○豊明市情報セキュリティ基本方針に関する規程

平成１５年８月２６日
訓令第４号
改正　平成２１年９月３０日訓令第２号
平成２６年３月２５日訓令第２号
平成２８年３月２８日訓令第４号
平成３０年３月２３日規程第８号
平成３０年６月２６日規程第１８号
令和元年６月２７日規程第７号
令和２年３月２４日訓令第８号
令和３年６月２４日訓令第８号

（目的）

第１条　この規程は、市が所掌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の対策（以下「情報セキュリティ対策」という。）を整備するために、豊明市情報セキュリティポリシーを定め、市民からの信頼の向上に寄与することを目的とする。

（定義）

第２条　この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（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）　内部ネットワーク　市における内部部局、各行政委員会事務局、議会事務局、及び各地方公営企業のコンピュータ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）で構成され、処理を行う仕組みをいう。

（３）　情報システム　コンピュータ（ソフトウェア及びハードウェア）、ネットワーク及び記録媒体で構成され、処理を行う仕組みをいう。

（４）　情報セキュリティ　以下の要素を維持することをいう。

ア　機密性　情報へのアクセスを認められた者以外への重要な情報の漏えいを防止すること。

イ　完全性　情報の改ざん、破壊による被害を防止すること。

ウ　可用性　情報にアクセスを認められた者に対し、必要な時に情報の利用が可能な状態を確保すること。

（５）　情報セキュリティポリシー　この規程及び豊明市情報セキュリティ対策基準（平成１５年８月１５日決裁）（以下、「情報セキュリティ対策基準」という。）をいい、市が所掌する情報資産を取り扱う業務に携わる者に浸透、普及、定着させ、情報セキュリティ対策の頂点に位置するものである。

（６）　職員等　職員（豊明市職員定数条例（昭和５１年豊明市条例第１号）第１条に規定する職員）、非常勤特別職の職員（豊明市特別職の職員で非常勤の者の報酬及び費用弁償等に関する条例（昭和４７年豊明市条例第３１号）第２条に掲げる特別職の職員で非常勤の者）、パートタイム会計年度任用職員（豊明市パートタイム会計年度任用職員の給与及び費用弁償に関する条例（令和元年豊明市条例第４２号）第１条に規定するパートタイム会計年度任用職員）及び定年前再任用短時間勤務職員（地方公務員法（昭和２５年法律第２６１号）第２２条の４第１項又は第２２条の５第１項の規定により採用された職員）をいう。

（７）　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。

（８）　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。）。

（９）　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。

（１０）　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。

（１１）　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。

（適用範囲）

第３条

（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。

ア　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

イ　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）

ウ　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

（職員等及び委託事業者等の義務）

第４条　市が所掌する情報資産に関する業務に携わる全ての職員等及び委託事業者等は、情報セキュリティの重要性について共通の認識を持つと共に、業務の遂行に当たっては、情報セキュリティポリシーを遵守する義務を負うものとする。

２　小中学校の教職員については、別に定めるものとする。

（情報セキュリティ管理体制）

第５条　情報セキュリティ対策を推進・管理するため豊明市情報セキュリティ委員会（以下「委員会」という。）を設置するものとする。

２　情報セキュリティ責任者（各部等の長）は、率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

（情報資産の分類と管理）

第６条　情報資産は、その内容に応じて分類し、重要度に応じた情報セキュリティ対策を行うものとする。

（情報資産に対する脅威）

第７条　情報資産に対する脅威として、次に掲げる脅威を想定し、情報セキュリティ対策を実施する。

（１）　不正アクセス、不正操作、ウイルス攻撃、サービス不能攻撃等のサ

イバー攻撃、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、重要情報の搾取、内部不正等

（２）　情報資産の無断持ち出し、プログラム上の欠陥、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、操作・設定ミス、メンテナンス不備、無許可アクセスのための認証情報及びパスワードの不適切管理、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、故障並びに事故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

（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、通信及び、水道供給の途絶等のインフラ障害からの波及等

（情報セキュリティ対策）

第８条　前条で示した脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講ずるものとする。

（１）　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。

ア　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。

イ　LGWAN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。

ウ　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として、都道府県及び市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。

（２）　物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨

害等から保護するために物理的な対策を講ずる。

（３）　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等及び委託事業者に情報セキュリティポリシーの内容を周知徹底する等十分な教育及び啓発が講じられるように必要な対策を講ずる。

（４）　技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、内部ネットワーク管理等の技術面の対策及びシステム開発等の業務委託を行う際のセキュリティ管理、内部ネットワークの監視、情報セキュリティポリシー遵守状況の確認等運用面の対策を講ずる。

（５）　業務委託と外部サービスの利用

ア　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。

イ　外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

ウ　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ごとの責任者を定める。

（６）　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。

２　緊急事態が発生した際に迅速な対応を可能とするための対策を講ずる。

（情報セキュリティ対策基準の策定）

第９条　前条の情報セキュリティ対策を講ずるに当たって委員会は、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要があるため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリ

ティ対策基準を策定するものとする。

（情報セキュリティ実施手順の策定）

第１０条　情報セキュリティ責任者（各部等の長）は、情報セキュリティ対策を実施するために、情報セキュリティ責任者が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

（非公開）

第１１条　情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより市の行政運営に重大な支障を及ぼす恐れがあることから非公開とする。

（情報セキュリティ監査及び自己点検の実施）

第１２条　情報セキュリティポリシーが遵守されていることを検証するため、委員会に監査班を設け定期的又は必要に応じて情報セキュリティ監査を実施するものとする。

２　情報システムを運用する者は、情報セキュリティポリシーが遵守されていることを自ら随時検証するものとする。

（評価及び見直しの実施）

第１３条　情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを定期的に実施する。

２　評価及び見直しは、委員会で審議し、決定するものとする。

（違反に対する措置）

第１４条　この規程に定める情報セキュリティ対策、情報セキュリティ対策基準及び情報セキュリティ実施手順に違反した職員等については、その重大性、発生した事案の状況等に応じて地方公務員法第２９条第１項による懲戒処分、損害賠償請求等の対象とし必要な措置を執るものとする。

２　この規程に定める情報セキュリティ対策に違反した委託事業者については、その重大性、発生した事案の状況等に応じて損害賠償請求等の対象とし、必要な措置を執るものとする。

（委任）

第１５条　この規程に定めるもののほか、この規程の施行に関し必要な事項は、市長が別に定める。

附　則

この規程は、平成１５年１０月１日から施行する。

附　則（平成２１年訓令第２号）

この規程は、訓令を発した日から施行する。ただし、改正後の豊明市情報セキュリティ基本方針に関する規程第２条第６号の規定は、平成２０年４月１日から適用する。

附　則（平成２６年訓令第２号）

この訓令は、平成２６年４月１日から施行する。

附　則（平成２８年訓令第４号）

この訓令は、発令の日から施行する。

附　則（平成３０年規程第８号）

この訓令は、平成３０年４月１日から施行する。

附　則（平成３０年規程第１８号）

この訓令は、発令の日から施行し、平成３０年４月１日から適用する。

附　則（令和元年規程第７号）

この訓令は、発令の日から施行し、平成３１年４月１日から適用する。

附　則（令和２年訓令第８号）

この訓令は、令和２年４月１日から施行する。

附　則（令和３年訓令第８号）

この訓令は、発令の日から施行し、令和３年４月１日から適用する。

附　則

この訓令は、令和５年４月１日から施行する。