坂城町情報セキュリティポリシー

基 本 方 針

令和8年3月

坂城町

目次

序　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、坂城町の情報資産に対する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものとする。 情報セキュリティポリシーは、坂城町の情報資産に関する業務に携わる職員等、及び外部委託業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら、一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）の2階層に分けて策定することとした。

（1）情報セキュリティ基本方針

坂城町としての情報セキュリティ対策に関する取り組み姿勢及び統一的な方針。

（2）情報セキュリティ対策基準

情報セキュリティ基本方針を実行に移すための坂城町における全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。

第1条　目的

坂城町の情報資産には、住民の個人情報をはじめ行政運営に必要な情報など、部外に漏洩、あるいは滅失した場合には極めて重大な結果を招く情報が多数含まれている。これらの情報資産を人的脅威や災害、事故等から防御することは、住民の財産、プライバシーを守るためにも、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠であり、ひいては、坂城町に対する住民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるDXの進展により、ネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件となる。

このため、坂城町の情報資産の機密性、完全性及び可用性を維持するための対策を整備することを目的として、坂城町情報セキュリティポリシーを定め、情報セキュリティの確保に最大限取り組むものである。

このうち情報セキュリティ基本方針は、坂城町の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等基本的な事項を定めるものとする。

第2条　用語の定義

(1)電子計算機

ハードウェア及びソフトウェアで構成するコンピュータ、及び周辺機器並びに電磁的記録媒体(磁気ディスク等並びに入出力帳票及び情報システム仕様書等)をいう。

(2)ネットワーク

電子計算機を相互に接続するための通信網及びその構成機器(ハードウェア及びソフトウェア)で構成され、情報処理を行う仕組みをいう。

(3)庁内ネットワーク

ネットワークのうち、坂城町役場本庁、出先機関、各種委員会、議会事務局、教育機関、福祉施設等の事務室で使用される電子計算機を相互に接続するための通信網及びその構成機器(ハードウェア及びソフトウェア)で構成され、情報処理を行う仕組みをいう。

(4)情報システム

坂城町の各種電子計算機(ネットワーク、ハードウェア及びソフトウェア)及び記録媒体で構成され、処理を行う仕組みをいう。

(5)情報資産

ネットワーク及び情報システムの開発と運用に係る全てのデータ並びにネットワーク及び情報システムで取り扱う全てのデータをいう。

(6)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。

(7)機密性

情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

(8)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。

(9)可用性

許可された利用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ことを確実にすること。

(10)職員

地方公務員法で規定された特別職、一般職の中で、坂城町に勤務する者の総称をいう。

(11)関係機関の職員等

各種委員会、議会事務局、福祉施設等に勤務し、坂城町が管理する情報資産を職務で利用する者の総称をいう。

(12)職員等

坂城町が管理する情報資産を職務で利用する職員及び関係機関の職員等(それぞれ非常勤職員及び臨時職員等を含む)の総称をいう。

(13)外部委託者

職務委託先社員等、契約に基づいて坂城町の機関で作業する者の総称をいう。

(14)部外者

職員等及び外部委託者以外の坂城町の情報資産に接することが認められていない者の総称をいう。

(15)公共端末

坂城町の情報資産のうち、坂城町の施設等に設置され、職員等及び外部委託者以外の者が操作する端末の総称をいう。

(16)不正アクセス

不正アクセス行為の禁止等に関する法律(平成11年法律第 128 号)第2条第4項に規定する不正アクセス行為その他の不正な手段により利用者以外の者が行うアクセス又は利用者が行う権限外のアクセスをいう。

(17) 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。

(18) 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。)。

(19)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。

(20)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。

(21)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。

第3条　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、坂城町が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

第4条　情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの適用範囲は、次の各項に定めるものとする。

(1)適用資産

情報セキュリティポリシーの適用対象資産は、坂城町における全ての情報資産とし、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

(2)適用対象者

情報セキュリティポリシーの適用対象者は、坂城町における情報資産に接する全ての職員等(内部部局、行政委員会、議会事務局含む。)とする。

第5条　職員等の義務

坂城町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外部委託者は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行に当たって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。

第6条　情報セキュリティ管理体制

坂城町の情報資産について、適切に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。

第7条　情報資産の分類

情報資産をその内容に応じて分類し、その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。

第8条　情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

(1)部外者の侵入、故意の不正アクセス、コンピュータウィルス攻撃、サービス不能攻撃等のサイバー攻撃または不正操作等の意図的な要因による機器又は情報資産の漏えい、破壊、改ざん、消去、重要情報の詐取、内部不正等

(2)職員等及び外部委託者による機器又は情報資産の持出、不正アクセス又は不正行為による盗聴、改ざん、搬送中の事故等による機器又は情報資産の盗難、規定外の端末接続によるデータ漏洩、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、火災等の災害並びに事故、故障等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

第9条　情報セキュリティ対策

坂城町の情報資産を第8条に示した脅威から保護するために、以下の情報セキュリティ対策を講ずるものとする。

(1)組織体制

坂城町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

坂城町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)人的セキュリティ対策

情報資産に接する職員等の情報セキュリティに関する権限や責任等遵守すべき事項を定めるとともに、全ての職員等及び外部委託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、教育、訓練、啓発等を実施する。

(5)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、災害による情報資産の破壊・情報システムの停止等から保護するためにサーバ、電算室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講ずる。

(6)技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、コンピュータ等の管理、情報資産へのアクセス制御、不正プログラム対策、ネットワーク管理、コンピュータウィルス対策等を実施する。

(7)運用

情報セキュリティポリシーの実効性を確保するため、また、不正なアクセス等から適切に保護するため、システム開発等の外部委託、システムの管理、情報システムの監視、情報セキュリティポリシー遵守状況の確認等、運用面における必要な措置を講ずる。

また、情報資産に対するセキュリティ侵害など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危機管理対策を講ずる。

(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。

第10条　情報セキュリティ対策基準の策定

坂城町の様々な情報資産について、第9条の情報セキュリティ対策を講ずるに当たっては、職員等が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。そのため、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。

第11条　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を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要があることから、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、情報セキュリティ実施手順を策定するものとする。

第12条　情報セキュリティポリシーの情報公開

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坂城町の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

第13条　情報セキュリティ監査の実施

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、定期的に監査及び自己点検を実施する。

第14条　評価及び見直しの実施

情報セキュリティ監査及び自己点検の結果等により、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、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の見直しを実施する。

附則

（施行期日）

この情報セキュリティ基本方針は、平成 16 年 6 月 1 日から施行する。

附則

（施行期日）

この情報セキュリティ基本方針は、令和８年４月１日から施行する。