天龍村情報セキュリティポリシー

情報セキュリティ基本方針

解説資料

平成１６年１１月　策定

令和８年３月　全面改訂

目次

序　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、天龍村の情報資産に対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文書を総称する。情報セキュリティポリシーは、天龍村の情報資産に関する業務に携わる職員等、及び外部委託業者に浸透、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）の2階層に分けて策定することとした。

（１）情報セキュリティ基本方針

天龍村としての情報セキュリティ対策に関する取り組み姿勢及び統一的な方針。

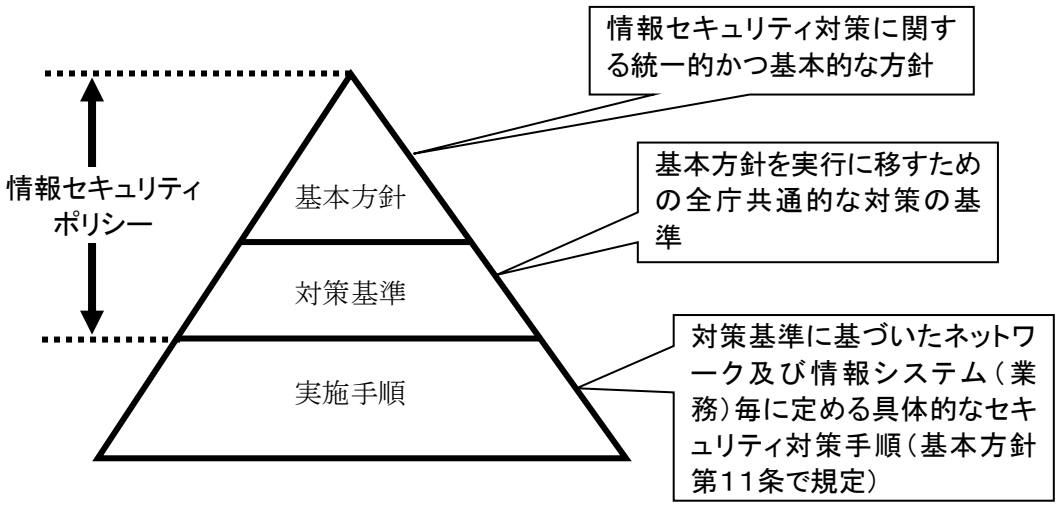
（２）情報セキュリティ対策基準

情報セキュリティ基本方針を実行に移すための天龍村におけるすべ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。

解説

情報セキュリティポリシー等の文書構成を示しています。

具体的には、以下のような構造になっています。



第１条　目的

天龍村の情報資産には、村民の個人情報をはじめ行政運営に必要な情報など、部外に漏洩、あるいは滅失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。これらの情報資産を人的脅威や災害、事故等から防御することは、村民の財産、プライバシーを守るためにも、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠であり、ひいては、天龍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、電子政府や電子自治体の実現が期待されている中で、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となる。

このため、天龍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を整備することを目的として、天龍村情報セキュリティポリシーを定め、情報セキュリティの確保に最大限取り組むものである。

このうち情報セキュリティ基本方針は、天龍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。

解説

セキュリティポリシー策定の目的が記述されています。

・自治体で取り扱う住民の個人情報の保護

・電子自治体等の高度な行政サービスへの対応に向けたシステムの安全性確保

これらの目的に対し、情報資産の機密性、完全性、可用性を維持するための対策を整備するため、情報セキュリティポリシーを策定し、情報セキュリティの確保に取り組むことを宣言します。

また、基本方針の位置付けは情報セキュリティ対策の基本的な方針です。

第２条　用語の定義

解説

今後の条文で使用する用語を定義します。

（1）ネットワーク

コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）で構成され、情報処理を行う仕組みをいう。

解説

この定義で対象となるネットワーク範囲を明確にします。

基本的な考え方として、組織が保有する情報資産を利用する部分を対象範囲とします。

教育機関、公共施設等に設置された住民等が利用する端末が庁内 LAN と物理的に分離されていない場合、対象範囲に含める必要があります。

（2）情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（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。

（4） 情報セキュリティポリシー

本基本方針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が認可された者だけがアクセスできることを確実にすること。

（6）完全性

情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

（7）可用性

許可された利用者が必要なときに情報にアクセスできることを確実にすること。

（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

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、コンピュータウィ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。

第3条　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、天龍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。

解説

情報セキュリティポリシーの位置付けを定めます。

情報セキュリティポリシーは、情報セキュリティ対策についてまとめた文書であり、セキュリティ対策の頂点、つまり、個々のセキュリティ対策の基本、拠り所となる文書です。

第４条　情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの適用範囲は、次の各項に定めるものとする。

（１）適用資産

情報セキュリティポリシーの適用対象資産は、天龍村における全ての情報資産とする。

（２）適用対象者

情報セキュリティポリシーの適用対象者は、天龍村における情報資産に接する全ての職員等とする。

解説

情報セキュリティポリシーが適用される範囲を定めます。

基本的に組織内におけるすべての情報資産（システムとデータ）と、それを利用する職員（本庁だけではなく、出先や関係機関を含みます）を対象範囲として定めます。

適用対象者としては、情報資産を利用する者を対象とするのが一般的ですが、本庁だけとする、村全体とするなどの選択肢からの検討が必要です。

第５条　職員等の義務

天龍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及び外部委託者は、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。

解説

全ての職員等（正式職員の他、嘱託等を含みます。）及び、部外の委託者に、情報セキュリティポリシーを遵守する義務があります。

この規定がなければ、情報セキュリティポリシーは無意味なものとなります。

第６条　情報セキュリティ管理体制

天龍村の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立するものとする。

解説

全庁統一的な情報セキュリティ対策を推進・管理するための体制を確立することを定めます。

具体的な体制については対策基準で定めます。

第７条　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。

解説

情報資産を機密性・完全性・可用性の観点から、段階的に分類します。

そして、分類された重要度に応じたセキュリティ対策を実施します。重要な情報資産に対する対策が不十分では問題であり、また、さほど重要でないものに対する対策に多額の費用を費やすのは非効率的です。

第８条　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）部外者の侵入による機器又は情報資産の破壊、盗難、故意の不正アクセスまたは不正操作による機器又は情報資産の破壊、盗聴、改ざん、消去等

（2）職員等及び外部委託者による機器又は情報資産の持出・誤操作、不正アクセス又は不正行為による破壊、盗聴、改ざん、消去、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、認証情報等の不適切な管理等

（3）コンピュータウィルス、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

解説

情報資産を脅かす脅威を列挙します。

(1)は、外部からの脅威（不正アクセス、物理的な盗難等）を表し、(2)は内部からの脅威（ミス、事故、不正アクセス等）を指します。

(3)は、コンピュータウィルス及び災害等によるサービスや業務の停止（特に可用性に対する侵害）を意味します。

第９条　情報セキュリティ対策

天龍村の情報資産を第8条に示した脅威から保護するために、以下の情報セキュリティ対策を講ずるものとする。

解説

第8条に列挙した脅威から情報資産を保護するために、次の4つのポイントからセキュリティ対策を実施します。

それぞれの具体的内容は対策基準に記述します。

（１）人的セキュリティ対策

情報資産に接する職員等の情報セキュリティに関する権限や責任等を定めるとともに、全ての職員等及び外部委託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、教育、訓練、啓発等を実施する。

解説

職員等に対するセキュリティ対策について記述します。秘密保持義務のある職員については、その権限や責任等を定める管理面での対策と、セキュリティポリシーを遵守するために、その理解を深めるべく教育・訓練を実施することが重要です。

また、外部委託者についても情報セキュリティポリシーを遵守するよう働きかける必要があります。

（２）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、情報資産への損傷・妨害等、災害による情報資産の破壊・情報システムの停止等から保護するために物理的な対策を講ずる。

解説

外部の人間及び権限のない職員等がサーバ室等に侵入し、損傷・妨害を与えたり、重要なデータ等の盗みだしを行えないよう、施設に施錠等の物理的な対策を実施します。

また、災害による破壊、停止などへの対処も実施します。

（３）技術的セキュリティ対策

情報資産を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、コンピュータウィルス対策等を実施する。

解説

外部及び内部の権限外者による不正アクセスや、コンピュータウィルスによる被害を防ぐため、認証やアドレス制限によるアクセス制御、ルータやファイアウォールを利用したネットワークセグメントの分割、コンピュータウィルス対策ソフトの適用など、技術面の対策を実施します。

（４）運用

情報セキュリティポリシーの実効性を確保するため、また、不正なアクセス等から適切に保護するため、システム開発等の外部委託、システムの管理、庁内ネットワークの監視、情報セキュリティポリシー遵守状況の確認等、運用面における必要な措置を講ずる。

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。

解説

運用面で必要なセキュリティ対策を実施することを定めます。

各種管理や監視、情報セキュリティポリシーの順守状況の確認（検査や監査など）は、情報セキュリティの維持において、必要不可欠といえます。

また、緊急事態（不正アクセスインシデントや災害等）が発生した場合に備えて、危機管理対策を整備することが必要です。

第１０条　情報セキュリティ対策基準の策定

天龍村の様々な情報資産について、第9条の情報セキュリティ対策を講ずるに当たっては、職員等が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。

解説

情報セキュリティ対策基準を策定することを定めます。

情報セキュリティ対策基準には、情報セキュリティ対策実施における基本的な要件を明記し、全庁統一的な行為、判断等の基準とします。

第１１条　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ことから、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、情報セキュリティ実施手順を策定するものとする。

解説

個別の情報資産について、情報セキュリティ対策基準に基づいて、具体的な対策を記述した情報セキュリティ実施手順を策定することを定めます。

第１２条　情報セキュリティポリシーの情報公開

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龍村の行政

運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

解説

情報セキュリティ対策について記述した文書は、組織におけるセキュリティ対策の具体的手順等が記述されますので、これらの文書が外部に公開された場合、組織におけるセキュリティ対策の手の内をあかすようなものであり、不正アクセス等の補助ともなり得ます。そのため、非公開とすることが重要です。

ただし、基本方針については、インターネット等で公開している地方公共団体も多数存在し、また、内容的にみても公開しても問題ないという考え方もあるため、基本方針のみ公開とすることも可能です。また、情報公開条例等との観点からも検討が必要です。

総務省のガイドラインでは、以下のようになっています。

「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○○市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。」

第１３条　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。

解説

情報セキュリティポリシーが遵守されていること、及び、情報セキュリティポリシーが実情に合ったものであるかなどを確認するために、定期的に監査を実施します。

監査結果は、セキュリティ対策の問題点を明らかにし、その後のセキュリティ対策の見直し等における参考とします。

第１４条　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。

解説

セキュリティ対策は、一度実施すればそれで良いものではなく、監査により明確になった問題点への対応や、技術の進歩や社会情勢の変化などを取り入れて、情報セキュリティポリシーの見直しから始まる、セキュリティ対策の再構築が重要です。

そのため、第14条では、評価・見直しの実施を行うことを定めます。