佐世保市
情報セキュリティ行動指針

令和６年６月１８日

１．情報セキュリティ行動指針策定の背景

佐世保市では、平成１６年６月、個人情報保護に対する市民の皆様の関心の高まりや、情報資産の漏えい等の防止に適切に対応することが地方自治体に求められたことを受け、本市情報セキュリティの一体的な推進を目的とした「佐世保市情報セキュリティポリシー」及び「佐世保市情報資産取扱要綱」を策定しました。

その後は、本市で定めたルールに基づき、本市の情報セキュリティの維持・向上を図るため、情報セキュリティに関する職員研修や情報セキュリティ監査の取組等、様々な対策を実施してきました。

昨今、インターネット等の情報通信技術が発展し、社会経済活動の基盤となった一方で、サイバーセキュリティにおける被害が年々増加しており、攻撃手法の高度化及び複雑化が深刻な問題となっています。そのため、市の保有する情報を守り、常に最新の攻撃手法に対応することで、市民の皆様の安心・安全の確保と、利便性の両立を実現する必要があります。

国では、施策の一環として、平成２５年５月に「行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（番号法）」が可決・成立し、平成２９年１０月１日から、自治体間での情報連携の本格運用が開始されました。

また、令和２年９月に閣議決定された「デジタル社会の実現に向けた重点計画」ではテレワークの活用を通じた場所にとらわれない働き方や、地方自治体のＡＩ・ＲＰＡの活用、セキュリティを踏まえた最適なクラウド化やデジタル人材不足の解消を中心としたＩＣＴ化を推進するとしています。さらに、誰もがデジタル化の恩恵を受けられる体制整備などを通じて、ＩＣＴリテラシーや情報モラルの向上を図り、巧妙化するサイバー攻撃に対応する技術開発や人材育成など、デジタル化の進展に合わせたサイバーセキュリティ対策に取り組むこととしています。

地方自治体では、重要インフラ事業者として、保有する情報を保護することで、市民サービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するシステム障害が市民生活や社会経済活動に重大な影響を及ぼさないよう、発生時の迅速な復旧を図ることが求められています。

このように日々複雑・多様化する社会情勢に対応し、情報セキュリティを継続的に向上させるために、中長期な視点に立ち、計画的に対策を講じ続けることが求められています。

2. 情報セキュリティ行動指針の目的・位置付け

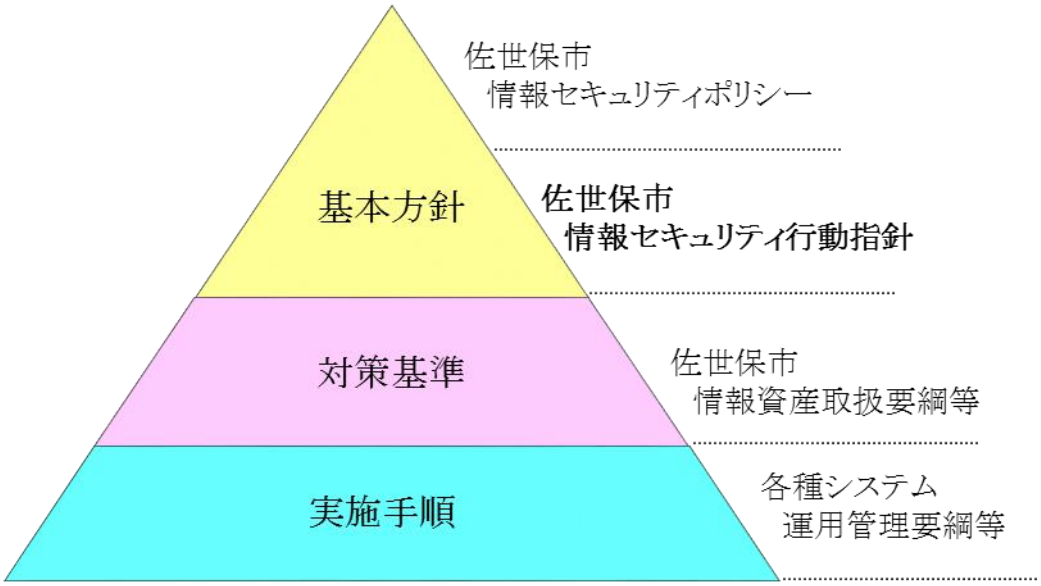
目的

本市の情報セキュリティに関する基本方針である「佐世保市情報セキュリティポリシー」に基づき、社会情勢の変化や国及び地方自治体に関連する情報セキュリティに関する方針を踏まえ、中長期な視点に立ち、重点的に取り組むべき項目を示し、本市の情報セキュリティを維持・向上させることを目的とします。

位置付け

本指針は、「佐世保市情報セキュリティポリシー」に定めた基本方針を実現するために重点的に取り組む項目を示す行動指針として定めます。

情報セキュリティに関する各種規程との体系図



3. 行動指針の見直し

本行動指針は、社会情勢、ICT 等の技術革新の著しい変化、国や地方自治体に関連する指針の変更、本市の情報化推進状況やインシデントの発生状況等を考慮し、必要に応じて見直しを行います。

4. 重点的に取り組む項目

「2. 情報セキュリティ行動指針の目的・位置付け」で述べた目的を達成するために、以下の項目について取組みます。

①　ＰＤＣＡサイクルの維持・推進

国は、「デジタル社会の実現に向けた重点計画」を策定して、世界最高水準のＩＴ利活用社会を実現するとしており、地方自治体においても、ＩＣＴの急速な進歩・普及による市民ニーズの多様化への対応が求められています。

本市では、「佐世保市情報セキュリティポリシー」に基づき、情報セキュリティ対策を推進しており、番号法等の新たな法令、情報システムの更改や新たな情報セキュリティにおける脅威にも適宜対応を行い、職員の意識を含めた情報セキュリティレベルを向上させています。

また、情報セキュリティの確保を本市の重要課題と捉え、社会情勢や市民ニーズへ対応すべく、ＰＤＣＡサイクル（計画、実行、評価、改善）の各段階における取組を継続し、情報セキュリティ対策の向上に取組みます。

②　重要システムにおける業務継続計画の策定・運用

本市では、防災危機管理局が策定した「佐世保市業務継続計画」に基づく個別行動計画として、総務省が策定した「地方公共団体におけるＩＣＴ部門のＢＣＰ策定に関するガイドライン」をもとに、「情報システム部門における業務継続計画（ＩＣＴ－ＢＣＰ）」を策定し、災害時の重要業務継続のための情報システム部門における対応策を整備しています。

また、「情報システム部門における業務継続計画（ＩＣＴ－ＢＣＰ）」に記載した訓練計画に基づき、定期的な訓練を実施し、その実効性を維持・向上することで、大規模災害発生時等にも、情報システムの早期復旧が可能となるよう努めております。最近では令和６年１月に能登半島地震のような大規模な災害も発生しており、今後も訓練の実施を通して、災害時等の重要業務継続のための対応力の向上を図ります。また、重要情報システムにおける業務継続計画の整備を進めます。

③　情報セキュリティに関する事故等への対応力向上

総務省は、「自治体情報セキュリティ対策緊急強化対策」において、情報セキュリティに関する事故等が発生した場合に、事態の把握、被害拡大防止、復旧、再発防止等を迅速かつ的確に行う体制であるＣＳＩＲＴ（シーサート：Computer Security Incident Response Team）の設立及び構築の必要性を報告しています。

本市においても、佐世保市ＣＳＩＲＴを構築し、情報セキュリティに関する事故等の発生に備えた緊急対応手順(佐世保市ＣＳＩＲＴ行動要領)の策定を行いました。あわせて、緊急時に備えた訓練を適宜実施し、体制が適切に機能する状態を維持し、訓練結果にもとづいて緊急対応手順の見直しを行うことで、その機能向上に務めています。

また、最新のセキュリティソフトの導入等、技術的な部分からも対策を行っていきま

す。

④　社会保障・税番号制度に関する安全管理措置の適切な実施

社会保障・税番号制度は、社会保障、税、災害対策の分野で効率的に情報を管理し、複数の機関が保有する個人の情報が同一人の情報であることを確認するために導入された制度です。これにより利便性が向上する一方、個人番号制度で利用される個人番号を含む個人情報（特定個人情報）は機密性が高く、厳格な利用範囲の限定や安全管理措置が求められています。

本市においても、特定個人情報を保護するための体制の整備と、安全な情報システム環境の構築を含む安全管理措置の実施及び運用が求められており、適切な運用を行うとともに、適宜見直しや特定個人情報に係る情報セキュリティ監査を実施することにより、安全管理措置の実施水準の維持・向上に努めます。

３．情報セキュリティ行動計画

本指針に基づく市の具体的な取り組みについては、別に情報セキュリティ行動計画を定めます。

なお、情報セキュリティ行動計画は、概ね３年ごとに、社会情勢の変化、ＩＣＴ等の技術革新の変化、国や地方自治体関連の指針の変更、本市の情報化推進状況やインシデントの発生状況等を考慮して、必要な見直しを行います。