高知県情報セキュリティポリシー

高知県文化生活部情報政策課

目　次

「情報セキュリティポリシー」とは
　組織内の情報セキュリティに関する基本的な方針や行動指針のことです。
組織内の情報システムやネットワークを不正な侵入や情報の漏えい等の被害（脅威）から守り、安全性を確保するために、情報システムの利用方法や運営管理方法等を明文化したものです。

高知県情報セキュリティポリシーの策定について

１　目的

電子自治体をはじめとする行政の情報化の進展に伴い、ネットワークや情報システムを利用する業務が増え、業務の効率化及び利便性が向上した一方で、県が情報システムで取り扱う情報は、改ざんや漏えい又はコンピュータウィルスによる情報の破壊やネットワークの停止等の脅威にさらされている。

県では、これらの脅威から情報を保護するため、適切な対策を行い、情報セキュリティを確保することによって、県民が安心してＩＴを活用した行政サービスが受けられる体制を整える必要がある。

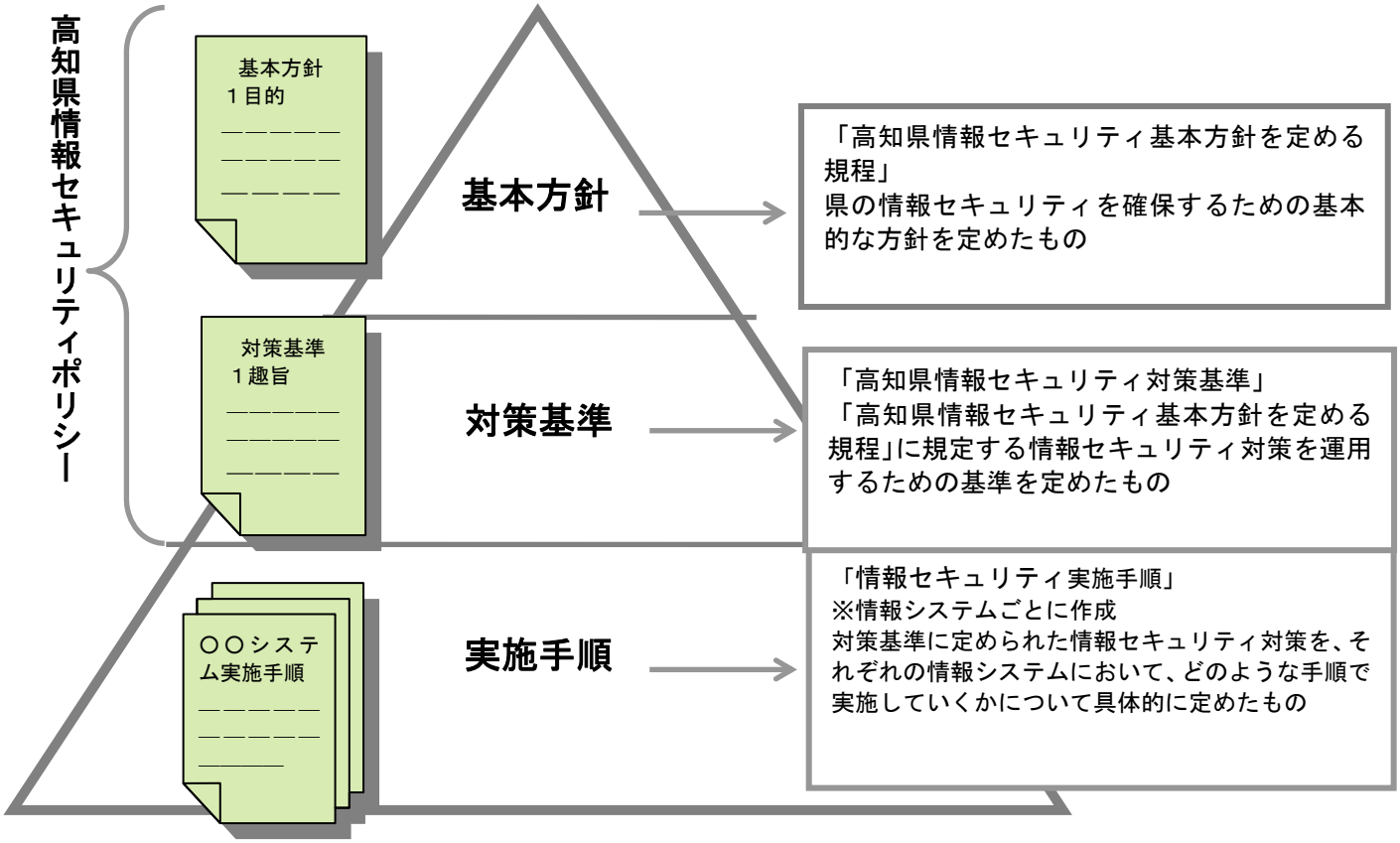
このため、県の情報セキュリティを確保し、情報資産を適切に取り扱うための対策を総合的、体系的かつ具体的にまとめたものが高知県情報セキュリティポリシー（以下「セキュリティポリシー」という。）である。

２　構成

セキュリティポリシーは、「基本方針」と「対策基準」の２階層から構成され、行政運営の根拠や指針とするため、基本方針を「高知県情報セキュリティ基本方針を定める規程」、対策基準を「高知県情報セキュリティ対策基準」に規定する。

また、セキュリティポリシーを形骸化させず、実効性のあるものとするため、セキュリティポリシーに基づく情報セキュリティ対策を、それぞれの情報システムごとに具体的に明記した情報セキュリティ実施手順を今後作成し、運用することによって、県全体の情報セキュリティを確保するものとする。

高知県情報セキュリティポリシーの構成図



訓　　令
公営企業局訓令
議　会　訓　令
教育委員会訓令
警察本部訓令
監査委員訓令
人事委員会訓令

高知県訓令第１１号
高知県公営企業局訓令第１号
高知県議会訓令第２号
高知県教育委員会訓令第７号
高知県警察本部訓令第17号
高知県監査委員訓令第１号
高知県人事委員会訓令第２号

本庁
各出先機関
労働委員会事務局
収用委員会事務局
公営企業局本局
公営企業局各事業所
公営企業局各病院
議会事務局
教育委員会事務局
各教育機関
各県立学校
警察本部
警察署
監査委員事務局
人事委員会事務局

高知県情報セキュリティ基本方針を定める規程を次のように定める。

平成19年４月１日

（改正平成19年11月30日）

高知県知事　橋本　大二郎
高知県公営企業局長　中澤　彰穂
高知県議会議長　山本　広明
高知県教育委員会委員長　宮地　彌典
高知県警察本部長　鈴木　基久
高知県代表監査委員　奴田原　訂
高知県人事委員会委員長　起塚　昌明

高知県情報セキュリティ基本方針を定める規程

（趣旨）

第１条　この規程は、県が管理する情報資産を適切に取り扱い、県の情報セキュリティを確保するための基本的な方針を定めるものとする。

（定義）

第２条　この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（１）　コンピュータ　高知県電子計算機運営規程（平成６年４月高知県訓令第８号）第２条第１号に規定する電子計算機その他の演算、記憶、制御及び入出力の各機能を有する装置及び機器をいう。

（２）　記録媒体　情報を記録するために用いるフロッピーディスク、磁気ディスク、光ディスク等の媒体をいう。

（３）　情報　職員（臨時的任用職員及び非常勤職員を含む。以下同じ。）が職務上作成し、又は取得したすべての情報（コンピュータ及び記録媒体に記録されたもの並びにこれらのものを印刷等により紙媒体としたものを含む。）をいう。

（４）　県庁ネットワーク　高知県情報通信基幹ネットワーク運営管理規程（平成15年４月高知県訓令第８号）第２条第１号アに規定する県庁ネットワーク及びこれに接続する同条第２号に規定する個別ネットワーク（同令第16条第１項の規定に基づき接続されるネットワークを含む。）をいう。

（５）　情報システム　コンピュータ、県庁ネットワークを構成する装置及び機器、プログラム等（第６条において「機器等」という。）の全部又は一部により構成される、情報を処理するための仕組みをいう。

（６）　情報資産　次に掲げる情報システム及び当該情報システムで利用される情報をいう。

ア　県庁ネットワーク及び県庁ネットワークを利用する情報システム

イ　県庁ネットワークを利用しない情報システムにあっては、知事が管理する知事部局の情報システム

（７）　機密性　権限のない者への情報の漏えいを防止し、情報の機密を守ることをいう。

（８）　完全性　情報の改ざん、破壊等による被害を防止し、正確かつ完全であることをいう。

（９）　可用性　権限のある者が、必要な時にいつでも情報資産を利用できることをいう。

（10）　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。

（職員の責務）

第３条　職員は、法令及びこの規程を守り、情報資産の適切な管理に努めなければならない。

２　職員は、情報資産を取り扱う事務の全部又は一部を事業者に委託する場合は、法令及びこの規程を守らせるために必要な措置を講ずるものとする。

（情報セキュリティ委員会）

第４条　情報セキュリティに関する対策（以下「情報セキュリティ対策」という。）を総合的に推進し、及び情報セキュリティ

対策に関する調整を行うため、情報セキュリティ委員会を置く。

２　前項の規定により置かれる情報セキュリティ委員会（第９条において「情報セキュリティ委員会」という。）に関し必要な事項は、別に定める高知県情報セキュリティ対策基準（以下「対策基準」という。）によるものとする。

（情報資産の分類）

第５条　情報資産を管理し、又は利用する所属の長は、対策基準に定める重要性分類に応じてその管理する情報資産を分類し、その分類に応じた情報セキュリティ対策を行うものとする。

（情報セキュリティ対策）

第６条　情報資産を管理し、又は利用する所属の長は、情報漏えい、不正アクセス、災害、コンピュータウイルス感染その他の情報資産に障害を与える原因となるものから情報資産を守るため、次に掲げる情報セキュリティ対策を行うものとする。

（１）　職員の役割及び責任の明確化並びに情報セキュリティに関する教育等の実施

（２）　機器等及び機器等を設置する施設への物理的な対策

（３）　機器等への技術的な対策

（４）　コンピュータウイルスへの対策

（５）　情報システムの開発、導入、保守等における適切な措置

（６）　情報資産への障害発生時における対応計画の策定

第７条　情報資産を管理し、又は利用する職員は、対策基準により情報セキュリティ対策を行わなければならない。

（情報セキュリティ実施手順）

第８条　情報システムを管理する者は、自らが管理する情報システムについて、対策基準に定める情報セキュリティ対策を実施するための具体的な手順をまとめた情報セキュリティ実施手順（以下この条において「実施手順」という。）を作成しなければならない。

２　情報システムを管理する者は、情報セキュリティを確保するため、情報セキュリティ対策の実施状況の点検を行い、必要に応じて実施手順の見直しを行うものとする。

３　情報システムを管理する者は、実施手順を公表しないものとする。

（情報セキュリティの監査）

第９条　情報セキュリティ委員会は、情報セキュリティ対策の実施状況を検証し、及び改善するため、定期的又は必要に応じて情報セキュリティの監査を実施するものとする。

（委任）

第10条　この規程の施行に関し必要な事項は、知事が別に定める。

附　則

この訓令は、平成19年4月1日から施行する。

附　則

この訓令は、平成19年11月30日から施行する。

高知県情報セキュリティ対策基準

第１　趣旨

高知県情報セキュリティ対策基準（以下「対策基準」という。）は、高知県情報セキュリティ基本方針を定める規程（平成 19 年４月高知県訓令第 10 号他共同発令。以下「規程」という。）第 10 条の規定に基づき、情報セキュリティ対策を統一的に行うために必要な事項を定めるものとする。

第２　定義

この対策基準において、使用する用語の意義は、規程で定めるもののほか、次に定めるところによる。

（１）　脅威

情報資産に対して、障害や影響を与える原因となるものをいう。

（２）　情報セキュリティに関する事案

情報漏えい、情報改ざん、不正アクセス、コンピュータウィルスの感染、情報資産の紛失・盗難・破壊及び情報システムの停止をはじめとする情報セキュリティに関する事故及び事件をいう。

（３）　部局等

知事部局の各部局、県議会事務局、教育委員会事務局、人事委員会事務局、監査委員事務局、警察本部、労働委員会事務局及び公営企業局をいう。

なお、収用委員会事務局は知事部局の土木部に含めるものとする。

（４）　所属

部局等のうち知事部局の各部局、教育委員会事務局、警察本部にあっては、課及びその出先機関をいい、部局等のうち県議会事務局、人事委員会事務局、監査委員事務局、労働委員会事務局及び収用委員会事務局にあっては事務局をいう。

第３　組織及び運用管理体制

１　情報セキュリティ委員会

規程第４条第２項の規定に基づき、情報セキュリティ委員会（以下「委員会」という。）について次のとおり定める。

（１）　所掌事務

委員会は、次に掲げる事務を所掌する。

ア　情報セキュリティ対策の総合的な推進及び調整に関すること。

イ　情報セキュリティの監査に関すること。

ウ　上記に掲げるもののほか、情報セキュリティに関連する重要な事項に関すること。

（２）　構成

ア　委員会は、委員長、副委員長及び委員をもって構成する。
イ　委員長は、副知事をもって充てる。
ウ　副委員長は、総務部長をもって充てる。
エ　委員は、別表１に掲げる職にある者をもって充てる。

（３）　職務
ア　委員長は、委員会を代表し、その事務を統括する。
イ　副委員長は、委員長を補佐し、委員長に事故があるときは、その職務を代理する。

（４）　専門的な知識を有する者等の参画
委員長は、必要に応じて委員会に専門的な知識を有する者又は委員以外の職員の参画を求めることができる。

（５）　情報セキュリティ推進部会
ア　委員長は、情報セキュリティ対策を推進する上で調整及び整理が必要と認めた事項について検討するため､委員会の下に情報セキュリティ推進部会（以下｢部会｣という。）を置く。
イ　部会は、部会長及び部員をもって構成する。
ウ　部会長は、総務部情報政策課長をもって充てる。
エ　部員は、別表２に掲げる職にある者をもって充てる。
オ　部会長は、必要に応じて推進部会に専門的な知識を有する者又は部員以外の職員の参画を求めることができる。
カ　部会長は、情報セキュリティ対策に関連する事項について調査を行うため、必要に応じて専門班を設置し、構成員を指名することができる。

（６）　事務局
ア　委員会の事務を処理するため、委員会に事務局を置く。
イ　事務局に事務局長を置き、事務局長は総務部情報政策課長をもって充てる。

２　運用管理体制
情報セキュリティ対策は、委員会のもと次に定める体制により運用し、管理するものとする。

（１）　情報セキュリティ最高統括責任者
ア　県の情報ネットワーク、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を総括する最高責任者として、情報セキュリティ最高統括責任者を置く。
イ　情報セキュリティ最高統括責任者は、情報セキュリティに関する事件・事故等（以下「情報セキュリティインシデント」という。）に迅速かつ的確に対応する組織（以下「CSIRT」という。）を統括する。CSIRT に関し必要な事項は、別に定める CSIRT 設置要綱によるものとする。
ウ　情報セキュリティ最高統括責任者は、副知事をもって充てる。
エ　副知事が不在の場合は、総務部長がその職務を代理する。

（２） 情報セキュリティ統括責任者

ア　情報セキュリティ最高統括責任者を補佐し、情報セキュリティ対策に関する連絡調整を統括するため、情報セキュリティ統括責任者を置く。

イ　情報セキュリティ統括責任者は、CSIRT 責任者として、緊急時には総務部長及び情報セキュリティ最高統括責任者に早急に報告を行うとともに、回復のための対策を講じなければならない。

ウ　情報セキュリティ統括責任者は、総務部情報セキュリティ推進監をもって充てる。

（３） 情報セキュリティ責任者

ア　部局等における情報セキュリティに関する総合的な調整を行い、適切に情報セキュリティ対策を行うため、情報セキュリティ責任者を置く。

イ　情報セキュリティ責任者(以下、「部局等の長」という。)は、別表３に掲げる職にある者をもって充てる。

（４） 県庁ネットワーク管理者

県庁ネットワークにおける統一的な情報セキュリティ対策は、高知県県庁ネットワーク運営管理要綱(平成 15 年４月１日施行)第２条第１号の県庁ネットワーク管理者(以下、「情報政策課長」という。)が行うものとする。

情報政策課長は､県庁ネットワークの情報セキュリティ対策を行うため必要な場合は、職員が使用しているパソコン等の端末の利用状況、アクセス記録、電子メールの送受信記録等を調査することができる。

（５） 情報システム管理者

ア　情報システムにおいて適切な情報セキュリティ対策を行うため、情報システム管理者を置く。

イ　情報システム管理者は、情報システムの運用を管理する所属長をもって充てる。

なお、人事委員会事務局、監査委員事務局、労働委員会事務局にあっては事務局の次長を、収用委員会事務局にあっては事務局の長をもって充てる。

（６） 情報セキュリティ管理者

ア　所属において適切な情報セキュリティ対策を行うため、情報セキュリティ管理者を置く。

イ　情報セキュリティ管理者は､情報資産を管理又は利用する所属の長をもって充てる。

なお、人事委員会事務局、監査委員事務局、労働委員会事務局にあっては事務局の次長を、収用委員会事務局にあっては事務局の長をもって充てる。

（７） 情報セキュリティ担当者

ア　情報セキュリティ管理者(以下「所属長」という。)を補助し、所属における情報セキュリティ対策を円滑に行うため、情報セキュリティ担当者を置く。

イ　情報セキュリティ担当者は、所属の中から所属長が指名する。

（８） 兼務の禁止

情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請者とその承認又は許可者は、同じ者が兼務してはならない。また、監査を受ける者とその監査を実施する者についても同様とする。

第４ 職員の責務

１ 職員の遵守義務

（１） 職員は、次に掲げるもののほか、情報セキュリティに関する法令等を守らなければならない。

ア 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)

イ 著作権法(昭和 45 年法律第 48 号)

ウ 高知県個人情報保護条例(平成 13 年高知県条例第２号)

エ 使用するソフトウェアの使用許諾契約等

２ 違反への対応

職員が情報セキュリティに関する法令等に違反した場合は、その重大性及び事案の状況に応じて、地方公務員法(昭和 25 年法律第 261 号)第 29 条の規定により、懲戒処分の対象となる。

第５ 情報資産の分類

規程第５条に規定する情報資産の分類は次のとおり行うものとする。

１ 情報の分類

所属長は、所属で管理している情報をその重要性に応じて、下表に掲げる情報の重要性分類に基づき分類し、当該情報を取り扱う情報システムごとに整理する。

情報の 重要性分類	情報の内容
情報分類Ａ	組織的に用いるものとして所属で管理している情報のうち、高知県情報公開条例第６条第１項各号のいずれかに該当する非開示情報をいう
情報分類Ｂ	組織的に用いるものとして所属で管理している情報のうち、高知県情報公開条例第６条第１項各号のいずれかに該当する非開示情報以外をいう
情報分類Ｃ	職員個人の段階で管理している情報をいう

２ 情報システムの分類

（１） 情報システム管理者は、下表に掲げる情報システム分類により、管理する情報システムの重要性分類を行う。

情報重要分類	情報の内容
情報分類Ａ	組織的に用いるものとして所属で管理している情報のうち、高知県情報

	公開条例第６条第１項各号のいずれかに該当する非開示情報をいう
情報分類Ｂ	組織的に用いるものとして所属で管理している情報のうち、高知県情報公開条例第６条第１項各号のいずれかに該当する非開示情報以外をいう
情報分類Ｃ	職員個人の段階で管理している情報をいう

（２） 複数の所属が利用する情報システムを管理する情報システム管理者は、自らが管理する情報システムの重要性分類を行うにあたり、当該情報システムで取り扱う情報の情報分類について、利用する所属長から報告を求めることができる。

（３） 情報システム管理者は、自らが管理する情報システムの重要性分類について、所管の部局等の長を経由して情報セキュリティ統括責任者(以下「情報セキュリティ推進監」という。)に報告する。

第６　人的な情報セキュリティ対策

規程第６条第１号に規定する情報セキュリティ対策は次のとおり行うこととし、職員、委託事業者その他情報資産を取り扱う者によるコンピュータの誤操作や不正行為等の脅威から情報資産を保護するものとする。

１　職員の管理責任

（１） 職員は、与えられた利用者ＩＤ、パスワード及び認証に用いるカード等を厳重に管理し、他の者による不正アクセスや不正利用を未然に防止しなければならない。

（２） 職員は、不適切な情報の発信、不正アクセス等、自らが加害者になる行為を行ってはならない。

（３） 所属長及び職員は、第５の１の規定に基づき重要性の分類をした情報について、「高知県公文書規程(昭和39年12月28日訓令第64号)」及び「電磁的記録取扱要綱(平成13年10月1日施行)」の規定に基づき、適切に管理しなければならない。

（４） 職員は、情報分類Ｃの情報であっても、その内容が非開示情報に該当する情報については、情報分類Ａと同様に特に注意して管理しなければならない。また、業務上必要のない情報の複写を行ってはならない。

（５） 職員は、情報分類Ａの情報を電子メールで送信してはならない。

ただし、所属長がやむを得ないと認めた場合はこの限りでない。この場合においては、暗号化できるシステムを使って暗号化するか、又は送信ファイルのパスワード設定を行わなければならない。

（６） 職員は、業務以外の目的でインターネットを利用してはならない。

（７） 職員は、コンピュータを庁舎外に持ち出してはならない。
ただし、情報システム管理者又は所属長が業務上必要であって、かつ、情報セキュリティの確保上支障がないと認めた場合はこの限りでない。

（８） 職員は、自己が所有するコンピュータ及び記録媒体を庁舎内の室（所属がその分掌事務を行うために使用する部屋等の区域、以下「室」という。）に持ち込み、かつ、使用してはならない。
ただし、自己が所有する記録媒体については、情報システム管理者又は所属長が業務上必要であって、かつ、情報セキュリティの確保上支障がないと認めた場合はこの限りでない。

（９） 職員は、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速やかに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。

２ 職員への教育

職員の情報セキュリティに対する意識の向上及び適切な情報セキュリティ対策を実施するため、職員に対して次のとおり教育を実施する。

（１） 啓発及び研修の実施

ア 情報セキュリティ推進監は、職員に対して情報セキュリティに関する啓発及び研修を行う。

イ 情報ステム管理者は、自らが管理する情報システムを利用する職員に対して、必要に応じて操作方法の他に情報セキュリティ対策に関する研修を行う。

ウ 上記ア、イの研修は、目標とする水準を定め、計画的に実施しなければならない。

エ 所属長は、職員を業務上必要な情報セキュリティに関する研修に積極的に参加させるよう努めなければならない。

（２） 研修結果の評価及び見直し

ア 情報セキュリティ推進監及び情報システム管理者は、研修を受けた者が目標とする水準に達したかどうかについて評価を行い、必要に応じて研修内容を見直す。

イ 情報セキュリティ推進監は、情報システム管理者から、研修の実績について報告を求めることができる。

ウ 情報セキュリティ推進監は、実績報告の内容を踏まえ、今後の研修内容に関して助言を行うことができる。

３ 委託事業者への対応

（１） 委託事業者への周知

情報システム管理者は、委託事業者に対してこの対策基準に規定する事項を周知する。

（２） 契約書への記載事項

情報システム管理者は、委託事業者が守るべき内容について、次に掲げるもののうち

必要な事項を契約書に明記する。

ア　再委託の禁止及び制限に関する事項
イ　委託事業者の守秘義務に関する事項
ウ　情報及び関連資料の保管、返還及び廃棄に関する事項
エ　責任者、従業者、作業範囲、作業場所の指定に関する事項
オ　情報及び関連資料の目的外の使用、複製及び複写の禁止に関する事項
カ　情報セキュリティに関する事案が発生した時の報告に関する事項
キ　知的財産権の保護及び著作権の帰属に関する事項
ク　業務記録等の定期報告に関する事項
ケ　委託事業者における情報資産の保護に関する管理体制や情報セキュリティ対策の実施状況等の調査に関する事項
コ　遵守されなかった場合の規定(損害賠償等)
サ　その他情報セキュリティを確保するために必要な事項

（３）　個人情報の取扱い

個人情報に関する情報資産を取り扱う事務については、上記に掲げるもののほか、「高知県個人情報取扱事務委託基準」の規定による。

４　職員及び委託事業者以外の者への対応

職員は、職員及び委託事業者以外の者が情報資産を利用する場合は、その取扱いに関して適切な指導を行う。

第７　物理的な情報セキュリティ対策

規程第６条第２号に規定する情報セキュリティ対策は次のとおり行うこととし、機器等を設置する施設への不正な立入り及び災害等の脅威から情報資産を保護するものとする。

１　施設の管理

（１）　庁舎の管理

「高知県庁舎管理規則(平成５年４月１日高知県規則第29号)」第４条第２項の庁舎管理責任者は、庁舎への不正な立入りを未然に防止する等、情報セキュリティを確保するために必要な措置を講じる。

（２）　室の管理

「高知県庁舎管理規則」第５条第２項の室管理者は、自らが管理する室に設置する機器等に対して、盗難防止のために必要な措置を講じる。

（３）　電算室の管理

情報システム管理者は、情報システムの重要性分類Ａの区分に該当する情報システムのサーバ等の重要な機器等については、原則として外から容易に侵入できないように外壁に囲まれた管理区域(以下「電算室」という。)に設置し、次に掲げる措置を講じる。

ア　入退室管理
イ　破壊、故障、停電及び災害時への備え

ウ　職員及び委託事業者に対する電算室内での作業に関する制限及び監視

２　機器等の管理

（１）　庁舎内への機器等の設置

情報システム管理者は、機器等を設置する庁舎管理責任者及び室管理者と連携を行い、次に掲げる措置を講じる。

ア　破壊、故障、停電及び災害時への備え

イ　既存の情報システム及び県庁ネットワークへの影響についての事前確認

ウ　配線の損傷及び相互干渉等の障害からの保護並びに点検

エ　機器等の搬入・搬出時における職員の立会い

（２）　庁舎外に設置する機器等の管理

情報システム管理者は、庁舎外に機器等を設置する場合は、庁舎内と同等の物理的セキュリティを確保するための措置を講じる。

（３）　庁舎外への機器等の持ち出し

情報システム管理者は、機器等を庁舎外に持ち出す場合は、次の措置を講じる。

ア　故障、盗難等からの保護

イ　管理簿による持ち出し管理の徹底

３　記録媒体の管理

記録媒体の管理については「電磁的記録取扱要綱」の規定によるほか、輸送を行う場合は、情報の複製及び記録媒体の物理的破壊による情報の漏えい及び滅失を防止するための措置を講じる。

第８　技術的な情報セキュリティ対策

規程第６条第３号に規定する情報セキュリティ対策は次のとおり行うこととし、不正アクセスや不正利用及び県庁ネットワークを経由するさまざまな脅威から情報資産を保護するものとする。

１　機器等に関する情報セキュリティ対策

（１）　情報システム管理者

ア　管理者権限を必要最小限の者に与え、厳重に管理すること。

イ　コンピュータのアクセス権限を明確にし、アクセス制御及びアクセス記録の取得等により厳重に管理すること。

ウ　コンピュータの利用者ＩＤを厳重に管理すること。

エ　パスワードの漏えいによる情報システムの不正利用を防止するため、パスワードに関する情報を厳重に管理すること。

オ　機器等の障害発生による情報及びプログラムの滅失や情報システムの運用停止を回避するため、情報システムの重要性に応じて、サーバの二重化等の必要な措置を行うこと。

カ　メールサーバを運用する場合は、第三者からの不正な電子メールの中継や転送を

防止するために必要な対策を行うこと。

キ　不正アクセス、情報の改ざん及びサーバへ負荷を与える通信等の脅威を検知するため、情報システムの重要性を考慮して情報システムの監視を行うこと。

ク　不正アクセスを防止するため、コンピュータに必要な措置を講じること。

ケ　セキュリティホールの緊急度に応じて、ソフトウェアの更新等の対策を実施すること。

コ　コンピュータに対して、職員が業務目的以外の使用を制限するために必要な措置を講じること。

サ　コンピュータに格納された情報は情報システムの重要性を考慮してバックアップを行い、バックアップに用いた記録媒体は「電磁的記録取扱要綱」の規定に基づき適切に管理すること。

シ　機器等の変更を行う場合は、作業内容を記録し、管理すること。

ス　機器等の障害発生時の処理記録を体系的に整理し、再発防止策を立案するために管理すること。

（2）　所属長

所属長は、自らが所管する所属で利用している機器等について、当該機器等を管理する情報システム管理者から指示があった場合は、速やかに所属の職員に指示事項を周知し、対処する。

（3）　職員

職員は、コンピュータに対して次の対策を行う。

ア　業務目的外及び情報システムに障害や影響を与えるソフトウェアを導入しないこと、特にウィニーなどのファイル交換ソフトの使用は禁止する。

イ　改造、機器等の増設及び設定の変更を行わないこと。ただし、情報システム管理者又は所属長が業務上必要であり、かつ、情報セキュリティの確保上支障がないと認めた場合はこの限りでない。

ウ　コンピュータの操作中に離席する場合は、他の者による不正操作及びディスプレイに写された情報の漏えいを防止するため、離席時のログアウト、スクリーンセイバー等の措置を講じること。

2　県庁ネットワークに関する情報セキュリティ対策

県庁ネットワークを経由する情報資産の情報セキュリティを確保するため、次に掲げる対策を行うものとする。

（1）　県庁ネットワークへの接続

ア　情報システム管理者は、自らが管理する情報システムを、県庁ネットワークを利用して構築しようとする場合は、情報政策課長に協議すること。

イ　所属長は、自らが管理するコンピュータ及び周辺機器を新たに県庁ネットワークに接続若しくはすでに接続しているコンピュータ及び周辺機器を変更又は廃止しようとする場合は、情報政策課長に協議すること。

ウ　情報政策課長は、同号ア、イの規定に基づく協議があった場合は、県庁ネットワーク及び他の情報システムへの影響を調査し、利用の適否を情報システム管理者又は所属長に通知すること。

（２）　県庁ネットワーク以外のネットワークとの接続

ア　情報システム管理者及び所属長は、県庁ネットワークを経由して専用回線又はインターネット等の県庁ネットワーク以外のネットワーク（以下「外部ネットワーク」という。）と接続をしようとする場合は、情報政策課長に協議すること。

イ　情報政策課長は、同号アの協議があった場合は、当該外部ネットワークの情報セキュリティ対策の実施状況、県庁ネットワーク及び他の情報システムへの影響を調査し、接続の適否を情報システム管理者に通知すること。

ウ　情報政策課長は、外部ネットワークと接続をする場合は、情報セキュリティ対策及び運用管理を適切に行うこと。

（３）　接続の協議

上記（１）及び（２）の接続に係る協議及び通知は、「高知県県庁ネットワーク運営管理要綱（平成15年4月1日施行）」第４条の規定によるものとする。

（４）　県庁ネットワークのアクセス制御

情報政策課長は、県庁ネットワークの不正利用を防止するため、アクセス制御について必要な措置を講ずる。

なお、県庁ネットワークに接続する機器等において、県庁ネットワークの情報セキュリティを確保する上で支障を及ぼす問題が認められた場合は、情報政策課長の判断で県庁ネットワークの利用を停止することができる。

（５）　無線ネットワークの導入

無線ネットワークの導入は、情報政策課長が解読の困難な暗号化や認証技術の使用等により、県庁ネットワーク上の安全が確保され、かつ必要性等を認めた場合のみとする。

第９　コンピュータウィルスへの対策

規程第６条第４号に規定する情報セキュリティ対策は次のとおり行うものとする。

１　未然の防止

（１）　情報政策課長

情報政策課長は、次のとおりコンピュータウィルス対策を行う。

ア　コンピュータウィルス対策を統一的に行うため、コンピュータウィルス対策の実施方法及び感染時の対応手順を作成し、情報システム管理者及び所属長に周知すること。

イ　対応手順の作成にあたっては、情報セキュリティ推進監が別に定める情報セキュリティに関する事案発生時の対応計画との整合を行うこと。

（２） 情報システム管理者

情報システム管理者は、次のとおりコンピュータウィルス対策を行う。

ア　自らが管理する情報システムのコンピュータウィルス対策の実施方法及び感染時の対応手順を作成し、関係する職員に周知すること。

イ　上記アの規定により作成する実施方法及び対応手順は、情報政策課長が第９の１の(１)のアの規定により作成する実施方法及び対応手順との整合を行うこと。

ウ　コンピュータウィルスチェックのためのパターンファイルは常に最新のものに保つこと。

エ　コンピュータウィルス対策の実施状況を定期的に確認すること。

オ　日頃からコンピュータウィルスに関する情報を収集し、必要に応じて関係する職員に周知すること。

カ　上記に掲げるもののほか、県庁ネットワークその他のネットワークに接続する情報システムについては、当該管理者から指示のあったコンピュータウィルス対策を行うこと、また接続していない情報システムについても、不正プログラムの感染、侵入が生じる可能性が極めて低い場合を除き、コンピュータウィルス対策を行うこと。

（３） 所属長

所属長は、次のとおりコンピュータウィルス対策を行う。

ア　情報政策課長及び情報システム管理者の指示により、所属におけるコンピュータウィルス対策を行うこと。

（４） 職員

職員は、次のとおりコンピュータウィルス対策を行う。

ア　所属長の指示により、コンピュータウィルス対策を行うこと。

イ　差出人が不明又は不自然に添付されたファイルは開かないこと。

ウ　外部(外部ネットワークを含む)からデータファイル又はソフトウェアを取り入れる場合は、ウィルスチェックを行うこと。

２　被害の拡大防止

（１） 職員は、コンピュータウィルスを発見した場合は、直ちにコンピュータを県庁ネットワークから切り離し、コンピュータウィルスの拡大防止に努めるとともに、情報システム管理者が定める対応手順に従い、適切な措置を講ずること。

（２） 再発防止及び対応手順の見直し

ア　情報システム管理者は、職員から報告のあった情報、原因、被害の範囲及び感染から復旧までの対応を時系列に記録し、再発防止策を講ずること。

イ　情報システム管理者は、必要に応じて対応手順の見直しを行うこと。

第10　情報システムの開発、導入及び保守等における措置

規程第６条第５号に規定する情報セキュリティ対策は次に定めるところにより行うもの

とする。

１　情報システムの調達

　情報システム管理者は、情報システムを調達する場合は、調達に関する仕様書等の記載内容が情報セキュリティを確保する上で問題にならないよう配慮しなければならない。

２　情報システムの開発、導入及び保守

　情報システム管理者は、情報システムの開発、導入及び保守における情報セキュリティを確保するため、責任の所在、作業範囲、作業手順を明確にする等の適切な措置を講じなければならない。

３　情報システムの変更管理

　情報システム管理者は、情報システムの機能追加、変更及び廃棄等を行ったときは、その設定及び構成等の履歴を記録し、管理しなければならない。

４　情報システムの更新

　情報システム管理者は、情報システムを構成する機器等の更新を行う場合、あらかじめ情報システムへの影響を調査しなければならない。

　また、情報セキュリティに大きな影響を及ぼす不具合に対する修正プログラム等については、速やかに対応をしなければならない。

５　コンピュータの修理又は廃棄

　情報システム管理者は、機器等を修理又は廃棄する場合は、機器等に格納している情報の漏えいを防止するための措置を講じなければならない。

第11　情報セキュリティに関する事案への対応

　規程第６条第６号に規定する情報セキュリティ対策は次に定めるところにより行うものとする。

１　情報セキュリティに関する事案発生時の対応計画の策定

　情報セキュリティ推進監は、情報セキュリティに関する事案（以下「事案」という。）の発生時に備え、総務部長に協議のうえ、事案発生時の対応計画を策定し、特に重要な事案が発生した時には情報セキュリティ委員会に報告を求める等、適切に対処をするための連絡体制を整備する。

２　情報システムにおける事案発生時の対応手順の作成

　情報システム管理者は、情報セキュリティ推進監が策定する事案発生時の対応計画に基づき、自らが管理する情報システムについて、事案発生時における、連絡、証拠保全、被害拡大の防止及び復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講ずるため、次に掲げる事案が発生した場合の対応手順を規程第８条第１項に規定する情報セキュリティ実施手順に定めるものとし、情報資産を取り扱う職員に周知する。

（１） 個人情報の漏えい、公開ホームページの改ざん及び情報システムの停止等、県民に被害や影響が生じる恐れがあるとき

（２） コンピュータウィルス等の不正プログラムが発生し、被害が拡大する恐れがあるとき

（３） 不正アクセスが判明したとき

（４） 情報資産の紛失、盗難、破壊

（５） その他情報資産への被害が想定されるとき

３　事案発生時の対応

職員は、事案を認めた場合は、情報システム管理者が作成する事案の対応手順に基づき、適切に対処する。

なお、自然現象により生ずる災害及び県民にとっての危機事象が発生し、高知県災害対策本部又は高知県危機管理本部が設置された場合は、当該対策本部の指示により対処する。

４　事案の再発防止

情報システム管理者は、事案が発生した場合、事案の内容、発生原因、対応方法、被害状況をもとに、事案の対応手順の見直し及び情報セキュリティ対策の改善等の再発防止策をまとめ、情報セキュリティ推進監に報告する。

５　事案発生時の対応計画の見直し

情報セキュリティ推進監は、前項の報告を踏まえ、総務部長に協議のうえ、必要に応じて事案発生時の対応計画を見直さなければならない。

第12　情報セキュリティの監査

１　規程第９条に規定する情報セキュリティの監査は、情報セキュリティ推進監が実施計画を策定し、定期的又は必要に応じて実施する。

２　被監査部門は、監査の実施に協力しなければならない。

３　情報セキュリティ推進監は、監査の結果を踏まえ、情報セキュリティ対策に関する重要な事項について見直しが必要な場合は、情報セキュリティ委員会に報告する。

別表１（第３の１の（２）のエ　関係）

職　名
危機管理部長
健康政策部長
地域福祉部長
文化生活スポーツ部長
産業振興推進部長
中山間振興・交通部長
商工労働部長
観光振興部長
農業振興部長
林業振興・環境部長
水産振興部長
土木部長
会計管理局長
教育長
監査委員事務局長
警察本部長
公営企業局長
総務部情報セキュリティ推進監

別表２（第３の１の（５）のエ 関係）

職　名
総務部法務課長
総務部文書情報課長
総務部行政管理課長
総務部人事課長
総務部管財課長
危機管理部危機管理・防災課長
会計管理局会計管理課長

別表３（第３の２の（３）のイ 関係）

部局等名	職　名
総務部	総務部長
危機管理部	危機管理部長
健康政策部	健康政策部長
地域福祉部	地域福祉部長
文化生活スポーツ部	文化生活スポーツ部長
産業振興推進部	産業振興推進部長
中山間振興・交通部	中山間振興・交通部長
商工労働部	商工労働部長
観光振興部	観光振興部長
農業振興部	農業振興部長
林業振興・環境部	林業振興・環境部長
水産振興部	水産振興部長
土木部	土木部長
会計管理局	会計管理局長
県議会事務局	議会事務局長
教育委員会事務局	教育長
人事委員会事務	人事委員会事務局長
監査委員事務局	監査委員事務局長
警察本部	警察本部警務部長
労働委員会事務局	労働委員会事務局長
公営企業局	公営企業局長

附 則
１ この対策基準は、平成16年11月26日から施行する。
附 則
１ この対策基準は、平成17年１月１日から施行する。
附 則
１ この対策基準は、平成17年４月１日から施行する。
附 則
１ この対策基準は、平成18年４月１日から施行する。
附 則
１ この対策基準は、平成19年４月１日から施行する。
附 則
１ この対策基準は、平成19年11月30日から施行する。
附 則
１ この対策基準は、平成21年４月１日から施行する。
附 則
１ この対策基準は、平成 22 年４月１日から施行する。
附 則
１ この対策基準は、平成29年４月１日から施行する。

【付録】
《用語の解説》５０音順

１．　アクセス権限
　ネットワークを通じて別の場所にあるコンピュータに接続し、情報システムを利用する権限をいう。

２．　コンピュータウィルス
　第三者のプログラムやデータベースに対して、意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能のいずれか一つ以上を有するものをいう。

３．　サーバ
　ネットワーク又は情報システムの利用サービスを提供するソフトウェア又はコンピュータ等の機器をいう。

４．　修正プログラム
　ソフトウェアの（情報セキュリティ上の）欠陥を修正するための追加的ソフトウェアをいう。

５．　セキュリティホール
　ソフトウェアの設計ミスなどによって生じた、システムの（情報セキュリティ上の）欠陥をいう。

６．　二重化
　構成の同じシステムが２つあること。又は、情報システム内にバックアップを設けることをいう。

７．　パスワード
　情報システムやネットワークにログイン（アクセスを開始すること）する時又はデータベース等の機密保持が必要なアプリケーションの利用時等に、利用者本人であることを証明するために入力する数字又は文字列の符号をいう。

８．　パターンファイル（＝定義ファイル）
　過去に発見されたウィルスの情報がまとめられているファイルをいう。

９．　ファイル交換ソフト（ファイル共有ソフトともいう）
　ネットワークを介して不特定多数のコンピュータの間でファイルを共有するソフトウェアをいう。例えばウィニー（Ｗｉｎｎｙ）などがある。

10.　不正アクセス
　「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）」第３条第２項に規定する不正アクセス行為その他の不正な手段により利用者以外のものが行うアクセス又は利用者が行う権限外のアクセスをいう。

11.　利用者ＩＤ
　情報システムやネットワークにログインする時に、利用者本人を識別するために入力す

る数字又は文字列の符号をいう。

12. ログアウト
アクセスを終了することをいう(⇔ログイン)。

《関連する要綱等の掲載ＵＲＬ》

１　高知県県庁ネットワーク運営管理要綱(平成15年４月1日施行)
http://info/~jyouhou/kijun/NW_youkou.doc

２　電磁的記録取扱要綱(平成13年10月１日施行)
http://info/~soumu/kensei/koubunsyo/denjiyoukou.htm

３　コンピュータ及び記録媒体を処分する際のデータの処理について(平成18年10月１日付け18高情企第146号情報企画課長通知)
http://bbs.pref.kochi.lg.jp/bbs/bunka/1412012006100100/bunka543.html

４　高知県個人情報取扱事務委託基準
http://info/~soumu/bunsho/kozinzyouhou/itakukijun.docx

５　私用の外部記録媒体の持ち込み禁止及びＵＳＢメモリの管理並びに共有フォルダの活用について(平成21年３月31日付け20高情政第1028号政策企画部長通知)
http://bbs.pref.kochi.lg.jp/bbs/bunka/1412012009033100/bunka13html