天川村情報セキュリティ基本方針

平成 31 年 3 月 27 日

目次

１　目的 3
２　定義 3
（１）ネットワーク 3
（２）情報システム 3
（３）情報セキュリティ 3
（４）情報セキュリティポリシー 3
（５）機密性 3
（６）完全性 4
（７）可用性 4
（８）マイナンバー利用事務系（個人番号利用事務系） 4
（９）LGWAN 接続系 4
(10) インターネット接続系 4
(11) 通信経路の分割 4
(12) 無害化通信 4
３　対象とする脅威 4
４　適用範囲 5
（１）行政機関の範囲 5
（２）情報資産の範囲 5
５　職員等の遵守義務 5
６　情報セキュリティ対策 5
（１）組織体制 5
（２）情報資産の分類と管理 5
（３）情報システム全体の強靭性の向上 5
（４）物理的セキュリティ 6
（５）人的セキュリティ 6
（６）技術的セキュリティ 6
（７）運用 6
（８）外部サービスの利用 6
（９）評価・見直し 7
７　情報セキュリティ監査及び自己点検の実施 7
８　情報セキュリティポリシーの見直し 7
９　情報セキュリティ対策基準の策定 7
10　情報セキュリティ実施手順の策定 7

１　目的

天川村の各情報システムが取り扱う情報には、村民の個人情報のみならず行政運営上重要な情報など、外部への漏洩等が発生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。

したがって、情報資産及び情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、村民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが天川村に対する村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IT革命の進展により、電子商取引の発展や電子自治体の構築が現実のものとなっている。天川村が電子自治体を構築するためには、全ての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である。

そのため、天川村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(情報セキュリティ対策)を整備するために天川村情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については天川村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、位置付け等を定めるものとする。

※ ２ 定義（5)、(6)、(7)参照

２　定義

（１）ネットワーク

天川村における内部部局、各行政委員会、各教育機関(事務室及び職員室のみ)を相互に接続するための通信網、その構成機器(ハードウエア及びソフトウエア)及び記録媒体で構成され、処理を行う仕組みをいう。

（２）情報システム

天川村が管理するコンピュータシステム（ハードウェア、ソフトウェア、ネットワーク及び可搬記録媒体）をいう。

（３）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。

（４）情報セキュリティポリシー

本規則及び情報セキュリティ対策基準をいう。

（５）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（６）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。

（７）可用性

情報にアクセスすることを認められた者が、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状態を確保することをいう。

（８）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。

（９）LGWAN 接続系

人事給与、財務会計及び文書管理等 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。

（10）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。

（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　対象とする脅威

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）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や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）情報資産の無断持ち出し、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、外部委託管理の不備、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、火災等の災害によるサービス及び業務の停止等
（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

4　適用範囲

（1）行政機関の範囲

本規則が適用される行政機関は、内部部局、各行政委員会とし、各教育機関(事務室及び職員室を除く)は対象外とする。

（2）情報資産の範囲

本規則が対象とする情報資産は、次のとおりとする。
① 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
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

5　職員等の遵守義務

天川村長をはじめとして天川村が所掌する情報資産に関する業務に携わる全職員、非常勤職員、臨時職員(以下「職員等」という)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。

6　情報セキュリティ対策

上記３の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じる。

（1）組織体制

天川村の情報資産について、幹部が率先して情報セキュリティ対策を推進・管理するため、天川村情報セキュリティ委員会のほか、必要な体制を整備する。

（2）情報資産の分類と管理

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。

（3）情報システム全体の強靭性の向上

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、端末からの情報持ち出し不可設定や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。

② 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。

（４）物理的セキュリティ

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・妨害等から保護するために物理的な対策を講ずる。

（５）人的セキュリティ

情報セキュリティに関する権限や責任を定め、全ての職員等及び外部委託事業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。

（６）技術的セキュリティ

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、ネットワーク管理等の技術的な対策を講ずる。

（７）運用

システム開発等の外部委託、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。また、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）外部サービスの利用

外部委託する場合には、外部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、外部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。

約款による外部サービスを利用する場合には、利用にかか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方針を定め、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、情報セキュリティポリシーの見直しを行う。

７　情報セキュリティ監査及び自己点検の実施

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、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する。

８　情報セキュリティポリシーの見直し

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。

９　情報セキュリティ対策基準の策定

天川村の様々な情報資産について、上記６、７及び８に規定する対策等を実施するために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。

10　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、内部部局の長等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。

なお、情報セキュリティポリシー(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天川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非公開とする。