## 第１章　情報セキュリティポリシーの構成

中札内村情報セキュリティポリシー（以下、「情報セキュリティポリシー」という）とは、 中札内村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を総称する。情報セキュリティポリシーは、中札内村が所掌する情報資産に関する業務に携わる全職員、非常勤、臨時職員（以下、「職員等」という。）及び業務委託事業者、外部サービス提供者に浸透、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）に分けて策定することとした。

具体的には、情報セキュリティポリシーを

① 情報セキュリティ基本方針

② 情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする（下表参照)。

情報セキュリティポリシーの構成

| 文　書　名 | | 内　容 |
|---|---|---|
| 情報セキュリティポリシー | 情報セキュリティ基本方針 | 情報セキュリティ対策に関する統一的かつ基本的な方針。 |
| | 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。 |
| 情報セキュリティ実施手順 | | ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順。 |

## 第２章　情報セキュリティ基本方針

### １　目的

この基本方針は、中札内村電子計算組織管理運営規則（平成１３年規則第６号。以下「規則」という。）第６条及び第９条の規定に基づき、個人情報及び記録情報等を守り、中札内村が運用する全ての情報システム及び情報資産を様々な脅威から防御するため、必要な事項を定める。

### ２　定義

⑴　ネットワーク

中札内村個人情報保護条例（平成１２年条例第３８号）第２条第１号に規定する実施機関内と各実施機関を相互に接続するための通信網と、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。

⑵　情報システム

業務系の電子計算機（業務系におけるネットワーク、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。

⑶　情報資産

ネットワーク、情報システム、これらに関する設備、電磁的記録媒体、及びそれらの開発・運用に係る情報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情報をいう。

なお、情報資産には紙等の有体物で出力された情報も含むものとする。

⑷　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をいう。

⑸　機密性

個人認証等により、情報にアクセスする正当な権限を持つ者だけが情報にアクセスできる状態にすること。

⑹　完全性

情報が正確かつ完全であり、改ざん又は消去がされていない状態を確保すること。

⑺　可用性

アクセスを許可されている利用者が、必要な時に中断されることなく情報資産にアクセスできる状態を確保すること。

⑻　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務に係る情報システム及びデータをいう。

⑼　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）。

(10)インターネット接続系

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。

(11)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。

(12)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。

3　情報セキュリティポリシーの位置付けと職員等、業務委託事業者及び外部サービス提供者の義務

情報セキュリティポリシーは、中札内村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。

したがって、中札内村長をはじめとして中札内村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、業務委託事業者及び外部サービス提供者は、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。

4　情報セキュリティ組織体制

情報セキュリティ対策を強力に推進するため、その責任及び権限を明確にした全庁的な組織体制を確立するものとする。

5　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。

6　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、情報資産への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)　部外者の侵入及び不正操作による機器又は情報資産の破壊・盗難・改ざん・消去等、及び不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃

(2)　職員等又は業務委託事業者による機器又は情報資産の持出、誤操作、アクセスのための認証情報又はパスワードの不適切管理、故意の不正アクセス又は不正行為による破壊・盗難・改ざん・消去等、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等

(3)　コンピュータウイルス、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

7　情報セキュリティ対策

上記６で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

(1)　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や、情報資産への損傷・妨害等を防止するために物理的な対策を講ずる。

(2)　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、業務委託事業者及び外部サービス提供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。

(3)　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、ネットワーク管理、不正プログラム対策等の技術面の対策、また、業務委託時のセキュリティ確保、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。

(4)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、端末への二要素認証の導入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、北海道自治体情報セキュリティクラウドへ加入し、不正通信の監視機能の強化等を実施する。

8　情報セキュリティ対策基準の策定

中札内村の様々な情報資産について、上記７の情報セキュリティ対策を講ずるに当たっては、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。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。

9　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。そのため、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、管理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。

10　情報セキュリティの公開

情報セキュリティポリシー及び情報セキュリティ実施手順は、公開することにより中札内村の行政運営に重大な支障を及ぼす恐れのある情報資産であることから、中札内村情報公開条例第６条第４号に規定に基づき非公開とする。

11　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、定期的に監査を実施する。

12　評価及び見直しの実施

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実施する。

## 第３章　中札内村行政全般における情報セキュリティ対策基準

中札内村行政全般における情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための中札内村行政全般の情報資産に関する情報セキュリティ対策の基準である。

### １　対象範囲

#### (1)　行政機関の範囲

この情報セキュリティポリシーの対象範囲は、中札内村が所掌する情報資産を取り扱う全ての機関とする。

#### (2)　情報資産の範囲

この情報セキュリティポリシーの対象となる情報資産は、次のとおりとする。

ア　ネットワーク、情報システム、これらに関する設備、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

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

### ２　組織・体制

中札内村の情報セキュリティ管理については、以下の組織・体制とする。

⑴最高情報セキュリティ責任書（Chief Information Security Officer、以下「CISO」という。）

・副村長をCISOとする。

・CISOは本村における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有す。

⑵統括情報セキュリティ責任者

・総務課長を統括情報セキュリティ責任者とする。

・統括情報セキュリティ責任者はCISOを補佐し、本村の全ネットワークにおける開発、設定の変更、運用、情報セキュリティ対策に関する権限及び責任を有す。

・統括情報セキュリティ責任者は、管理責任者及び情報システム担当者に対して情報セキュリティに関する指導及び助言を行う権限を有する。

・統括情報セキュリティ責任者は、本村の情報資産に対するセキュリティ侵害が発生した場合又はそのおそれがある場合、直ちに必要な措置を行い、CISOに報告しなければならない。また、CISOが不在の場合には自らの判断に基づいて必要な措置を行う権限及び責任を有する。

⑶管理責任者

・各課等の課長、事務局の長を管理責任者とする。

・管理責任者は、その所管する情報システム及び情報資産のセキュリティを保護するための権限と責任を有する。

・管理責任者は、本村の情報資産に対するセキュリティ侵害が発生した場合、直ちにCISO及び統括情報セキュリティ責任者へ報告し、必要な措置を講じなければならない。

⑷情報システム担当者

・管理責任者の指示に従い情報システムの開発、設定の変更、運用、更新などの作業を行う者を、情報システム担当者とする。

・情報システム担当者は、本村の情報資産に対するセキュリティ侵害が発生した場合、直ちに統括情報セキュリティ責任者及び管理責任者へ報告し、必要な措置を講じなければならない。

⑸庁内情報化検討委員会

・庁内情報化検討委員会は、本村の情報セキュリティ対策を統一的に管理するため、情報セキュリティポリシーの策定や改正等、情報セキュリティに関する重要な事項を審議する。

## 3　情報資産の分類と管理

### ⑴　情報資産の管理責任

ア　管理責任

情報資産は、当該情報資産を作成した各課等の管理責任者が管理責任を有する。

イ　利用者の責任

情報資産を利用する者は、情報資産の分類に従い利用する責任を有する。

ウ　個人の責任

管理責任の明確でない情報については、個人が適切に管理する責任を有する。

エ　重要性の効力

情報資産が複製又は伝送された場合には、当該複製等も分類に基づき管理しなければならない。

(2)　情報資産の分類と管理方法

ア　情報資産の分類

対象となるネットワーク及び情報システムの情報資産は、各々の情報資産の機密性、安全性及び可用性を踏まえ、次の重要性分類に従って分類する。

| 区分 | 内　　容 |
|---|---|
| Ⅰ | 個人番号及び個人番号に代わって用いられる記号や符号であって住民票コード以外のものをその内容に含む個人情報 |
| Ⅱ | 個人情報及びセキュリティ侵害が中札内村の住民の生命、財産等へ重大な影響を及ぼす情報 |
| Ⅲ | 公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報 |
| Ⅳ | 外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等に軽微な影響を及ぼす情報 |
| Ⅴ | 上記以外の情報 |

イ　情報資産の管理方法

(ｱ)　情報資産の分類の表示

・情報システムで扱う情報資産について、第三者が重要性の識別を容易に認識できないように留意しつつ、印刷、ディスプレイ等への表示、記録媒体等に格納する際の媒体（ＦＤへのラベル等）について、ファイル名、記録媒体等に情報資産の分類が分かるように表示をする等適切な管理を行わなければならない。

(ｲ)　情報資産の管理

・情報資産の分類に従い、アクセス権限を定めなければならない。

・重要性分類Ⅰの情報資産を取扱うにあたっては、特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）（平成26年　特定個人情報保護委員会告示第6号）を遵守しなければならない。

・職員等は、情報資産（複製を含む。）の保管場所からの移動及び庁外への持出しが業務上必要となったときは、移動については管理責任者、持出しについてはCISOの許可を得

なければならない。

・重要性分類がⅠ～Ⅲの情報資産を電子メール等により送信する際は、信頼のできるネットワーク回線を使用しなくてはならない。

・各情報資産については、該当する重要性分類に応じ機密性を高めた管理をしなければならない。

(ｳ) 記録媒体の管理

・取り出しが可能な記録媒体は、適切な管理を行わなければならない。

・最終的に確定した情報資産を記録した記録媒体は、書込禁止措置を行った上で保管しなければならない。

・情報資産を記録した記録媒体は、施錠可能な場所に適切に保管しなければならない。

・記録媒体に納められた情報資産は全て別の記録媒体に複製し、当該記録媒体は自然災害を被る可能性の低い場所に別途保管しなければならない。

・記録媒体を送る場合は信頼できる者を選定し、複製の禁止や適切な管理等について指導及び監督を行わなければならない。

(ｴ) 情報資産の変更又は廃棄の管理

・記録媒体が不要となった場合は、当該媒体に含まれる重要な情報資産（重要性分類Ⅰ～Ⅲ）は、記録媒体の初期化など情報資産を復元できないように消去を行った上で廃棄しなければならない。

・重要な情報資産（重要性分類Ⅰ～Ⅲ）を記録した記録媒体の廃棄は、管理責任者の許可を得ることとし、行った処理について、日時、担当者及び処理内容を記録しなければならない。

4 情報システム全体の強靭性の向上

(1) マイナンバー利用事務系

ア マイナンバー利用事務系と他の領域との分離

(ｱ) マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定（MAC アドレス、IP アドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行う。また、その外部接続先についてもインターネット等と接続しない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先についてはこの限りではなく、インターネット等からマイナンバー利用事務系との双方向でのデータの移送を可能とする。

イ 情報の持ち出し不可設定

(ｱ)マイナンバー利用事務系へアクセスする場合は、二要素認証を利用しなければならない。

(ｲ)原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しをしてはなら

ない。ただし、業務上必要である場合は、実施手順に従い統括情報セキュリティ責任者に許可を得て必要最低限での持ち出しを行うことができる。

(2) LGWAN 接続系

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、インターネット接続系の端末から LGWAN 接続系の端末へデータを取り込む場合は、無害化した上で取り込まなければならない。

(3) インターネット接続系

インターネット接続系においては、北海道自治体情報セキュリティクラウドへの接続、通信パケットの監視、ふるまい検知等の不正通信監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

5 物理的セキュリティ

(1) サーバ類

ア 装置の設置等

(ｱ) サーバの設置に際しては、温度、湿度等の環境条件を十分留意した電算室又はラック（固定式）を準備し、地震にも耐えられるような対策を施さなければならない。また、盗難防止対策を施さなければならない。

(ｲ) 統括情報セキュリティ責任者及び操作の認められた職員、委託業者以外の者が容易に操作できないように、パスワードの設定等の措置を施さなければならない。また、必要に応じ当該パスワードの設定等を変更しなければならない。

イ 電源

(ｱ) サーバ類の機器の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

(ｲ) 落雷等による過電流に対してサーバ等の機器を保護するための措置を施さなければならない。

ウ 配線

(ｱ) 配線は、防護等の措置を施し、主要な部分については定期的に点検し、損傷のないようにしなければならない。

(ｲ) ネットワーク接続口（ハブ等）は、設置場所に留意し、他の者が容易に発見できない場所に設置しなければならない。

(ｳ) 統括情報セキュリティ責任者及び操作の認められた職員、委託業者以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

(2) 機器の定期保守及び修理

ア 統括情報セキュリティ責任者は、情報資産の分類区分Ⅰ～Ⅲのサーバ等の機器の定期保守

を実施しなければならない。

(3)　庁外への機器の設置

統括情報セキュリティ責任者は、庁外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策について確認しなければならない。

(4)　機器の廃棄やリース返却等

統括情報セキュリティ責任者は、機器を廃棄やリース返却等する場合、機器内部の記憶装置から全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

(5)　管理区域

ア　管理区域

(ｱ)　ネットワークの基幹機器及び重要な情報システムを設置し、管理及び運用をするための部屋は、災害及び機密性を考慮した管理区域にしなければならない。

(ｲ)管理区域への入退室は許可された者のみとし、IC カードによる入退室を行うものとする。

(ｳ)統括情報セキュリティ責任者は、外部からの訪問者が管理区域に入る場合は、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

イ　機器等の搬入出

(ｱ)　管理区域へ機器等を搬入する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について、職員による確認を行なわなければならない。

(ｲ)　機器等の搬入出には職員が同行する等の必要な措置を講じなければならない。

(6)　ネットワーク

ア　外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

イ　ネットワークに使用する回線は、伝送途上において破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策が実施されたものでなければならない。

6　人的セキュリティ

(1)　職員等の役割・責任

ア　職員等は、情報セキュリティポリシー及び実施手順に定められている事項を遵守し、情報システム及び情報資産を適切に管理しなければならない。

イ　職員等は、事故等セキュリティ上の問題を発見したときは、管理責任者及び統括情報セキュリティ責任者に速やかに連絡し、その指示に従い、必要な措置を講じなければならない。

ウ　職員等は、端末や記録媒体を使用するに当たり、外部に情報が漏れることのないように最新の注意を払い、必要な措置を講じなければならない。

エ　非常勤職員及び臨時職員の端末操作については、ネットワークへのアクセス、インターネ

ット及び電子メール等において必要に応じ使用上の制限を設ける。

(2)　業務委託

ア　統括情報セキュリティ責任者及び管理責任者は、情報システムの開発やネットワークの保守等、業務を委託するときは、情報セキュリティポリシーの遵守すべき内容及び守秘義務を明記した上で契約を締結するとともに、名札の着用のほか必要に応じ身分証明書の提示を求め、疑義がないかを確認しなければならない。

イ　統括情報セキュリティ責任者及び管理責任者は、委託業者との契約において、損害賠償等、情報セキュリティポリシーが遵守されなかった場合について規定を定めなければならない。

(3)　教育・訓練

ア　CISOは、情報セキュリティポリシーについての説明会等の実施により全ての職員等及び関係者に対しその内容を周知させなければならない。また、新規採用の職員等に対しても同様とする。

イ　統括情報セキュリティ責任者は、最新のセキュリティ情報を収集するとともに、情報セキュリティポリシーに関する技術的な教育及び訓練を受けなければならない。また、緊急時対応を想定した訓練を職員等に計画的に行わせなければならない。

ウ　職員等は、情報セキュリティポリシー及び実施手順を正しく理解し実施するために、定められた研修等に参加しなければならない。

(4)　情報セキュリティインシデントの報告

ア　職員等は、情報セキュリティインシデントを認知した場合には、速やかに統括情報セキュリティ責任者及び管理責任者に報告し、統括情報セキュリティ責任者の指示に従って必要な措置を講じなければならない。また、管理責任者は、報告のあったインシデントについて全てCISOに報告しなければならない。

イ　統括情報セキュリティ責任者は、これらの事故等を分析し、再発防止のための情報資産として記録を保存した上で、必要に応じてCISOに報告しなければならない。

(5)　ID、パスワード、ＩＣカード等の管理

ア　IDの取り扱い

職員等は、自己の管理するIDについて、自己が利用しているIDを他人に利用させてはならない。また、共用IDを利用する場合は、共用IDの利用者以外に利用させてはならない。

イ　パスワードの管理

職員等は、自己の保有するパスワードに関し、次の事項を遵守しなければならない。

(ｱ)　パスワードを秘密にし、パスワードの照会等には一切応じないこと。

(ｲ)　パスワードのメモ等は作らないこと。

(ｳ)　パスワードは４文字以上で、できる限り推測が困難なものにすること。

(ｴ)　パスワードが流出した恐れがある場合には、パスワードを速やかに変更すること。

(ｵ)　パスワードを他の職員等と共有してはならない。

ウ　ＩＣカード等の管理

職員等は、自己の保有するＩＣカード等に関し、次の事項を遵守しなければならない。

(ｱ)　ＩＣカード等を職員等間で共有してはならない。

(ｲ)　ＩＣカード等は厳格に管理し､紛失したときは速やかにCISO及び統括情報セキュリティ責任者に報告しなければならない。また、統括情報セキュリティ責任者は、通報があり次第速やかに当該ＩＣカード等を使用したアクセス等を停止しなければならない。

(ｳ)　ＩＣカード等はカードリーダ又は端末のスロット等に常時挿入してはならない。

7　技術的セキュリティ

(1)　ネットワーク、情報システム及び情報資産の管理

ア　統括情報セキュリティ責任者は、アクセスログ等システム及びセキュリティの維持に必要な情報を一定の期間適切に保存し、必要に応じそれらのログを解析し、監視しなければならない。

イ　管理責任者は、管理する情報システムの変更等に係る処理について、その記録を適切に管理しなければならない。

ウ　管理責任者は、システムの構築や変更に関し業務委託を行ったときは、契約書等において守秘義務を課さなければならない。

エ　統括情報セキュリティ責任者及び管理責任者は、情報システム仕様書等のドキュメント類に関して、重要性分類に応じ適切に管理しなければならない。

オ　統括情報セキュリティ責任者及び管理責任者は、ネットワーク又はシステムの障害対応をしたときは、その内容を記録し、適切に管理しなければならない。

カ　統括情報セキュリティ責任者及び管理責任者は、情報システムのミラーリング等に関わりなく情報資産の重要度に応じて期間を設定し、定期的に情報資産のバックアップを取得し、事故時に備えなければならない。

(2)　ネットワーク及び情報システムを使用する際の規定

ア　業務目的以外の使用の原則禁止

職員等によるネットワーク及び情報システムの使用は、業務目的に沿ったもののみが許可される。業務目的以外での情報システムへのアクセス、メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

イ　職員等は支給以外のパソコン、モバイル端末及び電磁的記録媒体等の利用を原則業務に利用してはならない。ただし、業務上必要である場合は、CISOに許可を得て利用することができる。

ウ　机上の端末等の管理

(ｱ)職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は統括情報セキュリティ責任者の許可なく情報を閲覧される

ことがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

エ　職員等は、人事異動や退職等により関係業務から離れるときは、業務により知り得た情報を外部に漏らしてはいけない。

オ　情報資産の持ち出し及びインターネット等による情報資産の送信禁止

職員等は、重要性分類Ⅰ～Ⅲの情報資産について、庁外への持ち出し及びインターネット等による庁外との送受信を行ってはならない。また、重要性分類Ⅰに該当する情報資産については、端末から持ち出すことを禁じる。

上記の規定に違反した職員等は、地方公務員法による懲戒処分の対象とする。ただし、法令で定めのある場合や、情報提供が業務上必要不可欠である場合、情報資産のバックアップ等、合理的理由がある時は、統括情報セキュリティ責任者の許可を得て行うことができる。

カ　無許可ソフトウェアの導入の禁止

職員等は、端末等に対して、無断でソフトウェアを導入してはならない。無断で導入又は使用した職員等は地方公務員法による懲戒処分の対象とする。ただし、合理的理由のある場合は、実施手順に沿って統括情報セキュリティ責任者及び管理責任者の許可を得た上で利用することができる。

統括情報セキュリティ責任者は、ソフトウェア等の端末へのインストールが許可なく行われた事を発見した場合は、その使用を停止することができる。

キ　機器構成の変更の禁止

職員等は、端末等に対して機器の増設又は改造を行ってはならない。特にモデム等の機器を増設して他の環境（インターネット等）へのネットワーク接続を行うことや、庁外からのアクセスを可能とする仕組みを構築した職員等は地方公務員法による懲戒処分の対象とする。ただし、業務を円滑に遂行するために必要な機器構成の変更については、合理的理由のある場合、かつ統括情報セキュリティ責任者及び管理責任者の許可を得た場合に限り、行うことができる。

統括情報セキュリティ責任者は、ネットワーク機器の増設、改造及び分解等を許可なく行われた事を発見した場合は、その使用を停止することができる。

ク　情報及びソフトウェアの交換

組織間において、情報システムに関する情報及びソフトウェアを交換する場合は、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者及び管理責任者の許可を得なければならない。

ケ　メールサーバ

統括情報セキュリティ責任者は、メールサーバの運用に対し次の事項を実施しなければならない。

(ｱ)　電子メールの送受信に関し、外部の攻撃に備えた設定を施す。

(ｲ)　送受信する電子メールの容量に上限を設定する。

(ｳ)　各課等に割当てるメールボックスの容量に上限を設定し、それを超えた場合は統括情報セキュリティ責任者の指示により管理責任者が削除等の対策を講ずる。

(ｴ)　その他メールサーバの運用に関する事項は、実施手順に定める。

コ　文書サーバ

統括情報セキュリティ責任者は、文書サーバの運用に対し次の事項を実施しなければならない。

(ｱ)　職員等が使用できる文書サーバの容量は、各課等１００ＧＢ以内とする。なお、サーバの更新等がある場合は、情報システム担当者は、各課等の使用容量を別途指示することができる。

(ｲ)　文書サーバは課等単位で構成し、他の課等のフォルダ及びファイルを閲覧及び使用できないような設定を施す。

(ｳ)　同一課等であっても、住民の個人情報、人事記録等特定の職員等しか取り扱うことのできないデータについては、別途ディレクトリを作成し、担当職員等以外の職員等が閲覧及び使用できないような設定を施す。

(ｴ)　その他文書サーバの運用に関する事項は、実施手順に定める。

サ　情報システムの入出力データ

(ｱ)　情報システムに入力されるデータは、適切なチェック等を行い、それが正確であることを確実にするための対策を施さなければならない。

(ｲ)　エラー又は故意の行為により情報が改ざんされる恐れがある場合、これを検出する手段を講じなければならない。

また、改ざんの有無を検出し、必要な場合は情報の修復を行う手段を講じなければならない。

(ｳ)　情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力されることを確認しなければならない。

シ　その他

職員等が利用できるプロトコル（通信手順、通信規約等）は、業務上必要最低限のものとする。

ス　Web 会議サービスの利用時の対策

(ｱ)統括情報セキュリティ責任者は、Web 会議を適切に利用するため適切な管理を実施しなければならない。

(ｲ)職員等は、Web 会議サービスを利用する場合、必要な対策を実施するとともに、事前に利用申請を行い承認を得なければならない。

セ　ソーシャルメディアサービスの利用

ソーシャルメディアサービスの利用については中札内村職員のソーシャルメディア利用に関するガイドラインに従うこと。

ソ　外部サービスの利用

(ｱ) 管理責任者は、外部サービスを利用する際は統括情報セキュリティ責任者の許可を得て利用しなければならない。

(ｲ) 管理責任者は、外部サービス提供者を選定する際は、必要なセキュリティが確保されていること及び信頼性が十分であることを確認しなければならない。

(3)　アクセス制御

ア　ユーザ登録等

(ｱ)　管理責任者は、情報システム等を利用する業務に従事する職員等（以下「ユーザ」という。）を指定し、統括情報セキュリティ責任者に報告しなければならない。

(ｲ)　統括情報セキュリティ責任者は、ユーザの新規登録、人事異動による変更、退職等による抹消等のほか、ユーザ全般の登録情報について、適切に管理しなければならない。

(ｳ)　統括情報セキュリティ責任者は、職員等のユーザ及びパスワードに関する情報を厳重に管理し、正しく運用されているかを定期的に調査しなければならない。

イ　管理者権限

(ｱ)　統括情報セキュリティ責任者は全ネットワークを管理する権限を持ち、その権限を代行する者は統括情報セキュリティ責任者が指名し、ＣＩＳＯが認めた者でなければならない。

(ｲ)　端末機等の管理者権限については、必要に応じて管理責任者に付与するものとする。

ウ　アクセス制御

(ｱ)　管理責任者は、所掌する情報システム等をネットワークに新たに接続するとき若しくは変更又は廃止するときは、統括情報セキュリティ責任者に申請しなければならない。

(ｲ)　統括情報セキュリティ責任者は、ネットワーク又はネットワーク上のサービスごとにアクセスできる者を定め、その権限を有しない職員等が当該サービスを使用できないようにしなければならない。

エ　経路制御

統括情報セキュリティ責任者は、不正アクセスを防止するため、適切なネットワーク経路制御を施さなければならない。

オ　外部からのアクセス

統括情報セキュリティ責任者は、外部から本村のネットワークにアクセスさせるときは、原則として外部に公開されているサーバに対してのみ行わせるものとし、直接内部ネットワークにアクセスすることを許可してはならない。ただし、業務上必要となる場合は実施ガイドラインに沿って、CISO の許可を得てアクセスすることができる。

カ　総合行政ネットワーク及び住民基本台帳ネットワークシステムとの接続

総合行政ネットワーク及び住民基本台帳ネットワークシステムについては、当該接続にお

いて取り扱う情報資産の重要性を考慮し、適切なアクセス制御を実施する。

キ　外部機関との接続

(ｱ)　ネットワークと外部機関との接続は、システムの保守及び管理上必要な場合にのみ期間を定めてCISOが許可する。この場合、接続しようとするネットワークの機器構成及びセキュリティレベル等を十分に勘案し、本村の情報システム及び情報資産に脅威を与えることがないことを確認しなければならない。

(ｲ)　その運用に当たっては、統括情報セキュリティ責任者の常時監視のもとに適切に行わなければならない。

(ｳ)　接続している外部機関が本村の情報システム及び情報資産に対し新たな脅威を与える可能性が生じたときは、統括情報セキュリティ責任者の判断により直ちにその接続を物理的に切断することができる。

ク　接続時間の制限

管理者権限によるネットワーク及び情報システムへの接続については、必要最小限のアクセス時間とし、その作業については、統括情報セキュリティ責任者が監督しなければならない。

(4)　情報システムの開発、導入、保守等

ア　情報システムの新規導入等

(ｱ)　統括情報セキュリティ責任者は、情報システムの新規導入及び機器又は基本ソフトの購入に係る基準等を実施手順に明記しなければならない。

(ｲ)　管理責任者は、情報システムの新規導入及び機器及び基本ソフト等の購入に際しては、情報セキュリティ上の問題点を十分に確認し、実施手順に明記された基準を遵守するとともに、必要に応じ統括情報セキュリティ責任者の意見を聴かなければならない。

(ｳ)　統括情報セキュリティ責任者及び管理責任者は、情報システムを新たにネットワークに接続させる際には、テストを十分に行い、既存のシステムに影響を及ぼさないようにしなければならない。

イ　情報システムの開発、保守、変更等

(ｱ)　管理責任者は、ソフトウェアの更新又は修正及びハードウェアの入替等情報システムの変更を行う場合は、既存のシステムとの相性等を十分確認の上、実施し、その内容について記録を残さなければならない。

(ｲ)　管理責任者は、委託により行う情報システムの開発及び保守に際しては事故及び不正行為等の防止のため、次に掲げる事項について明示又は遵守させた上で作業を実施させなければならない。

・作業責任者及び作業者並びに作業内容の報告

・リスク分析及びセキュリティ要件の抽出

・ソースコード等ドキュメントの提出及びその適切な管理

・セキュリティ上問題のある基本ソフト、ミドルウェア及びアプリケーションソフトの使用禁止

・開発時のアクセス制限

(ｳ)　統括情報セキュリティ責任者は、開発又は保守等により臨時で設定したＩＤ、パスワードその他の権限について、作業終了後速やかに抹消しなければならない。

ウ　機器の修理及び廃棄やリース返却等

(ｱ)　管理責任者は、記録媒体にデータ（個人情報等）のある機器を外部への持出しにより修理させるときは、守秘義務を契約書等に明記しなければならない。

(ｲ)　管理責任者は、記録媒体にデータのある機器を廃棄やリース返却等するときは、記録媒体を初期化し、乱数を書込む等適切な措置を施さなければならない。

(5)　不正プログラム対策

ア　統括情報セキュリティ責任者は、不正プログラム対策として次に掲げる事項を実施しなければならない。

(ｱ)　外部のネットワークから受信したファイル（電子メール等）は、ファイアウォールレベルで不正プログラムのチェックを行い、内部への侵入を未然に防止する。

(ｲ)　外部のネットワークに送信するファイル（電子メール等）は、ファイアウォールレベルで不正プログラムのチェックを行い、外部への拡散を未然に防止する。

(ｳ)　ネットワーク上にあるサーバ及び端末に対して、最新の不正プログラムチェック用のパターンファイルを配信するなどの対策を講ずる。

(ｴ)　不正プログラムに関する最新情報を常に収集し、必要に応じ職員等に提供し、注意喚起を促す。

イ　管理責任者は、不正プログラム対策として次に掲げる事項を実施しなければならない。

(ｱ)　サーバ及び端末において、不正プログラムチェック用パターンファイルが最新であるかどうか常に確認する。

(ｲ)　サーバ及び端末において、不正プログラムが発見されたときは、速やかに統括情報セキュリティ責任者に報告する。

ウ　職員等は、不正プログラム対策として次に掲げる事項を実施しなければならない。

(ｱ)　外部から持ち込まれる記録媒体については、必ず実施手順に沿って不正プログラムのチェックを実施し、安全性を確認する。

(ｲ)　差出人不明の電子メール又は添付ファイルは、統括情報セキュリティ責任者に報告し、その指示に従い処理する。

(ｳ)添付ファイルが付いた電子メールを送受信する場合は、ウイルス対策ソフトでチェックを行う。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルをLGWAN接続系に取り込む場合は無害化しなければならない。

(ｴ)統括情報セキュリティ責任者から提供される不正プログラムの情報を常に確認する。

(6)　不正アクセス対策

ア　統括情報セキュリティ責任者は、次の事項を実施しなければならない。

(ｱ)　ポートの管理を徹底し、空けるポートは必要最小限のポートのみとする。

(ｲ)　セキュリティホールの最新情報を常に収集し、メーカー等からパッチの提供があったときは、速やかにそのパッチをあてバージョンアップ等の対策を施す。

(ｳ)　ネットワークの基幹部分及び重要なシステムの設定に係るファイル等については、定期的に調査し、改ざんされていないかを確認する。

(ｴ)　標的型攻撃による内部への侵入を防止するために、職員等への教育やネットワークの入口対策等を行う。

イ　攻撃を受けることが明確な場合には、統括情報セキュリティ責任者はシステムの停止を含む必要な措置を講じなければならない。

ウ　職員等による不正アクセスがあった場合、統括情報セキュリティ責任者は当該職員等が所属する課等の管理責任者に通知し、適切な処置を求めなければならない。

職員等による不正アクセスの結果、データの漏洩、破壊、改ざん又はシステムダウン等により行政業務に深刻な影響がもたらされた場合、当該職員等を地方公務員法による懲戒処分の対象とする。

(7)　セキュリティ情報の収集

ア　統括情報セキュリティ責任者は、情報セキュリティに関する情報を収集し、中札内村の全てのネットワーク及び情報システムについてソフトウェアにパッチを当てる等、セキュリティ対策上必要な措置を講じなければならない。

イ　CISOは、これらの情報を定期的に取りまとめ、関係部局等に通知するとともに、情報セキュリティポリシーの改定につながる情報については、庁内情報化検討委員会に報告しなければならない。

8　運用

(1)　情報システムの監視

統括情報セキュリティ責任者は、次の事項を実施しなければならない。

ア　外部と常時接続するネットワークについては、ファイアウォール等を設置し、接続状況を常時監視する。

イ　全ての情報システムについて、アクセスログ等により運用を監視する。

ウ　監視により得られた結果を定期的にチェックし、必要な措置を講じ、消去又は改ざんされることのないように適切に保管する。

(2)　情報セキュリティポリシーの遵守状況

ア　管理責任者は、情報セキュリティポリシーの遵守状況について常時監視し、問題が生じたときはCISO及び統括情報セキュリティ責任者に速やかに報告しなければならない。

イ　CISOは、速やかに発生した問題に適切に対処しなければならない。

ウ　職員等は、情報セキュリティポリシーの違反が発生した場合には、その内容の重大性にかかわらず、直ちに管理責任者に報告しなければならない。

(3)　運用管理における留意点

CISO及び統括情報セキュリティ責任者は、セキュリティ上の重大な問題が発生したときには、アクセス記録及びメールの内容について閲覧することができる。

(4)　侵害時の対応

情報セキュリティインシデントの発生により、情報システム及び情報資産が侵害されたときは、被害の拡大防止、迅速な復旧、証拠保全及び再発防止を図るため、次に掲げる対策を実施する。

ア　連絡及び報告

情報システム及び情報資産への侵害を発見した者は、実施手順に定める連絡系統に基づき直ちに連絡及び報告をしなければならない。

イ　調査

統括情報セキュリティ責任者は、報告に基づき詳細な調査を実施し、CISO及び庁内情報化検討委員会に報告しなければならない。

ウ　対策

(ｱ)　統括情報セキュリティ責任者は、次に掲げる本村の情報システム及び情報資産が脅威にさらされた状況が発生したときは、それらを保護するためネットワークを切断することができる。

a　異常なアクセスが継続しているとき

b　不正アクセスが発見されたとき

c　システムの運用が支障をきたすとき

d　不正プログラムが増殖しているとき

e　その他に情報資産へ重大な被害を与える可能性のあるとき

(ｲ)　管理責任者は、次に掲げる状況が発生した場合は所管の情報システムを停止しなければならない。

a　不正プログラムが増殖し、さらに被害が拡大する可能性があるとき

b　災害等により長時間の停電が発生する可能性があるとき

c　その他に情報資産へ重大な被害を与える可能性のあるとき

(ｳ)　職員等は、次に掲げる状況が発生した場合は、端末からLANケーブルを取り外し、モバイル端末の場合は通信を不可設定にしなければならない。

a　不正アクセスが発見されたとき

b　不正プログラムが実行されているとき又はその疑いがあるとき

c　その他に情報資産へ重大な被害を与える可能性のあるとき

エ　再発防止

統括情報セキュリティ責任者及び管理責任者は、発生した事案についてのリスク分析を実施し、再発防止に向け関連する情報セキュリティポリシー及び実施手順を改正しなければならない。

9　法令の遵守

職員等は、職務の遂行において次の法令等を遵守し、これに従わなければならない。

(1)　著作権法（昭和４５年法律第４８号）

(2)　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）

(3)　個人情報の保護に関する法律（平成１５年法律第５７号）

(4)　行政手続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（平成２５年法律第２７号）

(5)　中札内村個人情報保護条例（平成１２年条例第３８号）

(6)　中札内村行政手続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に基づく個人番号の利用及び特定個人情報の提供に関する条例（平成２７年条例第２３号）

(7)サイバーセキュリティ基本法

10　情報セキュリティに関する違反に対する対応

情報セキュリティポリシーに違反した職員等及びその監督責任者に対しては、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による懲戒処分の対象とする。

なお、職員等に情報セキュリティポリシーに違反する行動が見られた場合には、速やかに次の措置を講じなければならない。

(1)　統括情報セキュリティ責任者が違反を発見した場合は、当該職員等が所属する課等の管理責任者に通知し、適切な措置を求めなければならない。

(2)　管理責任者が違反を発見した場合は、速やかに統括情報セキュリティ責任者に報告し、その指示に従って必要な措置を講じなければならない。

(3)　統括情報セキュリティ責任者及び管理責任者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムの使用に関する権利を停止あるいは剥奪することができる。その場合速やかに、統括情報セキュリティ責任者が職員等の権利を停止あるいは剥奪した旨を CISO 及び当該職員等が所属する課等の管理責任者に通知しなければならない。

11　評価・見直し

(1)　情報セキュリティ監査

庁内情報化検討委員会は、ネットワーク及び情報システムの情報セキュリティポリシーの遵守状況について、定期的に監査を実施しなければならない。開発又は運用等を業務委託している場合も同様とする。その他監査の実施に関する事項は、実施手順で定める。

(2) 情報セキュリティポリシーの見直し

庁内情報化検討委員会は、ネットワーク環境の変化又は新たな対策の発生等により情報セキュリティポリシーを見直す必要が生じたときは、監査の結果を踏まえ、これを見直さなければならない。

【用語解説】

・個人番号…行政手続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（平２５年法律第27号）第２条第５項に規定する個人番号のこと。
・情報セキュリティインシデント…情報セキュリティを脅かす危険のある事件や事故のこと。ウイルス感染や不正アクセス、Webサイトの改ざん、情報漏洩などを含む。
・ログ…データベースの変更に関する情報の記録のこと。ネットワークの運用においてはディスクなどに保存した利用履歴を指す。
・ドキュメント…説明書や仕様書のこと。
・ミラーリング…ハードディスクの共有領域にまったく同じデータを保存し、ディスクにおけるデータ破壊の危険を少なくする方式のこと。
・インストール…ソフトウェアをコンピュータに導入し、使用可能な状態にする処理や作業のこと。
・ディレクトリ…ディスクなどにあるファイルを管理するための表のこと。ここにファイルの場所や作成日付や属性などの情報が含まれている。フォルダとほぼ同義。
・プロトコル…データ通信の実行に必要な通信規約のこと。
・ＩＤ…ユーザを識別するための符号のこと。
・ソースコード…コンピュータプログラムの動作を人間が読み書きできるテキストファイルの形式で記述したコードのこと。
・ミドルウェア…アプリケーションを起動させるための最も基本的なソフトウェアであるＯＳと、アプリケーションの中間に位置するソフトウェアのこと。ＯＳよりも分野や用途がやや限定されたサービスを提供する。
・アプリケーション…ある特定の目的のために開発されるソフトのこと。文書作成や画像編集など幅広い分野で開発されている。
・不正プログラム…ウイルスやワームなどシステムやネットワークに害を及ぼすプログラムの総称。
・ファイアウォール…外部ネットワーク（インターネット）とＬＡＮなどの内部ネットワークの間に設置するセキュリティ対策用のシステムのこと。
・ポート…コンピュータと周辺機器の接続部で、ここを通じてデータが出入りする。
・標的型攻撃…特定の組織に狙いを絞り、その組織の内部状況に合わせて最適化した方法を用いて

執拗に行われるサイバー攻撃のこと。

・LGWAN…インターネットから切り離され、高度なセキュリティを維持した地方公共団体を相互に接続するネットワークのこと。

・北海道自治体情報セキュリティクラウド…道内市町村のインターネットの出入り口を一つに集約することで高度な情報セキュリティ対策を実施する外部機関のこと。

・業務委託…庁内等の情報システムの一部又は全部について、契約をもって外部の者に実施させること。

・外部サービス…庁外等の事業者が情報システムの一部又は全部の機能を提供するもののこと。ただし、情報資産の分類区分ⅠからⅣまでの情報を取り扱う場合に限る。