西目屋村情報セキュリティポリシー

平成１５年１１月　７日　策定
平成２８年　６月１３日　改正
令和８年　４月１日　改正

西目屋村

目　　次

序章　情報セキュリティに対する考え

地方公共団体は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有し、他に代替することができない行政サービスを提供している。行政サービスの業務の多くは、情報システムやネットワークを活用していることから、情報セキュリティ対策を講じて、住民生活や地域の社会経済活動を保護するために、保有する情報を守り、業務を継続することが必要となっている。

また、社会保障・税番号制度の導入により、各地方公共団体内で取り扱う情報がさらに重要なものになっており、個人番号を含む特定個人情報の漏えいには特に注意しなければならない。

今後、各種手続のオンライン利用の本格化や情報システムの高度化等により、情報システムへの依存度が増え、システムトラブルが発生した場合、複数に及ぶ行政サービスが継続できなくなることで、住民生活や地域の社会経済活動に重大な影響を与えることになり得る。LGWAN 等のネットワークにより地方公共団体が相互に接続されていることから、一部の団体のシステムトラブルがネットワークを介して他の地方公共団体に連鎖的に拡大することも考えられる。

これらの事情から、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが必要となっている。

情報セキュリティ対策は、情報の保護の点では、個人情報保護対策と内容的に重なる部分も多く、自然災害による被災時の対応という点では防災対策とも重なる部分がある。関連部署が相互に連携をとって、それぞれの対策に取り組み、情報セキュリティに関する事故の未然防止のための計画、事故が発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

西目屋村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、全ての情報資産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		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個々の情報資産に関する具体的な対策手順。

第１章　情報セキュリティ基本方針

１　目的

西目屋村の各情報システムが取り扱う情報には、村民の個人情報を筆頭に、外部への漏えい等が発生した場合に、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、情報セキュリティポリシーを策定し、機密性、完全性及び可用性（注）を維持するために情報セキュリティに関する基本的事項を定めることにより、情報資産、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よう高度な安全性を有することは、村民の財産やプライバシー等を守るためにも、また、業務の安定性確保のためにも必要不可欠であり、ひいては、このことが西目屋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。

（注）：国際標準化機構（ISO）が定めるもの（ISO 7498－2：1989）

機密性（confidentiality）：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。

完全性（integrity）：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。

可用性（availability）：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。

２　定義

（１）ネットワーク

西目屋村のパソコン、サーバ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）をいう。

（２）情報システム

電子計算機（ハードウェア及びソフトウェア）及び電磁的記録媒体で構成され、処理を行う仕組みをいう。

（３）情報資産

ネットワーク及び情報システムの開発と運用に係る全ての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に出力された情報も含むものとする。

（４）情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

（５）情報セキュリティポリシー

情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

3　情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務

本情報セキュリティポリシーは、西目屋村の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、地方自治法第２４４条の６に基づく「サイバーセキュリティを確保するための方針」として位置付ける。

したがって、西目屋村の情報資産に関する業務に携わる全ての職員（再任用職員及び任期付職員を含む）、非常勤職員、臨時職員（以下「職員等」という）及び外部委託事業者は、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しなければならない。

4　情報セキュリティ管理体制

情報セキュリティ対策を推進するため、最高情報セキュリティ責任者（CISO）を定め、情報資産に対するリスクの特定、評価及び対策の選定を継続的に行う全庁的な体制を確立する。

必要な体制、役割、権限等については、情報セキュリティ対策基準にて定める。

5　情報資産の分類

西目屋村が保有する情報資産を、機密性、完全性及び可用性に応じて分類し、当該分類に基づいて情報セキュリティ対策を実施する。

6　情報資産への脅威

情報セキュリティ対策を講ずるうえで、情報資産に対する脅威の発生度合い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）サイバー攻撃をはじめとする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又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）職員等又は外部委託事業者による機器若しくは情報資産の無断持出、誤操作、アクセスのための認証情報若しくはパスワードの不適切管理、故意の不正アクセス若しくは不正行為による破壊・盗聴・改ざん・消去等、搬送中の事故等による機器若しくは情報資産の盗難又は規定外の端末接続によるデータ漏えい等

（３）コンピュータウイルス、並びに事故、故障等によるサービス及び業務の停止

（４）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

（５）地震、落雷、火災等の災害によるサービス及び業務の停止

（６）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

（７）電力供給の途絶、通信の途絶、水道供給の途絶等の提供サービスの障害からの波及等

（８）ランサムウェア等による業務停止

（９）クラウドサービス及び外部委託先に起因する情報漏えい

（１０）サプライチェーンを通じた侵害

7　情報セキュリティ対策

西目屋村の情報資産を上記6の脅威から保護するため、以下の情報セキュリティ対策を適切に組み合わせ、情報資産の重要性及びリスク評価の結果を踏まえて、選択的に実施する。

（１）物理的セキュリティ対策

管理区域への不正な立入りを防ぎ、情報システム損傷等から保護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、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を行う。

（３）技術的セキュリティ対策

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、情報システムの管理、情報資産へのアクセス制御、不正プログラムの防御等の技術面の対策を講ずる。

8　情報セキュリティ対策基準の策定

西目屋村の情報資産について、上記7の情報セキュリティ対策を講ずるに当たっては、職員等が遵守すべき事項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こととする。

9　情報セキュリティ実施手順（運用マニュアル）の策定

情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定することとする。

なお、情報セキュリティ実施手順は、公開することにより西目屋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。

10　自己点検及び見直しの実施

情報セキュリティポリシーの遵守状況を検証するため、必要に応じて自己点検を実施する。

自己点検の結果等により、情報セキュリティ対策基準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２章　情報セキュリティ対策基準

１　対象範囲

この情報セキュリティポリシーは、村長部局に適用する。

教育委員会（学校を除く）、農業委員会事務局、議会事務局、選挙管理委員会、監査委員会、固定資産評価審査委員会については、地方自治法第１８０条の７の規定に基づき、情報セキュリティポリシーの策定及び運用に関する事務を村長の補助機関に委任し、本ポリシーを適用するものとする。

２　定義

この情報セキュリティ対策基準における用語の意義は、第１章 情報セキュリティ基本方針の２に規定する用語の定義を準用する。

３　組織・体制・役割等

ア　最高情報セキュリティ責任者（CISO：Chief Information Security Officer）

・情報政策を所管する企画財政課長を CISO とする。CISO は、西目屋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る。

・CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有する専門家をアドバイザーとして置くことができる。

イ　統括情報セキュリティ責任者

・住民課長を、CISO 直属の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 を補佐する。

・統括情報セキュリティ責任者は、西目屋村の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、CISO の指示に従い、CISO に事故がある等指示を仰げない場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

・統括情報セキュリティ責任者は、全庁の情報セキュリティ対策に関する統括的な権限及び責任を有する。

・統括情報セキュリティ責任者は、西目屋村の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

・統括情報セキュリティ責任者は、西目屋村の情報システムにおける開発、設定の変更、運用、見直し等を把握し、助言及び指示を行う。

・統括情報セキュリティ責任者は、西目屋村の共通的な情報資産に関する情報セキュリティ実施手順の策定及び維持・管理を行う権限及び責任を有する。

・統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者を網羅する連絡体制を整備し、管理しなければならない。