報告事項No. ５・６　資料

１　川崎市教育委員会情報セキュリティ基本方針に関する規程の新規制定について

（１）地方自治法の改正（地方自治法第２４４条の６第１項の新設。令和８年４月１日施行）に伴い、普通地方公共団体の議会及び長その他の執行機関は、サイバーセキュリティを確保するための方針を定めることが義務付けられた。

（２）従来は「川崎市情報セキュリティ基本方針に関する規程」（市長訓令）を教育委員会などの市長以外の執行機関が保有する情報資産にも適用していたが、今回の地方自治法の改正を踏まえて、執行機関ごとに基本方針を整備することとなったものである。

（３）川崎市教育委員会において、市立学校が保有する情報資産については、「川崎市学校情報セキュリティ基本方針に関する規程」（教育委員会訓令）が定められているが、教育委員会（市立学校を除く。）が保有する情報資産については、サイバーセキュリティを確保するための方針を新たに定める必要が生じるため、「川崎市教育委員会情報セキュリティ基本方針に関する規程」（教育委員会訓令）を制定する。

【新規制定に当たっての参考】

・「川崎市情報セキュリティ基本方針に関する規程」（市長訓令）
・「地方公共団体における情報セキュリティポリシーに関するガイドライン」の
「第１章　情報セキュリティ基本方針（例文）」（総務省策定）

２　川崎市学校情報セキュリティ基本方針に関する規程の一部改正について

（１）市立学校が保有する情報資産について、「川崎市学校情報セキュリティ基本方針に関する規程」を地方自治法第２４４条の６第１項のサイバーセキュリティを確保するための方針として位置付けるため、所要の整備を行う。

（２）また、教育委員会（市立学校を除く。）が保有する情報資産について、「川崎市教育委員会情報セキュリティ基本方針に関する規程」（教育委員会訓令）を新たに制定することに伴い、紛れが生じないように文言の整理を行う。

・教育次長をもって充てる「情報統括監理者」→「学校情報統括監理者（学校ＣＩＳＯ）」
・学校教育部長をもって充てる「情報監理者」→「学校情報監理者」
・校長をもって充てる「情報管理責任者」→「学校情報セキュリティ管理者」
・情報・視聴覚センター室長をもって充てる「情報システム管理者」→「学校情報システム管理者」

地方自治法の一部を改正する法律の概要

○　第33次地方制度調査会「ポストコロナの経済社会に対応する地方制度のあり方に関する答申」（令和5年12月21日）を踏まえ、以下の改正を行う。

1. ＤＸの進展を踏まえた対応

① 情報システムの適正な利用等

- 地方公共団体は、事務の種類・内容に応じ、情報システムを有効に利用するとともに、他の地方公共団体又は国と協力し、その利用の最適化を図るよう努めることとする。
- 地方公共団体は、サイバーセキュリティの確保の方針を定め、必要な措置を講じることとする。総務大臣は、当該方針の策定等について指針を示すこととする。

② 公金の収納事務のデジタル化

eLTAXを用いて納付するものとして長が指定する公金（地方税以外）の収納事務を、地方公共団体が地方税共同機構に行わせるための規定を整備する。

2. 地域の多様な主体の連携及び協働の推進

地域住民の生活サービスの提供に資する活動を行う団体を市町村長が指定できることとし、指定を受けた団体への支援、関連する活動との調整等に係る規定を整備する。

3. 大規模な災害、感染症のまん延その他その及ぼす被害の程度においてこれらに類する国民の安全に重大な影響を及ぼす事態における特例

現行の国と地方公共団体との関係等の章とは別に**新たな章を設け**、**特例を規定**する。

① 国による地方公共団体への資料又は意見の提出の求め

事態対処の基本方針の検討等のため、国は、地方公共団体に対し、資料又は意見の提出を求めることを可能とする。

② 国の地方公共団体に対する補充的な指示

適切な要件・手続のもと、国は、地方公共団体に対し、その事務処理について国民の生命等の保護を的確かつ迅速に実施するため講ずべき措置に関し、必要な指示ができることとする。

【要件】個別法の規定では想定されていない事態のため個別法の指示が行使できず、国民の生命等の保護のために特に必要な場合（事態が全国規模、局所的でも被害が甚大である場合等、事態の規模・態様等を勘案して判断）

【手続】・あらかじめ、地方公共団体に対し、資料又は意見の提出の求め等の適切な措置を講ずるよう努める
・閣議決定
・事後の国会報告

③ 都道府県の事務処理と規模等に応じて市町村（保健所設置市区等）が処理する事務の処理との調整

国民の生命等の保護のため、国の指示により、都道府県が保健所設置市区等との事務処理の調整を行うこととする。

④ 地方公共団体相互間の応援又は職員派遣に係る国の役割

国による応援の要求・指示、職員派遣のあっせん等を可能とする。

【施行期日】　1①、2及び3：令和6年9月26日（1①の一部は令和8年4月1日）
1②　：公布の日（令和6年6月26日）から起算して2年6月を超えない範囲内において政令で定める日

地方自治法（昭和22年4月17日法律第67号）

（サイバーセキュリティを確保するための方針等）

第二百四十四条の六　普通地方公共団体の議会及び長その他の執行機関は、それぞれその管理する情報システムの利用に当たつてのサイバーセキュリティを確保するための方針を定め、及びこれに基づき必要な措置を講じなければならない。

２　普通地方公共団体の議会及び長その他の執行機関は、前項の方針を定め、又はこれを変更したときは、遅滞なく、これを公表しなければならない。

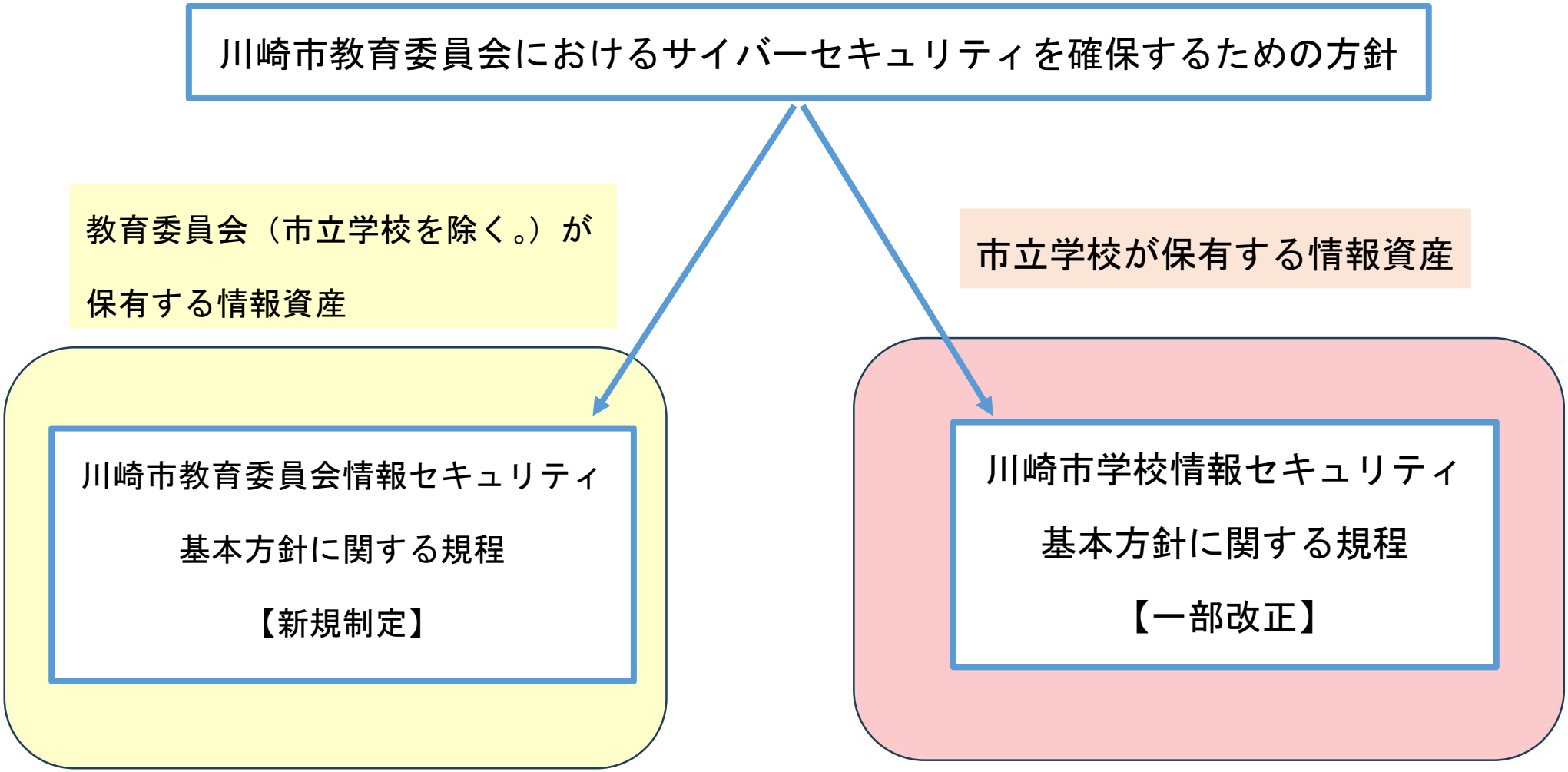
３　総務大臣は、普通地方公共団体に対し、第一項の方針（政令で定める執行機関が定めるものを除く。）の策定又は変更について、指針を示すとともに、必要な助言を行うものとする。

４　総務大臣は、前項の指針を定め、又は変更しようとするときは、国の関係行政機関の長に協議しなければならない。

川崎市情報セキュリティ基本方針に関する規程の一部を改正する訓令

新	旧
○川崎市情報セキュリティ基本方針に関する規程 平成19年３月30日訓令第１号 （趣旨） 第１条　この訓令は、地方自治法（昭和22年法律第67号）第２４４条の６第１項の規定に基づき、市が保有する情報資産をさまざまな脅威から保護するため、情報セキュリティに関する基本的な方針を定めるものとする。 （定義） 第２条　この訓令において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。 （１）　各局　川崎市事務分掌条例（昭和38年川崎市条例第32号）第１条に掲げる局及び本部並びに市民オンブズマン事務局、会計室、区役所及び消防局をいう。 略 （各局の長の責務） 第６条　各局の長は、対策基準に基づき情報セキュリティ対策を実施するものとする。 略 ４　各局の長は、情報資産を取り扱う業務の全部又は一部を事業者に委託する場合又は地方自治法第２４４条の２第３項の規定により市の指定を受けたもの若しくは公営住宅法（昭和２６年法律第１９３号）第４７条の規定により公営住宅の管理を代わって行うものが市の情報資産を利用する場合は、情報セキュリティに関する法令、この訓令、対策基準及び実施手順の	○川崎市情報セキュリティ基本方針に関する規程 平成19年３月30日訓令第１号 （趣旨） 第１条　この訓令は、市が保有する情報資産をさまざまな脅威から保護するため、情報セキュリティに関する基本的な方針を定めるものとする。 （定義） 第２条　この訓令において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。 （１）　各局　川崎市事務分掌条例（昭和38年川崎市条例第32号）第１条に掲げる局及び本部並びに市民オンブズマン事務局、会計室、区役所、上下水道局、交通局、病院局、消防局、教育委員会事務局、選挙管理委員会事務局、監査事務局、人事委員会事務局及び議会局をいう。 略 （各局の長の責務） 第６条　各局の長（教育委員会事務局にあっては、教育次長。以下同じ。）は、対策基準に基づき情報セキュリティ対策を実施するものとする。 略 ４　各局の長は、情報資産を取り扱う業務の全部又は一部を事業者に委託する場合又は地方自治法（昭和２２年法律第６７号）第２４４条の２第３項の規定により市の指定を受けたもの若しくは公営住宅法（昭和２６年法律第１９３号）第４７条の規定により公営住宅の管理を代わって行うものが市の情報資産を利用する場合は、情報セキュリティに関する法令、この訓

新	旧
規定を遵守させるために必要な措置を講ずるものとする。 略 附　則 この訓令は、令和８年４月１日から施行する。	令、対策基準及び実施手順の規程を遵守させるために必要な措置を講ずるものとする。 略



川崎市教育委員会においては、２つの基本方針をもって、保有する全ての情報資産（情報及び情報システム並びにこれらに関連する施設、設備等）のサイバーセキュリティを確保するための方針とする。

川崎市情報セキュリティ基本方針に関する規程

平成１９年３月３０日

訓令第１号

（趣旨）

第１条　この訓令は、地方自治法（昭和２２年法律第６７号）第２４４条の６第１項の規定に基づき、市が保有する情報資産をさまざまな脅威から保護するため、情報セキュリティに関する基本的な方針を定めるものとする。

（定義）

第２条　この訓令において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（１）各局　川崎市事務分掌条例（昭和３８年川崎市条例第３２号）第１条に掲げる局及び本部並びに市民オンブズマン事務局、会計室、区役所及び消防局をいう。

（２）情報　各局の職員が職務上作成し、又は取得した文書、図画及び電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。）をいう。

（３）ネットワーク　電子計算機を相互に接続し、情報を伝送するための通信回線網その他の仕組みをいう。

（４）情報システム　ハードウェア、ソフトウェア、ネットワーク及び記録媒体で構成され、情報の処理を行う仕組みをいう。

（５）情報資産　情報及び情報システム並びにこれらに関連する施設、設備等をいう。

（６）情報セキュリティ　情報資産に係る機密性、完全性及び可用性を維持することをいう。

（７）機密性　アクセスすることを認められた者に限り、アクセスできる状態

をいう。

（８）完全性　破壊、改ざん、消去等をされていない状態をいう。

（９）可用性　アクセスすることを認められた者が、必要なときに中断されることなく、アクセスできる状態をいう。

（１０）アクセス　情報資産に接触するあらゆる行為をいう。

（１１）脅威　情報資産に対して障害又は影響を与える原因となるものをいう。

（情報セキュリティ対策）

第３条　脅威から市の情報資産を保護するための情報セキュリティに関する対策（以下「情報セキュリティ対策」という。）は、次のとおりとする。

（１）情報セキュリティに関し、職員が遵守すべき事項を定めるとともに十分な研修及び啓発を行う等の人的な対策

（２）情報システムを管理する施設への不正な立入りによる危害、妨害等から情報資産を保護することを目的とした入退室の管理等の物理的な対策

（３）不正なアクセス等から情報資産を保護することを目的としたアクセスの制御、ネットワークの管理、不正プログラム対策、不正アクセス対策等の技術的な対策

２　前項の情報セキュリティ対策は、情報資産を機密性、完全性及び可用性の内容に応じて分類し、当該分類に基づいて実施するものとする。

３　第１項に掲げるもののほか、情報システムの監視の実施、情報セキュリティ対策の実施状況の確認及び情報資産への侵害が発生した場合等に迅速かつ適切に対応するための緊急時対応計画の策定を行うものとする。

（情報セキュリティ管理体制）

第４条　市長は、情報セキュリティ対策を統一的、効果的かつ効率的に実施するため、役割と責任を明確にした管理体制（以下「情報セキュリティ管理体

制」という。）を整備するものとする。

２　情報セキュリティ管理体制は、川崎市情報化施策の推進に関する規則（平成１９年川崎市規則第１２号）第５条に規定する情報統括監理者（以下「情報統括監理者」という。）が統括するものとする。

（情報セキュリティ対策基準）

第５条　情報統括監理者は、第３条に規定する情報セキュリティ対策を実施するための遵守すべき事項、判断基準等を定める情報セキュリティ対策基準（以下「対策基準」という。）を定めるものとする。

（各局の長の責務）

第６条　各局の長は、対策基準に基づき情報セキュリティ対策を実施するものとする。

２　各局の長は、所掌する情報システムについて情報セキュリティ対策を実施するために、情報セキュリティ実施手順（以下「実施手順」という。）を作成するものとする。

３　各局の長は、情報セキュリティを確保するため、情報セキュリティ対策の実施状況の確認を行い、必要に応じて実施手順の見直しを行うものとする。

４　各局の長は、情報資産を取り扱う業務の全部又は一部を事業者に委託する場合又は地方自治法第２４４条の２第３項の規定により市の指定を受けたもの若しくは公営住宅法（昭和２６年法律第１９３号）第４７条の規定により公営住宅の管理を代わって行うものが市の情報資産を利用する場合は、情報セキュリティに関する法令、この訓令、対策基準及び実施手順の規定を遵守させるために必要な措置を講ずるものとする。

（情報セキュリティ監査）

第７条　市長は、情報セキュリティ対策の実施状況を検証するため、情報セキュリティに関する監査を実施するものとする。

（委任）

第８条　この訓令に定めるもののほか、必要な事項は、別に定める。

附　則

（施行期日）

１　この訓令は、平成１９年４月１日から施行する。

（川崎市電子計算組織による処理に係るデータの保護管理に関する規程の廃止）

２　川崎市電子計算組織による処理に係るデータの保護管理に関する規程（昭和５３年川崎市訓令第２号）は、廃止する。

附　則

この訓令は、平成２０年４月１日から施行する。

附　則

この訓令は、平成２１年４月１日から施行する。

附　則

この訓令は、平成２２年４月１日から施行する。

附　則

この訓令は、平成２８年４月１日から施行する。

附　則

この訓令は、平成２９年４月１日から施行する。

附　則

この訓令は、令和８年４月１日から施行する。

地方公共団体における
情報セキュリティポリシーに関する
ガイドライン(令和７年３月版)

平成13年３月30日　策　定
令和７年３月28日　改　定

総　務　省

第１章

情報セキュリティ基本方針
（例文）

（目次）

第1章　情報セキュリティ基本方針（例文）

1.　目的

本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2.　定義

（１）　ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（２）　情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（３）　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（４）　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（５）　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（６）　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（７）　可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（８）　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（９）　LGWAN 接続系

LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

（１０）　インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（１１）　通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安

全が確保された通信だけを許可できるようにすることをいう。

（１２） 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

3. 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３） 地震、落雷、火災等の災害によるサービス及び業務の停止等

（４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５） 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4. 適用範囲

（１） 行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。

（２） 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③情報システムの仕様書及びネットワーク図等のシステム関連文書

5. 職員等の遵守義務

職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6. 情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１） 組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（２） 情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３） 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４） 物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

（５） 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（６） 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（７） 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（８） 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（9） 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7. 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8. 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

9. 情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10. 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

（注）情報セキュリティ基本方針は、基本的事項を規定する形式で作成する必要がある。また、宣言書形式での情報セキュリティポリシー基本方針の作成は任意とする。これらの形式の詳細は「第３編　地方公共団体における情報セキュリティポリシー（解説）」の「第１章　情報セキュリティ基本方針（解説）」を参照されたい。