第２編　情報セキュリティ対策基準

第１章　目的

千歳市情報セキュリティ基本方針（以下、「基本方針」という。）を実現するための具体的な運営方法、遵守内容、判断基準を示します。

第２章　組織・体制

基本方針第１条に基づき、情報セキュリティに対して責任を明確にした体制による運営を行います。ただし、情報セキュリティは、事業方針と連動して設定、運営する必要があり、事業運営体制と連動した体制で運営を行います。

2.1　情報セキュリティ管理体制

情報セキュリティポリシーを運営していく体制として、情報セキュリティ管理体制を定めます。情報セキュリティ管理体制の最高責任者は、情報化推進本部長（副市長）とします。（付表１）

2.2　情報セキュリティ責任の割り当て

個々の情報資産を効率良く保護すること、また、発生した問題に速やかに対処するために、責任と権限を明確にします。

職務分掌の割り当てには、不注意や故意による誤った使用を避けるために、汎用機、サーバー及びその周辺装置（以下「情報処理設備」という。）の管理責任とデータの管理責任を分離します。

2.3　外部委託に関わるセキュリティ対策

外部委託を行う場合、セキュリティ要求事項を契約書に明記し、情報の機密性が特に高い場合には、守秘義務契約を別途締結します。

2.4　千歳市以外の組織とのデータ共有のセキュリティ

他組織とのデータ共有を行う場合、双方の取扱における管理策の要求事項を明らかにし、リスクを回避できると判断した場合においてのみ接続を許可します。

2.5　外郭団体の指導・助言

外郭団体の情報の取り扱いに関しては、所管する各担当課の職員が指導・助言します。

第３章　情報の分類と管理

基本方針第２条に基づき、守るべき情報資産とその価値を明確にすることで適切なレベルでの保護と対策時の優先順位決定をします。

3.1　情報資産目録

情報資産を分類するとともに、管理責任の所在と情報資産の価値を定義し、「情報資産台帳（目録)」により管理します。

3.2　情報の価値

情報資産ごとに以下の３つの側面により価値を定義します。

1. **機密性：アクセスを認可された者だけが情報にアクセスできることを確実にすること**
2. **可用性：認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること**
3. **完全性：情報及び処理方法が、正確であること及び完全であることを保護すること**

情報資産の価値の基準は、付表２「資産価値の基準」に定めるとおりとします。

3.3　リスク評価

情報資産ごとに想定される脅威とそれに対しての脆弱性を評価し、情報資産価値と合わせたリスク評価値を決定して対策を進めます。

第４章　人的対策

基本方針第３条、第４条、第５条に基づき情報を取り扱う人による誤用、ケアレスミス、不正行為のリスクを軽減することを目的として定めます。

4.1　職務定義及び任用時における対策

全ての職員（常勤、非常勤、臨時雇用を含む）を対象とし、採用時に情報セキュリティに関する義務と責任について、明確に文書を持って周知します。これらの責任については、離職後においても継続することを明確にします。

さらに、職員が情報セキュリティ要求事項に違反した場合は、関係法令、条例等に基づき措置します。

4.2　教育・訓練

基本方針及び実施手順について、全ての職員と外部委託者に対して情報セキュリティ教育を実施します。また、防災、緊急連絡についての訓練を適宜実施します。

4.3　セキュリティ事件・事故及び誤動作への対処

情報セキュリティに影響を及ぼす事件・事故は、情報セキュリティ管理体制を通じて、速やかに報告および指示を行います。

また、情報化推進本部は、事件・事故の再発と予防を目的とし、発生した事件・事故については、その原因と対策を分析し管理します。

第５章　物理的・環境的対策

基本方針第６条に基づき、情報の誤用や盗難などから情報資産を守るためと、円滑な業務遂行のバランスを取るためにセキュリティの区画を識別し、区画のレベルに応じた対策を講じます。

5.1　セキュリティ区画の定義

情報を取り扱う区画を分類するとともに、境界を明確にし、それぞれの区画に応じた入退管理を実施します。

5.2　施設・設備対策

(1)　電源

重要な情報処理設備に対しては、無停電電源装置（ＵＰＳ）などの設置を行い、瞬電への対策を講じます。

(2)　ケーブル配線

電源及び通信ケーブルは、傍受と損傷から守るために、床下埋設またはカバーを設置するなどの対策を講じます。

(3)　装置の保守

装置の継続利用を維持するために装置ごとに定められた適正な保守を実施します。

(4)　装置等の廃棄

情報処理装置等（パソコンやＦＤなど）を廃棄または再利用する場合、電子的に読み込みが完全に不可能な状態にして廃棄または再利用します。

5.3　クリアデスク及びクリアスクリーン

情報の紛失や盗難、盗み見などから重要な情報を守るために、クリアデスク（机上及び机周辺への資料などの放置の禁止）及び、クリアスクリーン（パソコンなどを利用可能な状態のまま離席することの禁止）を実施します。

5.4　情報資産の移動

情報資産を移設や持ち出す場合、情報資産の管理責任者の許可を得て行います。特に、自宅などへの資料やデータの持ち帰りを禁止します。

第６章　通信及び運用の管理

基本方針第７条、第８条に基づき、セキュリティを保った運用を継続していくために、情報処理設備や情報資産の変更などに関して適切に管理します。

6.1　運用管理

(1)　運用時間管理

情報システムの運用時間（開始と終了時間など）は、予め計画したスケジュールで行い、変更する場合は、情報システム管理責任者の認可を得て運用します。

(2)　情報システムの変更

情報システムの変更については、情報システム管理責任者の承認を得て行い、その

変更内容を管理します。

(3)　トラブル管理

情報システムに関わる障害等の情報は、情報システム管理責任者に報告をするとともに、その情報を管理します。

(4)　運用設備と開発設備の分離

安定した情報システムの稼働を確保するための運用設備と開発及び試験運用するための開発設備は分離します。

(5)　運用の外部委託

運用を外部の請負業者に委託する場合は、委託業務内容上必要となるセキュリティ要件を明確にして、契約に盛り込んで実施します。

6.2　システムの計画と受け入れ

システム障害のリスクを軽減するために、システム資源を管理します。

(1)　処理能力・記憶容量の管理

システムの処理能力と記憶容量の状況を監視し、将来必要となる能力と容量を計画的に管理します。

(2)　受入れ管理

新しい情報システムの導入や追加、変更等をする場合は、情報セキュリティ上問題がないか、十分な検証を実施します。

6.3　コンピュータウイルスなどからの保護

ソフトウェアやデータの完全性を守るために、コンピュータウイルス（※注１）などの悪意のあるソフトウェアの侵入の予防と検知及び発見時の対応策を整備します。

※注１：第三者のプログラムやデータベースに対して、何らかの意図的な被害を及ぼすように作られた悪質なプログラム。自己伝染機能、潜伏機能、発病機能のいずれか一つ以上を有するもの

- **自己伝染機能とは、自らをコピーし、他のシステムなどに伝染する機能**
- **潜伏機能とは、発病するための条件が満たされるまで症状を出さない機能**
- **発病機能とはプログラムやデータ等を破壊したり、コンピュータに異常な動作をさせたりする等の機能**

6.4　システムの維持管理

不測の事態に備えたバックアップの保持とトラブル原因の究明及び復旧対策決定のために、システムの運用記録を管理します。

(1)　バックアップ

システム復旧のために、バックアップの取得内容、方法、サイクル、保管期限、保管方法などについて、個々のシステムごとに定めます。

(2)　運用記録

システムや処理の起動、終了の記録、システムからのエラー情報などを適正な期間、記録し保管します。

6.5　ネットワークの管理

データ伝送路としてのネットワークにおける脅威から情報資産を守るために、ネットワークの維持管理と伝送データに対しての管理を実施します。

(1)　ネットワークの分離

行政サービスと庁内サービスのネットワークは分離します。

(2)　回線の利用

組織内における施設間の通信には、専用線または同等のセキュリティレベルの回線を利用します。

公衆網及びインターネット網を利用する場合には、暗号化を行います。

(3)　変更管理

ネットワークの変更及びネットワークへの接続機器（サーバー、パソコンやプリンタなど）の変更は、情報システム管理責任者の許可を得て行います。

ネットワークの構成は、常に最新の状態で管理し、ネットワークの維持管理に関与する特定の職員以外には、開示しないものとします。

(4)　個人資産の接続

個人資産の機器（パソコンなど）は、庁内ネットワークへの接続を禁止します。

6.6　媒体の取り扱い

情報資産の盗難や無許可の持ち出しからデータを守るために、媒体（光学式記憶媒体や磁気記憶媒体のディスク等）の取り扱い方法を定めます。

文書（紙）についての取り扱い方法は「千歳市文書管理規程（昭和48年千歳市訓令第１号)」に定めるとおりとします。

(1)　取り扱い方法

適正な管理を行うことによって誤用の防止や容易に検索が可能となる管理方法を実施します。

(2)　媒体の処分

磁気または光学式の記憶媒体等は、いかなる方法によっても復元できないよう消去等を行ったうえで廃棄します。

6.7　情報交換についてのセキュリティ

組織間で交換される情報の紛失、改ざんからの保護と移送中の事故に備えるために情報交換または移送について以下の内容を取り決めて実施します。

(1)　情報交換

他の組織と情報・ソフトウェアを交換する場合は、以下の点を確認または取り決めたうえで実施します。

・情報・ソフトウェアの管理権、著作権
・取り扱い上の技術標準
・交換方法と改ざんや盗聴防止策

(2)　移送

データの移送には、信頼のおける配送業者を利用し、移送中の事故へ配慮して施錠できる容器を利用します。

(3)　電子メール

電子メールによる情報漏えいやコンピュータウイルスなどの侵入を防止するために、電子メールの適正な利用方法を定めます。

(4)　庁内ＯＡシステム

庁内ＯＡシステム(ファイルサーバー、庁内イントラ、プリンタ、ファクシミリ等)を適正かつ安全に利用するために、利用方法を定めます。

(5)　情報公開システム

インターネット経由で公開している情報を改ざんから守るために、情報公開システムを監視します。また、公開した情報が正規の内容であることを確実にするために、掲載内容等の変更記録を管理します。

第７章　アクセス制御

基本方針第８条に基づき、どのような情報資産をどのような人が利用可能であるかを明確にし、情報資産の取り扱いにおいての誤用を防止し、円滑な業務遂行を目的として情報へのアクセスを制御します。

7.1　アクセス制御方針

情報へのアクセス制御は、次の事項を遵守するものとします。

1. 業務用ソフトウェアは、情報の識別による権限設定を行う。
2. アクセス権限は、個人に割り当てる。
3. アクセス権限の共同利用や貸し出しは行わない。

7.2　利用者の管理

(1)　利用者登録

許可された者だけに情報システムへのアクセスが、可能となるよう利用者登録を行います。

利用者登録は、業務と情報の関連によりアクセス権を設定します。

(2)　特権管理

特権（情報システムへの変更権限など特別な機能を有する権限）の割り当てと使用を制限します。

(3)　パスワードの利用

利用者の登録とともに、利用が利用者本人であることを確認する手段としてパスワードの利用を原則とします。

7.3　利用者の責任

利用者には、情報システムを利活用するためにＩＤ及びパスワードを付与することから厳格に管理しなければならない責任があります。

7.4　ネットワークのアクセス制御

情報処理設備間の経路についての識別と利用方法を明確にするとともに、外部からのネットワーク利用についての制限を管理します。

(1)　接続経路

情報システムを利用するための経路は、二重化するなどの冗長化対策（※注２）も含めて、限定した経路とします。

※　注２：最低限必要な量より多めに設備を用意しておき、一部の設備が故障してもサービスを継続して提供できるようにシステムを構築すること。

(2)　Ｗｅｂサイトの利用制限

私的利用など公序良俗に違反するＷｅｂサイト（ホームページ）の利用を禁止します。

(3)　ネットワークサービスの利用

ネットワークサービス（回線業者、ＩＳＰ事業者（※注３）、ＡＳＰ事業者（※注４）などによるサービス）を受ける場合は、使用するサービスのセキュリティ特性について、十分な説明と確認を受けたうえで利用します。

※注３：インターネット・サービス・プロバイダの略。インターネット接続サービスを提供する通信事業者。インターネットを利用するための種々のサービスを提供する。

※注４：アプリケーション・サービス・プロバイダの略。データセンターで業務アプリケーションを一括稼働させ、インターネットを通じてその機能を提供し、利用者はソフトウェアを購入しないで利用期間の使用料として支払いを行うサービスを提供する事業者。

7.5　業務用ソフトウェアのアクセス制御

情報システムが保有する情報を正当な利用者にのみ提供し、未許可のアクセスによる侵害を防御するための対策を考慮して、業務用ソフトウェアの導入・構築を行います。

7.6　システム使用状況の監視

許可されていないシステム使用状況を検出するためとセキュリティ事件・事故の場合の証拠となるように、システムへの接続操作状況（アクセスログ）を記録し、検査します。

7.7　時刻同期

コンピュータ及び通信装置内の時計は、記録した情報の保証及び情報システムの正常な稼動のために、日本標準時刻と同期を取ります。

第８章　システムの開発及び保守

基本方針第７条に基づき情報システムへのセキュリティ対策を確実に組み込むために、情報システムに対してのセキュリティ要求事項を明確にし、情報セキュリティポリシーとの整合を図ります。

8.1　情報システムへのセキュリティ要求事項

基本方針及び対策基準に規定する事項を遵守するほか、取り扱う情報の価値とリスク評価に基づき、情報資産の価値に適した内容で確定します。

8.2　業務用システムのセキュリティ

業務用システムにおけるデータの消失や誤用を防止するために、データの取り扱いについて情報システムごとに取り扱いを定めます。

8.3　システムファイル（※注５）の保護

システムファイルの変更は、任命した特定の管理者によってのみ変更可能とします。

また、セキュリティ上の欠陥を除去するソフトウェアパッチ（※注６）については、業務ソフトウェアへの影響がないことを確認のうえ、反映します。

※注５：システムライブラリ。ＯＳや業務プログラムの実行形式ファイルやその設定情報などが格納されているファイルまたはライブラリ

※注６：一旦完成したプログラムの一部を修正すること。修正を行うために変更点（差分情報）のみを抜き出して列挙したファイル

8.4　テストデータの取り扱い

テストデータについては、本稼働データとは別に維持管理します。

8.5　外部委託によるソフトウェア開発

ソフトウェア開発を外部事業者に委託する場合、次の項目を考慮して実施します。

・使用許諾に関する取決めとコードの所有権及び知的所有権
・外部委託先が不履行の場合の預託契約に関する取決め
・　作業の品質の監査権

第９章　行政サービスの継続管理

基本方針第９条に基づき、情報システムが受けた重大な障害や災害による行政サービスの中断に的確に対応し、行政サービスの継続と復旧を成し遂げるために緊急事態対応計画を策定します。

9.1　行政サービス継続のための分析

緊急事態対応計画を策定するにあたり、以下の点を分析し、計画を策定します。

・事業の中断を引き起こす可能性のある事象の特定
・復旧の優先順位の決定
・復旧に要する時間
・代替手段の有無

9.2　緊急事態対応計画

重大な障害や災害からの復旧手順を「緊急事態対応計画」として策定し、評価・見直し及び緊急事態対応計画に基づく訓練を実施します。

第１０章　適合性

基本方針第１０条、第１１条に基づき、法令等の遵守及び情報セキュリティポリシーの適合性を確認します。

10.1 法令等の遵守

刑法及び民法、その他の法令等及び契約上定められた義務とセキュリティ要求事項に対しての違反を回避するために、関連する要求事項を明確にして遵守します。

関連法令、条例等については、付表３に示します。

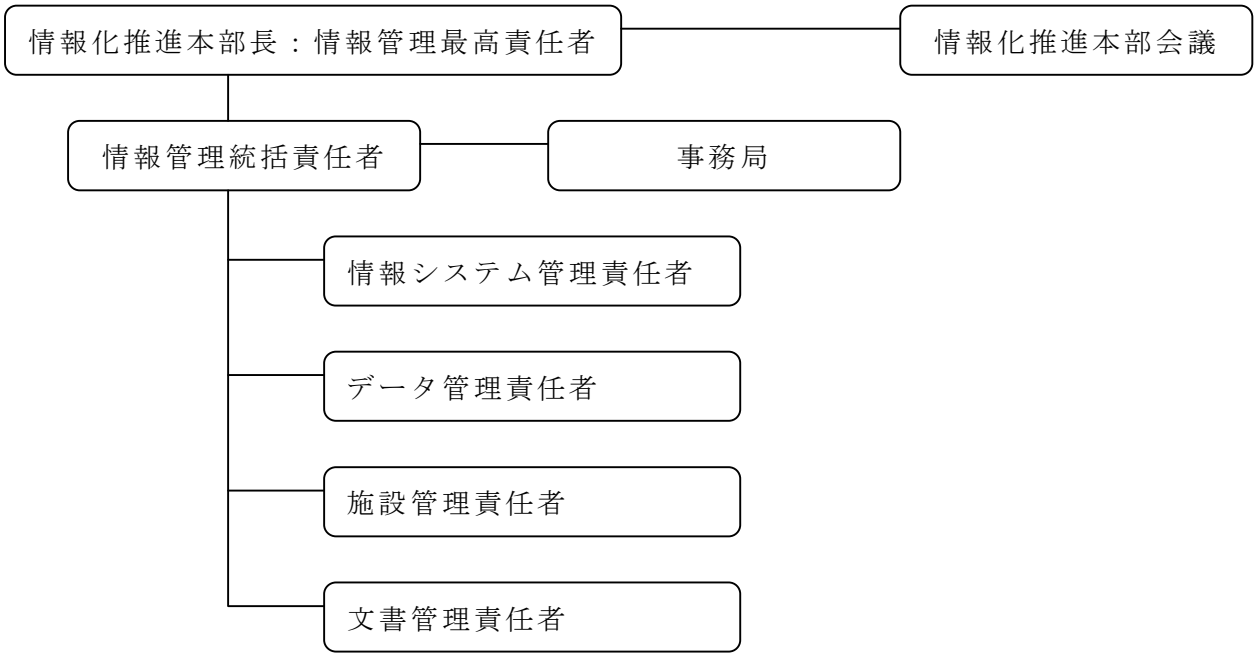
10.2 情報セキュリティ基本方針との適合性

常に実態に即した情報セキュリティポリシーを維持及び情報セキュリティ水準を高く保つために、基本方針に基づき①運営の適合性、②技術的な適合性、③実施手順等の実施状況を確認し、評価、見直します。

附　則

この情報セキュリティ対策基準は、平成１６年３月２６日から施行する。

付表１　　情報セキュリティ管理体制と職務分掌



名称	任命職	責任と権限
情報管理最高責任者	副市長	情報化推進及び情報セキュリティに対しての総責任者
情報管理統括責任者	総務部次長	情報管理最高責任者を補佐し、情報化推進及び情報セキュリティに対しての実質的な指揮を取る
情報システム管理責任者	行政管理課長	情報処理設備、情報処理周辺機器、ソフトウェア、システム設定情報を管理 ネットワークを統括的に管理し、適正な状態を維持する
データ管理責任者	各所管課長	情報資産の内、データについての取扱及び管理
施設管理責任者	総務課長	施設の統括的な管理と施設内における防犯を管理する
文書管理責任者	総務課長	文書の統括的管理
事務局	行政管理課 行政情報係	情報管理統括責任者の任務を補佐し、情報セキュリティ対策についての運営上の実務を遂行する

付表２　　資産価値の基準

情報資産台帳（目録）でグループ化された情報資産の機密性、完全性、可用性を維持するため、各要素の判断基準「資産価値」を下記のとおりとする。

(1) 機密性

値		データ	ドキュメント	インフラ	ハード	ソフト
1	一般	第三者に開示・提供可能	第三者に開示・提供可能	第三者がその存在を知り利用可能	第三者がその存在を知り利用可能	第三者が利用可能
2	庁外秘	庁内では開示・提供可能（第三者には不可）	庁内では開示・提供可能（第三者には不可）	庁内では庁内職員のみがその存在を知り利用可能	庁内では庁内職員のみがその存在を知り利用可能	庁内職員のみが利用可能
3	課外秘	特定の関係者または特定の部署のみに開示・提供可能	特定の関係者または特定の部署のみに開示・提供可能	特定の関係者または特定の部署の職員がその存在を知り利用可能	特定の関係者または特定の部署の職員がその存在を知り利用可能	特定の関係者または特定の部署の職員のみが利用可能
4	極秘	所定の関係者のみに開示・提供可能	所定の関係者のみに開示・提供可能	所定の関係者のみがその存在を知り利用可能	所定の関係者のみがその存在を知り利用可能	所定の関係者のみが利用可能

(2) 完全性

値		データ	ドキュメント	インフラ	ハード	ソフト
1	低	情報の内容を変更された場合、行政事務の執行上への影響は小さい	情報の内容を変更された場合、行政事務の執行上への影響は小さい	情報設備の内容を変更された場合、行政事務の執行上への影響は小さい	情報設備の内容を変更された場合、行政事務の執行上への影響は小さい	ソフトウェアの内容を変更された場合、行政事務の執行上への影響は小さい
2	中	情報の内容を変更された場合、行政事務の執行上への影響は大きい	情報の内容を変更された場合、行政事務の執行上への影響は大きい	情報設備の内容を変更された場合、行政事務の執行上への影響は大きい	情報設備の内容を変更された場合、行政事務の執行上への影響は大きい	ソフトウェアの内容を変更された場合、行政事務の執行上への影響は大きい
3	高	情報の内容を変更された場合、行政事務の執行上への影響は深刻かつ重大	情報の内容を変更された場合、行政事務の執行上への影響は深刻かつ重大	情報設備の内容を変更された場合、行政事務の執行上への影響は深刻かつ重大	情報設備の内容を変更された場合、行政事務の執行上への影響は深刻かつ重大	ソフトウェアの内容を変更された場合、行政事務の執行上への影響は深刻かつ重大

(3) 可用性

値		データ	ドキュメント	インフラ	ハード	ソフト
1	低	1 時間以上データの利用ができない状態が許容される	特別な状態を除き、取り出しにかかる時間を特に制限しない	1 時間以上の設備停止が許容される	1時間以上のハードウェアの停止が許容される	1時間以上のソフトウェアの停止が許容される
2	中	1 時間のデータの利用ができない状態が許容される	利用に際し、取り出しまでの時間が１時間前後を許容する	1 時間の設備の停止が許容される	1時間のハードウェアの停止が許容される	1時間のソフトウェアの停止が許容される
3	高	５分以上のデータの利用ができない状態が許容されない	必要とする場合即時利用できる必要がある	５分以上の設備の停止が許容されない	５分以上のハードウェアの停止が許容されない	５分以上のソフトウェアの停止が許容されない

付表３　　遵守法令一覧

項　　目		遵　守　法　令　等
情報の保護	(1) 守秘義務 (2) 個人情報・機密情報の保護	・個人情報の保護に関する法律 ・不正アクセス行為の禁止等に関する法律 ・地方公務員法 ・地方税法 ・千歳市個人情報保護条例 ・千歳市情報公開条例 ・その他
	(1)知的財産権の保護・尊重	・特許法 100 条～106 条（権利侵害） ・特許法 196 条（侵害の罪） ・特許法 201 条（両罰規程） ・著作権法 112 条～118 条（権利侵害） ・著作権法 119 条（罰則） ・知的財産基本法第 6 条（地方公共団体の責務）