東白川村情報セキュリティ対策

（東白川村情報セキュリティポリシー
東白川村情報セキュリティ対策基準
東白川村情報セキュリティ実施手順）

東白川村役場

第1.0版

令和８年４月

目　次

Ⅰ　東白川村情報セキュリティポリシー

第１条　セキュリティ基本方針(趣旨)

情報通信技術の進展は著しく、その利用機会の拡大とともに、行政内部にも様々な情報資産の蓄積が進んでいる。

東白川村(以下「村」という。)においても、役場及び出先機関の各所に電算機器が設置され、各種媒体を用いて大量の電子データが保存管理されている。

これらの情報資産は、今日、様々な脅威に晒されており、個人情報等(東白川村情報公開及び個人情報保護に関する条例(平成14年東白川村条例第11号)第１条に規定する個人情報等をいう。)をはじめとする重要な情報について、その管理体制や対策を継続的に強化しながら、組織的に取り組んでいくことが不可欠になっている。

このため、村の保有する情報資産の保存・管理に関する基本方針と具体的方策を定め、その取り扱いルールの浸透・徹底を図る。

村の情報資産を取り扱う全ての者は、村民のプライバシーを守り信頼される行政運営を行うべく、情報セキュリティ対策の重要性を認識し、「東白川村情報セキュリティポリシー(以下「セキュリティポリシー」という。)」を遵守しなければならない。

第２条　適用範囲

セキュリティポリシーは、以下の組織(以下「村」という。)の情報資産に関連する人的・物理的・環境的資源について適用する。

（１）村長の事務局(村長公室、総務課、村民福祉課、産業建設課、会計管理者及び会計室、保育園)
（２）教育委員会の事務局（小学校、中学校を含む。)
（３）農業委員会の事務局
（４）選挙管理委員会の事務局
（５）監査委員の事務局
（６）議会の事務局
（７）国保診療所の事務局

第３条　職員等の義務

全ての職員(会計年度任用職員及び嘱託員を含む。以下、「職員等」という。)に対して基本方針の趣旨を理解・認識し、遵守させるため必要な措置を講じる。職員等はセキュリティポリシーに同意し、遵守しなければならない。

職員等には、村の情報資産の使用を認めるが、それは、円滑な業務遂行の手段としての使用を認めることであり、私的利用を許可するものではない。また、外部委託業者(指定管理者及び派遣労働者を含む。)及び外郭団体に対しても、契約等を通じて、または別途取り決めを行うことによりセキュリティポリシーを遵守させるための必要な措置を講じる。

第４条　セキュリティ対策基準

本セキュリティポリシーを遵守すべき行為及び判断等の基準を統一的に定めるため、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(以下、「対策基準」という。)」を村の管理する情報システムの規格、要求事項ごとに記述する。

第５条 情報セキュリティ実施手順の策定

セキュリティポリシー及び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、個々の情報システムについて、具体的な遵守事項と実施手順を明記した「情報セキュリティ実施手順」(以下、「実施手順」という。)を策定するものとする。

第６条　その他関連法規の遵守

関連法令等を遵守するとともに、必要に応じ自主管理基準を設定し、継続的な情報セキュリティの確保と関連規格に遵守した管理策を導入し問題の改善を進める。

法令等には、次のものを含む。

- 行政手続における特定の個人を識別する番号の利用等に関する法律(平成25年法律第27号)
- 東白川村情報公開及び個人情報保護に関する条例(平成14年東白川村条例第11号)
- 東白川村行政手続における特定の個人を識別する番号の利用等に関する法律に基づく個人番号の利用に関する条例(平成27年東白川村条例第23号)
- 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)

第７条　体制の整備

情報セキュリティ統括責任者を定め情報セキュリティマネジメントの組織と運営体制を整備し、役割と責任の明確化を図る。

第８条 職員等の教育

基本方針及び対策基準の職員等への浸透と情報セキュリティ意識の向上のため、情報セキュリティに関する教育プログラムを策定し、それを実施する。

第９条　評価及び見直しの実施

情報セキュリティ実施状況の検証結果等を踏まえるとともに、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、セキュリティポリシー、基本方針、対策基準及び実施手順の見直しを適宜行う。

第10条　情報セキュリティ実施状況の検証

基本方針及び対策基準が遵守されていることを確認するため、定期的に情報セキュリティ実施状況の検証を行う。

第11条　違反への対応

基本方針及び対策基準等関係規定に違反した場合は、地方公務員法等に基づき、懲戒処分等の対象とするとともに、その結果に責任を負わなければならない。

令和８年４月１日

本セキュリティポリシーは、職員等に周知し、実行、維持する。

東白川村長　今 井 俊 郎

Ⅱ　東白川村情報セキュリティ対策基準

１章　総則

1　目的

この情報セキュリティ対策基準は、東白川村情報セキュリティポリシーをもとに村のセキュリティ対策を実行に移すために全ての情報資産やシステムに共通する情報セキュリティ対策の基準や手順を定めるものである。

2　定義

この基準において揚げる用語は次のとおりとする。

(１) 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。

(２) 個人情報等　東白川村情報公開及び個人情報保護に関する条例(平成14年東白川村条例第11号)第１条に規定する個人情報等をいう。

(３) 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(平成25年法律第27号)の規定により、住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。

(４) 特定個人情報　個人番号をその内容に含む個人情報をいう。

(５) セキュリティポリシー　東白川村情報セキュリティポリシーを指す。

(６) 対策基準　東白川村情報セキュリティ対策基準を指す。

(７) 情報保護　情報資産のうち個人に関する情報、その他の特に適正に管理を必要とするものの漏えい、改ざん、滅失又は損傷を防止することをいう。

(８) 情報資産　各部署で保有する電子媒体及び文書による情報並びにソフトウェア、ハードウェア、ネットワーク、磁気ディスクなどの記録媒体やその情報をいう。

(９) 重要情報資産　個人情報等及びセキュリティ推進員が特定した情報をいう。

(10) 情報システム　情報処理業務を一体的に行うため、ハードウェア、ソフトウェア、ネットワーク、記録媒体などにより構成されたものをいう。

(11) 緊急時　情報漏えいやウイルス感染時のことをいう。

(12) 副村長・課長・係長などの表記は役職名のことをいう。

２章　推進体制

１　役職及び組織

村の情報セキュリティ対策を総合的に実施するため、次の役職と組織を置く。

（１）情報セキュリティ統括責任者
（２）システム責任者
（３）情報資産責任者
（４）セキュリティ責任者
（５）ネットワーク管理者
（６）個人情報等管理者
（７）住民情報管理者
（８）セキュリティ推進員
（９）情報セキュリティ監査責任者
(10) セキュリティ内部監査員

２　役割

村の情報セキュリティ対策を継続的に推進するための役割は次のとおりとする。

（１）情報セキュリティ統括責任者(以下「統括責任者」という。)は、副村長をもって充て、セキュリティ対策の確立、セキュリティポリシー等の実施、維持及び管理を行う。また、統括責任者に事故があるとき又は統括責任者が欠けたときは、総務課長がその職務を代理する。

（２）システム責任者及び情報資産責任者は、総務課長及び教育委員会教育課長をもって充て、総務課長は小中学校を除く村全体の、教育委員会教育課長は小中学校のシステム、ネットワーク及び情報資産の管理の統括、セキュリティ対策の実施、教育及び緊急時対応を行う。

（３）セキュリティ責任者は、各課長をもって充て、各担当事務局の情報セキュリティ対策の確立、実施、管理及び緊急時対応を行う。

（４）ネットワーク管理者は、情報通信係長をもって充て、総務課長は小中学校を含む村全体のネットワーク管理、セキュリティ対策の推進及びシステム責任者の補佐をする。システム責任者に事故があるとき、またはシステム責任者が欠けたときは、その所管に合わせて職務を代理する。

（５）個人情報等管理者は、総務課長をもって充て、個人情報等の管理を推進する。

（６）住民情報管理者は、村民福祉課長をもって充て、住民情報の利用に関する管理の推進及び情報資産責任者の補佐をする。情報資産責任者に事故があるとき、または情報資産責任者が欠けたときは、その職務を代理する。

（７）セキュリティ推進員は、各課長が各課に１名以上指名し、各課の責任者として所管内の情報資産及びネットワークの管理を実施するとともに、すべての職員(各学校の教職員及び会計年度任用職員、嘱託員を含む。以下「職員等」という。)へのセキュリティ対策の周知徹底を行う。

(８) 各課の課長及び各小中学校の教頭は、所管の情報資産及びネットワークを適正に運用するためにセキュリティ推進員とともに台帳管理を行わなければならない。
(９) 情報セキュリティ推進会議(以下「セキュリティ会議」という。)については東白川村情報セキュリティ推進会議設置要綱で定める。このセキュリティ会議は、本条項の(１) から(７) の者で組織し、次のことを掌握し審議する。
① セキュリティポリシー、対策基準の決定及び見直しに関すること。
② セキュリティ対策の遵守状況(情報漏えい対策や緊急対策を含む。)に関すること。
③ 監査の実施に関すること。
④ 職員の教育及び研修に関すること。
⑤ 新たに行う情報資産の持出し及び外部委託並びにネットワーク接続に関すること。
(10) 情報セキュリティ監査責任者は、総務課長をもって充て、情報セキュリティ監査を指揮するとともに、監査結果をセキュリティ会議へ報告する。
(11) セキュリティ内部監査員は、各課に置くセキュリティ推進員を持って充て、情報セキュリティ内部監査を実施する。セキュリティ内部監査員は、別に情報セキュリティ監査責任者が指名することができる。

3　連絡網の整備

セキュリティ推進員は、緊急時等の連絡体制を整備し、各職員の役割を明確にしておくこと。情報システム導入課においては、関係機関への緊急連絡網を整備すること。

4　所属長の役割

(１) セキュリティ責任者は、所管するセキュリティ推進員の管理、教育が適正にされているか確認しなれければならない。
(２) セキュリティ推進員は、所属内(出先含む)の情報を把握し、重要情報資産を決定し、課内に周知しなければならない。
(３) セキュリティ推進員は、所属内において職員等を対象とした研修を実施し、セキュリティを確保しなければならない。
(４) セキュリティ推進員は、住民情報の新たな利用や変更をする場合は、住民情報管理者に許可を得なければならない。
(５) セキュリティ推進員は、個人情報等に係わる新たな業務や変更をする場合は、個人情報等管理者の許可を得なければならない。
(６) セキュリティ推進員は、住民情報システムや職員のネットワーク、学校のネットワークへ接続する場合は、所管するネットワーク管理者の許可を得なければならない。

３章　入退室管理

【入退室管理基準】

１　室のセキュリティ区分

セキュリティポリシーが適用される組織が管理する室について、情報資産の利用状況に応じたセキュリティ区分を以下のとおり定める。

表１

セキュリティ区分	情報資産の利用状況
レベル３	村全体の業務に係る情報システムのサーバ設置室及び重要情報資産の保管室。【サーバー室等】
レベル２	各業務に係る情報システムのサーバ、ネットワーク機器等の設置室。【一部の執務室等】
レベル１	クライアント端末の設置室【執務室、職員室等】
レベル０	応接や相談の出来る室及び誰でも出入りが自由な室。【相談室、ロビー等】

2　室の管理措置

室を管理する各課の長(以下「室の管理者」という。)は、セキュリティ区分に応じた以下の入退室管理措置を実施する。

表２

セキュリティ区分	入退室管理措置
レベル３	・室の施錠を行うこと。 ・入退室者は、室の管理者から事前に許可を得ること。 ・識別を行うため、入退室者には名札の着用を義務付けること。 ・セキュリティ区分レベル３の室の要件(※)を満たすよう、室の管理者は措置を講じること。
レベル２	・室の施錠を行うこと。室の施錠が困難な場合は、施錠可能で床等に固定したラック等に機器等を格納すること。 ・入退室者は、室の管理者から事前に許可を得ること。 ・鍵等の貸出に関する記録を行うこと。
レベル１	・職員等以外が入退室するときは、室の管理者から事前に許可を得ること。 ・作業等により職員等以外が入退室するときは、識別を行うため、入退室者には名札の着用などを義務付けること。 ただし、入退室管理簿への記録により名札の着用の代わりとすることができる。
レベル０	・相談室などの利用にあたっては、必要に応じて相談者のプライバシー等が確保できる措置をとること。 ・誰もが出入できるロビー等は、重要情報資産の放置などがないよう気をつけること。

※セキュリティ区分レベル３の室の要件

（１）許可されていない者の立ち入り防止するため、以下の措置を講じること。

①　施錠可能な室であること。

②　外部に通じるドアは最小限とすること。

③　窓に格子を嵌めるなど、外部から容易に侵入できない対策を講じること。

④　ＩＣカード、バイオメトリクス認証装置などを設置し、入退室者の識別と記録を行うこと。

⑤　サーバの設置室は、監視装置などを設置すること。

⑥　予備電源の確保、配線の損傷防止等の措置が講じられていること。

（２）サーバの設置室は、機器の転倒及び落下防止等の耐震対策、消火設備の設置、防水処置などを講じること。消火設備の消火薬は、機器、記録媒体及び人体に影響を与えないものとすること。

3　室の管理者

（1）室の管理者は、表1に掲げるセキュリティ区分に応じて、表2に定める入退室の管理を行うほか、情報セキュリティを確保するために必要な措置をとらなければならない。

（2）室の管理者は、業務上の必要から、常時あるいは定期的にセキュリティ区分レベル2以上の室に入退室する職員等に対して、あらかじめ入退室の資格を付与することができる。

4　鍵等の管理

（1）鍵等の管理は、室の管理者が行う。

（2）セキュリティ区分レベル2以上の室の管理者は、事前に入退室の許可を与えた者に限り、鍵等を貸与するものとする。

5　管理簿の作成

（1）セキュリティ区分レベル3の室の管理者は、入退室管理簿を作成し、これを保存するものとする。

（2）セキュリティ区分レベル2の室の管理者は、鍵等の貸出管理簿を作成し、これを保存するものとする。

6　指示

（1）室の管理者は、必要に応じて、管理する室の入退室管理措置を行う者(以下「入退室管理者等」という。)を定めることができるものとする。

（2）室の管理者は、適切な入退室管理が行われているかどうか、入退室管理者等から報告を聴取し、調査を行い、また必要な指示を行うものとする。

【入退室管理手順】

セキュリティポリシーが適用される組織が管理する室について、対策基準で定めるほか、以下の管理策を行う。

1　入退室管理

（1）職員等は名札を着用し、常に身分を明らかにすること。また、セキュリティ区分レベル2以上の室に入退室する場合は、身分証明書等を携帯すること。

（2）外部からの訪問者(以下「訪問者」という。)は、セキュリティ区分レベル1以上の室に入退室する場合は、事前に室の管理者から承諾を得ること。

（3）作業等を目的とした訪問者は、セキュリティ区分レベル1以上の室に入退室する場合は、名札の着用及び身分証明書の携行により身分を明らかにすること。また、室の管理者は、腕章等を着用させることで許可された入室であることを明示するとともに、外見上職員等と区別させるものとする。

（４）室の管理者は、必要に応じて、前項の身分証明書等の提示を求めることができるものとする。
（５） 訪問者がセキュリティ区分レベル１以上の室に入退室する場合、室の管理者は、必要に応じて、立ち入り区域の制限、職員等の立ち会いなどを指示するものとする。
（６）室の管理者は、住民が入室可能な場所について、重要な情報が目に触れないような対策をとること。

２　入退室に係る資格の付与
（１）職員等に対する資格の付与
①　室の管理者は、対策基準に従い、職員等に入退室の資格を付与する。
②　付与した資格は毎年度再調査し、登録、削除の管理を適切に行うこと。
（２）訪問者に対する資格の付与
①　室の管理者は、セキュリティ区分レベル２以上の室に設置した機器等の保守業務等委託者(以下「保守業者等」という。)に対し、入退室の資格を付与することができるものとする。
②　保守業者等が入退室する場合は、複数の者で入退室を行うか職員等の立会を必要とする。
③　室の管理者は、その他の訪問者に対して、特に必要と認める場合には入退室の資格を付与することができるものとする。ただし入退室にあたっては、職員等の立会を必要とする。

３　入退室者の記録
（１）入退室管理簿への記録(レベル３)
①　職員等の入退室記録
室の管理者は、入退室する職員等の氏名、入退室日時等を記録する。記録にあたっては、ＩＣカード及び生体認証等を用いた入退室管理システムによることもできるものとする。
②　訪問者の入退室記録
保守業者等が業務のために入退室する場合、室の管理者は、入退室者の氏名、入退室日時等を記録する。その他の訪問者については、入退室者の氏名、所属、入退室目的及び入退室日時を管理簿に記録する。
（２）鍵等の貸出管理簿への記録(レベル２)
室の管理者は、鍵等を貸出する者の氏名、入退室日時、入退室目的等を鍵等の貸出管理簿に記録する。
（３）入退室管理者の記録の保存
入退室管理システムによる入退室の記録、登録簿及び管理簿に関しては、レベル３は３年以上、レベル２の鍵の管理簿は1年以上前までさかのぼって解析できるよう保存する。

４章　利用者管理

【利用者管理基準】

1　利用者の権限管理を行う機器

（１）ネットワーク管理者は、次に掲げる情報資産について、利用する職員等に利用者権限を付与することができる。

①　サーバ等

②　業務端末

③　重要情報資産(記録媒体及び書類等を含む)

（２）利用者権限は、機器操作に関してのＩＤ及びＩＤの認証方法(パスワード、ＩＣカード、指紋等のバイオメトリクス認証など。以下「パスワード等」という。)により正当な権限を確認することとする。また、重要情報資産に関しては、保管庫等の鍵の貸出管理簿により利用者の正当な権限を確認する。

2　利用者権限の管理

ネットワーク管理者は、情報システムの利用に関し、次に掲げる事項を実施する。

①　サーバ及びクライアントのＩＤ及びパスワード等の管理方法を定めること。

②　ＩＤ及びパスワード等の使用は、利用者権限を付与した者(以下「操作者」という。)のみに限定すること。

③　操作者の管理簿を作成すること。

④　会計年度任用職員及び嘱託員に利用者権限を付与するときは、セキュリティポリシー及び対策基準の内容を理解させ、遵守させなければならない。

3　操作者の責務

操作者は、ＩＤ及びパスワード等の管理方法を遵守しなければならない。

4　操作履歴の記録

ネットワーク管理者は、情報システムの操作記録を取得すること。一時的な操作については、紙等に記録を残すこと。システム的に操作記録が取得できない場合は、システム更新時等に変更を行うこと。

5　電子メールの利用者管理

（１）ネットワーク管理者は、電子メールを利用できる職員等を限定しなければならない。

（２）ネットワーク管理者は、電子メールの利用に関する手順を定めなければならない。

【利用者管理手順】

1　利用者権限の管理方法

(１) ネットワーク管理者は、所管する情報システムの利用者権限を決定し、利用を許可した職員等に限定してＩＤ及びパスワード等を付与する。

(２) ネットワーク管理者は、業務上の必要がある場合は、グループＩＤ及びパスワード等を付与することができる。ただし、職員等はアクセス権限を有する場合であっても、業務上の目的以外の目的でアクセスしてはならない。

(３)システム責任者は、住民情報システムや財務システムの利用者権限を決定し、ネットワーク管理者へ申請する。ネットワーク管理者から付与されたＩＤ及びパスワード等は、適正に管理し外部に漏れないようにする。

(４) 職員等は、住民情報システムへの利用者権限取得前に、セキュリティ研修を受け、「住民情報システム遵守事項」を理解し、それに同意しなければならない。

(５) 他の部署が管理する情報システムを利用する場合、セキュリティ推進員は、利用する者を指定し、情報システムを管理するネットワーク管理者へ申請する。

(６) システム責任者は、会計年度任用職員等を雇用する際に身元調査(履歴書等の確認)を行い、住民情報システム遵守事項への同意を求めて機密保持合意文書を取得し、各課で扱う個人情報等の保護の研修等を経たのちに会計年度任用職員等に利用者権限を付与する。

(７) ネットワーク管理者は、操作者に対し、必要に応じてセキュリティ研修の実施または受講をさせなければならない。

(８) 操作者は、利用者権限の他者への貸与、目的外の利用等を行わない。

(９) 操作者は、指定された端末で操作を行う。

(10) ネットワーク管理者は、個人番号及び特定個人情報を取り扱う事務を実施する区域を明確にし、物理的安全措置を講じなければならない。

(11) ネットワーク管理者は、個人番号及び特定個人情報の秘匿性等、その内容に応じて、その処理を行う端末を限定するために必要な措置を講じなければならない。

(12) ネットワーク管理者は、適正に利用者権限が利用されているか検査を行う。

(13) ネットワーク管理者が利用者権限の利用に関する検査を行う場合、操作者は協力する義務を負う。

2　パスワード等の適正管理

(１) 操作者は、パスワードを秘密にし、パスワードの照会等には応じない。

(２) 操作者は、パスワードのメモを作らない。ただし、記録がセキュリティを確保して保管され、保管方法が承認されている場合は、その限りではない。

(３) 操作者は、情報システムやパスワードに対する危険の恐れがある場合は、パスワードを速やかに変更すること。

(４) 操作者は、パスワードは適宜変更すること。

(５) 操作者は、個人用のパスワードを共有しない。

(６) 操作者は、仮のパスワードは、初期のログオン時に変更する。

（７）ネットワーク管理者は、重要情報資産を扱うサーバのパスワードは６文字以上とし、英文字、数字(記号)を混在させること。
（８）質の良いパスワードとは次の条件を満たすものをいい、この条件を満たすパスワードを重要度に合わせて設定することが望ましい。
① 覚えやすい。
② 操作者の関連情報(例えば、名前、電名番号、誕生日など)から、他の者が容易に推測できる事項に基づかない。
③ 同一文字を連ねただけ、数字だけ、またはアルファベットだけの文字列でない。
④ 辞書に含まれる語から成り立っていない。

３　操作履歴の保管

ネットワーク管理者は、システムの操作履歴については、データの重要性に合わせて複数年(1年以上)さかのぼって解析できるよう保管するものとする。ただし、重要情報を扱うシステムは３年以上さかのぼって解析できるようにする。

４　電子メールの利用制限

（１）システム責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールフィルタリングの確認や設定変更を行い危険があると判断した時は、メールサーバの運用を停止しなければならない。
（２）ネットワーク管理者は、職員等が利用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を周知しなければならない。
（３）職員等は、外部の複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
（４）職員等は、重要な電子メールを誤送信した場合は、セキュリティ推進員を通じて、システム責任者へ報告しなければならない。
（５）職員等は、ウェブで利用できるフリーメール、ＳＮＳ、グループウェア等を使用してはならない。ただし、業務上必要な場合は、セキュリティ推進員及びネットワーク管理者の許可を得て送受信することができる。この場合、各々の案件ごとに許可を得ることとする。

５章　情報資産管理

【情報資産管理基準】

１　情報資産管理

各課が管理する情報資産の管理責任者は各課の長(以下「情報資産管理責任者」という。)とする。また、情報資産の管理方法を以下のとおりとする。

表３

管理方法	管理対象
１.情報システム等管理	各課で導入した情報システム及び単独で動作するパソコン等機器、ソフトウェア等(以下「情報システム等」という。例：サーバ、パソコン、外付けハードディスクドライブ、ＨＵＢ、プリンタ、オペレーションシステム、ミドルウェア、アプリケーションソフトウェアなど。)
２．記録媒体管理	記録したデータの追加・更新・削除を行う記録媒体。(例：ＵＳＢメモリ、ＭＯ、フロッピーディスク、ＣＤ－ＲＷ、ＤＶＤ－ＲＷ、フラッシュメモリ、ＤＡＴ、ＬＴＯ、ＭＤ、カセットテープなど。)
３．文書管理 (ファイリング)	紙文書及び記録したデータをそのまま保管することを目的とした記録媒体等。(例：他機関から配布されたＣＤ－ＲＯＭ、データ登録済のＣＤ－ＲやＤＶＤ－Ｒ、完成図書として業者から納品されたＭＯなど。)

(１) 情報資産管理責任者は、「記録媒体管理手順」に基づき情報資産を管理する。また、情報資産管理責任者は、施設の状況等に応じて独自の管理手順等を作成できることとする。

(２) 情報資産管理責任者は、重要情報資産を新たに外部提供する場合は、セキュリティ会議の審査を経て、統括責任者の承認を得なければならない。

(３) 前項の基準に関わらず緊急性が高い場合、情報資産管理責任者は、個人情報管理者の審査を経た後に提供することを可能とする。ただし、後日のセキュリティ会議で報告し、統括責任者の承認を得なければならない。

(４) 情報資産管理責任者は、個人番号及び特定個人情報を記録している情報資産を保管している区域に立ち入る権限を有する者を定めるとともに、入退の管理、部外者についての識別化、部外者が立ち入る場合の職員の立会い又は監視設備による監視、外部電磁的記録媒体等の持込み、利用又は持出しの制限又は検査等の措置を講ずる。

(５) 職員等は、情報資産を外部に持ち出す場合は、情報資産管理責任者の許可を得なければならない。

(６) 職員等は、私有のパソコン及び記録媒体等を庁舎等の職場に持ち込んではならない。

(７) 職員等は、パソコンや記録媒体、情報が印刷された文書等が第三者に使用されるこ

とのないよう、離席時の端末ロック、記録媒体や文書等を容易に閲覧されない場所へ保管するなど、適切な処置を講じなければならない。

（８）職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

【情報システム等管理手順】

1　情報資産管理責任者の業務

情報資産管理責任者は、情報システム等を、管理する区分毎に明確化する(以下「構成管理」という。)とともに、それぞれの区分毎に、以下の内容を規定する。

- 情報システム等の障害に関すること
- 情報システム等の保守に関すること
- 情報システム等の性能に関すること

2　構成管理の留意事項

（１）管理区分の明確化

住民情報管理者は、住民情報システムに係る全ての情報、ハードウェア、ソフトウェア、ネットワーク及び電子媒体を管理する上で明確に区分する。

＜構成管理の例示＞

- ハードウェアに関する情報資産
- ソフトウェアに関する情報資産
- ネットワークに関する情報資産
- その他の情報資産

（２）導入、移設、廃棄等移管処理手順

情報資産管理責任者は、情報システム等の導入時、移設時、廃棄等移管処理を行う場合の手順を作成する。

- 作業責任者及び作業者の特定
- 導入前のセキュリティ機能と保守の確認
- 導入前のハードウェア、ソフトウェアの特定
- データの正確性の確保
- 導入前のテスト
- 移設時のテストとバックアップ
- 廃棄時のデータ消去等

（３）管理方法

情報資産管理責任者は情報資産管理簿を作成する。情報資産管理簿においては、変更履歴を記録する。また、不要な機器等の持ち込みがなされないよう措置を講じる。

表４　情報資産管理簿

台帳名称	内容	記載事項の例
システム構成表	システムを構成する機器についての一覧表	管理番号 機器の名称 台数　等
機器管理台帳 (総括表)	システムを構成する機器ごとに、管理を行う上で必要となる項目を記入した台帳	管理者に関すること 担当者に関すること 保守会社に関すること 品名、設置場所　等
ソフトウェア管理台帳	システムで使用するソフトウェアの導入状況等を記載した台帳	品名、バージョン、仕様、数量、問合せ先、インストール機器　等
操作者一覧表	システムを取り扱う者の所属、氏名及び権限等を記載したもの	操作者に関すること、 氏名、所属、役割　等

（４）検査

情報資産管理責任者は、情報システム等が適正に管理されているかどうかを確認する。

３　資産管理ソフトの活用

（１）ネットワーク管理者は、職員パソコンなどイントラネットに接続する端末に、資産管理ソフトを導入することとする。

（２）セキュリティ推進員は、配下の職員等が情報資産を適切に使用していることを確認し、万一、情報資産の漏えいや改ざん等があった場合は早期に発見し対応するため、資産管理ソフトを活用することとする。

【記録媒体管理手順】

１　この手順で対象とする記録媒体は、記録したデータの追加、更新、削除等を行う記録媒体(フロッピーディスク、ＭＯ、ＵＳＢメモリなどのフラッシュメモリ、ＣＤ‐ＲＷ、ＤＶＤ‐ＲＷ、ＤＡＴ、ＬＴＯ、ＭＤ、カセットテープ等)とする。また、搬送可能なパソコン等端末及び重要情報資産に指定された紙文書等に関しても一部の取り扱いを準用する。

２　記録媒体の管理方法について以下のとおり定める。

（１）業務で使用できる記録媒体は、情報資産管理責任者が承認した記録媒体のみとする。

（２）情報資産管理責任者は、承認した記録媒体を管理するため、記録媒体管理簿を整備する。記録媒体管理簿は所属単位で作成するが、情報資産管理責任者が認める場合は、本課と出先機関等は分けて作成することができるものとする。この場合、情報資産管理責任者は、出先機関等における記録媒体の管理責任者を指定することとする。

(３) 情報資産管理責任者は、記録媒体に、記録媒体管理簿で登録した媒体管理番号をラベル等で貼付すること。
(４) 情報資産管理責任者(出先機関における記録媒体の管理責任者を含む。以下同じ。)は、記録媒体の保管場所を定めること。保管場所は、原則として、施錠できる場所とする。また、パソコンはセキュリティワイヤーで固定するなど盗難防止措置を講じること。
(５) 情報資産管理責任者は、記録媒体の利用状況を管理するため、記録媒体利用簿を整備する。記録媒体利用簿は課単位で作成するが、情報資産管理責任者が認める場合は、本課と出先機関は分けて作成することができるものとする。
(６) 職員等は、記録媒体の使用にあたっては、事前に情報資産管理責任者から利用承認を得ること。
(７) 職員等は、施設外へ記録媒体、パソコン及び重要情報資産に指定された紙文書等を持ち出す場合は、情報資産管理責任者から事前に許可を得ること。
(８) 職員等は、重要情報資産を持ち出す場合は、データにパスワードや暗号化をかける、データを登録した記録媒体を鍵の掛かるケース等に入れるなどの情報漏えい対策を実施しなければならない。
(９) 職員等は、重要情報資産を複写・複製等する場合は、事前に情報資産管理責任者の許可を得ること。
＜重要情報資産の複写・複製等の例＞
・　別の記録媒体へ複写・複製をすること。
・　パソコンのハードディスク等へ複写、複製、データ作成をすること。
・　紙にプリントアウトすること。
・　紙媒体の資料、帳票をコピーすること。
(10) 職員等は、記録媒体を使用した後は、格納した情報の削除及びウイルスチェックを行い、速やかに保管場所へ返却すること。
(11) その他の取り扱い
①　不要となった記録媒体を再利用する場合は、格納している内容を削除すること。
②　全ての記録媒体は、製造者の仕様に従ってセキュリティが保たれた環境で使用し保管すること。
③　情報を記録媒体の寿命より長く保管する場合は、媒体の劣化による情報消失を避けるため、当該情報を他の記録媒体にも記録し保管すること。

【記録媒体搬送手順】

1　この記録媒体搬送手順は、組織間で交換する情報の紛失、改ざん及び誤用を防止するための措置を定める。

2　情報資産管理責任者は、外部組織と情報資産の交換を行う場合、次のことを外部組織に対して明らかにすること。

（１）情報資産の発信及び受領の責任者。
（２）情報資産の引渡し記録をとること。
（３）情報資産の梱包の方法。
（４）宅配業者を利用する場合の事前承諾と宅配業者の特定を行うこと。
（５）情報資産の紛失時の責任の所在。

３　職員等が記録媒体を搬送する場合
（１）記録媒体を搬送する職員等は、事務所内においても記録媒体を無人の状態で放置しないこと。(例：台車に載せたまま車を取りにいかない。)
（２）記録媒体等は、搬送ケースに入れ施錠すること。
（３）職員等は、盗難等を防止するため２名で搬送すること。やむを得ず１名で搬送する場合は、搬送ケースが他からわからないようにすること。
（４）職員等は、搬送途中に目的地以外に立ち寄らないこと。やむを得ず立ち寄りをする場合は、搬送ケースは常に携行し車内に放置等しないこと。

４　宅配業者等が搬送する場合
（１）信頼できる運送業者を用いること。また、利用する宅配業者についてセキュリティ推進員の合意を得、搬送の収受を確認できるようにすること。
（２）梱包は、輸送途中で発生しがちな物理的損傷から内容物を保護するために、十分な強度のものとする。
（３）重要度に応じ、セキュリティのある宅配方法をとること。

５　パソコン等の搬送
　パソコン及び重要情報資産に指定された紙文書等の搬送についても、この記録媒体搬送手順に準じておこなうこと。

【情報資産の廃棄手順】

１　買い取りによるパソコン、サーバ等機器の廃棄
（１）情報資産管理責任者は、買い取りによるパソコン、サーバ等機器を廃棄する場合は、専門業者によるデータの消去、または職員等がデータ消去専用ソフト等によりデータを抹消するかハードディスク等の物理的な破壊を行ったうえで産業廃棄物として処分すること。専門業者によるデータ消去を行った場合は、消去したことの証明を受領すること。また、産業廃棄物処理業者から管理票(マニュフェスト)を取得すること。
（２）情報資産管理責任者は、買い取りによるパソコン、サーバ等機器を他用途に転用する場合は、ハードディスク等のフォーマットを行ったのち新規ＯＳのインストールを行うこと。

2　レンタル、リースによるパソコン、サーバ等機器の返却

情報資産管理責任者は、レンタル、リース期間の満了に伴いパソコン、サーバ等機器を返却する場合は、専門業者によるデータの消去、または職員等がデータ消去専用ソフト等によりデータを抹消するかハードディスク等の物理的な破壊を行うこと。専門業者によるデータ消去を行った場合は、消去したことの証明を受領すること。

3　記録媒体の廃棄

情報資産管理責任者は、記録媒体を廃棄する場合は、物理的な破壊を行うこと。

（1）ＦＤ(フロッピーディスク)　金属部分を取り除き、内部のマグネットシートを取り出しはさみで切断する。

（2）ＣＤ・ＤＶＤ　反射面にカッター等で傷をつけて割る。

（3）ＭＯ　金槌等で破壊する。

（4）テープ等　テープを引き出してはさみを入れる。

（5）フラッシュメモリ(ＵＳＢメモリ、ＳＤカード等)　金槌等で破壊する。

4　帳票類(文書)の廃棄

情報資産管理責任者は、重要情報を含む紙文書を廃棄する場合は、一般のゴミとして処分せず、次の点に留意して廃棄すること。

（1）廃棄方法は、焼却、溶解や用紙を細かく裁断する等によって、記述内容が判読できないようにすること。

（2）保管していた帳票は、保管期間終了時には、その廃棄すべき帳票の内容及び数量を記録し、廃棄時にチェックを行う。

（3）廃棄すると決定した帳票は、速やかに廃棄処分を行う。

（4）重要情報を含む紙文書の廃棄は、直接焼却施設に持ち込む、機密文書回収業者に処理を委託する、又はシュレッダーにかける方法により行う。また、裏紙等の再利用のないように適切に処理をすること。

（5）一時的に記録された用紙についても、重要な情報が記載されていれば、(1)と同様な処理を行う。

【重要情報資産管理手順】

1　個人情報等と重要情報の特定

セキュリティ推進員は、課内の取り扱い情報の中から、個人情報等及び機密情報などの特定を行い、重要情報資産として職員等に周知しなければならない。また、特定された重要情報資産の電子データについては、文書管理で定める方法により管理しなければならない。

2　重要情報資産を取り扱うことができる者の指定

セキュリティ推進員は、重要情報資産を取り扱うことができる者を指定する。

3　重要情報資産を取り扱う者

セキュリティ推進員は、法により個人情報の漏えい、滅失及びき損の防止、その他の個人情報等の適切な管理のために必要な措置の実施が義務付けられていることを踏まえて、指定した者が個人情報等を取り扱うに際して、次の留意事項を遵守させること。特定した機密情報等も個人情報等に準じた取り扱いを行うこと。

(１) 重要情報資産を画面表示する場合の取り扱い

①　職員等は、業務上必要のない情報等を表示しないこと。

②　職員等は、情報等を利用した後は速やかにログイン画面に戻すなど、情報等を長時間ディスプレイに表示したままの状態にしないこと。

③　セキュリティ推進員は、重要情報資産を表示したディスプレイが、来庁者等から見えないような処置を行うこと。

④　職員等は、業務上必要のない画面のハードコピーを取らないこと。また、必要以外に画像データとして保管することを禁止し、紙媒体への出力については細心の注意を持って行うこと。

(２) 重要情報資産の正確性の確保

①　セキュリティ推進員は、重要情報資産の入力、削除及び訂正を行う際には、正確性を確保するために、入力、削除及び訂正を行った者以外の者に確認させる等、必ず入力、削除及び訂正した内容を適切に確認すること。

②　セキュリティ推進員は、入力、削除及び訂正作業に用いた帳票等は、適切に管理し、保管すること。

③　職員等は、重要情報資産に誤りがあった際に訂正を行う場合には、セキュリティ推進員の許可を得て行うこと。また、訂正した内容等については、その記録を残し、適正な期間保管を行うこと。

(３) 重要情報資産の検索・抽出

①　職員等は、業務上必要のない検索・抽出は行わないこと。

②　職員等は、業務上の検索・抽出を行う場合には、事前に検索・抽出要件を明確にすること。

(４) 重要情報資産の記録媒体への保存

①　職員等は、重要情報資産を記録媒体に保存する場合には、セキュリティ推進員の許可を得て行うこと。また、保存したことの記録を残し、適正な期間保管を行うこと。

②　職員等は、パソコンや記録媒体により重要情報資産を管理する場合は、ファイルの暗号化やパスワード設定、閉じたネットワークの利用など安全な保管をしなければならない。

③　重要情報資産の持ち出しは原則として禁止する。業務上、止むを得ず持ち出す場合は、セキュリティ推進員の許可を得なければならない。なお、重要情報資産の入った記録媒体も同様の扱いとする。

④　職員等は、重要情報資産を持ち出しする場合は、できる限りの漏えい防止対策(ファイルの暗号化やパスワード設定、重要情報資産の入った記録媒体を鍵の掛かるケース入れるなど)を実施しなければならない。

⑤　重要情報資産の返却確認は、セキュリティ推進員が責任を持って行わなければならない。(返却届け等による確認と複数職員による確認等)

(５) 重要情報資産の出力

①　職員等は、業務上必要のない帳票の出力は行わないこと。

②　職員等は、重要情報資産が記載されている帳票を出力した場合には、適正に管理すること。

(６) 重要情報資産に関する秘密保持義務

①　秘密保持義務は、重要情報資産に関する文書及び電子計算機処理等に関する秘密を対象とする。

②　これらの秘密は、単に重要情報資産の情報のみならず、セキュリティに関する技術情報やパスワード、具体的な運用方法、マニュアル等も含まれるものである。

4　帳票の管理

(１) 対象

本項は、重要情報資産の記録された帳票を管理対象とする。また、これらの帳票を基に作成した帳票等がある場合には、その帳票についても管理対象とする。

(２) 帳票の取り扱い

①　帳票を出力する場合

セキュリティ推進員は、出力した帳票について以下のような事項を記録する。

・　出力帳票の種類
・　出力月日
・　使用目的
・　申請者等

②　帳票を保管する場合

セキュリティ推進員は、帳票は、施錠のできる書庫等に保管を行い紛失及び盗難を防止するための措置を講じること。セキュリティ推進員が交代する場合には、必ず引継書を作成して、現況を確認し、引き継ぎを行うこと。

６章　委託管理

【委託管理基準】

1　委託を受けようとする者の管理体制等の調査

セキュリティ推進員は、情報資産及び重要情報資産を使用する業務を新たに委託するときは、委託を受けようとする者における情報の保護に関する管理体制等についてあらかじめ調査することとする。

2　業務委託の承認

セキュリティ推進員は、情報資産及び重要情報資産を使用する業務を新たに委託するときは、委託する業務の内容、理由及び情報の保護に関する事項等について、あらかじめネットワーク管理者、住民情報管理者、個人情報等管理者及び情報資産責任者の承認を得なければならない。また、情報資産責任者は、必要に応じてセキュリティ会議を開催し、統括責任者及びセキュリティ責任者の承認を得なければならない。

3　委託契約書への記載事項

業務委託に係る契約書には、情報の保護に関して次の各号に掲げる事項を明記しなければならない。

（１）再委託の禁止又は制限に関する事項
（２）情報が記録された資料の保管、返還又は廃棄に関する事項
（３）情報が記録された資料の目的外使用、複製・複写及び第三者への提供の禁止に関する事項
（４）情報の秘密保持に関する事項
（５）重要情報資産の漏えい等の事案の発生時における対応に関する事項
（６）事故等の報告に関する事項
（７）委託終了時における重要情報資産の消去及び媒体の返却に関する事項
（８）違反した場合における契約解除、損害賠償責任その他必要な事項
（９）その他情報の保護に関し必要と思われる事項

4　受託者の管理状況の調査

セキュリティ推進員は、必要に応じ受託者における当該業務委託に係るセキュリティ対策の実施状況について調査するものとする。

5　労働派遣契約書への記載事項

重要情報資産の取扱いに係る事務を派遣労働によって行わせる場合には、労働派遣契約書に重要情報資産の取扱いに関する事項を明記しなければならない。

【委託管理手順】

1　委託先事業者を選定する場合

セキュリティ推進員は、委託先事業者を選定する場合には、委託する業務の内容に応じて以下の点に留意して事業者の安全度、信頼度等を確認し選定することとする。また、契約時において東白川村個人情報等取扱事務委託基準及び個人情報等取扱特記事項を遵守させること。なお、契約書等を省略する業務委託についても、個人情報等などの重要情報が含まれる場合も同様に処理すること。

（1）事前調査

委託業者を選定する場合には、その事業者に関して、経営の健全性、安定度、営業規模、営業地域等を事前に調査し確認する。

契約を締結する際は、東白川村個人情報等取扱事務委託基準及び個人情報等取扱特記事項を遵守させること。

（2）業務完遂能力

事業者の業務完遂能力(信用度)について、要員の技術力や要員の教育体制等のみで判断するのではなく、個人情報等保護措置やセキュリティ対策の実施状況等についても調査し、判断する。

さらに、損害賠償能力や社会的関心を呼んだ不祥事の有無等についても調査を行い、総合的に判断する。

（3）再委託に関する考え方

重要情報資産の電子計算機処理等の委託を受けた者若しくはその役職員又はこれらの者であった者は、法により罰則で担保された秘密保持義務が課されるが、再委託先については法による秘密保持義務が課されない。よって重要情報資産についても再委託先で取り扱うこととなるような場合は、再委託を承認することは適当ではない。

やむなく再委託を承認する場合は、委託先とその再委託先連名で秘密保持の誓約取り、当村の条例の遵守と罰則の承諾及び損害賠償について明らかにすること。

（4）秘密保持等に関する誓約書の提出

委託契約を締結する際には、委託先事業者に対し、委託先事業者の従事者の意識を高めるために、秘密保持等に関する誓約書を提出させる等の措置を講ずるよう依頼する。

2　重要情報資産の委託に関する誓約事項

セキュリティ推進員は、重要情報資産を取り扱う委託については、委託先事業者に対し次の事項を遵守させなければならない。

（1）基本的事項

委託先事業者は、情報保護の重要性を認識し、契約による業務を処理するための個人情報等の取扱いに当たっては、個人の権利利益を侵害することのないよう、個人情報等を適正に取り扱わなければならない。

(２) 秘密の保持

委託先事業者は、契約による業務に関して知り得た個人情報等を他人に知らせ、又は不当な目的に使用してはならない。契約が終了し、又は解除された後においても同様とする。

(３) 適正管理

委託先事業者は、契約による業務の処理のために取り扱う個人情報等について、漏えい、滅失及びき損の防止その他個人情報等の適正な管理のために必要な措置を講じなければならない。

(４) 再委託の禁止

委託先事業者は、契約による業務の全部又は一部について第三者に再委託をしてはならない。ただし、委託先事業者は、あらかじめ委託先及び委託の範囲を村に対して報告し、村の書面による承諾を得た場合に限り、再委託をすることができる。

この場合において、委託先事業者は、契約により委託先事業者が負う義務を再委託先に対しても遵守させなければならない。このため、委託先事業者は、委託先事業者と再委託先との間で締結する契約書においてその旨を明記すること。

(５) 収集の制限

委託先事業者は、契約による業務の処理のために個人情報等を収集するときは、当該業務の目的を達成するために必要な範囲内で、適法かつ公正な手段により行わなければならない。

(６) 従事者の監督

委託先事業者は、契約による事務に従事する者(資料等の運搬に従事する者を含む。以下「従事者」と総称する。)に対し、在職中及び退職後においても当該契約による業務に関して知り得た個人情報等を他人に知らせ、又は不当な目的に使用してはならないこと、個人情報等の違法な利用及び提供に対して罰則が適用される可能性があることその他個人情報等の保護に関して必要な事項を周知しなければならない。また、委託先事業者は、契約による業務を処理するために取り扱う個人情報等の適切な管理が図られるよう、従事者に対して必要かつ適切な監督を行わなければならない。

(７) 複写又は複製の禁止

委託先事業者は、村が承諾した場合を除き、契約による業務を処理するために村から提供を受けた個人情報等が記録された資料等を村の承諾なしに複写し、又は複製してはならない。また、事務の処理を行う場所に、資料等の複写が可能な媒体を持ち込んではならない。

(８) 作業場所の指定等

委託先事業者は、契約による業務の処理について、村の庁舎内において村の開庁時間内に行うものとする。この場合において、委託先事業者は、その従事者に対して常にその身分を証明する書類を携帯させなければならない。

なお、委託先事業者は、村の庁舎外で事務を処理することにつき、当該作業場所(住所等)の特定及び当該作業場所における適正管理(東白川村情報セキュリティ対策の各手順以上の管理)の実施その他の安全確保の措置についてあらかじめ村に届け出て、村の承諾を得た場合は、当該作業場所において事務を処理することができる。

(９) 資料等の運搬

委託先事業者は、その従事者に対し、資料等の運搬中に資料等から離れないこと、電磁的記録の資料等は暗号化等個人情報等の漏えい防止対策(東白川村情報セキュリティ対策の各手順以上の防止対策)を十分に講じた上で運搬することその他の安全確保のために必要な指示を行わなければならない。

(10) 目的外利用及び提供の禁止

委託先事業者は、村の指示がある場合を除き、この契約による業務の処理のために取り扱う個人情報等を当該契約の目的以外の目的に利用し、又は第三者に提供してはならない。

(11) 実地調査等

村は、契約による安全確保の措置の実施状況を調査するため必要があると認めるときは、実地に調査し、委託先事業者に対して必要な資料の提出を求め、又は必要な指示をすることができる。

(12) 資料等の返還

委託先事業者は、契約による業務の処理のために、村から提供を受け、又は委託先事業者自らが収集し、若しくは作成した個人情報等を記録した資料等は、この契約による業務処理の完了後直ちに村に返還し、又は引き渡すものとし、村の承諾を得て行った複写又は複製物については、廃棄又は消去しなければならない。

(13) 事故発生時における報告

委託先事業者は、個人情報等の漏えい、滅失又はき損その他の事故が発生し、又は発生するおそれのあることを知ったときは、速やかに村に報告し、村の指示に従わなければならない。委託契約が終了し、又は解除された後においても同様とする。

(14) 損害賠償

委託先事業者は、その責めに帰すべき事由により、契約による業務の処理に関し、村又は第三者に損害を与えたときは、その損害を賠償しなければならない。再委託先の責めに帰する事由により村又は第三者に損害を与えたときも同様とする。

(15) 変更届

この特記事項に基づいて委託先事業者が村に届け出て、村の承諾を得て実施する事項に関して変更が生じた場合は、委託先事業者は変更届を村に届け出て、村の承諾を得なければならない。

７章　教育・研修

１　情報資産を安全に管理していく上でセキュリティ対策及び運用オペレーションについて、情報資産責任者及びシステム責任者は、所管内の管理者研修としてセキュリティ責任者、セキュリティ推進員及び新規採用職員、内部監査員を、セキュリティ推進員は所属の職員等に計画的に教育・研修を行う。

（１）管理者研修

情報資産を取り扱う各責任者に対して、その管理に関する必要な知識や技術を習得させる研修を行う。

（２）職員研修

情報資産を取り扱う各職員に対して、その管理に関する必要な知識や技術を習得させる研修を行う。

（３）初任者研修

新規採用職員に対して、必要な知識の修得に資するための研修を行う。

（４）情報セキュリティ内部監査員研修

情報セキュリティ内部監査を担当する職員に対して、一定期間毎に必要な知識の修得に資するための研修を行う。

（５）会計年度任用職員等の研修

会計年度任用職員等を雇用する各課の責任者は、当該施設の情報資産を取り扱う皆生年度任用職員等に対して、採用時及び一定期間毎に、必要な知識の修得に資するための研修を行う。

（６）法令・内部規程違反等に対する厳正な対処

法令又は内部規程等に違反した職員等に対し、法令又は内部規程等に基づき厳正に対処する。

８章　緊急時対応

【緊急時対応基準】

この緊急時対応基準は､障害編と不正行為編の２編に分け､次のように緊急時対応を特定する。

- 電算機器の障害発生による稼働停止
- ソフトウェアの障害発生による稼働停止
- データの破損による資産損失
- 操作ミスによるハード・ソフトの障害及び異常データの発生
- 情報資産(電算機器､ソフトウェア､データ､帳票・各種資料､記録媒体等)の紛失及び盗難
- 天災による情報資産の損失

また､重要情報資産の漏えいは､個人情報等漏えい危機管理マニュアルに即した対応を行うこと。

【緊急時対応手順(障害編)】

１　障害の特定

当該施設(情報資産)利用者は､障害が発生した場合障害の種類及び障害箇所を特定する｡障害の種類とは､以下の３種類がある。

表５　障害の種類

障害の種類	事象
ハードウェアの障害	故障　等
ソフトウェアの障害	バグ　等
ネットワークの障害	ハブ(ＨＵＢ)の故障､構内回線切断　等

2　原因の究明

セキュリティ推進員もしくはセキュリティ推進員に任命された担当者(以下「復旧担当者」という。)は事前に定められた手順で、原因を究明する。手順例は、以下のとおりである。

表６　原因究明の手順例

障害の種類	手順例
ハードウェアの障害	電源スイッチ・コンセントの確認 警告ランプの確認 形状異常の確認　等
ソフトウェアの障害	バグ情報の確認 (提供会社への問い合わせ) 障害内容のチェックと確認　等
ネットワークの障害	電源スイッチ・コンセントの確認 警告ランプの確認 コマンドによる確認 目視チェック　等

復旧担当者は、障害の特定及び原因の究明結果をセキュリティ推進員へ連絡する。

原因が不明の場合、セキュリティ推進員もしくは復旧担当者は、保守委託事業者に協力を要請し、原因の究明を行う。

3　障害報告

セキュリティ推進員は、被害状況に応じてセキュリティ責任者に障害報告を行う。セキュリティ責任者は、障害の復旧が直ちにできない場合は、部会で協議して次表のＢ及びＣの項目について決定し、所管のネットワーク管理者及び統括責任者に報告する。

障害の状態が長期に及ぶ場合は、統括責任者は、セキュリティ会議のメンバーを招集し次の項目について決定する。

表７　セキュリティ会議での決定項目

	決定する項目	対応例
A	関係機関への連絡	総務省、岐阜県主管課 関係市町村　等
B	技術的支援依頼	保守委託業者　等
C	緊急時体制の確立	役割分担の確認 指揮命令系統の確認
D	住民対応	来所者への対応 ホームページ等での告知 問合せ対応 苦情処理
E	代替措置の実施	あらかじめ、業務ごとにサーバ等が停止した場合の事務処理を検討しておき、実施する。

4　保守作業の実施

セキュリティ推進員は、必要に応じて保守委託事業者等に、修理、修復、交換を依頼する。

5　運用の再開

セキュリティ推進員は、情報資産の整合性を確認し、必要があれば修復した後、運用を再開する。

6　再発防止対策(緊急時対応計画の対象外とする)

再発の防止を行うためには、同様の原因で障害が起きないように、以下の技術面、運用面からの対策を検討する。

(1) 技術面の対策

- 障害監視の強化
- 技術情報の収集　等

(2) 運用面の対策

- 定期点検実施時期の見直し
- オーバーホールの実施
- 予備装置の確保
- 教育・研修等

【緊急時対応手順(不正行為編)】

緊急時対応計画書(不正行為編)を作成するためには、情報資産管理における不正行為発生時の対応手順を確立する必要がある。そのため、以下に対応手順を例示する。

1　状況の把握

当該施設(情報資産)利用者は、情報資産に脅威を及ぼす恐れのある事象が発生したら、まず以下の項目を正確に把握し、セキュリティ推進員に伝える。

- いつ(時刻)
- どこで(場所)
- 誰が(人)
- 何を(内容)
- どうした　等

2　緊急措置

セキュリティ推進員は、考え得る対応策のうち、情報資産への脅威が大きいものを直ちに着手する。必要に応じて保守委託事業者の助言を得る。また必要に応じて、ネットワーク管理者、個人情報等管理者、住民情報管理者、情報資産責任者及びシステム責任者に報告する。

3　住民情報に重大な脅威を及ぼす恐れがあるかの判断

システム責任者は、情報資産に重大な脅威を及ぼす恐れがあると判断した場合には、統括責任者にセキュリティ会議の開催を要請する。統括責任者はセキュリティ会議を開催することとしたときは、事案の状況等についてあらかじめ村長へ報告する。

4　セキュリティ会議

統括責任者は、連絡網を利用してセキュリティ会議のメンバーを招集する。

統括責任者は、議長となって以下の項目について決定する。

- 関係機関への連絡
- 緊急時体制の確立
- 詳細な被害状況等の把握
- 住民対応
- 緊急措置の見直しの判断
- 広報
- 恒久対策の立案

5　原因の究明

セキュリティ推進員は、被害情報、ログ情報、記録簿及び管理簿等を分析し、不正が行われた時期、場所、方法を究明する。必要に応じて、保守委託事業者等からの支援を得る。

6　県、国への報告

システム責任者は、総務省及び岐阜県主管課へ別紙様式により報告を行う。

7　緊急措置の見直し

セキュリティ推進員は、既に実施した緊急措置を見直し、利用者権限の設定変更、情報資産管理の停止解除等を実施する。必要に応じて、保守委託事業者等からの支援を得る。

8　恒久対策の実施

セキュリティ推進員は、セキュリティ会議を中心に立案した恒久対策を実施する。必要に応じて審議会等や監査を実施し、答申や監査報告書により体制、規程等の整備を見直す。

９章　コンピュータウイルス対策

【コンピュータウイルス対策基準】

1　対策責任者

セキュリティ推進員は、各情報機器に対して対策責任者を置き管理体制を明確化すること。

2　対策ソフトの導入

(１) 各システムのネットワーク及び東白川村ローカルエリアネットワーク内に接続するパソコン等は、最新のコンピュータウイルス対策ソフトを導入すること。

(２) コンピュータウイルス対策ソフトは、対策責任者が常に最新の状態を保つように管理を行うこととする。

3　運用ルールの遵守

以下の項目をコンピュータウイルス対策ソフトの運用ルールとして対策責任者は遵守しなければならない。

(１) 情報機器に対し、毎日ウイルス検査を実施する、あるいはコンピュータウイルス対策ソフトの常時検査機能を有効とすること。

(２) 機器を導入した場合はウイルス検査を行うこと。

(３) 重要情報資産を扱うコンピュータにソフトウェアの導入や媒体接続を行う場合は、事前にウイルス検査を行うこと。

(４) インストールする全てのソフトウェアをセキュリティ推進員に報告すること。

(５) 被害発生に備え、システム及びデータのバックアップなどの安全対策を実施すること。

(６) 各情報機器の利用者権限は、最小限とすること。

(７) 重要情報資産を扱うコンピュータにデータ等のダウンロードを行う場合は、事前にセキュリティ推進員に許可を得ること。

(８) 業務とは関係のない、あるいは不要な情報機器の操作は行わないこと。

(９) 不明な記録媒体を情報機器で使用しないこと。

(10) 情報機器専用のシステム及びアプリケーションが存在する場合、必ずバックアップを取得しておくこと。

(11) 無許可のパソコンや記録媒体を持ち込まないこと。また、使用しないこと。

4　コンピュータウイルス発見時の対応

コンピュータウイルスに感染した場合、対策責任者は以下の手順に沿って対応すること。

(１) 感染被害の防止措置

感染した情報機器をネットワークより物理的に切り離すこと。(ＬＡＮケーブルを取り外すこと)

（２）感染連絡(報告)

必要な情報をネットワーク管理者に速やかに連絡(報告)すること。感染した機器は原因調査を行うため操作は行わないようにすること。

（３）ウイルス被害の状況把握

ウイルスの種類及び感染範囲の解明に努めること。

（４）復旧手順を確立

安全な復旧を確立し、システムの復旧作業にあたること。

（５）ウイルス被害の再発防止

原因を分析し、再発防止策を講ずること。

５　教育・情報収集

（１）セキュリティ推進員は、ウイルス対策のレベルアップを図るため、ウイルス関連情を収集して周知・徹底すること。

（２）セキュリティ推進員は、セキュリティ対策及びウイルス対策について、対策責任者の教育を行うこと。

（３）セキュリティ推進員は、不正アクセス、ウイルス感染の事案に加え、標的型攻撃等の被害を受けた場合の対応について、関係者において定期的に確認又は訓練等を行うこと。

10章　ソフトウェア管理

【ソフトウェア管理基準】

1　資産管理

ネットワーク管理者は、業務を遂行するために保有するソフトウェアの保有種類及び数量を取得ライセンスと合わせて把握すること。

2　運用管理

セキュリティ推進員は、情報資産管理システムを運用する上で以下の措置を講ずること。

（1）ソフトウェアは、販売者又は配布責任者の連絡先及び更新情報が明確なものを入手すること。

（2）ソフトウェアは、使用上の注意に従い、不正な使用は行なわないようにすること。

（3）不正利用を防止するため、保守機能を含むソフトウェア及びその情報は厳重に管理すること。

（4）原本となるソフトウェア媒体は、ライトプロテクト措置、バックアップの確保等の安全な方法で保管すること。

（5）サービスに用いるディスクは、初期化したディスクを用いて、オリジナルプログラムから作成すること。

（6）ウイルス被害に備えるため、サービスに用いるディスクの構成情報を保存すること。

11章　情報セキュリティ監査の実施

【情報セキュリティ監査実施基準】

1　監査の目的

セキュリティポリシーを有効なものにするためには、組織の全ての領域においてセキュリティポリシーに沿った業務やシステムの運用が行われなければならない。

情報セキュリティ監査責任者は、組織活動における適用技術の適正性及びセキュリティポリシーの適用状況をチェックするため、情報セキュリティ監査を実施する。

2　情報セキュリティ監査の実施

（1）情報セキュリティ外部監査(以下「外部監査」という。)

情報セキュリティ監査責任者は、情報システム等における安全性の技術的検証を外部の専門家等に委託して行うこととする。

（2）情報セキュリティ内部監査(以下「内部監査」という。)

情報セキュリティ監査責任者は、職員等によるセキュリティポリシーの適用状況の確認を定期的に行うこととする。

3　監査による改善

情報セキュリティ監査責任者は、情報セキュリティ監査により技術的な問題点やセキュリティポリシーの不適切な運用などが判明した場合は、適切な指導・改善を行うこととする。

4　外部監査の注意点

情報セキュリティ監査責任者は、外部監査において侵入試験等を行う場合は、試験がシステムの運用や情報セキュリティに悪影響を及ぼさないよう注意しなければならない。

5　内部監査の注意点

情報セキュリティ監査責任者は、内部監査の実施にあたっては、効果的な監査が円満に行われるようにするとともに、日常の業務への影響を極力なくすように注意しなければならない。

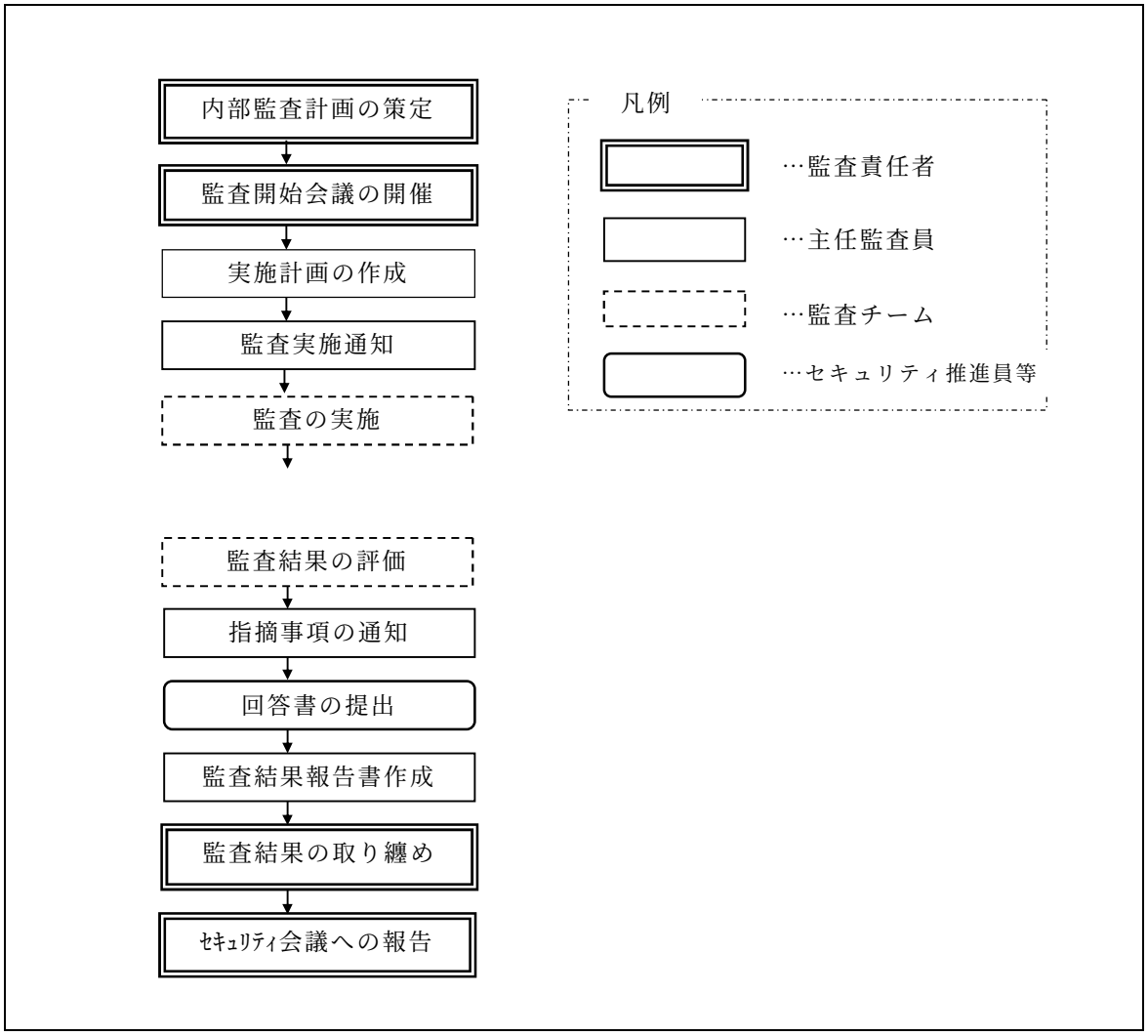
6　監査結果の報告

情報セキュリティ監査責任者は、監査の実施結果についてセキュリティ会議に報告し、改善の必要がある場合は、その改善策について審議に諮ることとする。

【情報セキュリティ内部監査実施手順】

この手順書は、情報セキュリティ内部監査(以下「内部監査」という。)の実施について定めるものとする。

表８　監査の流れ



1　内部監査計画の策定

（1）情報セキュリティ監査責任者は、内部監査の目的、中期方針、内部監査員の選出方法、監査項目等を定めた内部監査計画を作成し、セキュリティ会議に諮り承認を得ることとする。

（2）情報セキュリティ監査責任者は、内部監査計画を受けて、内部監査員を選出する。また、内部監査員の中から主任監査員を選出する。監査を実施する監査チームは、主任監査員及び内部監査員により結成する。

2　監査開始会議

情報セキュリティ監査責任者は、監査の実施に先立ち、次の要領で監査開始会議を主催する。

（1）監査チームのメンバーを紹介する。
（2）監査の目的、基準、及び日程(時間割り)を説明する。
（3）監査の概要及び監査項目等を説明し、被監査部署へのインタビュー、文書類の審査、現場観察の内容を確認する。
（4）監査の開始を宣言する。

3　内部監査実施計画書の作成と事前準備
（1）主任監査員は、被監査部署のセキュリティ推進員と日程、場所等の調整を行い、内部監査実施計画書を作成する。
（2）主任監査員は、被監査部署のセキュリティ推進員に内部監査実施計画書を送付することで監査の実施を通知する。
（3）主任監査員は、監査当日の手順と時間割りを決定する。また、監査チェックリストを作成する。

4　内部監査の実施
内部監査の内容は、被監査部署の職員等へのインタビュー、文書類の審査及び現場観察等とする。
（1）被監査部署の職員等へのインタビュー
監査チームは、監査チェックリストを基に情報セキュリティ対策基準等が適切に運用されているかを確認する。
（2）文書類の審査
監査チームは、次の要領で文書類の審査を行う。
①　情報セキュリティ対策基準等に定めた台帳等を、適切に整備し運用しているか監査チェックリストを基に確認する。
②　被監査部署が自ら定めた基準や手順がある場合、それらが適切に運用されているか手順書や記録により確認する。
③　情報セキュリティに関連する法律等(著作権法など)の要求事項が確実に守られているか確認する。
（3）現場の観察
監査チームは、次の要領で現場の観察を行う。
①　入退室管理、重要情報資産、機器の管理状況等、手順書等で定めた運用・管理策が実施されているか確認する。
②　法規制等の要求事項(届出、必要資格者、ソフト管理など)が確実に守られているか確認する。

5　監査結果の評価(基準)
（1）監査チームは、監査結果について、セキュリティポリシー、対策基準及び実施手順で定めた内容に適合しているかどうかに着目して、監査チェックシートの項目ごとに「重大な不適合」、「軽微な不適合」、「観察」、「適合」及び「該当しない」の５段階で評価する。

表９　監査結果の評価

項番	評価	評価の基準
1	重大な不適合	対策基準や実施手順等のとおり実施していない。
2	軽微な不適合	対策基準や実施手順等のとおり実施しているが、要求事項には不適合。
3	観察	不適合ではないが、定められた手続きのとおり行われていない。
4	適合	対策基準や実施手順等のとおり実施されており、要求事項等にも適合。
5	該当しない	関係するシステムが存在しない等、質問項目に該当しない。

（２）監査結果の評価で「重大な不適合」、「軽微な不適合」及び「観察」となった項目は指摘事項とする。なお、「１」の「重大な不適合」の事項が認められなかった場合でも、「２」の「軽微な不適合」に該当する項目が多数あった場合には、全体として「重大な不適合」と判定する。

6　指摘事項の通知

（１）主任監査員は、評価の結果、指摘事項があった場合は、その内容を被監査部署のセキュリティ推進員に口頭などで説明し確認を受ける。

（２）主任監査員は、指摘事項を是正処置回答書に記載し、被監査部署のセキュリティ推進員に通知する。なお、「重大な不適合」がみられた場合は、セキュリティ責任者にも合わせて通知することとする。

7　是正措置回答書の作成

被監査部署のセキュリティ推進員は、次の手順を踏んで是正措置回答書を作成し、主任監査員に提出する。なお、指摘事項に「重大な不適合」があった場合は、被監査部署のセキュリティ推進員は、是正措置回答書の内容についてセキュリティ責任者の承認を得ることとする。

（１）原因を確定する。

（２）行動計画を作成し、早急に適合性を回復する。

（３）再発を防止する。

（４）取られた処置が効果的に運用されるようにする。

（５）課等で作成した手順書等がある場合は、見直しを検討する。

（６）「観察」については特に回答を要しないこととするが、業務を行ううえで十分留意するなど、以後の運用に反映させる。

8　回答書の検証

主任監査員は、セキュリティ推進員から提出された回答書の内容を検証する。

（１）回答書の内容が適当であり、かつ、改善の取組みが文書で明確にされているかにより回答書の有効性を確認する。

（２）回答書の内容が不十分である場合または改善の取組みが文書等で確認できない場合は、再度、提出を求めるものする。
（３）指摘事項が「重大な不適合」である場合は、改善の取組みを検証し、妥当であることを確認する。
（４）指摘事項が「軽微な不適合」である場合は、次回の監査で実施状況を確認する。

9　監査報告書の作成

主任監査員は、監査報告書を作成する。監査報告書の内容は、次のとおりとする。
（１）監査の目的及び範囲
（２）監査の実施日時
（３）主任監査員及び監査員の氏名
（４）被監査部署の出席者
（５）監査結果
（６）指摘事項及び是正処置の内容
（７）再監査の報告
（８）その他必要事項

主任監査員は、監査報告書に実施計画及び是正措置回答書を添付し、情報セキュリティ監査責任者に提出する。また、被監査部署のセキュリティ推進員へ(「重大な不適合」がある場合はセキュリティ責任者にも)監査報告書及び是正措置回答書の写しを送付する。

10　セキュリティ会議への報告

情報セキュリティ監査責任者は、監査結果をとりまとめ、意見を付してセキュリティ会議に報告する。

12章　セキュリティ対策の改廃

この基準及び手順等の変更及び改廃についてはセキュリティ会議において審議し定める。

【セキュリティ対策の見直し手順】

1　目的

対策基準、手順書、各課が管理している文書等(以下「当該文書」と言う。)の管理責任者は、当該文書が継続して適切であり、妥当であり、かつ、効果が上がるように機能しているかどうかを確認するため、毎年当該文書の見直しを行う。

2　情報の収集

(1) 当該文書の管理責任者は、見直しに必要な情報を収集する。
(2) 当該文書の管理責任者は、セキュリティ会議等の会議において協議した結果をまとめる。

3　見直しのための情報提供

セキュリティ推進員はセキュリティ推進員に、セキュリティ推進員及びネットワーク管理者は情報資産責任者及びシステム責任者に、見直しのために次の情報を提供する。

(1) 内部監査の結果
(2) 苦情を含む外部からのコミュニケーションに関する情報
(3) 研修の実施状況
(4) 機器やソフトの管理状況
(5) 是正処置に関する情報
(6) 改善のための提案

4　見直しの実施

システム責任者及び情報資産責任者は、提供された情報に基づき、次の事項について見直しを実施する。

(1) セキュリティポリシーの妥当性・有効性・適切性
(2) 対策基準、実施手順の運用状況
(3) 情報セキュリティ対策のその他の要素の変更の必要性

5　結果及び記録

(1) 統括責任者は、見直しの結果、セキュリティポリシー、対策基準、手順書並びに各当該文書等の変更の必要性があるかどうかを判断し、必要に応じ、システム責任者及び情報資産責任者に変更を指示する。また、各課で定める基準等の見直しは、セキュリティ推進員等が作成し、所属のセキュリティ責任者の承認を得、職員に周知する。

（２）システム責任者及び情報資産責任者は、見直しの結果を所管する全職員に周知する。

13章　その他のセキュリティ対策

1　各課が管理する情報システム等のセキュリティ対策は、東白川村情報セキュリティ対策に基づき、セキュリティ責任者及びセキュリティ推進員が独自に定めることができるものとする。

2　東白川村情報セキュリティ対策基準は、セキュリティ対策の安全確保のため、原則非公開とする。ただし、重要情報資産管理手順、媒体管理手順、媒体搬送手順、廃棄手順等については、必要に応じて示すことができることとする。

3　東白川村情報セキュリティ対策基準の改正、廃止等は、セキュリティ会議における審議を経て行うものとする。

この東白川村情報セキュリティ対策は、令和８年４月１日から施行する。

改定履歴