減からの直接的保守契約費用の低減 保守ベンダ拠点の集約による専門システム担当者の配置
	4).他自治体等での実績があること	信頼ある実績からのサービスの提供 セキュリティの信頼性、設備施設のライセンス

①.ダウンタイムの大幅短縮

システムの仮想化、高障害対応性からシステム保守に関して保守サービス員の専門性も求められる中、担当システムエンジニア（SE）直接訪問にて対応するには、迅速な対応が出来ない事も想定される。

システムダウンタイム、障害復旧、オペレーションリカバリーなど、システムが影響する事務処理ダウンタイムの大幅短縮と職員の作業負担低減を可能とすること。

②.保守費用の大幅低減

保守サービス担当が拠点もしくはベンダ拠点から実際に本市に出向く頻度と滞在期間などの直接的経費削減が見込める。

③.本市側職員の対応軽減

障害でのダウンタイムの大幅短縮や作業による立会などの負担も軽減されることが期待される。

安定した保守サービスを行うため、サービス導入によるセキュリティの担保と保守サービスでの申請許諾について、相互の確認を必要とする。

※.リモート保守サービスの導入経費及び維持経費に関しては、保守事業者側の負担を前提とする。

(3).リモートアクセス保守のリスクアセスメント

リモートアクセス保守サービスを導入する上で、相互にそのリスクアセスメントを明確に認知し検討する事が必要となる。

個人情報漏洩、メンテナンス時の誤操作によるシステムダウン、適用資産の検証検収不備からの不具合の誘発、ネットワークセキュリティ脆弱性からのウイルス感染による様々なリスクに関しての対策が必要となる。

①.ネットワーク上の問題

・リモートネットワークからの不正侵入
・リモートネットワークからのウイルス感染
・リモートネットワークへのなりすまし
・データ漏洩
・アクセスポイントへの攻撃
・システムへのダメージ、データの改ざん

②.リモート拠点(センター)でのリスク

・保守サービス員の不正行為からの情報漏洩、システム改ざん
・保守サービス員のなりすましによる不正行為
・不認可(未届け)での不正利用による障害・事故
・取扱不備に伴うセキュリティアクシデント(ウイルス感染、データ漏洩の起因)

③.保守サービスでのシステムダウンや安定稼働へのリスク

・作業に伴うシステム不具合、障害、ダウン、サービス障害
・作業誤りによるシステムへのダメージ
・取扱の誤りによる本番データへのダメージ(更新・削除)

④.保守作業での資産管理とデータの取り扱い

・資産管理誤りによる適用誤り事故
・システム更新適用での検証検収漏れによる事故

⑤.セキュリティ事故発生時の責任のあり方

・セキュリティ事故発生時の責任分界点の定義
・障害発生時の対応責任の明確化

⑥.安全管理の実施

・セキュリティ対策の点検監査
・定期的な作業報告と内容の点検
・リモート作業の開始と終了、作業の報告

(4).リスクアセスメントに対する考え(対策)

表 2.リモートアクセス保守の各導入要件(苫小牧市リモートメンテナンスの許可等に関する要領　別表 1 より抜粋)

項目	内容	左記解説
2.環境要件	1).作業場所が監視できること	監視カメラによる 24h 録画等
	2).作業者の入退室管理がされること	IC 管理や生体認証による入退室もしくは入退室帳等
	3).セキュリティ区画であること	何らかの施錠管理ができること
	4).アクセス記録が残ること	アクセスログの記録と保管、必要時の提出
3.リモート端末等の要件	1).本市専用端末を用意すること	他市町村、社内設備との区別
	2).端末費用及び回線利用料など構築・維持運用にかかる経費は保守事業者の負担とし、故障や更新についても対応すること	※.別途、端末の要件として入出力デバイスの接続等の制約
	3).使用機器は最新の Windows アップデートを行い、ウイルス対策ソフト等を施し、最新のパターンファイルを適用すること	
	4).データの入出力を不可にすること	
4.機能要件	1).印刷は原則禁止とし、動作確認はシステムの参照のみとすること	但し、検証にて印刷が必要な資産に関しては、プレビューで終わらせること無く、現地環境での印刷テストを実施すること
	2).インターネット環境や社内ネットワーク等への接続がされていないこと	インターネット網が存在するネットワーク、社内ネットワークとは完全分離をすること
5.運用要件	1).利用は市の承認を得ること	
	2).接続記録と作業報告を行うこと	

2.リモートアクセス保守契約の原則

(1).法的適合性・個人情報保護

・個人情報の取り扱いに関する内容を契約に含めること。
・再委託先について、選定の妥当性の説明、適正な個人情報の取り扱いを確認の上、再委託申請書を事業者に提出させること。
・問題が発生した際に適切な対応をとること。
・契約先、再委託先の作業を行うすべての担当者の誓約書の提出すること。

(2).苫小牧市情報セキュリティ対策基準に関する要綱の厳守

・物理セキュリティ	通信ケーブル等の配線に対する措置
	庁外への機器の設置
・管理区域の管理	管理区域の構造等の一部
	管理区域の入退室の一部
・通信回線及び装置	通信回線及び装置、接続ポイントについての必要なセキュリティ水準
・人的セキュリティ	外部委託事業者に対する説明
・技術的セキュリティ	システム管理記録及び作業の確認
・ログの取得	各種ログ記録の一定期間の保存
・ネットワークの接続経路制御	フィルタリング及びルーティング、アクセス制御の措置
・外部ネットワーク接続制限	統括セキュリティ責任者への申請許可
	外部接続事業者との損害倍書責任の契約上担保
	統括セキュリティ責任者の審査
	問題の発生、脅威が生じる想定の場合の物理的遮断
	特定用途機器のセキュリティの対策と無線 LAN の対策
・アクセス制御	システムへのアクセス制御とパスワードの取り扱い
	特権による接続時間(必要最低限)の制限
・外部(委託)サービス利用	事業者の選定基準、契約事項

(3).契約・合意事項

・利用サービス申請と合意事項と必要設備の申請及び審査
・守秘義務契約の結束
・保守要員の登録
・作業計画書、作業結果の報告(報告方法や提出内容についての確認)
・リモート保守サービス開始、終了時の接続手順と連絡ルール
・契約者、サービス提供事業者の責任分界点
・契約者、サービス提供事業者が必要なデータを取得する場合の手続き

第 3 章　リモートアクセス環境のセキュリティガイドライン

リモートアクセス保守サービスを行うにあたり、そのサービス契約を行える前提事項として、リモートアクセス環境に関する接続アクセスポイント(サービス拠点側)の制約、ネットワーク環境、システム機器、ソフトウェア、人的な運用についてのガイドライン(制約)について次に示す。

1 .リモートアクセスネットワークセキュリティ(導入基準)

(1).外部接続ネットワーク(アクセスポイント)の制約

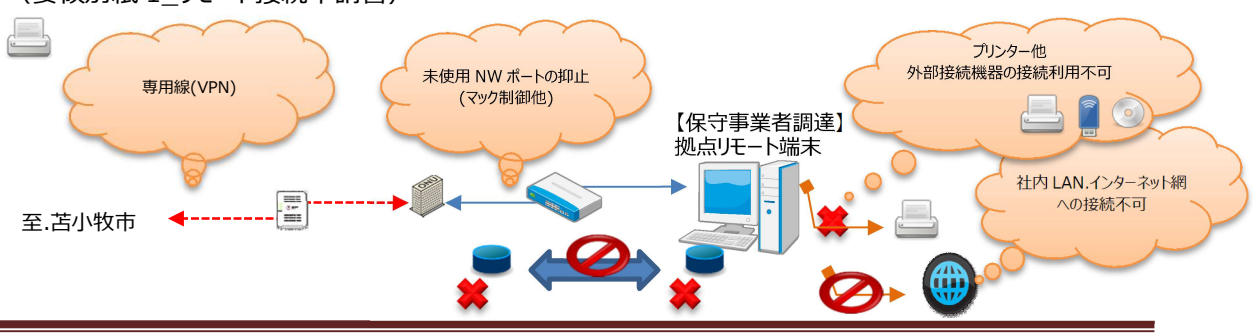
リモート保守拠点側は、以下の環境セキュリティを維持すること。

・リモート保守端末が設置される場所は、事前に申請許可されたセキュリティ区画とする。
・保守拠点は必要最低限とし、同時接続数は対向するリモート制御端末の台数を上限とする。
・セキュリティ区画は、常に監視カメラなどでの監視が行われ一定期間の記録保持を可能とする。（期間については別途協議とする。）
・セキュリティ区画への入退室は、IC カードなどの認証システムでの入退室制限が行われ、作業者の特定及び作業時間の記録ができること。
・サービス利用開始前にその環境状況を、本市情報セキュリティ管理者を通しての許可を得ること。
・期間中の本市セキュリティ管理者側からの視察監査が行われる場合、その受け入れを行うこと。

(2).接続リモート保守拠点のネットワークの制約

保守拠点のネットワークに関しては、以下のネットワークセキュリティを維持すること。

・リモート保守接続帯域のネットワークは、社内ネットワーク網と完全分離すること。
・インターネット網との接点を物理的に持たないネットワーク網とすること。
・ネットワーク機器は、専用機器として他ネットワークとの共有は行わないこと。
・ネットワークポートは他端末の利用ができない様、MAC アドレス制御又はポートロックなどの対策を行うこと。
・本市と接続する回線網は、専用の VPN 回線とし、その接続は対向する先を固定する制御を行うこと。
・全ての設備及びネットワーク通信にかかる費用は、事業者側の負担を前提とする。
・その機器設備一式の構成を本市に届けること。また、機器及び回線の更新時は、再提出とすること。
（要領別紙 1_リモート接続申請書）



(3).接続リモート保守本市側ネットワーク接続の制約

本市接続側の内部情報システムへのネットワーク接続に関しては、以下のネットワークセキュリティを維持すること。

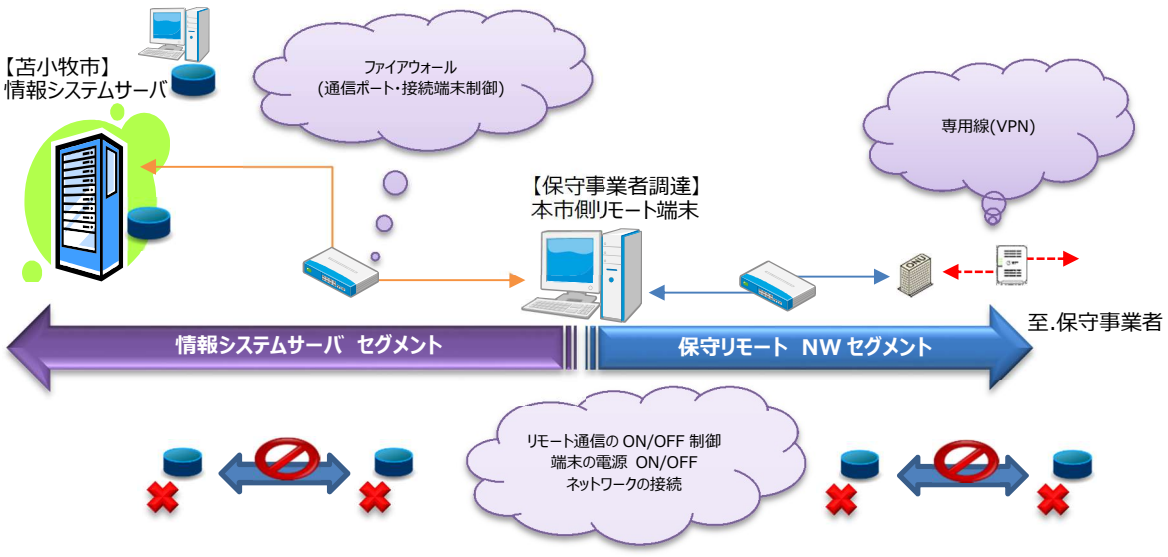
・リモート接続は、本市側の専用リモート保守端末への接続として、情報システム内部のネットワークには直接接続を行わないこと。(行うことができない様措置すること)
・本市側の専用リモート保守端末は、接続用のネットワークと情報システム側のネットワークの二系統の帯域をそれぞれのネットワーク機器に接続すること。
・リモート接続の方法として、専用リモート保守の端末を踏み台としてのリモートソフトウェアもしくは、多段でのリモートセッションを開設しての操作とすること。
・専用リモート保守端末と情報システムネットワークの間には、特定のセッション・ポートのみネットワークを疎通させるフィルターを考慮し、その先のネットワーク経路に付いてもアクセスリストなどで制限を行うこと。
・リモートネットワークは、リモートデスクトップの接続と画面操作のみ許可として、ファイルの共有や資源のコピーを行えない様、制限を行うこと。

※.資産の適用やログ採取などで、資産ファイルデータファイルの入出力が必要となる場合、事前に情報システムの所管課システム担当とのやり取りを行い、適用資産の送付（電子メール等)を行った後、市職員による資産適用(事前に共有ドライブを指定)の作業が必要となる。又、調査などでログファイルの外部出力が必要となった場合は、保守事業者側で指定ドライブへの出力後、市職員による点検の後、情報システム環境から抽出しての送付の手順となる。

※.本市のシンクライアント端末サーバは、カード認証でのログインセキュリティを行っている為、登録カード以外でのログインは不可。端末サーバの動作確認は専用の仮想環境管理コンソールの構築が必要。

※.個人情報を含むデータの提供は行う事は不可。

・リモート保守セッションを開設する場合、そのネットワーク接続・切断のロックを本市側の操作で可能とする運用とすること。（リモートソフトウェアの起動・停止、ネットワークのポートの ON・OFF、リモート端末の電源投入、経路ネットワーク機器の ON・OFF など)
・保守接続帯域のネットワークは、社内ネットワーク網と完全分離すること。



(4).リモートアクセス端末の制約

①.端末の条件 (保守事業者拠点操作端末、本市リモート端末共通)

・デスクトップ型、ノート型は問わないが、端末は固定常設として保守事業者が調達準備すること。
(リモートメンテナンスに関する要領:端末費用及び回線利用料など構築・運用にかかる経費は保守事業者の負担とし、故障や更新についても対応すること。)

・端末はセキュリティ区画からの持ち出しを禁止し、本市リモート保守専用機とすること。

・端末は施錠される区画で又は施錠されるロッカーでの保管を行うこと。

・利用する端末は、原則最新の Windows バージョンとし、OS アップデートとウイルス対策を施し、最新のパターンファイルを適用すること。

・端末は、データの入出力デバイス及び接続ポート(USB 等)の利用を不可とすること。

②.認証方法(保守事業者拠点操作端末)

・端末の操作は二要素以上の認証でのセキュリティが可能な環境とすること。
(ログインパスワードの他、登録指紋などの生体認証又は、カード・USB キーによる物理キー認証の二要素以上とする。)

・ネットワーク認証として、中継するネットワーク機器で端末を特定(MAC など)するセキュリティを行うこと。

③.リモート接続制御(本市リモート端末)

・端末は必要最低限の起動とし、起動を遠隔にて行える機器か、電源投入切断のルールを行うこと。

・リモート接続開始時に、ソフトウェアもしくはネットワーク装置で、疎通制限(ON/OFF)を行える仕組みを行うこと。

④.外部デバイスの制御

・端末への外部デバイスの接続を禁止すること。

・利用端末へのプリンター接続及びリダイレクトの設定は禁止すること。

⑤.アプリケーションの制約(保守事業者拠点操作端末、本市リモート端末共通)

・リモート操作を行うアプリケーションについては事前に利用ソフトウェアを申請し許諾を行うこと。

・リモートデスクトップでの接続操作する場合は、特定の接続ユーザ名とパスワードを設定すること。

・リモートデスクトップでのログインは、保守ベンダ専用ユーザを作成し、指定のユーザでの作業を行うこと。

・リモートデスクトップ接続のローカルリソースのプリンターとクリップボードのリダイレクトは禁止すること。

・リモートソフトウェアは特定のユーザとパスワード、接続先を指定できる場合はアクセスポイントを固定すること。

・リモートソフトウェアのファイル共有制御設定とリダイレクトは利用禁止とすること。

・リモート操作開始時に、リモートソフトウェアもしくはネットワーク装置で、疎通制限を行える仕組みを行うこと。

⑤.ライセンス、ハード保守費用(保守事業者拠点操作端末、本市リモート端末共通)

・リモートアクセス保守を行う上で必要なライセンス等は保守事業者側での調達・費用負担を前提とする。

2.リモートアクセス保守運用セキュリティ(導入基準)

リモートアクセスでの保守サービスは、基本は障害時の対応、不具合調査、随時保守メンテナンスでの遠隔拠点からのリモートアクセスを利用したメンテナンスなどのスポット接続要求を前提とする。

システム開発及びシステム導入での常時接続での利用は禁止とする。

(1).保守サービスの開始と終了

・保守事業者からのリモートアクセス申請に基づき、本市システム担当が市側リモート保守端末の起動を行う。
・リモート保守拠点からの接続要求について、市側の運用として接続許可の操作を行う。
・保守事業者のリモートアクセス保守を開始する。
・リモートアクセス保守終了にて、保守事業者側からの操作切断を行う。
・保守事業者側からのリモート接続が終了した旨、本市システム担当へ連絡すること。
・本市システム担当者は、リモート保守端末の終了処理を行う。
※.夜間、休日作業の場合は市よりデータセンターへ作業依頼をする。（代替）
※.リモート接続を行った状態での端末放置や、不要な長時間の接続を原則禁止する。一定時間無操作となる場合、アカウントロックやセッションタイムアウト等の対策を講じること。

(2).リモートアクセス・保守サービスの申請と報告

・リモートアクセスを行う場合、以下事項を明確にして情報システムのシステム担当への申請を行う。
(アクセス期間(日付・時間)、操作目的、操作保守内容、対象サーバ、操作者、保守事業者責任者の承認、注意依頼事項)
・リモートアクセス・保守サービスを実施した後、その保守申請毎にその作業結果をまとめ報告を行う。
(実施時間、保守対応の具体的内容とその結果、継続するメンテナンスの有無、操作者、保守事業者責任者の承認、その他報告事項)
※.事故、障害、不具合の場合は、そのリモート操作報告とは別途、障害報告を行うこと。

(3).リモートアクセス・保守操作アクセスログ記録

・リモートアクセス保守にて、保守操作を行った場合、以下の措置毎にアクセスログ又は操作記録を行うこと。

- 資産適用又はシステム環境の変更 ・・・・・・・・・・・・ 資産適用操作台帳
- データベース環境を操作しての作業 ・・・・・・・・・・・・ 保守メンテナンス台帳
- データベースの内容変更(復元含む) ・・・・・・・・・・・・ データメンテナンス報告
- システム本番環境の操作(動作検証含む) ・・・・・・・・・・・・ システムアクセスログ
- 障害不具合調査及びリカバリー ・・・・・・・・・・・・ 障害報告に記録を記載

※.システムを操作する場合、操作者個別にシステムアカウントを作成しログイン操作を行うこと。
（事業者で一つのアカウントを使いまわししないこと。）

第 4 章　リモートアクセス環境の監査

リモートアクセスネットワークを導入しての外部からの保守事業者接続でのサービス導入を行うにあたり、セキュリティ安全対策として、導入時の環境及び運用に関する評価と定期的な運用及び設備の監査を実施する。

リスク分析と安全管理措置の締結された内容で、運用実態が遂行されているか、記録及びリスクアセスメントの対策が行われているか、現地の環境点検・視察を実施する。

又、点検・視察の結果として想定されるリスクが発生した場合、本市統括情報セキュリティ管理者より、リスクコントロール措置、厳守事項の違反に伴う是正措置、セキュリティ脅威への対策指示を保守事業者へ行う。

1 .リモートアクセスネットワークセキュリティの評価

(1).リスク分析と安全措置の締結

・事前に本市が示すガイドラインに沿った環境・設備に対するリスクアセスメントを分析し報告とする。

・ガイドラインに準拠する状態を示しその環境の報告と接触するリスクがある場合対策案を示し協議とする。

・リスク分析と安全措置の結果をもってリモートアクセス保守サービス導入の申請とする。

・本市、統括セキュリティ管理者と情報システム所管のセキュリティ管理者にて審査し結果をもって締結とする。

(2).セキュリティ事故時の措置

・セキュリティ事故(アクシデント)、セキュリティ違反(インシデント)が発生した時点で、リスク対策が行われ、その対策に対しての監査評価と審査されるまでのリモートアクセス保守サービスは凍結とする。

(3).技術的・制度的・セキュリティ脅威への対応

・可能な技術的(セキュリティ機器の導入)や制度的(環境・ルール・ペナルティー)な是正措置対策を速やかに行う。

・その内容をもって是正報告として申請、本市セキュリティ管理者にて判断し凍結したサービスの解除とする。

(4).導入時の事前環境監査(視察)

・本ガイドラインに従い申請された環境について、導入基準の監査を実施する。

・事前環境監査は、主要リモート拠点として、その拠点が変更される場合は再監査とする。

・例外として、既に他市同規模団体にてリモート保守サービスの実績がある場合、その実績にて監査を省略することができる。

第 5 章　事故・重大過失・違反時の措置

リモートアクセスネットワークを導入後に、セキュリティリスクを含むアクシデント(事故)又は、インシデント(重大過失、ヒヤリハット含む)が発生した場合の措置について協議すること。

又、監査・維持審査での不適合(違反)が発見された場合、速やかに是正・対策・改善を行うための是正措置に関する事項を以下にまとめる。

1 .セキュリティリスク発生時の措置

(1).セキュリティアクシデント・インシデント措置

・保守事業者に起因する原因でインシデントが発生した場合、本市がその対応で発生した実害の実費と SLA に準じたペナルティーを措置とする。

・保守事業者に起因する原因でアクシデントが発生した場合、本市及び影響する範囲(市民法人他)への賠償責任を含めた措置を命令する。

(2).監査・維持審査後の是正措置

・監査審査時に、不適合や運用違反などが判明した場合、必要な是正措置を示すこと。

・是正措置の内容に違反(期限超過)した場合は、サービス凍結を含めた対応を協議する。

改定一覧

No.	版数	改定日付	頁	改定内容	備考
1	第 1.0 版	令和２年 11 月 10 日	表紙 目次 １頁～15 頁	新規作成	
2	第 1.1 版	令和３年４月１日	表紙 ３頁	組織名変更 情報推進課→ＩＣＴ推進室	
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					

苫小牧市役所 Tomakomai City
〒053-8722 北海道苫小牧市旭町４丁目５番６号
TEL0144-32-6111(代表)