佐世保市
情報セキュリティ行動指針

平成３０年４月１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さんの関心の高まりや、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公共団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います。その中でも、機密情報等の窃取を目的として特定の個人や組織を標的として行われる「標的型攻撃」や、パソコン等をウィルスに感染させ身代金を要求する「ランサムウエア感染」等、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、市民の皆さんの安心・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（以下、「番号法」という）」が可決・成立し、平成２９年１１月１３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。

地方公共団体では、重要インフラ[1]事業者として、情報を防護することで、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。

---

[1] 重要インフラ：他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの

出典：内閣府・内閣サイバーセキュリティセンター「重要インフラとは」より

2. 情報セキュリティ行動指針の目的・位置付け

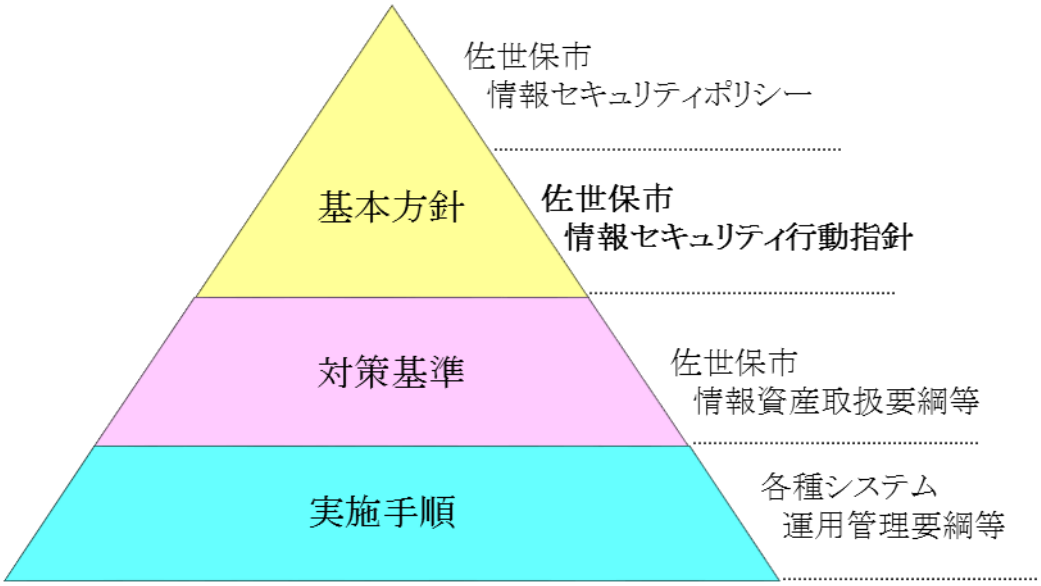
目的

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、「世界最先端 IT 国家創造宣言・官民データ活用推進基本計画」を策定（平成２９年５月改定）して、すべての国民がＩＴ利活用やデータ利活用を意識せず、その便益を享受できる、真に豊かさを実感できる社会の構築を目指しており、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おります。

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　情報セキュリティ監査の実施

総務省は、「地方公共団体における情報セキュリティ監査に関するガイドライン」を策定（平成２７年３月改定）して、地方自治体における情報セキュリティ監査の実施について、自主的に取り組むことを求めています。

本市では、情報セキュリティポリシー等に基づき、各種情報セキュリティ対策を実施しておりますが、これらの対策が、適切に運用されているかを職員により点検・評価するために情報セキュリティ監査を実施しています。あわせて、外部の専門家と共同で実施する情報セキュリティ監査を行うことで、客観性や専門性も担保しています。

今後も引き続き、情報セキュリティ監査を継続するとともに、特定個人情報関連の情報セキュリティ監査についても実施します。

③　重要システムにおける業務継続計画の策定・運用

総務省は、東日本大震災の教訓を踏まえて、平成２５年５月に「災害に強い電子自治体に関する研究会報告書」 をまとめました。報告書では、発災後、概ね７２時間以内の初動対応が十分にできるかどうかが、その後の復旧・復興に大きく影響することから、初動業務の実効性を確保するため、情報システム部門の業務継続計画の重要性をあげています。

本市においても、本市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」を策定し、災害時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。

今後は、「情報システム部門における業務継続計画」 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るとともに、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。

④　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、平成２７年８月「自治体情報セキュリティ対策緊急強化対策ついて 中間報告」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）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の策定を行います。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ます。

また、平常時から県等外部のＣＳＩＲＴを含め、必要な連携体制の構築についても推進します。

⑤　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

国は、社会的基盤として社会保障・税番号制度を導入されました。平成２９年１１月には、国や地方自治体間での情報連携の本格運用が始まり、社会保障分野の申請の際に必要な添付書類の一部省略が可能になりました。

本市においても、個人番号を含む個人情報（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います。そのため、体制整備、規程の策定及び情報システムの改修を行いました。今後は、適切な運用を行とともに、適宜見直しを行うことで、安全管理措置の実施水準の向上に務めます。

５．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の実施期間は、平成３０年度からの３年間とし、以後、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。