

名古屋市情報セキュリティ管理基準

令和5年3月24日策定
令和6年4月1日施行
名古屋市

改訂履歴

年月日	改定内容等
令和 5 年 3 月 24 日	初版策定（令和 5 年 4 月 1 日施行）
令和 6 年 3 月 27 日	クラウドサービス利用に係る規定の見直し等（令和 6 年 4 月 1 日施行）

目次

1	目的及び位置づけ	1
2	定義【市対策基準 2 関係】	1
3	適用範囲【市対策基準 4 関係】	1
4	組織体制【市対策基準 5 関係】	1
5	情報システム全体の強靱性の向上【市対策基準 6 関係】	2
	(1) マイナンバー利用事務系	2
	ア マイナンバー利用事務系と他の領域との分離	2
	イ 特定通信	2
	ウ 情報のアクセス及び持ち込み・持ち出しにおける対策	5
	エ マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの取扱	6
	オ マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱	7
	(2) LGWAN 接続系	8
	(3) インターネット接続系	10
	(4) その他のセキュリティ対策	10
	ア プリンター及び複合機の情報セキュリティ対策	10
	イ 専用回線サービスによる外部との通信	11
6	物理的情報保護対策【市対策基準 7 関係】	12
	(1) サーバー等の管理	12
	ア 機器の取付け	12
	イ 機器の外部施設等への設置	12
	ウ 機器の廃棄等	13
	(2) 管理区域（情報管理室等）の管理	15
	(3) 通信回線及び通信機器の管理	15
	(4) 職員の利用する端末や記録媒体等の管理	16
7	人的情報保護対策【市対策基準 8 関係】	19
	(1) 職員の遵守事項	19

(2) 研修・訓練.....	20
(3) ID 及びパスワード等の管理	21
8 技術的情報保護対策【市対策基準 9 関係】	22
(1) 情報システム及びネットワークの管理.....	22
ア ログの取得等.....	22
イ ネットワークの接続制御、経路制御等.....	22
ウ 外部ネットワークとの接続制限等.....	22
エ IoT 機器を含む特定用途機器の情報セキュリティ管理	23
オ 無線 LAN の情報セキュリティ管理.....	24
カ 電子メールの情報セキュリティ管理.....	24
キ データの暗号化等.....	25
ク ソフトウェアの資産管理.....	26
ケ 機器構成の変更の制限.....	27
(2) アクセス制御等.....	27
ア アクセス制御等.....	27
イ 外部からのアクセス等の制限.....	28
ウ 認証情報の管理.....	29
(3) 情報システムの開発、導入、保守等.....	30
ア 情報システムの調達.....	30
イ 情報システムの開発.....	30
ウ 情報システムの導入.....	30
エ 情報システムの開発・保守に関連する資料等の整備・保管	32
オ 情報システムにおける入出力データの正確性の確保	32
(4) 不正プログラム対策.....	33
(5) 不正アクセス対策.....	33
(6) 情報セキュリティに関する情報の収集等	36
9 運用【市対策基準 10 関係】	37
10 外部サービスの利用【市対策基準 11 関係】	38
11 情報セキュリティ監査（評価・見直し）【市対策基準 12 関係】	38

名古屋市情報セキュリティ管理基準

1 目的及び位置づけ

名古屋市情報セキュリティ管理基準（以下「市管理基準」という。）は、名古屋市情報セキュリティ対策基準（以下「市対策基準」という。）に記載されている事項について、その具体的な考え方や求められる措置等を記載したものである。

なお、市管理基準における用語の定義、適用範囲、組織体制等は、市対策基準に準拠するものである。

2 定義【市対策基準 2 関係】

- ・市対策基準 2 (10)における「インターネット接続系」とは、統括管理者が用意したLGWAN接続系からネットワーク分離されたインターネット領域（仮想デスクトップにてアクセスを行う領域）をいう。
- ・市対策基準 2 (12)における「外部サービス」の例としては以下が挙げられる。
 - クラウドサービス
 - ウェブ会議サービス
 - SNS（ソーシャルネットワーキングサービス）
 - 検索サービス、翻訳サービス、地図サービス
 - ホスティングサービス

3 適用範囲【市対策基準 4 関係】

- ・名古屋市立大学と教育委員会の一部は、市対策基準とは別に独自で対策基準等に相当する規定を策定しており、適用範囲には含んでいない。

4 組織体制【市対策基準 5 関係】

- ・市対策基準 5 (1)ウにおける「緊急事態対応計画」とは、名古屋市情報あんしん条例第25条第2項に規定する緊急事態対応計画をいう。
- ・市対策基準 5 (10)アにおける「やむを得ない場合」とは、特定の職員のみ認められた承認について、当該職員が申請する場合などをいう。
- ・市対策基準 5 (10)イにおける「やむを得ない場合」とは、代替する者がいな

い場合などをいう。

- ・市対策基準 5 (11)における「CSIRT」は、CSIRT設置要綱（令和元年6月1日策定）に基づき設置・運用している。

5 情報システム全体の強靱性の向上【市対策基準 6 関係】

(1) マイナンバー利用事務系

ア マイナンバー利用事務系と他の領域との分離

- ・市対策基準 6 (1)アにおける「マイナンバー利用事務系と他の領域との分離」とは、特定個人情報等の重要な住民情報の流失を防ぐ必要があることから、マイナンバー利用事務系とLGWAN接続系及びインターネット接続系等との通信をできないように論理的に分離することをいう。分離に当たっては、以下の事項を遵守すること。

①マイナンバー利用事務系と他の領域との端末等は分けなければならない。

②マイナンバー利用事務系とLGWAN接続系のサーバーが仮想化基盤上にあり、物理的なサーバーに共存する場合は、各系統の通信について、分離を徹底しなければならない。なお、地方公共団体が共同で利用するデータセンターに構築しているネットワークについても、庁内ネットワークとして同様の措置を行わなければならない。

イ 特定通信

- ・マイナンバー利用事務系において、外部接続先と通信をする必要がある場合は、以下の全ての措置を講じ、特定通信にて行われなければならない。また、あらかじめ統括管理者の許可を受けなければならない。

①L2SW/L3SW等による通信経路の限定（IPアドレス等）

②ファイアウォール等による通信プロトコル制限（ポート番号）

③外部ネットワークとの通信が発生する場合は専用回線サービス（IP-VPN、広域イーサネット、LGWAN等）にて接続

- ・外部接続先の対象は、十分に情報セキュリティが確保された通信先であり、具体的には以下の例が挙げられる。ただし、そのような場合であっても、後述の例外を除いて原則としてインターネット等と接続されてい

てはならない。

①住民基本台帳ネットワークシステム

②マイナンバー制度における中間サーバー連携

③住民票の写し等のコンビニ交付用のLGWAN接続

④LGWAN-ASPサービス

⑤データバックアップセンターや共同利用／クラウドセンター等

- ・インターネット等と接続される外部接続先でも、十分な安全性が確認されていると統括管理者が判断したものについては、接続を認めるものとする。これらの外部接続先と特定通信を行う場合、以下に定める方法による通信の限定を行わなければならない。

①外部接続先とは、連携サーバー又はプロキシを設置して通信を行うこととする。外部接続先からのデータやファイルは、連携サーバーを介してマイナンバー利用事務系と通信する。また、ファイアウォールやプロキシサーバー等でマイナンバー利用事務系から外部接続先に直接通信する経路が許可されないよう設定する。

②ファイアウォールや連携サーバーで外部接続先との通信を制限（FQDN指定）することで通信先を限定する。

③マイナンバー利用事務系のサーバー、端末については、マルウェア対策ソフトを導入し、最新の定義ファイルを常時更新する。また、OSの修正プログラムについても最新の修正プログラムを常時更新する運用や対策を行わなければならない。

④マイナンバー利用事務系のサーバーのOS等への修正プログラムの常時適用が困難な場合は、IPSやWAF等を用いて、脆弱性を悪用した攻撃を防ぐといった対処も考えられる。これらの対処においては、シグネチャの更新が必要な場合があるが、マイナンバー利用事務系においては、インターネットとの接続が出来ないため、シグネチャの更新方法（自治体情報セキュリティ向上プラットフォームの活用や媒体による手動更新等）を確認する必要がある。また、脆弱性を根本的に解決するためには、サーバーのOS等の修正プログラムの適用が必須となるため、これらの暫定的対処を行っている間に、修正プログラム適用の計

画、テスト、実施等を進める必要がある。

- ⑤悪意のあるソフトウェアや攻撃者は一つの脆弱性だけでなく、複数の脆弱性や、サーバー・ネットワークの設定不備等も組み合わせた上で攻撃を行う場合がある。そのため、サーバーの設定の確認（不要なポートを閉じる、サービスを停止させる等）を行うことや、ネットワークの通信ログの取得・監視等も重要な対策となる。
- ⑥住民の情報を扱う場合は、外部接続先とはTLSプロトコルを利用し、認証、暗号化、改ざんの検知等の対策を実施する。これらの対策に加え、ファイアウォール及び連携サーバーの通信の履歴等を取得することが望ましい。
- ⑦USBメモリ等の記録媒体により不正プログラムに感染する場合があるため、マイナンバー利用事務系の端末及び外部接続先との接続に利用する端末について、記録媒体の利用制御を実施しなければならない。
- ⑧ウェブアプリケーションを利用している情報システムの場合は、ウェブアプリケーションの実装面として脆弱性を作り込まない対策、定期的な診断などを行って脆弱性を検出・対処する対策が必要となる。
- ⑨外部接続先の仕様等により、①～⑧による措置が実現できない場合は別途統括管理者が指定した対策を実施する。

・マイナンバー利用事務系において遠隔地から保守を行う場合は、以下の事項を遵守すること。なお、マイナンバー利用事務系以外のオンプレミスシステムに対する遠隔保守についても本項の考え方に準じた対応を採用すること。

- ①通信は特定通信としての設定を行い、専用回線サービスを利用する。
- ②専用保守端末を用意し、他のネットワークに接続せず、持ち出し禁止とする。
- ③端末は本市と同等の保護措置を適用する。

※多要素認証、不要ソフトウェアインストール制限、ディスク暗号化、端末監視ソフトによるログ記録、外部記録媒体持ち出し無効化、OS更新、マルウェア対策、一定時間経過ロック等。

※端末は本市が直接管理（認証、ポリシー制御、パッチ配信等）するこ

とを推奨。

- ④端末及び作業エリアへのアクセス権限設定は必要最小限にする。
- ⑤作業エリアは、専用エリアを用意し、本市の管理者が許可した者以外立ち入り禁止とする。
- ⑥作業エリアは、監視カメラ、入退ログ等を駆使し入退室管理を徹底する。
- ⑦定期的に監査を行う。
- ⑧必要に応じて本市立ち入り調査することを含めた、委託先への要求事項を調達仕様書等に定め、契約条件とする。

ウ 情報のアクセス及び持ち込み・持ち出しにおける対策

- ・市対策基準 6 (1) ウ(イ)における「原則として」とは、納付書など大量帳票のアウトソーシングや指定金融機関に対する口座振替情報の提供、取り込み等の記録媒体の利用が止むを得ない場合を例外として想定するものである。その場合においては、管理者権限を持つ職員によってその都度限定を解除する又は管理者権限を持つ職員のみ許可する設定とすることを例外として取り扱わなければならない。
- ・USBメモリ等の記録媒体による端末に対する情報の持ち込み持ち出しを行う場合は、次の手段により実施しなければならない。
 - ①端末には利用許可された専用の記録媒体のみ接続すること。
 - ②マイナンバー利用事務系の端末に記録媒体を挿抜する前の段階で、一度記録媒体に対してマルウェアチェックを実施すること。この際、チェックを行う端末は万一侵害が発生しても問題が無い独立した環境にあることが望ましい。また、zip等で暗号化されている場合、解凍しなければ有効なチェックができない場合もあることに留意する。
 - ③データ又は記録媒体を適切に暗号化すること。
 - ④利用媒体は、全て管理し利用履歴を残すこと。また、利用後は速やかに内容を消去すること。
 - ⑤データの受け渡し時は、端末等管理者の承認と承認記録を残すこと。
- ・特定通信の許可を受けた接続先以外の外部等（許可が得られないLGWAN-ASP及びインターネット上の接続先等）について、止むを得ずデータをや

り取りする場合は、外部のネットワークと通信する専用の端末を管理区域内に設置した上で、必要最小限の通信とし、記録媒体を経由したデータのやり取りを行わなければならない。その際には、他の職員の立ち会い又は監視カメラで撮影された状態で、管理区域内において作業を行うなどの取扱いを行わなければならない。

エ マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの取扱い

- ・ 情報システムの稼働において必須となる通信について（OS等の修正プログラム、マルウェア対策ソフトのパターンファイル更新、ソフトウェアのアクティベーション）インターネットと通信が必要な場合は、先述の特定通信の要件を満たす必要がある。その上で通信の中継方法について留意する点として、クラウドサービス上のマイナンバー利用事務系と異なる新たなネットワーク（DMZ）を構築し、そのネットワーク内に連携サーバー（修正プログラム及びマルウェア対策ソフト等の更新サーバー）を配置した上で限定された通信の設定（FQDNのホワイトリスト設定やファイアウォール（FW）によるクラウドサービス上に構築したクライアント及びサーバー等からインターネットへのアウトバウンド通信の制御・インターネットからクラウドサービス上に構築したクライアント及びサーバー等へのインバウンド通信の禁止）を行うとともに、不正なアクセスが無いか日常的な監視（通常時のネットワークトラフィックの状態と異なる場合は、異常と判断し詳細を確認する等）を徹底する。また、これら対策が適切に実施されているのか、運用前に事前テストを実施し、確認するとともに、定期的に監査（内部監査又は外部監査）を行うこと。
- ・ クラウドサービスの管理コンソールは、例外的にインターネット経由でアクセスすることが許容されるが、以下の要件を満たす必要がある。
 - ①ユーザー認証を多要素とする。（②は要素として計上不可）
 - ②端末認証（MAC アドレス、シリアル番号及び電子証明書等）又は接続する機器や拠点のIPアドレス等の認証情報を利用し接続元を制限する。
 - ③操作履歴などの監査ログを取得し、適切に管理する。

- ④アクセス者に対して必要最小限の権限設定を行う。
- ⑤外部委託で管理を行う場合、委託先の情報セキュリティ対策が確実に実施されるよう委託先への要求事項を調達仕様書等に定め契約条件とするとともに、当該条件が遵守されているか、委託先を定期的に確認（運用開始前を含む。）し、遵守していない場合には、職員等が委託先に適切に指導を行う。
- ⑥管理コンソールからは特定個人情報を含む本番業務データにアクセスできないような措置を講ずる。

オ マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱

- ・クラウドサービス（ガバメントクラウドを含む。）との情報のやり取りにおいては、情報の転送時、保存時又は実行時など、それぞれの状況において機密性に応じたセキュリティ対策を実施する必要がある。特に機密性の高い情報を転送又は保存する場合は、暗号化を行い情報漏えいや情報の盗み見等のリスクに対応する必要がある。また、クラウド基盤上で処理が実行されている状態では、原則として暗号化されない状態で処理されるため、メモリ領域や記憶領域に残留データとして残ることがある。このため、処理が終了した時にメモリ領域や記憶領域に残留データが残らないように領域を開放しているか、クラウドサービスの利用前に仕様や動作を確認するなど注意が必要である。なお、暗号化には、通信の暗号化とデータの暗号化があり、この両方を十分な強度の暗号を用いて実施する必要がある。また、クラウドサービスにおいては、データが分散されて保存される場合がある。予め提供されるサービスの仕組みを確認し、その仕組みに応じて、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」の「電子政府推奨暗号リスト」中で推奨された暗号利用モードで暗号化されるのか確認する。なお、通信の暗号化については、通信元と通信先それぞれでサポートしている暗号の違いにより、意図しない脆弱な暗号が使われる、通信が失敗するといったリスクがある。これを避けるためには、クラウドサービス側だけでなく、その通信先（回線事業者や庁内の通信機器等）でも「電

子政府推奨暗号リスト」中の暗号をサポートしているかを確認する必要がある。またあわせて、「運用監視暗号リスト」にあるものが有効になっていないかも確認すること。可能であれば、実際の通信から、想定した暗号で暗号化されているかを確認することが望ましい。

(2) LGWAN接続系

- ・ LGWAN接続系とインターネット接続系の分離とは、一旦両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにすることをいう。また、電子メールやファイル等をLGWAN接続系に取り込む場合の実現方法等に関しての留意事項などは以下のとおりである。

①インターネット環境で受信した電子メールの本文のみをLGWAN接続系に転送するメールテキスト化方式

- LGWAN接続系へ電子メールを転送する際には、電子メールの転送に必要な特定サーバー間以外の通信を遮断するとともに、LGWAN環境とインターネット環境はSMTP以外のウェブ通信を始めとするプロトコルを遮断し、電子メールの添付ファイルの削除及びHTMLメールのテキスト化を行う。

②インターネット接続系の端末から、LGWAN接続系の端末へ画面を転送する方式

- インターネット接続系の端末を仮想デスクトップ化し、LGWAN接続系の端末から添付ファイルを含む電子メールの閲覧を可能とする。

③危険因子をファイル等から除去し、又は危険因子がファイル等に含まれていないことを確認し、インターネット接続系から取り込む方式

- 危険因子が埋め込まれたファイル等をLGWAN接続系に取り込んだ場合、脆弱性を突いた悪意あるコード等が実行される恐れがある。インターネット接続系からLGWAN接続系にファイル等を取り込む際は、以下のような手法により、危険因子をファイル等から除去又は危険因子がファイル等に含まれていないことの確認を行った上で、取り込まなければならない。

(いずれかの手法のみ又は複数の手法を組み合わせ採用することが考えられる。)

- ・ファイル等からテキストのみを抽出
- ・ファイル等を画像又はPDFに変換
- ・サービス等を活用してサニタイズ処理（ファイル等を一旦分解した上で危険因子を除去した後、ファイル等を再構築し、分解前と同様なファイル形式に復元する）
- ・インターネット接続系において内容を目視で確認するとともに、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等で危険因子が含まれていないことを確認

なお、上記のいずれか又は複数の手法による対策を実施した場合であっても、マルウェア等の除去が完全に保証されるものではないため、LGWAN接続系において以下のようなセキュリティ対策を実施しなければならない。

- ・OS等の修正プログラムの適時適用
- ・マルウェア対策ソフトの適時更新
- ・業務に必要なファイルや電子メール等の定期的なバックアップ
- ・LGWAN接続系において外部サービスを利用する場合は原則としてLGWAN-ASPを利用することになるが、LGWAN回線のトラフィック制約等によりLGWAN-ASPでは対処できない場合、セキュリティ上のリスクを勘案し、関連部門と協議した上で、例外的にインターネット上の外部サービスに対しローカルブレイクアウト接続を行うことができる。接続に当たっては以下の要件を遵守すること。
 - ①対象サービスをローカルブレイクアウト接続しなければならない妥当な理由があること。
 - ②対象サービスは十分な信頼がおける接続先であること。具体的には第三者機関により妥当なセキュリティ評価、認証制度（ISO/IEC15408、21017、27018、ISMAP等）を受けていることを検討材料とする。
 - ③インターネットとの境界における通信機器を適切に設定すること。具体的には、接続元IP、接続先IP、ポート番号、TCP/UDP、インバウンド/アウトバウンド通信、ステートフル制御について、通信先と必要最小限の通信に限定することを徹底する。
 - ④通信機器の設定管理に係るアカウント設定及び運用について、権限を持

たない職員等から徹底的に分離、秘匿する。管理セグメントについては物理的論理的に専用の端末、エリアに限定することが望ましい。

- ⑤不正なアクセスや設定変更等が無い、通信機器について不審な挙動を検知できる仕組み、体制を構築すること。
- ⑥これら対策が適切に実施されているのか、運用前に事前テストを実施し、確認するとともに、定期的に監査（内部監査又は外部監査）を行うこと。

(3) インターネット接続系

- ・インターネット接続系で実施する情報セキュリティ対策の内容は具体的には以下のものがある。

①サーバー等の監視

- ウェブサーバー、メールリレーサーバー、プロキシサーバー、外部DNSサーバーのログの監視

②情報セキュリティ機器の導入

- 通信パケットの監視及び破棄、通信ポートの制御、不正なプログラムの検知、不審な電子メールの検知及び遮断、不審なURLへのアクセス遮断、ログ監視、コンテンツの改ざん検知等の機能を持った高度な情報セキュリティ機器の導入

③情報セキュリティ運用監視

- 情報セキュリティ専門人材による高水準な情報セキュリティ運用監視

(4) その他のセキュリティ対策

ア プリンター及び複合機の情報セキュリティ対策

- ・プリンター及び複合機は、必要に応じてマイナンバー利用事務系、LGWAN接続系、インターネット接続系のネットワーク毎に設置されることが望ましい。ネットワーク間で共有する場合には、1台のプリンター・複合機にネットワーク毎に専用のLANポート等を設け、他の領域と分離された通信を保証する必要がある。それが困難である場合には、ネットワークの一方をLANポートに、もう一方はUSBポートに繋ぐ等の方法を検討する。ただし、共有する場合においてもマイナンバー利用事務系又はLGWAN

接続系について、インターネット接続系と共有することは認められない。

イ 専用回線サービスによる外部との通信

- ・遠隔での情報システム保守により、マイナンバー利用事務系及びLGWAN接続系について通信を許可する場合は、特定通信としての設定がされており、かつIP-VPN等の閉域網又はLGWANで接続されなければならない。

6 物理的情報保護対策【市対策基準 7 関係】

(1) サーバー等の管理

ア 機器の取付け

- ・市対策基準 7 (1) アにおける「影響を可能な限り排除した場所」とは、以下の措置が講じられた場所をいう。
 - ①耐震・免震…耐震又は免震構造である。
 - ②防火…情報管理室内に容易に燃える物品を持ち込まないようにしている。水などの液体を用いず、二酸化炭素等を利用した消火設備がある。
 - ③防水…水を使用する設備（洗面所等）と区分された構造である。飲み物の持ち込みを禁止している。
 - ④防じん…定期的に清掃を行うこととしている。食べ物の持ち込みを禁止している。
 - ⑤温度・湿度…専用又は適切な規模・機能の空調設備を設置している。
- ・市対策基準 7 (1) アにおける「必要な措置」とは、市対策基準に記載の事項のほか、以下の措置をいう。
 - ①床面に頑強に固定された施錠可能な保管庫内に設置し、平常時は施錠している。
 - ②夜間等無人となるときは情報管理室を施錠している。
 - ③やむをえず情報管理室外に設置する場合、保管庫の鍵について、個人を特定した上で情報システム管理者などの許可を得なければ使用できない運用としている。

イ 機器の外部施設等への設置

- ・市対策基準 7 (1) カにおける「対策の実施状況」の確認は、以下の点を踏まえ実施すること。
 - ①受託者等を定期的に訪問し、定期報告では把握しきれない設置室内の状況の変化、当該受託者等の要員の変化等を把握する。
 - ②地方公共団体職員によるデータセンター内部への立入りがデータセンターのセキュリティポリシーに違反する等、受託者等を訪問できない場合は、訪問調査に代えて第三者による情報セキュリティ監査報告

書、受託者の内部監査部門による情報セキュリティ監査報告書等によって確認する。

ウ 機器の廃棄等

- ・ 市対策基準 7 (1) キにおける「必要な措置」とは、以下のことをいう。
 - 機器が不要になった場合やリース会社へ返却等を行う場合には、機器内部の記録媒体からの情報漏えいのリスクを軽減する観点から、情報を復元困難な状態にする措置を徹底する必要がある。この場合、一般的に入手可能な復元ツールの利用によっても復元が困難な状態とすることが重要であり、OS及び記録媒体の初期化（フォーマット等）による方法は、記録媒体の記憶演算子にはデータの記憶が残った状態となるため、適当でないことに留意が必要である。また、原則として以下の表に記載されている方法により、記録されている情報の機密性に応じて、情報システム機器の廃棄等を行わなければならない。

【機器の廃棄等について】

分類	機器の廃棄等の方法	確実な履行を担保する方法
(1) マイナンバー利用事務系に属する機器のうち、住民情報を保存する、又は保存したことがある記憶媒体	当該媒体を分解・粉碎・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすること。 (NIST SP800-88「破壊」に相当) リース契約により調達する場合においても、契約終了後、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記すること。	職員自身が実行する。 業者委託する場合は、職員が左記措置の完了まで立ち会いによる確認を行う。 又は、庁舎内において後述(3)で記述する方法でデータの消去を行った上で、受託者等に引き渡しを行い、写真その他の証拠を添えた証明書等により確認する。証明書等については、提出期限が定められていることが望ましい。なお、職員による左記措置の完了までの立ち会いについては、委託先事業者の作業状況が確認出来る場合、カメラによるリアルタイムでの監視やカメラ映像の記録の確認などで代替できる。
(2) 機密情報を保存する、又は保存したことがある記憶媒体(上記(1)に該当するものを除く。)	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うこと。(NIST SP800-88「除去」に相当) 具体的には、以下の方法が挙げられる。 ①物理的な方法による破壊 ②磁気的な方法による破壊 ③データ消去装置又はデータ消去ソフトウェアによる上書き消去(OS等からのアクセスが不可能な領域も含めた領域) ④ブロック消去 ⑤暗号化消去	職員自身が実行する。 業者委託する場合は、職員が左記措置の完了まで立ち会いによる確認を行う。 又は、写真その他の証拠を添えた証明書等により確認する。
(3) 機密情報を保存したことが無い記憶媒体	データ消去ソフトウェアによる上書き消去(OS等からアクセス可能な全てのストレージ領域)を行う(NIST SP800-88「消去」に相当)、又は(2)に記述した方法でもよい。 なお、OS及び記録媒体の初期化(フォーマット等)による方法は、適当ではない。	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。
<p>※上記(1)は、オンプレミスの場合を想定したもの(ハウジングやプライベートクラウドを含む)。</p> <p>※「写真その他の証拠を添えた証明書等」とは、消去作業の実施日、実施者、対象機器一覧、消去方式が記載され、消去方式が物理的破壊・磁気的破壊・消去装置による消去の場合はハードディスクのシリアル等が写った本体又は消去作業等の写真、ソフトウェアによる消去の場合は対象機器一覧が含まれて出力されるログ・レポート・消去作業時の操作画面ハードコピー等が添付された証明書又は報告書等が相当する。</p> <p>※抹消処理方法についてはNIST SP800-88も併せて参照されたい。</p>		

(2) 管理区域（情報管理室等）の管理

- ・市対策基準 7 (2) イ (ウ) における「外部からの訪問者」とは、施設に設置している設備等の保守・点検を行う者や機器等の搬出入を行う者などを行う。
- ・市対策基準 7 (2) イ (ウ) における「許可された職員の立会い等の措置」とは、職員の立会いのほか、監視カメラによる監視などを想定している。
- ・市対策基準 7 (2) イ (エ) における「原則として」とは、業務上やむを得ない事情等により管理区域の管理者が認める場合を例外として想定するものである。
- ・民間データセンターを利用する場合は、日本データセンター協会が制定する「ファシリティスタンダード」のティア3以上であれば市対策基準に記載する情報管理室に関する物理的情報保護対策を満たすものと判断してよい。

(3) 通信回線及び通信機器の管理

- ・市対策基準 7 (3) ア における「通信回線及び通信機器に関連する文書」とは、通信回線敷設図、結線図、ネットワーク構成図、通信回線等の文書をいう。
- ・市対策基準 7 (3) ウ における「集約」とは、独立ネットワークやドメインは最小限にして、可能な限り安全性の高い名古屋市行政情報ネットワークにて一元管理することを目的とするものである。ただし、情報システム等の性質や運用上、集約しないことでより高い情報セキュリティを確保することが可能となる場合はこの限りではない。
- ・市対策基準 7 (3) エ における「適正な回線を選択」について、以下の取り扱いとする。
 - ①「適正な回線」とは、専用線、広域イーサネット、IP-VPN、閉域SIM回線などの専用回線サービスをいう。マイナンバー利用事務系及びLGWAN接続系は原則として、これらの回線のみ利用可能とする。
 - ②インターネットVPNを利用する場合は、適切な認証及び暗号化を実施すること。VPNルーター等の機器及びソフトウェア等について、脆弱性を把握できる体制を整えるとともに、脆弱性が判明した場合は即座に対応する

ファームウェア等を更新するか、接続を切る等の対応を行うことを徹底したうえで利用すること。

③インターネット回線の利用は、適切な暗号化を施したうえで、以下の場合に限り情報システムの回線として利用可能とする。

- 監視カメラ等の映像通信サービスを利用する場合
- 対策基準 9 (1) クの特定用途機器により通信する場合
- ウェブサイト等インターネット回線上の情報システムへ保守等のために接続する場合で、接続認証の徹底（原則多要素認証を実施し、接続元IP制限やロックアウト等も併用することが望ましい）を行う場合

(4) 職員の利用する端末や記録媒体等の管理

- ・市対策基準 7 (4) アにおける「措置」とは、以下のことをいう。
 - パソコンやNAS、外付けハードディスクなど、執務室等で固定して利用する端末等は、ワイヤーによる固定又は持ち出しできないラック等に格納し施錠管理するなどの適切な対策を行うこと。
 - モバイル端末（フリーアドレス等で利用する小型ノートパソコン、ハンディターミナル、スマートフォン等）や外部記録媒体など、持ち運びでの利用を前提とし、固定等による管理が困難な端末等は、利用時以外の保管庫等における施錠管理を行うこと。また、利用している最中は目を離れた状態で放置しない等、職員の管理下における運用を徹底すること。
- ・市対策基準 7 (4) イにおける「別に定めがあるもの」とは以下の規定等という。

（外部記録媒体）

- 各局区室で定めている外部記録媒体利用基準

（NAS）

- NASの導入・運用に関するガイドライン

- ・市対策基準 7 (4) ウ、エにおける「設定」に当たっては、以下のことに注意等する必要がある。

①認証手段の具体例としては、以下のとおりである。

【認証の種類と手段】

種類	認証の手段・具体例
知識	正規の利用者“だけが知っている情報（知識）”をその人が知っているか否かで判断する。 例：パスワード、パスフレーズ、PIN、暗証番号
所持	正規の利用者“だけが持っているモノ（所持品）”をその人が持っているか否かで判断する。 例：ICカード、USBトークン、SIMカード、電子証明書
存在	正規の利用者の“身に備わっている特徴（利用者自身の存在）”でその人か否かを判断する。 例：バイオメトリックス認証（指紋、声紋、静脈、顔等）

②知識による認証においてパスワード等の数字等を組み合わせた方法を用いる場合は、十分な複雑性を持った設定とすること。具体的には以下を推奨する。

- オフライン環境等で回線速度や回数制限等の制限なくパスワードの高速解析が可能な状態（Wi-Fi機器の暗号化キー、パスフレーズ、Word等ファイル単体やZIP等に設定した保護パスワード等）の場合、英大文字小文字・数字・記号の3種類以上を組み合わせ、20桁以上であること。
- 回数制限により、一定数認証に失敗するとアカウント・データへのアクセスに対してロック（時間経過では解除不可能）又は初期化（ワイプ処理）がかかる場合、6桁以上であること。ただし、ゾロ目や連番、記念年月日、業務で連想しやすい数字（3739=南区 等）を含む等のような容易に予想できるものは除く。
- 上記以外の場合、英大文字小文字・数字・記号から3種類以上を組み合わせ、10桁以上であること。

③所持又は存在による認証においても必要に応じて複数回の認証失敗をした場合にロックをかけることを推奨する。なお、認証方法によっては、指紋の摩耗等により複数回の認証失敗が見込まれる場合もあるため、柔軟な対応ができるよう適切な回数制限又は代替措置を適宜検討すること。

- ・市対策基準7(4)カにおける「十分な情報セキュリティ」とは、全庁ドメインのパソコン管理用ドメインで管理される端末で、認証ドメインの個人認証を利用する場合又はそれに準ずる措置を行っていることを想定してい

る。この場合、業務に必要な最小限度に限り保存することができる。

- ・市対策基準 7 (4) キにおける「確認」について、具体的には月に一回以上、所在や設定の不正な変更・データ保存の有無等を確認すること。

7 人的情報保護対策【市対策基準8関係】

(1) 職員の遵守事項

- ・市対策基準8(1)ウにおける「所管課長の許可」とは、外部に持ち出す情報に機密情報を含む場合は、名古屋市情報あんしん条例規則第32条第2号及び第3号の許可をいう。また、機密情報を含まない場合であっても、出張命令などと合わせて、許可を受ける必要がある。
 - ・市対策基準8(1)ウにおける「外部」とは、執務室のある庁舎の外をいう。
 - ・市対策基準8(1)ウにおける「必要な措置」とは、以下のことをいう。
 - ①持ち出す情報は、必要最小限とする。
 - ②施錠可能なかばん等を使用し、ひったくり等に注意を払いながら手元から離さないように常に携行する。
 - ③公共の場又は公共の乗り物内においては原則として機密情報を取り扱ってはならない。
 - ④のぞき見を防止するため、外部において職員等以外の目に触れないように取り扱わなければならない。
 - ⑤不正使用を防止するため、使用しないときは他者に端末等が使用されないように中断時は画面をロックし、認証に必要な所持品（ICカード等）がある場合は取り外す等の必要な対策を取らなければならない。
 - ・市対策基準8(1)ウ、エにおける「許可」とは、行政文書による決裁を想定している。
 - ・市対策基準8(1)エ(ア)における「措置」とは、以下のことをいう。
 - 支給以外のパソコン及びモバイル端末に市が保有する情報を保存してはならない。
- ※外部への持ち出し及び利用に当たっては、市対策基準8(1)ウに定める盗難等を防止するための必要な措置を講じること。
- ・市対策基準8(1)エ(ア)のただし書きの場合であっても、市のネットワークに接続してはならない。
 - ・市対策基準8(1)エ(ア)及び(イ)における「許可」とは、局区等における情報の保護対策に関する運用要項の様式6「支給以外の端末使用許可簿」等の行政文書による決裁を想定している。

- ・市対策基準 8 (1) エ(ア)において、許可を行った所管課長は、許可した端末の利用状況等を定期的に確認するとともに、当該職員が情報セキュリティポリシーを遵守するように必要な教育等を実施しなければならない。
- ・市対策基準 8 (1) エ(イ)における「措置」とは以下のことをいう。
 - 端末ロック設定を適切に行う。
 - マルウェア対策を適切に実施する。
 - OSの脆弱性対策を適切に実施する。
 - ファイル共有機能を有するアプリ又はソフトウェアは導入しない。
 - 第3者への貸与を禁止する。
 - 特定個人情報を取り扱わない。
 - 不正アプリのインストールを制限する。
 - 公衆無線Wi-Fi又は脆弱性を抱えたままの無線Wi-Fiを利用しない。
 - 業務利用するアプリ等は、端末に機密データを保存できない（スクリーンショット・ローカルコピー禁止をする等）ものを利用する。
 - 業務利用するアプリ等は、通信内容が適切に暗号化処理されるものを利用する。
 - 業務利用するアプリ等は、アプリ等自身の利用、又はアプリ等上で機密情報にアクセスする際に、利用者認証を的確に行うことができるものを利用する。
 - 業務利用する必要がなくなった場合は、支給以外のパソコン及びモバイル端末から業務に関係する情報やアプリ等を削除する。
- ・市対策基準 8 (1) オにおける「記録」とは、機密情報を含む場合は、名古屋市情報あんしん条例規則第32条第2号及び第3号の許可に係る記録をいう。また、機密情報を含まない場合であっても、出張命令などと合わせて記録を作成する必要がある。

(2) 研修・訓練

- ・市対策基準 8 (2) イにおける「訓練」について、特に情報システムが停止した場合に市民や複数の部署に影響を及ぼすようなことが想定される重要性が高い情報システムは、障害時等において迅速な対応が求められることから、定期的な訓練の実施に努める必要がある。訓練の実施に当たっては、

ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、効果的に実施するように努める必要がある。

(3) ID及びパスワード等の管理

- ・市対策基準 8 (4) イ (ア) ③における「十分な複雑性」は、市管理基準の「6 物理的情報保護対策 (4) 職員の利用する端末や記録媒体等の管理」の推奨方法を参照すること。

8 技術的情報保護対策【市対策基準 9 関係】

(1) 情報システム及びネットワークの管理

ア ログの取得等

- ・市対策基準 9 (1) エ(ア)における「アクセスログ」では、ID、IPアドレス、対象となった個人名、その項目の情報、利用日時、アクセス行為の種類（閲覧、入力、変更、削除、印刷、ファイル出力（情報の複製））及びアクセスが失敗したこと等を記録することを推奨する。
- ・市対策基準 9 (1) エ(ア)における「その他ログ等」とは、端末操作ログのほか、情報システム稼働ログ、障害時の情報システム出力ログ、障害対応記録などをいう。
- ・市対策基準 9 (1) エ(ア)における「ログ」は、原則として 1 年以上保管することが望ましいが、情報システムが遵守すべき法令等によって保管期間が定められている場合もあるため、関係法令等を確認の上、決定する必要がある。なお、特定個人情報へのアクセスログは、名古屋市における特定個人情報の適正な取扱いに関する方針に基づき、7 年間保存する必要がある。
- ・市対策基準 9 (1) エ(ウ)に記載の「点検又は分析」では、該当する情報システムにおいて、以下の対応を実施すること。
 - ①機密情報を取り扱う情報システムにおいて、定期的に及び必要に応じ随時に、異常なアクセス数、データ量の通信等の有無を確認する。
 - ②特定個人情報を取り扱う情報システムにおいて、定期的に及び必要に応じ随時に、不正アクセス等の検知を行う。

イ ネットワークの接続制御、経路制御等

- ・市対策基準 9 (1) カ(ア)において、ネットワーク上では、フィルタリング、ルーティング、侵入検知システム等が機能しているが、これらの機能を十分活用するため、ハードウェア及びソフトウェアの設定を適正に行うよう注意する必要がある。

ウ 外部ネットワークとの接続制限等

- ・市対策基準 9 (1) キにおける「外部ネットワーク」とは、本市が所管するネットワーク（データセンター等の本市領域に接続する専用回線等も含

む。)を除いたネットワークをいう。具体的には、インターネット、LGWAN、SINET(学術情報ネットワーク)等が該当する。

- ・市対策基準9(1)キ(ア)における「対応」としては、事前に十分な技術的調査を実施し、障害時に物理的又は論理的に遮断が可能なこと等を契約書等に記載すること等が挙げられる。
- ・市対策基準9(1)キ(ウ)について、具体的にはネットワーク等を構成する各種機器等の脆弱性情報を継続的に把握し、脆弱性が判明した場合は対応するファームウェアのアップデート等の適切な対応が実施できるよう努めなければならない。

エ IoT機器を含む特定用途機器の情報セキュリティ管理

- ・市対策基準9(1)クにおける「特定用途機器」とは、テレビ会議システム、IP電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の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記録媒体を内蔵しているものをいう。これらの機器についても当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により想定される脅威に注意が必要である。例えば、テレビ会議システム、IP電話システム等は本市が所管するネットワーク等を経由してインターネットに接続されて利用されることが想定され、その場合外部からの攻撃対象となり得る。これらのIoT機器等の脆弱性がサイバー攻撃の標的となることが懸念される。また、内蔵記録媒体を備える場合は、運用終了時に内蔵記録媒体に残された情報が漏えいするおそれがある。そのため、特定用途機器の特性に応じて、以下の対策を講じる必要がある。
 - 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点を有す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、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。
- 特定用途機器を廃棄する場合は、特定用途機器の内蔵記録媒体を市対策基準 7 (1) キに基づき適切に廃棄等行う。

オ 無線LANの情報セキュリティ管理

- ・ 市対策基準 9 (1) ケにおける「無線LAN」の脅威として、無線電波の解析による通信内容の盗聴、なりすましアクセスポイント (AP) などによる情報漏えいや、認証の隙を突いた不正アクセス等がある。それらの対策として適切な対応を行う必要がある。
- ・ 暗号方式については、脆弱性を抱える方式を採用してはならない。現時点 (令和5年3月時点) においてはWPA2 (ただしTKIPを除く。) 又はWPA3が候補である。
- ・ 無線機器設定については、アクセスポイントの管理者パスワードを適切に設定 (強固なID・パスワードの設定、アクセスポイント単位での管理) するとともに、無線端末間の通信が行われないう適切な設定 (プライバシーセパレータ機能等) を行わなければならない。
- ・ 認証方式については、LGWAN接続系のようなネットワーク内において機密情報を蓄積する情報システム等を保有するネットワークで無線LANを利用する場合は、認証サーバーを利用したエンタープライズによる認証 (IEEE802.1X認証) を採用しなければならない。それ以外において、同一SSID内で認証鍵を共有するパーソナル認証を採用する場合は、SSIDパスフレーズに十分な複雑性を持たせなければならない。
- ・ 市対策基準 9 (1) ケにおける「副統括管理者による点検」とは、市対策基準 10 (2) イの「情報セキュリティ対策に関する点検」をいう。

カ 電子メールの情報セキュリティ管理

- ・ 市対策基準 9 (1) コ (ア) における「必要な措置」とは以下のことをいう。
 - 外部からの電子メール受信及び外部への電子メール送信においてなりすましを防ぐため、電子メールサーバーの情報セキュリティ対策とし

て電子署名を用いたDKIM (DomainKeys Identified Mail) やSPF (Sender Policy Framework) 等の対策を実施すること。

- 電子メールの不正な中継を行わないように電子メールサーバーを設定すること。
- インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、必要に応じて、SMTPによるサーバー間通信をTLSによる保護や、S/MIME等の電子メールにおける暗号化及び電子署名の技術の利用等、電子メールのサーバー間通信の暗号化の対策を検討すること。
- 職員等が電子メールの送信等により情報の外部への不正な持ち出しをしていないか監視するために、必要に応じてフィルタリングソフトウェア等の導入を検討すること。

キ データの暗号化等

- ・ 市対策基準 9 (1) シ(ア)について、インターネット接続系のファイル転送サーバーを利用することができないネットワーク環境にある場合等、別途用意されたセキュアなファイル共有サービス等の利用を妨げるものではない。
- ・ 市対策基準 9 (1) シ(イ)における暗号化に際しては、暗号技術検討会及び関連委員会 (CRYPTREC) により安全性及び実装性能が確認された「電子政府推奨暗号リスト」の方式 (暗号技術) を用いること。なお、方式によっては求められる鍵長を満たさないと当該リストの基準を満たさないものがある (同CRYPTREC「暗号強度要件 (アルゴリズム及び鍵長選択) に関する設定基準」参照) ことに留意すること。例えば、2040年までの利用想定ならば、情報セキュリティ強度要件としては128ビットセキュリティ以上が必要となるため、公開鍵暗号であれば鍵長3072ビットのRSA、共通鍵暗号であれば鍵長128ビットのAES、ハッシュ関数であればSHA-256などが選択肢となる。
- ・ 暗号化に際してパスワードを設定する場合は、十分な複雑性を持たせること。具体的には市管理基準の「6 物理的情報保護対策 (4) 職員の利用する端末や記録媒体等の管理」の推奨方法を参照すること。
- ・ 具体的な方法の例としては、以下のようになる。

①圧縮ソフト（7-Zip等）でzipファイルを暗号化する場合

- 暗号化方式は、「AES-128」か、より情報セキュリティ強度（ビットセキュリティ）が高い「AES-256」等を選択する。Windows等の標準でサポートされている方法「ZipCrypto」では情報セキュリティ強度が低い
ため、推奨されない。
- パスワード設定は、英大文字小文字・数字・記号の3種類以上を組み合わせ、20桁以上を推奨する。

②Word、Excel等のOfficeファイルを暗号化する場合

- 暗号化方式は、現時点（令和5年3月時点）でサポートされているOfficeソフトにて暗号化する場合「AES-128」以上になるため、暗号化方式に関する要件を満たす。
- パスワード設定は、英大文字小文字・数字・記号の3種類以上を組み合わせ、20桁以上を推奨する。
- ・ パスワードを送信先の相手に知らせる場合、原則としてファイルの送付手段とは別の方法を用いることを推奨する。例えば、電子メールにファイルを添付した場合、その電子メールに返信する形でパスワードを送付してはならず、電話、別の電子メールアドレス、セキュアなチャットツール、事前の取り決め等により共有すること。

ク ソフトウェアの資産管理

- ・ 市対策基準 9 (1) スにおける「ソフトウェアの資産管理」の実施に当たっては、情報システム導入・運用ガイドライン（ソフトウェア資産管理編）も踏まえ、適切に対応を行うこと。
- ・ 市対策基準 9 (1) ス(ア)における「管理」に当たっては、クラウド基盤上でシステム等を構築する場合は、ソフトウェアによっては、オンプレミス用とクラウド用でライセンス体系が異なる場合があるため留意すること。オンプレミス環境で使用しているソフトウェアをクラウド環境でも利用する際は、改めてライセンスの体系や条項を確認し、ライセンス違反とならないよう注意する必要がある。
- ・ 市対策基準 9 (1) ス(ウ)における「許可」に当たっては、当該ソフトウェアの情報を収集し、必要に応じて試験環境を構築し、動作確認を行うな

どし、あらかじめ不正プログラムの感染、侵入及び外部への不正な通信等の恐れがないことを確認するとともに、既設のソフトウェアに不具合が発生しないことを確認する必要がある。

ケ 機器構成の変更の制限

- ・市対策基準 9 (1) セ(イ)における「許可」に当たっては、当該機器の情報を収集し、必要に応じて試験環境を構築し、動作確認を行うなどし、既設のパソコンやネットワークに不具合が発生しないことを確認する必要がある。

(2) アクセス制御等

ア アクセス制御等

- ・市対策基準 9 (2) ア(ア)について、NASの利用に関しては、今後インターネット接続系が主体となる次期分離モデルへの移行も見据えて令和8年5月以降は、一定の情報セキュリティ要件を満たす場合を除き原則利用禁止とする予定である（全庁ドメインにおいてはR7年3月以降、次期全庁ドメイン対応ファイルサーバーへ統合予定）。
- ・市対策基準 9 (2) ア(イ)②について、やむを得ず共用IDを利用する場合は、利用者を把握するとともに、異動や退職によりアクセス権限を失うべき者が当該IDのパスワード等を把握したまま異動等するような場合は速やかにパスワードを変更するなど管理を徹底すること。
- ・市対策基準 9 (2) ア(イ)について、モバイル端末の場合は、市対策基準に記載の措置に加え、以下の措置を講じること。
 - 利用者IDは利用者毎に分けることを原則とするが、分けられない場合は、利用者管理簿等により、誰がいつ使ったのかを管理する。
 - 管理者権限は利用者が利用できないような仕組み又は運用とする。
 - 機密情報を保存する場合は、端末の操作ログを取得することが望ましい。
 - 一定時間操作のない状態が続いたときはログイン画面に戻ること。
- ・市対策基準 9 (2) ア(ウ)①における「原則として」とは、課室を跨いだセキュアなデータのやり取りの方法として、ファイルサーバーを利用することを例外として想定したものである。その場合であっても情報システ

ム管理者は、適切なアクセス制御を行うとともに、業務上必要がなくなったファイルやフォルダは速やかに削除する必要がある。

- ・市対策基準 9 (2) ア(ウ)①における「設定」においては、利用者IDのみならず、管理者IDについても適切に管理しなくてはならない。具体的には対象管理者IDを利用していた職員が異動した場合等は見落としがちであるため注意が必要である。この場合、対象IDの削除やパスワードの変更等の対応が必要となる。

イ 外部からのアクセス等の制限

- ・市対策基準 9 (2) イ「外部からのアクセス等の制限」に当たって、LGWAN 接続系においてテレワークを行う場合は、以下のリスク・概要・対策の方向性を踏まえ、適切な情報セキュリティ対策を行わなければならない。

リスク		概要	対策の方向性
①なりすまし		悪意のある第三者のID・パスワードの窃取等により、庁内の情報システムが不正アクセスされるリスク	許可された端末・職員のみ可能となるよう認証の仕組みの整備
② 漏えい（盗聴・改ざん等）	通信	インターネット上で、悪意のある第三者に通信内容を傍受されるリスク	通信回線は、閉域網を使用する等、安全な接続方式を採用
	データ	不正アクセスにより、データを窃取／改ざんされるリスク	端末内での業務データ非保持（端末仮想化等）、端末データの暗号化等、第三者による端末の操作・データ窃取の防止や被害拡大を防ぐ仕組みの整備
③盗難／紛失		端末の盗難・紛失により、情報漏えいするリスク	盗難／紛失時に端末内の情報をリモートで管理できる仕組みの整備
④不正利用		<p>利用者が故意又は過失により、情報システムを不正に利用することに起因するリスク</p> <p>例) 権限を持たない第三者による不正なアクセスフリーソフト等許可されていないアプリケーションに起因した</p>	<p>権限に応じた情報へのアクセス制限、ポリシーの一元管理</p> <p>業務に不要なアプリケーション導入の制限操作ログの収集・管理</p>

	マルウェア感染	
⑤不正持ち出し	利用者が故意又は過失により、不正なデータ持ち出しを行うリスク 例) 外部記録媒体などを用いたデータ不正持ち出し	端末に対する記録媒体の接続制限
⑥脆弱性・マルウェア	OSやソフトウェアの脆弱性を利用した攻撃により、端末がマルウェアに感染するリスク 感染端末がセキュリティホールとなり、庁内のサーバーや端末等に不正アクセスやマルウェア感染を引き起こすリスク	端末のOS／ソフトウェアの適切なプログラム更新、パターンファイルの最新化ネットワークの情報セキュリティ対策の実施
※上記リスクのうち①～③がリモートアクセス特有のリスク		

- ・また、具体的には、以下のモデルを採用し、各モデルを導入する際は、「新型コロナウイルスへの対応等を踏まえたLGWAN接続系のテレワークセキュリティ要件について」（令和2年8月18日総行情第111号総務省自治行政局地域情報政策室長通知）にある技術要件を遵守しなければならない。

インターネット回線を使用しないモデル：

- ・閉域SIMによる接続サービスを利用するモデル

インターネット回線を使用するモデル：

- ・LGWAN-ASPサービスを利用して庁内にあるLGWAN接続系の端末に接続するモデル
- ・インターネット接続系を経由してLGWAN接続系の端末に接続するモデル

ウ 認証情報の管理

- ・市対策基準 9 (2) ウ「認証情報の管理」に当たっては、市対策基準に記載の事項のほか、以下の点に注意する必要がある。
 - ①ICカードを利用する際は紛失時に直ちにそのカードを無効化する等の処置を講じなければならない。
 - ②利用者が情報システムを利用する必要がなくなった場合は、IDの無効化や認証情報の廃棄等、当該利用者のIDや認証情報の不正な利用を防止するための措置を講じなければならない。

③利用者が認証情報を変更する際に、以前に設定した認証情報の再設定を防止する機能を実装することが望ましい。

④パスワード認証のみである場合、ログイン試行回数を制限することが望ましい。

(3) 情報システムの開発、導入、保守等

ア 情報システムの調達

- ・市対策基準 9 (3) ア(ア)における「調達仕様書」を作成するに当たっては、以下の事項を遵守すること。
 - 当該情報システムで取り扱う情報の重要性に応じて、情報システムのライフサイクルで必要となる情報セキュリティ機能を洗い出し、調達仕様書にアクセス制御、機器の廃棄方法等の必要となる情報セキュリティ要件を明記する。
 - 一般に公開する仕様書等には機密情報は記載しないこと。また、市の保有する情報を委託する場合は契約書等に「情報取扱注意項目」を添付すること。

イ 情報システムの開発

- ・市対策基準 9 (3) イ(ア)における「作業体制等を定める」とは、以下の事項を必要に応じて定めることをいう。
 - ①責任者
 - ②作業者及び作業範囲
 - ③関係するネットワーク及び情報システムとの調整
 - ④事故及び不正行為に係る危険性の分析、対応
 - ⑤テスト環境による動作確認
 - ⑥情報システムに係るソースコードの提出義務
 - ⑦作業記録の提出義務
 - ⑧情報セキュリティ対策上問題となるソフトウェア使用禁止事項

ウ 情報システムの導入

- ・市対策基準 9 (3) ウ(イ)③における「原則」とは、個人情報等の保護の観点から、例えば十分に安全性の確認や監督が難しいような受託者の所有する開発環境等において生データを持ち出してテスト等に利用すること

を危険視するものであり、安全性の確認された庁舎内等本番環境等において生データを利用してテストすることまで制限するものではない。

- ・市対策基準 9 (3) ウ(ウ)①における「作業体制等」とは、以下のことをいう。

①運用・保守業者等の作業者、作業範囲、及び処理権限を明確にし、これに応じた情報システム上の設定をする。また、運用・保守業者等のID登録・変更及び抹消を適切に行う。

②作業指示書を作成する。

③作業を実施した際は作業実績記録を作成する。

④②、③を所定の棚や保管庫等に保管する手続きを定め、実施する。

⑤保守又は運用作業は2名以上の作業者で行わせる（努力義務）とともに、適切に指揮監督する。

- ・市対策基準 9 (3) ウ(ウ)①における「データ等のバックアップに関する対応」とは、以下のことをいう。

- データやプログラム等の滅失、毀損に備えて、取り扱う電子情報を定期的にバックアップすること。

- 機密情報を取り扱う情報システムにおいて、バックアップ処理の実行権限を持つ者を限定すること。

- ・市対策基準 9 (3) ウ(ウ)①における「不具合の是正に関する対応」とは、以下のことをいう。

- 通信機器、サーバー等及びソフトウェアの不具合に関する情報を収集すること。

- 悪影響を及ぼす不具合を発見した場合は、速やかに是正すること。

- ・市対策基準 9 (3) ウ(ウ)②における「必要な保護対策」とは以下のとおりである。

①機密情報を取り扱う情報システム

- サーバーからデータを抽出（複製）する必要がある場合、その手続き等を定める。

- サーバーからデータを抽出（複製）する場合、ファイル又は記録媒体の暗号化を適切に実施する。

- 暗号化にあたっては、閲覧権限を有しない者が容易に復元できないよう、暗号鍵及びパスワード等の運用管理、パスワードの複雑性を検討する。

②特定個人情報を取り扱う情報システム

- 番号法第2条第9号に規定する特定個人情報ファイル（以下「特定個人情報ファイル」という。）を機器又は記録媒体等に保存（複製）する場合、ファイル又は記録媒体の暗号化を適切に実施する。
- 特定個人情報ファイルを削除、または記録媒体等を廃棄した記録を保存する（これらの作業を委託した場合には、委託先が確実に削除、廃棄したことを証明書等で確認する）。
- 情報システムの外に特定個人情報ファイルのデータを抽出（複製）した場合、その生成、使用、削除等の取扱い履歴を記録する。
- サーバー、クライアント及び連携する情報システム間の通信を暗号化することを推奨する。

エ 情報システムの開発・保守に関連する資料等の整備・保管

- ・ 市対策基準 9 (3) エ(ア)における「システム開発・保守に関する資料及び情報システム関連文書」のうち、システム開発時においては、システム開発仕様書を作成するとともに、その後当該仕様書を変更した場合には履歴も作成すること。また、当該仕様書は所定の棚や保管庫等に保管する手続を定め確実に実施すること。

オ 情報システムにおける入出力データの正確性の確保

- ・ 市対策基準 9 (3) オ(ウ)における「出力されるデータ」について、ウェブサイトの場合は内部処理の他にも運用するドメインにも注意が必要である。ウェブサイトの閉鎖等により利用していたドメインを運用停止する場合、手放したドメインを悪意のある第三者が取得して不正サイトへの誘導に利用される場合があるため、停止する場合も一定期間ドメインを登録、保持することが望ましい。また、第三者が使用できない地域型ドメイン等の手放すことを前提としていないドメインを利用することも有効であり、本市においては city.nagoya.jp がこれに該当する。詳細は名古屋市公式ウェブサイトに係る名古屋市ウェブサイト運営要綱等を確

認されたい。

(4) 不正プログラム対策

- ・市対策基準 9 (4) イ(エ)におけるコンピューターウイルス等の不正プログラムに感染した場合又は感染が疑われる場合の対応としては、被害の拡大を防ぐため、該当の端末においてLANケーブルの取り外し（パソコン等の端末の場合）や、通信を行わない設定への変更（モバイル端末の場合）などを実施するとともに、既に不正侵入済である可能性もあるためCSIRTと連携を図って適切に対応を行っていく必要がある。

(5) 不正アクセス対策

- ・市対策基準 9 (5) ア(オ)①における「必要な措置」とは、以下のことをいう。
 - ①OS、ウェブサーバーソフトウェア、CMS、その他情報システムを構築する上で組み込まれるソフトウェア(ミドルウェア等)の修正プログラムを適用し、脆弱性を抱えない状況を維持する。また、最新の情報を入手する体制を整備する。
 - ②テスト稼働前に、アプリケーション診断及びプラットフォーム診断を行うなど、ウェブアプリケーションや、ネットワーク機器・OS・サーバー・ミドルウェア等に脆弱性がないことを確認する。なお、これらの脆弱性の確認については、脆弱性のない状態を維持するため、1年に1回など定期的に実施すること。
 - ③ウェブアプリケーションの脆弱性（クロスサイトスクリプティング（XSS）、SQLインジェクション等）対策を適切に講じる。（参考：情報処理推進機構（IPA）による「安全なウェブサイトの作り方」及び「ウェブアプリケーションのセキュリティ実装チェックリスト」）
 - ④不要なサービスプログラムを停止する。
 - ⑤更新、保守等を行う際の通信は、適切な暗号化を施したうえで、接続認証の徹底（ワンタイムパスワードの併用による多要素認証や接続元IP制限等）を行う。
 - ⑥その他推奨対策としては、IDSによる不正侵入検知、IPSによる不正侵入防御、負荷分散装置等によるDoS攻撃対策、ファイル書き換え検知・防御

システム、WAFによる総合対策が挙げられる。

- ・市対策基準 9 (5) ア(オ)②における「必要な措置」とは、以下のことをいう。
 - ①機密情報の収集又は蓄積を行う際の通信は適切な暗号化を施すこと。
 - ②外部のネットワークとの接続点にファイアウォール等を設置し、通過するプロトコルを必要最小限に限定する。
 - ③機密情報を集積するデータベースに対するアクセス制御は適切に制御し、インターネット等の外部ネットワークから直接侵害を受けることのないよう対策を講じる。
 - ④ウェブサーバーには不要なファイルを置かない。
 - ⑤収集する機密情報は、平文で保存することなく、暗号化することを推奨する。パスワードの場合、ハッシュ化の上、ソルト加工することを検討する。
- ・市対策基準 9 (5) ア(カ)における「適切な措置」とは、サーバーへのアクセスについて、通信プロトコルやIPアドレスを必要最低限に制限する、認証情報による制限をかける等がある。
- ・市対策基準 9 (5) カにおける「情報システム等の可用性を確保する対策」とは、以下のことをいう。
 - ①情報システムを構成する機器の装備している機能による対策の実施
 - サーバー、端末及び通信機器について、サービス不能攻撃に対抗するための機能が実装されている場合は、これらを有効にする。
 - 通信事業者と協議し、サービス不能攻撃が発生時の対処手順や連絡体制を整備する。
 - ②サービス不能攻撃を想定した情報システムの構築
 - サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断したり、通信回線の通信量を制限したりするなどの手段を有する情報システムを構築する。
 - サービスを提供する情報システムを構築するサーバー、端末、通信機器及び通信回線を冗長化し、許容される時間内に切り替えられるようにする。

- サービス不能攻撃の影響を排除又は低減するための専用の対策装置を導入する。

③通信事業者の提供するサービスの利用

- 通信事業者が別途提供する、サービス不能攻撃に係る通信の遮断等のサービスがある場合は、これを利用する。

④情報システムの監視及び監視記録の保存

- 庁外からアクセスされるサーバーや、そのアクセスに利用される通信機器及び通信回線の中から、特に高い可用性が求められるものを優先的に監視する。
- 監視の記録については、監視対象の状態の変動を考慮した上で記録を一定期間保管する。

- ・ 市対策基準 9 (5) キにおける「標的型攻撃による組織内部への侵入を低減する対策（入口対策）」や「内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる等の措置」とは、以下のことをいう。

①人的対策例（標的型攻撃メール対策）

- 差出人に心当たりがない電子メールは、たとえ興味のある件名でも開封しない。
- 不自然な電子メールが着信した際は、ウェブ等の当該電子メール以外の情報源から当該組織の電話番号や問合せ電子メールアドレスを調べ、この差出人が実在するか、この電子メールを送信したかなどを確認する。
- 電子メールを開いた後で標的型攻撃と気付いた場合、添付ファイルは絶対に開かず、電子メールの本文に書かれたURLもクリックしない。
- 標的型攻撃と気付いた場合、必要に応じて情報システム管理者に対して着信の事実を通知し、組織内への注意喚起などを依頼する。
- 情報システム管理者は、電子メールやログを確認し、不正な電子メールがなかったかチェックする。（事後対策）

②記録媒体に対する対策例

- 出所不明の記録媒体は決してネットワーク上の端末に接続させない。
- 記録媒体をパソコン等の端末等に接続する際、マルウェア対策ソフトを用いて検査する。

- パソコン等の端末について、自動実行機能を無効化する。
- パソコン等の端末について、記録媒体内にあるプログラムを媒体内から直接実行できないようにする。

③ネットワークに対する対策例

- ネットワーク機器のログ監視を強化することにより、情報を外部に持ち出そうとするなどの正常ではない振る舞いや外部との不正な通信を確認し、アラートを発する又はその通信を遮断する。
- 不正な通信がないか、ログをチェックする。（事後対策）

(6) 情報セキュリティに関する情報の収集等

- ・ 市対策基準 9 (6) アにおける対策について、基本的には開発元等から提供される脆弱性の修正パッチやバージョンアップ等があり、OSやソフトウェア等の更新・修正プログラム等の形態で提供されるものを、原則速やかに適用することが必要である。
- ・ 修正プログラム等が用意されるまで時間がかかる場合もあるため、その場合は、脆弱性から考えられる又は提示される緩和策（影響を受けるサービスを停止する、通信ポートを遮断する等）の実施を検討して攻撃者からの侵害に備えること。
- ・ システムサーバー等、修正プログラム等を適用するとシステム動作に影響を与える懸念がある機器においては、速やかにパッチ適用することが困難となる場合がある。その場合、脆弱性がシステムに与える影響度の判断は迅速に行い、影響を与える場合は緩和策を調査、検討及び実行し、その暫定的対処を行っている間に、パッチ適用の検証を進めること。なお、影響度判断の結果、侵害可能性が無いことが確実と判断できる場合は定期保守まで見送る等、一定期間適用を見合わせることも想定される。ただし、潜在的なリスクを抱え続けることになるため、情報システム管理者等は慎重に判断すること。

9 運用【市対策基準10関係】

- ・市対策基準10(1)ウにおける「監視」では、機密情報を取り扱うような重要性の高い情報システムは原則として、常時監視とする。主にネットワーク機器のログの監視、情報システム及び機器等の稼動状況の監視、IDSによる不正アクセス監視等を対象とし、情報システム管理者は各情報システムの重要度、特性を考慮し、監視対象を決定する。
- ・市対策基準10(2)アにおける「遵守状況の確認」の方法としては、情報セキュリティ監査、情報に関する点検表を利用した自己点検、情報セキュリティインシデントの報告、ログ等からの異常時の発見などが挙げられる。
- ・市対策基準10(2)イにおける「情報セキュリティ対策に関する点検」では、以下の事案は対象外とする。

①ネットワークの構築・変更

- 単一の課室で利用され、かつ、複数の拠点間を結ばないネットワークの構築
- 単純な機器更新など既存の機器構成の変更を伴わず、新たな対策の実施等を要しない変更
- 過去に点検済のネットワークについて、接続先拠点を増設又は移転することに伴う変更
- 通信事業者の変更

②情報システムの開発・変更

- 一時的又は専ら試験的な情報システムの開発
- 職員が専ら学術研究の用に供するためその発意に基づき稼働する情報システムの開発
- 単一の課室で利用され、かつ、情報システムによる処理の影響が本市内部にとどまる開発・変更
- 単純な機能追加や機器更新など、既存の情報セキュリティ対策の変更を伴わず、新たな対策の実施等を要しない変更
- パスワードの強化など、情報セキュリティ対策を向上するために行う変更

なお、情報システム管理者は、開発等する情報システムにおいて外部サービ

スを利用する場合（IaaS上に情報システムを構築する等）は、情報セキュリティ対策に関する点検と合わせて、副統括管理者への外部サービスの利用に係る事前申請も行う必要がある。

- ・副統括管理者は、市対策基準 10 (2)イにおける「情報セキュリティ対策に関する点検」の結果を取りまとめ、年に 1 回、電子情報保護部会に報告する。
- ・市対策基準 10 (4)における「例外措置」では、情報セキュリティポリシーの適用を例外的に排除するものであることから、その承認は、情報セキュリティポリシーの適用が著しく行政事務の遂行を妨げる、緊急を要し通常の手続を取る時間的な猶予がない、技術的に困難であるなどの合理的な理由が必要である。また、その場合でも、例外措置は単に適用を排除するだけでなく、リスクに応じて代替措置を定めること及び期限を設けて認めることが望ましい。
- ・市対策基準 10 (4)における「例外措置」を適用した情報システム等については、年に 1 回以上のセルフチェックにおいて例外適用の実施状況を確認し、統括管理者に報告すること（ただし、審査当該年度は除く。）。

10 外部サービスの利用【市対策基準 11 関係】

- ・外部サービスの利用に当たっては、名古屋市外部サービス利用基準の解説も参照すること。

11 情報セキュリティ監査（評価・見直し）【市対策基準 12 関係】

- ・市対策基準 12 (1)における「情報セキュリティ監査」の実施に当たっては、情報システム導入・運用ガイドライン（監査編）も参照すること。
- ・市対策基準 12 (3)における「見直し」について、情報セキュリティポリシーを見直す場合は、原則として、電子情報保護部会員への意見聴取等を実施することとする。