平成15年3月4日
政 策 会 議 決 定

兵庫県情報セキュリティ対策指針

第１章　情報セキュリティ対策基本方針

（目的）

第１条　この指針は、兵庫県の情報資産を適切に保持するため、情報システムの信頼性及び安全性の確保に必要な情報セキュリティ対策の基本方針と具体的な対策を講ずるに当たっての基準を定めるものとする。

（定義）

第２条　この指針の用語の定義は、当該各号に定めるところによる。

(1) 情報資産　情報システムの開発、運用、利用等に係るすべての電磁的に記録されたデータをいう。

(2) 情報セキュリティ対策　情報資産の完全性、可用性、機密性を保持し、適正な利用を確保することをいう。

(3) 情報システム　コンピュータ、通信機器、通信回線及び記録媒体で構成され、業務に関する情報処理を行う仕組みをいう。

(4) ネットワーク　複数のコンピュータを通信回線により、互いに資源を共有することができるように結合させた仕組みをいう。

(5) サーバ　情報システムを構成する機器のうち、特定のサービスを提供するコンピュータをいう。

(6) ＩＤ　情報システムの利用者を識別するための記号をいう。

(7) ＩＤカード　情報システムの利用者を識別するための磁気又はＩＣカードをいう。

(8) パスワード　情報システムの利用者であることを確認するために使用される記号をいう。

(9) 不正アクセス　情報システムを利用する権限のない者が不正な手段でこれを利用することをいう。

(10) バックアップ　データの滅失、き損に備えた複製をいう。

(11) コンピュータウィルス　情報システムの正常な動作を意図的に妨げるプログラムをいう。

（対象範囲）

第３条　この指針は、県の各機関が構築・運用するすべての情報システムを対象とする。

２　前項の機関の範囲は、知事、議会、教育委員会、選挙管理委員会、人事委員会、監査委員、労働委員会、収用委員会、海区漁業調整委員会、内水面漁場管理委員会並びに公営企業及び病院事業の管理者とする。

３　この指針は、前項の機関のすべての職員（臨時職員、再任用職員、非常勤職員等を含む）及び前項の機関から情報システムの開発・運用を委託された外部委託事業者等（以下「利用者」という。）に適用する。

（情報資産の分類）

第４条　情報セキュリティ対策は、情報資産をその内容に応じて分類し、その重要度に応じて行うものとする。

（情報資産への脅威）

第５条　情報セキュリティ対策は、兵庫県が保有する情報資産を次の各号に掲げる脅威から的確かつ効率的に保護することを目的とする。

(1)　情報システムへの不正アクセス、不正操作、利用者による意図しない操作、コンピュータウィルスの頒布、過剰な負荷をかける行為等によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難、情報システムの中断及び停止等。

(2)　利用者による記録媒体の持出、規定外の端末接続等によるデータやプログラムの漏洩、流出等。

(3)　地震、落雷、火災等の災害並びに事故、故障等による情報システムの損傷、中断及び停止。

（情報セキュリティ対策）

第６条　前条で示した脅威から情報資産を保護するために、次の各号に掲げる対策を講ずるものとする。

(1)　物理的セキュリティ対策

情報システムを構成する機器及びこれらの機器･設備を設置する施設の入退室管理等情報システムの設置に伴う安全性を確保するために必要な対策を講ずる。

(2)　人的セキュリティ対策

情報システムの利用者の責務を明らかにするとともに情報セキュリティ対策に関する研修や啓発を行うなど情報システムの適正な利用を確保するために必要な対策を講ずる。

(3)　技術的セキュリティ対策

情報システムへの不正アクセスの防止、コンピュータウィルス対策、情報システムにおけるアクセス制御等の情報システムの開発及び運用における技術的信頼性を確保するために必要な対策を講ずる。

(4)　運用面の対策

情報システムの監視、指針の遵守状況の確認、緊急事態に対応した危機管理等により情報システムの運用面における信頼性を確保し、この指針を効果的に運用するために必要な対策を講ずる。

（情報セキュリティ対策統括者）

第７条　この指針に基づき、全庁的な情報セキュリティ対策を統括する責任者として、情報セキュリティ対策統括者（以下「統括者」という。）を置く。

２　統括者には企画県民部科学情報局長をもって充てる。

（情報セキュリティ対策委員会）

第８条　県における情報セキュリティ対策を円滑に推進するため、情報セキュリティ対策委員会（以下「委員会」という。）を置く。

２　委員会の委員長は統括者をもって充てる。

３　委員会は、情報セキュリティ対策の推進方策や指針の見直し等について協議、調整を行う。

４　その他委員会の運営に関し必要な事項については別に定める。

（運用管理者の責務）

第９条　この指針に基づき、情報システムの適正な運用を図るために、各情報システムに情報セキュリティ対策の運用管理者（以下「運用管理者」という。）を置く。
２　運用管理者には、当該情報システムの業務主管課室長（企画参事を含む。）をもって充てる。ただし、当該情報システムにおいて他の業務管理者が定められている場合はこの限りではない。
３　運用管理者は、当該情報システムの適正な運用を図るために必要な情報セキュリティ対策の実施手順を策定しなければならない。
４　運用管理者は、この指針及び実施手順の遵守状況を適宜点検し、これらの実効性が保たれるよう必要な措置を講じなければならない。

（利用責任者の責務）
第１０条　情報システムの適正な利用を確保するため、各所属に情報システムの利用責任者（以下「利用責任者」という。）を置く。
２　利用責任者には次の各号に掲げる者をもって充てる。
⑴　本庁においては課室長（企画参事を含む。）とする。
⑵　地方機関においては地方機関の長、教育機関の長、県立学校の校長とする。ただし、県民局及び県民センターにあっては室等の長及び事務所の長等とする。
３　利用責任者は、各所属においてこの指針及び運用管理者が定める実施手順が遵守されるよう必要な措置を講じなければならない。

（利用者の責務）
第１１条　利用者は、この指針及び実施手順を遵守し、情報システムを適正に利用しなければならない。

（評価及び見直し）
第１２条　運用管理者は、この指針を踏まえた情報セキュリティ対策の遵守状況について定期的に監査し、その結果を統括者に報告しなければならない。
２　統括者は、委員会での協議を踏まえ、必要に応じて指針の見直しを行わなければならない。

第２章　情報セキュリティ対策基準

第１節　物理的セキュリティ対策

（機器の設置）
第１３条　運用管理者は、情報システムの機器の設置について、次の各号に掲げる措置を講じなければならない。
⑴　火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう固定する等の措置を講ずること。
⑵　情報システムを設置する事務室への不正な侵入や盗難を防止するため施錠の徹底等必要な措置を講ずること。
⑶　利用者以外の者が容易に操作できないように、利用者のＩＤ及びパスワードの設定等の措置を講ずること。
⑷　ディスプレイ装置、配線等から放射される電磁波による情報の外部への漏えいを防止する措置を講ずること。

(5)　当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備えつけること。
(6)　落雷等による過電流に対して機器を保護するために必要な措置を講ずること。
(7)　機器の配線に当たっては、損傷等を受けることがないよう必要な措置を講ずること。

（情報システム室の設置管理）
第１４条　運用管理者は、重要な情報システムの設置、運用及び管理を行うための施設(以下「情報システム室」という。)を設置する場合は、次の各号に掲げる対策を講じなければならない。
(1)　情報システム室には、耐震対策、防火対策、防犯対策等の措置を講ずること。
(2)　情報システム室の入退室はあらかじめ許可した者のみとし、ビデオカメラによる監視装置、カード、指紋認証等による入退室管理又は入退室管理簿の記載を行うこと。
(3)　情報システム室へ機器等を搬入する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について確認を行うこと。
(4)　情報システム室内の機器の配置は、緊急時に利用者が円滑に避難できるように配慮すること。
２　情報システム室に入室する者は、身分証明書等を携帯し、運用管理者の指定する担当職員の求めに従い提示しなければならない。
３　情報システム室に機器等を設置しようとする者は、当該情報システム室を設置する運用管理者の指示に従わなければならない。
４　運用管理者は、民間事業者等他の機関が管理する施設に情報システムを設置して運用を委託するときは、次の各号に掲げる事項を遵守しなければならない。
(1) 当該施設が第１項に規定する対策が講じられていることを確認すること。
(2) 当該施設におけるセキュリティ対策の実施状況について定期的に監査すること。
(3) その他、この指針で定める対策基準に基づき適正な外部委託の管理を行うこと。

第２節　人的セキュリティ対策

（情報資産の管理）
第１５条　情報資産の管理に当たって、利用者は次の各号に掲げる事項を遵守しなければならない。
(1)　データのき損、滅失等に備えるため、保管するデータのバックアップを定期的に作成すること。
(2)　重要な情報資産はパスワードを施すなど適切な管理を行うこと。
(3)　退庁時及び長時間離席する場合は、使用する端末等の電源を切ること。
(4)　運用管理者の許可を得ず、情報システムで処理するデータ及びその複製を定められた場所から移動させないこと。
(5) その他、自己の管理する情報が他に流出しないよう保護すること。

（記録媒体の管理）
第１６条　情報資産をハードディスク、フロッピーディスク等の記録媒体で管理する場合は、次の各号に掲げる措置を講じなければならない。
(1)　取り出し可能な記録媒体は、盗難や損傷の防止のために適切な管理を行うこと。
(2)　記録媒体は、防犯、耐火、耐熱、耐水及び耐湿対策等を講じた施錠可能な場所に保管し、管理簿を設けるなど適切な管理を行うこと。

(3)　記録媒体が不要となった場合は、当該媒体に含まれる情報は、記録媒体の初期化など情報を復元できないように消去を行ったうえで廃棄すること。

（利用禁止行為）

第１７条　利用者は、情報システムの利用について次の各号に掲げる行為を行ってはならない。

(1)　業務に関連しない目的で情報システムを利用すること。

(2)　法令又は公序良俗に反した利用を行うこと。

(3)　他の利用者又は第三者の著作権、人権及びプライバシーを侵害するおそれのある利用を行うこと。

(4)　情報の改ざん、き損及び滅失並びに虚偽の情報提供を行うこと。

(5)　通信を阻害する行為及び情報資産に損害又は不利益を及ぼす利用を行うこと。

２　運用管理者は、前項に該当する利用が行われていると認める場合は、当該利用者に対して情報システムの利用を停止することができる。

（ＩＤ及びパスワードの管理）

第１８条　利用者は、自己の保有するＩＤ及びパスワードに関し、次の各号に掲げる事項を遵守しなければならない。

(1)　他の利用者のＩＤは使わないこと。

(2)　パスワードは十分な長さとし、文字列はアルファベット、数字及び記号を混在させるなど容易に推定できないものとすること。

(3)　パスワードは定期的に変更し、古いパスワードの再利用はしないこと。

(4)　パスワードを秘密にし、パスワードの照会等には一切応じないこと。

(5)　パスワードの盗用や漏えいがあった場合は、直ちに利用責任者に連絡すること。

(6)　その他、ＩＤ及びパスワードの適正な管理を行うこと。

２　利用者はＩＤカードの利用について、次の各号に掲げる事項を遵守しなければならない。

(1)　ＩＤカードを利用者間で共有しないこと。

(2)　ＩＤカードを、カードの読み取り装置又は端末に常時挿入しないこと。

(3)　ＩＤカードを紛失した場合には、速やかに利用責任者に通報し、指示を仰ぐこと。

（教育・訓練）

第１９条　統括者は、すべての職員がこの指針について理解を深め、遵守を徹底するよう、情報セキュリティ対策に関する研修の実施や普及啓発を行わなければならない。

２　運用管理者は、情報システムに不測の事態が発生した場合に備えた訓練を計画的に行わなければならない。

（事故等の報告）

第２０条　利用者は、情報資産の流出、漏えい、改ざん、情報システムの障害及び誤動作等の事故（以下「事故等」という。）を発見した場合には、直ちに利用責任者に報告し、その指示に従い必要な措置を講じなければならない。

２　利用責任者は、事故等の報告を受けた場合は、直ちに当該事故等の内容を運用管理者に報告しなければならない。

（外部委託に関する管理）

第２１条　運用管理者は、情報システムの開発・保守運用を民間事業者等に委託する場合は、こ

の指針を踏まえ当該外部委託事業者が遵守すべき事項を明記した契約を締結しなければならない。

2　運用管理者は、個人情報取扱事務その他の個人情報を取り扱う事務を外部委託事業者に委託しようとするときは、当該外部委託事業者との契約書に、個人情報取扱特記事項（「個人情報を取り扱う事務の委託に伴う措置について(平成9年11月21日付け文第294号知事公室長通知)」）を規定しなければならない。

3　運用管理者は、外部委託事業者との契約書には、この指針及び実施手順が遵守されなかった場合の損害賠償等の規定を定めなければならない。

4　運用管理者は、外部委託事業者及び再委託する場合の当該再委託事業者（以下「外部委託事業者等」という。）とのデータの受け渡しに係る内容、日付等を記録しなければならない。

5　運用管理者は、外部委託事業者等の責任者や業務に携わる社員の名簿を作成しなければならない。

6　運用管理者は、身分証明書の提示を外部委託事業者等に求めるなどにより、契約で定められた資格を有するものが作業に従事しているか確認を行わなければならない。

第３節　技術的セキュリティ対策

（アクセス記録の取得等）

第２２条　運用管理者は、各種アクセス記録及び情報セキュリティ対策に必要な記録をすべて取得し、１年以上の期間を定めて、保存しなければならない。

2　前項に掲げる以外の情報については、その重要度に応じて期間を設定し、バックアップを作成しなければならない。

3　運用管理者は、定期的にアクセス記録等を分析、監視しなければならない。

4　運用管理者は、アクセス記録等が窃取、改ざん、消去されないように必要な措置を講じなければならない。

（情報システムの入出力データ）

第２３条　運用管理者は、当該情報システムに入力されるデータの正確性を確保するための対策を講じなければならない。

2　運用管理者は、利用者又は利用者以外の者の故意又は過失による誤ったデータの入力により情報が改ざんされるおそれがある場合、これを検出する手段を講じなければならない。また、改ざんの有無を検出し、必要な場合は情報の修復を行う手段を講じなければならない。

3　運用管理者は、情報システムから出力されるデータが、正しく情報処理され、出力されることを確保しなければならない。

（電子署名・暗号化）

第２４条　運用管理者は、機密情報及び重大な情報については、機密性を保護するために暗号化しなければならない。

2　暗号化に係る運用管理については別に定める。

（機器構成の変更）

第２５条　運用管理者は、情報システムの機器に業務上必要でないプロトコル（通信手順）を設定してはならない。

2　利用者は、端末の改造及び機器の増設・交換を行ってはならない。

３　利用者は、運用管理者の許可なく、その使用する端末にＩＤの追加、共有データの設定、ソフトウェアの追加等の設定変更を行ってはならない。

（利用者の管理）

第２６条　運用管理者は、情報システムの利用者の登録、変更、抹消等登録情報の管理及び異動、退職した職員等のＩＤ及びパスワードの管理等利用者を適正に管理しなければならない。

（情報システムにおけるアクセス制御）

第２７条　運用管理者は、情報システムにおけるアクセス制御について次の各号に掲げる事項を遵守しなければならない。

(1)　アクセス権限の許可は必要最少限にすること。

(2)　不正アクセスを防止するため、ユーザ認証、論理的なネットワークの分割、ファイアウォール(組織内の情報通信機器や端末に外部からの侵入を防ぐ目的で設置してあるセキュリティシステム）の設置等の適切なネットワーク経路制御を講ずること。

(3)　アクセス方法等は利用者の真正性が確保できるものにすること。

(4)　接続した情報通信機器についてセキュリティに問題が認められ、情報システムの情報資産に脅威が生じることが想定される場合には、速やかに当該情報通信機器を内部ネットワークとの接続から物理的に遮断すること。

（外部ネットワークとの接続）

第２８条　県の情報システムと県以外の機関が管理する情報システム（以下「外部ネットワーク」という。）との接続については、次の各号に掲げる事項を遵守しなければならない。

(1)　不正アクセスを防止するためのファイアウォールの設置や利用者の認証、論理的なネットワークの分割等適切なネットワーク経路制御を講ずること。

(2)　外部から情報システムにアクセスする場合は、ユーザ認証、ファイアウォールの設置等のネットワーク上の制御を講ずること。

(3)　外部ネットワークとの接続により情報システムの運用及び情報資産の保持に支障が生じるおそれがある場合は、直ちに当該情報システムと外部ネットワークとの接続を物理的に遮断すること。

（情報システムの開発）

第２９条　運用管理者は、情報システムの開発について次の各号に掲げる事項を実施しなければならない。

(1)　情報システムの開発、保守等に関する事故及び不正行為に係るリスク（危険性）の評価を行うこと。

(2)　プログラム、設定等のソースコードを整備すること。

(3)　セキュリティの確保に支障が生じるおそれのあるソフトウェアは使用しないこと。

(4)　情報システムの開発及び保守に係る記録を作成するとともに、運用、管理等に必要な説明書等の書類は定められた場所へ保管すること。

(5)　不要になった利用者ＩＤ、パスワード等は速やかに抹消すること。

（情報システムの調達）

第３０条　運用管理者は、情報システムの機器及びソフトウェアの調達に伴う仕様書の作成については、情報セキュリティ対策上支障が生じるおそれのある内容を記載しないようにしなけれ

ばならない。
2　運用管理者は、機器及びソフトウェアを調達する場合は、当該製品の安全性及び信頼性を確認しなければならない。

（ソフトウェアの保守及び更新）
第３１条　運用管理者は、独自開発ソフトウェア及びＯＳ等を更新し又は修正プログラムを導入する場合は、不具合及び他のシステムとの適合性の確認を行い、計画的に更新し又は導入しなければならない。
2　運用管理者は、情報セキュリティに重大な影響を及ぼす不具合に関して常に情報を収集し、発見した場合は、修正プログラムの導入等速やかな対応を行わなければならない。

（コンピュータウィルス対策）
第３２条　運用管理者は、コンピュータウィルスによる情報システムの安全性を確保するため、次の各号に掲げる事項を実施しなければならない。
(1)　外部のネットワークからデータを取り入れる際には、ファイアウォール、メールサーバ等においてウィルスチェックを行いシステムへの侵入を防止すること。
(2)　外部のネットワークへデータを送信する際にも、前号と同様のウィルスチェックを行い、外部へのコンピュータウィルスの拡散を防止すること。
(3)　コンピュータウィルス情報について利用者に対する注意喚起を行うこと。
(4)　端末においてウィルス対策用のソフトウェアを導入すること。
(5)　ウィルスチェック用のパターンファイルは常に最新のものに保つこと。
(6)　コンピュータウィルスに対する修正プログラムの入手に努め、サーバ及び端末に速やかに適用すること。
(7)　コンピュータウィルスの感染のおそれの少ないソフトウェアの選定を行うこと。
2　利用責任者は、利用者がコンピュータウィルスを発見した場合、又はコンピュータウィルスにより障害が生じたと認められる場合は、直ちに運用管理者に連絡し、その指示に従わなければならない。
3　利用者は、コンピュータウィルスによる被害を防止するため、次の各号に掲げる事項を遵守しなければならない。
(1)　差出人が不明な電子メールや不審なファイルが添付された電子メールを受信した場合は開封せず、直ちに削除すること。
(2)　添付ファイルのあるメールを送信する場合は、ウィルスチェックを行うこと。
(3)　外部から入手したデータは、必ずウィルスチェックを行うこと。
(4)　万一のコンピュータウィルス被害に備えるため、データのバックアップを作成すること。
(5)　運用管理者が提供するウィルスチェック用のパターンファイルは常に最新のファイルに更新すること。
(6)　運用管理者が提供するコンピュータウィルス情報を常に確認すること。

（不正アクセス対策）
第３３条　運用管理者は、不正アクセスを防止するため、次の各号に掲げる対策を講じなければならない。
(1)　使用終了又は使用される予定のないポート（ネットワーク上のサーバがサービスを区別するために使っている番号）を長時間空けた状態のままにしないこと。
(2)　情報通信機器及び端末上の不要なＩＤは速やかに削除すること。
(3)　ソフトウェアの不備に伴うセキュリティホールに対しては、速やかに修正プログラムを適

用すること。

(4)　不正アクセスによるウェブページの改ざんを防止するために、ウェブページ改ざんを検出し、運用管理者へ通報する設定を講ずること。

(5)　重要な情報システムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検査すること。

(6)　不正アクセスを受けるおそれが認められる場合には、情報システムの停止を含む必要な措置を講ずること。

2　運用管理者は、不正アクセスを受けた場合は、直ちに統括者及び関係機関に連絡を行い、情報システムの復旧等必要な措置を講じなければならない。

3　利用責任者は、不正アクセスを受けた場合は、直ちに運用管理者に連絡し、その指示に従わなければならない。

（セキュリティ情報の収集）

第３４条　統括者は、情報セキュリティに関する情報を積極的に収集し、運用管理者や利用責任者等に速やかに周知し、必要な措置を講じなければならない。

2　統括者は、前項の情報を定期的に取りまとめ、関係部局等に通知するとともに、この指針の改定につながる情報については委員会に報告しなければならない。

第４節　運用面の対策

（情報システムの監視）

第３５条　運用管理者は、情報システムの円滑な運用を確保するため、情報システムを定期的に監視し、障害が起きた際は速やかに対応しなければならない。

2　運用管理者は、外部と常時接続するシステムについては、ネットワーク侵入監視装置を設置し、２４時間監視を行わなければならない。

3　運用管理者は、情報システム内部において、適正なアクセス制御を行い、運用状況について監視を行わなければならない。

4　運用管理者は、監視した結果を正確に記録するとともに、消去や改ざんをされないよう必要な措置を施し、安全な場所に保管しなければならない。

（指針の遵守状況の確認）

第３６条　利用者は、この指針に違反した場合及び違反の発生を確認した場合は、直ちに利用責任者に報告を行わなければならない。

2　利用責任者は、この指針の遵守状況及び情報資産の管理状況について常に確認を行い、支障を認めた場合には速やかに運用管理者に報告しなければならない。

3　運用管理者は、情報システムにおけるこの指針の遵守状況及び情報資産の管理状況について定期的に確認を行い、支障を認めた場合には、迅速かつ適切に対処しなければならない。

（緊急時対応計画等）

第３７条　運用管理者は、情報資産への侵害が発生した場合に備えて、あらかじめ関係機関との連絡体制や復旧対策など緊急時対応計画を策定しなければならない。

2　利用責任者は、情報資産への侵害発生及び侵害発生の危険性を発見した場合は、事案の内容、原因、被害の状況等を速やかに運用管理者に報告しなければならない。

3　運用管理者は、情報資産への侵害に起因して、住民に重大な被害が生じるおそれがある場合、

又は行政の運営に重大な支障が生じる場合は、統括者に直ちに報告するとともに、関係機関に速やかに連絡しなければならない。

4　運用管理者は、情報システムに障害が発生し、情報資産の保持のために情報システムの停止がやむを得ないと認められる場合は、ネットワークを切断することができる。

5　運用管理者は、各種セキュリティに関する事案の詳細な調査を行うとともに、再発防止計画を策定しなければならない。

（法令遵守）

第３８条　利用者は、情報システムの運用については、次の各号に掲げる法令を遵守し、これに従わなければならない。

(1)　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)

(2)　著作権法(昭和45年法律第48号)

(3)　個人情報の保護に関する条例（平成8年兵庫県条例第24号）

(4)　その他情報セキュリティ対策に関する法令

附　則

この指針は、平成１５年３月４日から適用する。

附　則

この指針は、平成１５年４月１日から適用する。

附　則

この指針は、平成１６年４月１日から適用する。

附　則

この指針は、平成１７年４月１日から適用する。

附　則

この指針は、平成１８年４月１日から適用する。

附　則

この指針は、平成２０年４月１日から適用する。

附　則

この指針は、平成２３年４月１日から適用する。

附　則

この指針は、平成２５年４月１日から適用する。

附　則

この指針は、平成２６年４月１日から適用する。

附　則

この指針は、令和２年４月１日から適用する。