宮崎県立学校情報セキュリティポリシー

宮崎県立学校情報セキュリティ基本方針

宮崎県立学校情報セキュリティ対策基準

平成２４年１２月１２日策定

宮崎県教育庁学校情報セキュリティ対策会議決定

－目　次－

宮崎県立学校情報セキュリティ基本方針

平成２４年１２月１２日
宮 崎 県 教 育 委 員 会

１　目的

本基本方針は、宮崎県立学校（以下「県立学校」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、県教育委員会及び県立学校が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２　定義

(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、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
コンピュータ、ネットワーク及び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まれる。

(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) 機密性
情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(6) 完全性
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をいう。

(7) 可用性
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をいう。

(8) 情報セキュリティポリシー

本基本方針及び宮崎県立学校情報セキュリティ対策基準をいう。

(9) 学校情報セキュリティ実施手順

情報セキュリティ対策基準で規定した事項をそれぞれの情報システムにおいて具体的な実施手順、手続きに展開し、個別の実施事項を定めたものをいう。

3　適用範囲

(1) 県立学校の範囲

本基本方針が適用される学校は、教育関係の公の施設に関する条例別表第１に掲げる学校とする。ただし、知事部局が管理運用する情報システムを利用する部署については、対象外とする。

(2) 情報資産の範囲

対象とする情報資産は、県立学校が保有する情報資産とする。

ただし、知事部局が管理運用する情報システムの利用にかかる情報資産については、対象外とする。

4　教職員等の遵守事項

教職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び学校情報セキュリティ実施手順を遵守しなければならない。

5　情報セキュリティ管理体制

県立学校の情報資産について、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。

6　情報資産の分類

県立学校の保有する情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

7　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上で、情報資産を脅かす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、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2) 情報資産の無断持ち出しや紛失、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

(3) 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

(4) 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

(5) 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　情報セキュリティ対策

上記７で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずる。

(1) 物理的セキュリティ対策
サーバ等の管理、入退室管理、通信回線の管理等について、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教職員等の責務の明確化、研修の実施及び外部委託の適正な管理など、人的な対策を講ずる。

(3) 技術的セキュリティ対策
コンピュータ等の管理、アクセス制御、コンピュータウイルス対策、不正アクセス対策等の技術的対策を講ずる。

(4) 運用におけるセキュリティ対策
ネットワーク等の監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保など、運用面の対策を講ずる。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。

９　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

10　評価及び見直しの実施

情報セキュリティ監査及び自己点検の結果により、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。

11　学校情報セキュリティ対策基準の策定

上記８、９、１０に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める学校情報セキュリティ対策基準を策定する。

12　学校情報セキュリティ実施手順の策定

学校情報セキュリティ対策基準に基づき、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定めた学校情報セキュリティ実施手順を策定するものとする。なお、学校情報セキュリティ実施手順のうち、公にすることにより県立学校の運営に重大な支障を及ぼすおそれがあるものについては非公開とする。

13 児童生徒への対応

県立学校長をはじめとして県立学校が保有する情報資産を取り扱う全ての教職員等は、授業又は教育目的で情報資産の使用を児童生徒に認める場合は、別に定める児童生徒向けの学校情報セキュリティ実施手順等に従って、遵守すべき事項を児童生徒に明示しなければならない。

附　則

この基本方針は、平成２４年１２月１２日から施行する。

宮崎県立学校情報セキュリティ対策基準

平成２４年１２月１２日
宮 崎 県 教 育 委 員 会

１　目的

宮崎県立学校情報セキュリティ対策基準（以下「対策基準」という。）は、宮崎県立学校情報セキュリティ基本方針（以下「基本方針」という。）に基づき、具体的な情報セキュリティ対策を講ずるに当たって遵守すべき行為及び判断等について統一的な基準を定め、情報資産等を様々な脅威から防御することを目的とする。

なお、この対策基準の使用する用語の定義は、基本方針に準じるものとする。

２　組織・体制

宮崎県立学校の情報セキュリティ管理については、以下の組織・体制とする。

(1) 学校情報セキュリティ統括責任者

ア　学校情報セキュリティ統括責任者（以下「統括責任者」という。）は、県立学校におけるネットワーク、情報システム及び情報資産の情報セキュリティ対策を統括して管理する。

イ　統括責任者は、県教育庁教育次長（総括）をもって充てる。

(2) 学校情報セキュリティ副統括責任者

ア　学校情報セキュリティ副統括責任者（以下「副統括責任者」という。）は、統括責任者を補佐するとともに、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、その職務を代理する。

イ　副統括責任者は、県教育庁教育次長（政策）及び県教育庁教育次長（振興）をもって充てる。

(3) 学校情報セキュリティ幹事

ア　学校情報セキュリティ幹事（以下「幹事」という。）は、情報セキュリティポリシーに対する重大な違反に関する調査及びその再発防止策を立案する権限及び責任を有する。

イ　幹事は、県教育庁学校政策課長及び特別支援教育室長をもって充てる。

(4) 学校情報セキュリティ責任者

ア　学校情報セキュリティ責任者は、基本方針の適用範囲で定める県立学校（以下「学校」という。）における情報セキュリティ対策を統括して管理する。

イ　学校情報セキュリティ責任者は、校長をもって充てる。

(5) 学校情報セキュリティ管理者

ア　学校情報セキュリティ管理者は、県立学校における情報セキュリティ対策を管理する。

イ　学校情報セキュリティ管理者は、副校長・教頭・事務長、又は主幹教諭をもって充てる。

ウ　学校情報セキュリティ管理者は、下記(6)の学校情報ネットワークシステム管理者を兼ねることができる。

(6) 学校情報ネットワークシステム管理者

ア　学校情報ネットワークシステム管理者は、県立学校のネットワークシステムにおける情報セキュリティ対策を管理する。

イ　学校情報ネットワークシステム管理者は、副校長・教頭・事務長、又は主幹教諭をもって充てる。

(7) 学校情報セキュリティ担当者

ア　学校情報セキュリティ担当者は、学校情報セキュリティ責任者の下、学校情報セキュリティ管理者を補佐し、所属する学校における情報セキュリティの管理を行う。

イ　学校情報セキュリティ担当者は、学校セキュリティ責任者が県立学校の教育の情報化を担当する教職員から選任する。

(8) 学校情報ネットワークシステム担当者

ア　学校情報ネットワークシステム担当者は、学校情報セキュリティ責任者の下、学校情報ネットワークシステム管理者を補佐し、所属する県立学校における情報資産の維持、管理を行う。

イ　学校情報ネットワークシステム担当者は、学校セキュリティ責任者が県立学校の教育の情報化を担当する教職員から選任する。

(9) 教職員等

学校の教職員、非常勤職員及び臨時的任用職員をいう。

(10) 宮崎県教育庁学校情報セキュリティ対策会議

宮崎県教育庁学校情報セキュリティ対策会議は、県立学校における情報セキュリティ対策を統一的、体系的に推進するため、情報セキュリティに関する重要事案を審議、決定する。

(11) 学校情報セキュリティ委員会

各県立学校における情報セキュリティを維持し、各学校が保有する情報資産を情報セキュリティポリシー及び学校情報セキュリティ実施手順（以下「実施手順」という。）に従ってマネジメントする。

また、各学校における緊急事態に対応する組織とする。

3　情報資産の分類及び管理

(1) 情報資産の分類

学校情報セキュリティ管理者、学校情報ネットワークシステム管理者（以下「各管理者」という。）は、各々が管理責任を有する情報資産について、各情報資産の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

重要性分類
Ⅰ　個人情報
Ⅱ　公開することを予定していない情報及び学校運営等に重要な影響を及ぼす情報
Ⅲ　上記以外の情報

(2) 情報資産の管理責任等

ア　管理責任

(ｱ)　学校で作成又は利用する情報資産は、当該校の学校情報セキュリティ管理者が管理責任を有する。

(ｲ)　ネットワークシステムの開発・運用・保守に係る情報資産は、当該ネットワークの学校情報ネットワークシステム管理者が管理責任を有する。

(ｳ)　情報システムの開発・運用・保守に係る情報資産は、当該情報システムの学校情報ネットワークシステム管理者が管理責任を有する。

イ　利用者の責任

情報資産を利用する者は、情報資産の分類に従い利用する責任を有する。

ウ　情報資産の重要性の効力

情報資産が複製または伝送された場合には、当該複製等も原本と同様の分類に基づき管理しなければならない。

(3) 情報資産の管理方法

情報資産の管理については、以下の方法により行う。

なお、重要性分類Ⅰの情報資産については、情報セキュリティポリシーで定めるもののほか、宮崎県個人情報保護条例（平成十四年宮崎県条例第四十一号）の定めによるものとする。

ア　情報資産の管理

(ｱ)　各管理者は、各々が管理責任を有する情報資産についてアクセス権限を定めなければならない。

(ｲ)　重要性分類Ⅰ・Ⅱの情報資産の外部への持出し及び送付は禁止する。ただし、教職員等は、業務上必要な場合に限り、当該情報資産の管理者の許可を得た上で外部への持出し等ができる。この場合において、外部への持出し等に当たっては、紛失及び盗難に注意しなければならない。

イ　記録媒体の管理

各管理者は、各々が管理責任を有する記録媒体の管理について次により行わなければならない。

(ｱ)　最終的に確定した情報を記録した記録媒体は、書き込み禁止措置を行った上で保管すること。

(ｲ)　重要性分類Ⅰ・Ⅱの情報を記録した記録媒体は、保管場所を定めて保管すること。

なお、重要性分類Ⅰの情報を記録した記録媒体は、施錠可能な場所に保管しなければならない。

(ｳ)　データバックアップのため記録媒体を外部施設等へ搬送する業務を外部委託事業者に発注する場合は、搬送時における盗難や不正コピー等の防止対策を厳重に行う旨を契約書に明記しなければならない。

(ｴ)　各管理者は、情報を USB メモリ、外付けハードディスク、FD、MO、CD、DAT 及び MT 等の記録媒体（以下「記録媒体」という。）に保存する場合は、第三者が重要性の識別を容易に認識できないよう留意しつつ、記録媒体に情報資産の分類が分かるよう表示をする等適切な管理を行わなければならない。

ウ　情報の送信

電子メール等により重要性分類Ⅰ・Ⅱの情報を送信する場合は、学校情報セキュリティ管理者の許可を得た上で行うものとし、必要に応じて暗号化又はパスワードを設定しなければならない。

エ　情報資産の提供・公表

重要性分類Ⅰ・Ⅱの情報資産を外部に提供又は公表する場合は、学校情報セキュリティ管理者の許可を得た上で行うものとし、必要に応じて暗号化又はパスワードを設定しなければならない。

オ　記録媒体等の取扱い

各管理者は、記録媒体等の取扱いについて次により適正に取り扱わなければならない。

(ｱ)　記録媒体（機器に内蔵されたハードディスク等を含む）が不要となった場合は、情報を消去するソフトウェア等の利用又は物理的な破壊等の方法を用いて、全ての情報が復元できない状態にした上で廃棄すること。

(ｲ)　ハードディスクを内蔵する機器を外部の業者に修理させる場合は、業者に対し秘密を守ることを契約に定めた上で行うこと。また、情報が外部に流出することを防止するため、事前に可能な限りハードディスクに記録された情報を消去すること。

4　物理的セキュリティ対策

(1) サーバ等

学校情報ネットワークシステム管理者は、サーバ等のセキュリティ対策について次により行わなければならない。

ア　機器の取り付け等

(ｱ)　機器の取り付けを行う場合は、火災、水害、落雷、埃、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適切に固定すること。

(ｲ)　次のサーバは、ハードディスクの二重化を行うなどシステムの運用が停止しないようにすること。

a　重要性分類Ⅰの情報を格納しているサーバ

b　外部に公開しているサーバ

c　ネットワークを運用するためのサーバ

(ｳ)　操作を認められた職員や外部委託業者以外の者が容易に操作できないように、利用者の ID、パスワード設定等の措置を施すこと。

イ　電源

サーバ等の機器の電源については、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無停電電源装置を可能な限り備えるとともに、落雷による障害を受けることがないよう避雷対策に努めること。

ウ　配線

(ｱ)　配線は、損傷等を受けることがないように可能な限り必要な措置を施すこと。

(ｲ)　主要な箇所の配線については、損傷等についての定期的な点検を実施するよう努めること。

エ　外部に設置する装置

外部に設置している装置について、定期的に当該装置の情報セキュリティの水準について確認すること。

(2) 入退室管理等

ア　学校情報ネットワークシステム管理者は、ネットワークの基幹機器（サーバ、ファイアーウォール､ルータ等のネットワークを構成する主要な機器)が設置されている部屋の入退室について、IC カード等の利用や入退室管理簿の記載等により入退室者の管理を行わなければならない。

イ　学校情報セキュリティ管理者は、ネットワーク用の端末など教職員等が校務や教育に用いるパーソナルコンピュータ（以下「校務用・教育用パソコン」という。）等の情報機器が設置されている部屋の入退室について、適切な管理を行わなければならない。

(3) 通信回線及び通信回線装置の管理

ア　学校情報ネットワークシステム管理者は、校内の通信回線及び通信回線装置を適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

イ　学校情報ネットワークシステム管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

ウ　学校情報ネットワークシステム管理者は、重要性分類Ⅰ・Ⅱの情報資産を取り扱う情報システムは、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行うなど、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

(4) 盗難防止対策

ア　教職員等は、帰校の際、職員室等に施錠しなければならない。

イ　各管理者は、各々が管理する情報資産の盗難防止に努めなければならない。

５　人的セキュリティ対策

(1) 教職員等の責務

ア　教職員等は、情報セキュリティポリシー及び学校情報セキュリティ実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに学校情報セキュリティ管理者に相談し、指示を仰がなければならない。

イ　教職員等は、情報セキュリティポリシーに関する研修に参加し、情報セキュリティポリシーを理解するとともに、自己の情報セキュリティ対策の実施状況等について自主点検を行い、情報セキュリティ上の問題が生じないようにしなければならない。

ウ　教職員等は、ネットワーク、情報システム及び情報資産を業務外の目的で利用してはならない。

エ　教職員等は、ID 及びパスワード等に関し、次の事項を遵守しなければならない。

(ｱ)　ID の取り扱い

a　自己で利用している ID を他人に利用させないこと。

b　共用 ID を利用している場合は、共用 ID の利用者以外に利用させないこと。

c　共用 ID の利用者が変更となった場合には、パスワードを変更しなければならない。

(ｲ)　パスワードの取り扱い

a　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こと。ただし、機器の修理等必要がある場合に照会に応じた場合は、速やかにパスワードを変更すること。

b　パスワードのメモを端末や机など第三者から見えるような場所に貼らないこと。また、端末にパスワードを記憶させないこと。

c　パスワードの長さは十分な長さをとり、文字列は想像しにくいものとすること。

d　パスワードは定期的に変更すること。

e　パスワードを第三者に不正に取得された恐れがある場合又は流出した恐れがある場合は、パスワードを速やかに変更するとともに、学校情報ネットワークシステム管理者に速やかに報告すること。

f　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

(ｳ)　教職員等は、IC カードの取り扱いに関し、次の事項を遵守しなければならない。

a　認証に用いる IC カード等は、第三者から見えない場所等で適切に保管・管理すること。

b　教職員等は、IC カード等を紛失した場合には、速やかに学校情報セキュリティ責任者及び学校情報ネットワークシステム管理者に報告すること。

c　学校情報ネットワークシステム管理者は、IC カード等の紛失等が判明し次第、当該 IC カード等を使用したアクセス等を速やかに停止すること。

d　学校情報ネットワークシステム管理者は、IC カード等を切り替える場合、切り替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄すること。

オ　教職員等は、パソコン等の端末の利用について、次の事項を遵守しなければならない。

(ｱ)　校務用・教育用パソコンの利用においては、宮崎県一般業務用パソコン管理要領に準じて

適正に取り扱わなければならない。

(ｲ) 個別の情報システムで導入している端末の利用においては、上記(ｱ)の要領に準じて各情報システム管理者が定める実施手順に従い適正に取り扱わなければならない。

カ　教職員等は、学校情報ネットワークシステム管理者が指定した端末以外の端末をネットワーク及び情報システムに接続してはならない。

キ　教職員等は、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持ち出してはならない。また、業務上知り得た情報を秘匿しなければならない。

ク　教職員等は、情報システム上の欠陥及び誤作動を発見した場合には、速やかに学校情報ネットワークシステム管理者に報告し、指示に従い必要な措置を講じなければならない。

ケ　教職員等は、自己が利用する情報資産に対する侵害又は侵害の恐れがある場合には、所属する課等の学校情報セキュリティ管理者に速やかに報告し、当該学校情報セキュリティ管理者の指示に従い必要な措置を講じなければならない。

コ　教職員等は、電子メールの利用において、次の事項を遵守しなければならない。

(ｱ) 宮崎県教育情報ネットワーク「教育ネットひむか」の電子メール利用においては、教育ネットワークひむかの運用管理基準に従い適切に行わなければならない。

(ｲ) 個別のネットワークや情報システムの電子メール利用においては、上記(ｱ)の基準に準じてそれぞれの管理者が定める実施手順に従い適切に行わなければならない。

(2) 教職員等への研修

ア　統括責任者は、全ての教職員等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　統括責任者は、新規採用の教職員等を対象とする情報セキュリティに関する研修を行う。

ウ　学校情報セキュリティ責任者は、所管する学校情報ネットワークシステムを利用する教職員等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に関する研修を行う。

エ　学校情報セキュリティ責任者は、教職員等を業務上必要な情報セキュリティに関する研修に参加させなければならない。

(3) 非常勤職員及び臨時的任用職員への対応

ア　学校情報セキュリティ管理者は、非常勤及び臨時的任用職員（以下「非常勤職員等」という。）に対し、採用時に情報セキュリティポリシー等のうち、非常勤職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

イ　学校情報セキュリティ管理者は、非常勤職員等にパソコン等の端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(4) 外部委託に関する管理

ア　学校情報ネットワークシステム管理者は、所管するネットワークの開発・運用・保守を外部委託事業者に発注する場合には、守秘義務等情報セキュリティの維持に必要な項目を明記した契約

を締結し、必要な指導を行わなければならない。

イ　学校情報ネットワークシステム管理者は、情報システムの開発・運用・保守を外部委託事業者に発注する場合には、守秘義務等情報セキュリティの維持に必要な項目を明記した契約を締結し、必要な指導を行わなければならない。

ウ　学校情報セキュリティ管理者は、所管する情報資産のうち重要性分類Ⅰ・Ⅱに該当する情報資産を取り扱う業務を外部委託事業者に発注する場合には、守秘義務等情報セキュリティの維持に必要な項目を明記した契約を締結し、必要な指導を行わなければならない。

６　技術的セキュリティ対策

(1) ネットワーク及び情報システムの管理

学校情報ネットワークシステム管理者は、所管するネットワーク及びコンピュータの管理について、次により行わなければならない。

ア　アクセス記録の取得等

(ｱ)　ネットワーク及び重要性分類Ⅰの情報を扱う情報システムについて、アクセス記録を取得し、盗難、改ざん、消去等を防止する措置を施したうえで一定期間保存すること。

(ｲ)　取得したアクセス記録について、可能な限り定期的に分析、監視すること。

イ　管理記録及び作業の確認

システム変更等の作業を行う場合は、可能な限り複数名で行うともに、行った作業の内容を記録し適切に管理すること。

ウ　障害記録の作成等

教職員等から報告のあったネットワーク及び情報システムの障害に対する処理等を記録し、常に活用できるよう保存すること。

エ　情報システム仕様書等の管理

ネットワーク構成図、情報システム仕様書等に関し、記録媒体の形態に関わりなく適切な保管をすること。

オ　バックアップ

ファイルサーバ等に記録された情報について、定期的にバックアップ用の複製を取得すること。

カ　外部の者が利用できるシステム

外部に公開するサーバは、必要に応じ他の情報システムと物理的に分ける等、情報セキュリティ対策については特に強固な対策をとること。

キ　情報システムの入出力情報

(ｱ)　情報システムに入力される情報は、範囲や妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むなどの対策を施すこと。

(ｲ)　情報システムから出力される情報は、保存された情報の処理が正しく反映され、出力されることを確保すること。

ク　メール等の設定

メールサーバに対し、ネットワークを介した不正な中継が行われないよう設定を施すこと。

ケ　プロトコル

教職員等が利用できるプロトコルを必要最低限の範囲で定め、それ以外については通信制限を行うこと。

コ　セキュリティ情報の収集

情報セキュリティに関し必要な情報の収集に努めること。

(2) アクセス制御

ア　学校情報ネットワークシステム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

イ　利用者 ID の取扱

(ｱ) 学校情報ネットワークシステム管理者は、利用者の登録、変更、抹消、登録情報の管理方法を定めるとともに、利用者の ID 及びパスワードを厳重に管理しなければならない。

(ｲ) 学校情報ネットワークシステム管理者は、利用されていない ID が放置されないよう年 1 回以上点検し、利用されていない ID は削除又は利用停止の措置を講じなければならない。

ウ　管理者権限の取扱

(ｱ) 学校情報ネットワークシステム管理者は、管理者権限の付与を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう厳重に管理しなければならない。

(ｲ) 外部委託事業者が管理者権限を利用する場合にも、ID 及びパスワードの利用は、すべて学校情報ネットワークシステム管理者が管理しなければならない。

(ｳ) 学校情報ネットワークシステム管理者は、特権を付与した ID のパスワードについて、定期的な変更や入力回数制限を設けるなど、一般の ID よりもセキュリティを強化しなければならない。

エ　外部ネットワークとの接続

学校情報ネットワークシステム管理者は、ネットワーク及び情報システムと外部ネットワークとの接続及び維持管理について、次により行わなければならない。

(ｱ) 外部へのネットワーク接続は、必要最低限のものに限定し、できる限り接続ポイントを減らすこと。

(ｲ) 外部ネットワークからの不正アクセスを防止するため、ネットワークと外部ネットワークの間にファイアーウォールを設置すること。

(ｳ) ネットワークと接続した外部ネットワークのセキュリティに問題があり、ネットワーク、情報システム及び情報資産に影響が生じると判断した場合には、速やかに当該外部ネットワークを物理的に遮断すること。

オ　無線 LAN の使用

学校情報ネットワークシステム管理者は、無線 LAN を利用する場合、解読が困難な暗号化機能及び認証機能を有する機器を使用しなければならない。

(3) コンピュータウイルス対策

ア　学校情報ネットワークシステム管理者は、ネットワークにおけるコンピュータウイルス対策として次の事項を実施しなければならない。

(ｱ) 外部ネットワークとの接続点において、受信したファイルのチェックを行い、ネットワークへのウイルス侵入を防止すること。

(ｲ) 外部ネットワークとの接続点において、送信するファイルのチェックを行い、外部へのウイルス拡散を防止すること。

(ｳ) ネットワークの共有ドライブに置かれたファイルに対して常時ウイルスチェックを行い、ネットワーク内でのウイルス拡散を防止すること。

(ｴ) ウイ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。

(ｵ) 不正プログラム対策のソフトウェアは、常に最新の状態に保つよう努めること。

(ｶ) コンピュータウイルス等の不正プログラム情報を必要に応じ職員等に対して周知し注意喚起すること。

イ　学校情報ネットワークシステム管理者は、情報システムにおけるコンピュータウイルス対策として次の事項を実施しなければならない。

(ｱ) サーバ及び端末において、ウイルスチェックを行うこと。

(ｲ) ウイ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。

(ｳ) 不正プログラム対策のソフトウェアは、常に最新の状態に保つよう努めること。

(ｴ) インターネットに接続していない情報システムにおいては、外部記録媒体からのウイルス感染を防止するため、情報システムに接続する前に当該媒体のウイルスチェックを行うこと。

ウ　教職員等は、パソコン等におけるコンピュータウイルス対策として次の事項を実施しなければならない。

(ｱ) 校務用・教育用パソコンの利用時においては、宮崎県一般業務用パソコン管理要領に準ずること。

(ｲ) 個別の情報システムで導入している端末の利用時においては、(ｱ)の要領に準じて学校情報ネットワークシステム管理者が定める実施手順に従うこと。

(ｳ) 学校情報ネットワークシステム管理者等の提供する不正プログラム情報を適宜確認しなければならない。

(4) 不正アクセス対策

ア　学校情報ネットワークシステム管理者は、不正アクセス対策として次の事項を実施しなければならない。

(ｱ) 使用されていない、又は使用される予定のないポートを閉じること。

(ｲ) 情報セキュリティに関する情報を収集し、必要に応じてネットワーク及び情報システムのソフトウェアにパッチをあてる等、セキュリティ対策上必要な措置を講ずること。

(ｳ) 情報システムの設定に係る重要なファイルについて、必要に応じて当該ファイルの改ざんの有無を検査すること。

(ｴ) 不正アクセスによるウェブページの改ざん等がないか、定期的に確認を行うこと。

イ　不正アクセス等による攻撃を受けることが明確な場合には、学校情報ネットワークシステム管理者はそれぞれ別個に定める緊急時対応マニュアルに基づき必要な措置を講じなければならない。

ウ　教職員等による不正アクセスがあった場合、学校情報ネットワークシステム管理者は当該教職

員等が所属する学校情報セキュリティ管理者に通報し、適切な処置を求めなければならない。

エ　学校情報ネットワークシステム管理者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、関係機関との緊密な連携に努めなければならない。

(5) システムの導入、保守等

ア　情報システムの調達

(ｱ)　学校情報ネットワークシステム管理者は、情報システム導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

(ｲ)　学校情報ネットワークシステム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題がないことを確認しなければならない。

イ　情報システムの導入

(ｱ)　開発環境と運用環境の分離及び移行手順の明確化

学校情報ネットワークシステム管理者は、システムの開発、保守及びテスト環境とシステム運用環境をできる限り分離しなければならない。

(ｲ)　テスト

学校情報ネットワークシステム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

ウ　システム導入・保守に関連する資料等の保管

学校情報ネットワークシステム管理者は、システム導入・保守に関連する資料及び文書を適切な方法で保管しなければならない。

エ　情報システムの変更管理

学校情報ネットワークシステム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成し適切な期間保管しなければならない。

オ　システム更新又は統合時の検証等

学校情報ネットワークシステム管理者は、システムを更新又は統合する場合は、システムの長時間の停止や誤動作等による業務への影響が生じないよう、事前に慎重な検証等を行わなければならない。

7　運用におけるセキュリティ対策

(1) ネットワーク等の監視

ア　学校情報ネットワークシステム管理者は、所管するネットワーク等のセキュリティに関する事案を検知するため、稼働状況の監視を行わなければならない。

イ　学校情報ネットワークシステム管理者は、重要なアクセスログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる機能の導入に努めるものとする。

(2) 対策基準の遵守状況の確認

ア　遵守状況の確認及び対処

学校情報ネットワークシステム管理者は、サーバ等のシステム設定が対策基準を遵守しているかどうかについて、また、情報セキュリティ上の問題が発生していないかについて確認を行い、問題が発生していた場合には速やかに発生した問題に適切に対処しなければならない。

イ　端末及び記録媒体等の利用状況の調査

学校情報セキュリティ責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、教職員等が使用しているパソコン等の端末、記録媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

ウ　教職員等の報告義務

(ｱ)　教職員等は、学校情報セキュリティポリシーに対する違反行為を発見した場合、直ちに学校情報セキュリティ管理者に報告を行わなければならない。

(ｲ)　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると学校情報セキュリティ管理者が判断した場合は、下記(4)で整備する緊急時マニュアルに従って適切に対処しなければならない。

(3) 基本方針及び対策基準の備え付け

学校情報セキュリティ管理者は、教職員等が基本方針、対策基準を常に参照できるよう所定の場所に備え付けておかなければならない。

(4) 実施手順及び緊急時対応マニュアルの整備

ア　学校情報ネットワークシステム管理者は、所管するネットワーク及び情報システムに係る実施手順を作成・運用しなければならない。また、所管するネットワーク及び情報システムに関して、緊急事態発生時の連絡先や復旧方法等について明記した緊急時対応マニュアルを作成しなければならない。

イ　緊急時対応マニュアルには、以下の内容を定めなければならない。

(ｱ)　緊急連絡先

(ｲ)　発生した事案に係る報告すべき事項

(ｳ)　発生した事案への対応措置

ウ　実施手順及び緊急時対応マニュアルは、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

エ　学校情報ネットワークシステム管理者は、実施手順及び緊急時対応マニュアルを所定の場所に備え付けるとととともに、実施手順及び緊急時対応マニュアルへのアクセス権を制限しなければならない。

(5) 緊急事態発生時の対応

各管理者は、各県立学校が所管するネットワーク、情報システム及び情報資産への侵害が発生し

た場合、連絡、証拠保全、被害拡大の防止、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じるために、次により対処するものとする。

ア　緊急連絡

学校情報ネットワークシステム管理者は、緊急時対応マニュアルに記載された連絡先、連絡担当者及び連絡手段に基づき、速やかに連絡を行う。

イ　校内の連絡体制

(ｱ)　各管理者は、所属する学校の学校情報セキュリティ責任者へ速やかに報告を行うとともに、必要な措置を講ずる。

(ｲ)　学校情報ネットワークシステム管理者は、所管する情報システム上の欠陥及び誤作動がネットワークに起因するものであるとき又はネットワークに影響を及ぼすと判断したときは、速やかに必要な措置を講ずる。

(ｳ)　学校情報セキュリティ責任者は、幹事へ報告を行うとともに、幹事は、発生した緊急事態のうち重要性分類Ⅰ・Ⅱの情報に係る事案を統括責任者まで報告する。

ウ　報告の内容

報告の内容については、被害が発生した状況、原因並びに被害及び影響範囲等とする。

エ　事案への対処

(ｱ)　学校情報ネットワークシステム管理者は、次の事案の発生に対し復旧に必要な措置を講じた上で、情報資産の防護のためにネットワークの切断がやむを得ないと判断した場合は、ネットワークを切断する措置を講じるものとする。

a　異常なアクセスが継続しているとき、または不正アクセスが判明したとき。

b　ネットワーク及び情報システムの運用に著しい支障をきたす攻撃が継続しているとき。

c　コンピュータウイルス等不正プログラムがネットワーク経由で拡がっているとき。

d　その他情報資産に係る重大な被害が想定されるとき。

(ｲ)　学校情報ネットワークシステム管理者は、次の事案の発生に対し復旧に必要な措置を講じた上で、情報資産の防護のために情報システムの停止がやむを得ないと判断した場合は、情報システムを停止するものとする。

a　コンピュータウイルス等不正プログラムが情報資産に深刻な被害を及ぼしているとき。

b　災害等により電源を供給することが危険又は困難なとき。

c　その他の情報資産に係る重大な被害が想定されるとき。

(ｳ)　学校情報セキュリティ管理者は、発生した事案に対して学校情報ネットワークシステム管理者の指示に従い、速やかに対処しなければならない。

オ　復旧等

学校情報ネットワークシステム管理者は、アクセス記録を保存し、経過や対処等を記録した上で再発防止の措置を講じ、その後ネットワーク及び情報システムを復旧させるものとする。

カ　再発防止の措置

学校情報ネットワークシステム管理者は、緊急事態が発生した原因を調査し、再発防止策を検討するとともに、必要に応じて実施手順の見直しを行うものとする。

(6) 外部委託

ア　学校情報ネットワークシステム管理者は、情報システム等の導入や保守等において外部委託を行う場合、外部委託事業者からの情報漏えい等を防止するため、契約でセキュリティの遵守事項を定めるとともに、必要に応じてセキュリティ対策の実施状況の確認を行わなければならない。

イ　契約に織り込むセキュリティ要件等については別途定める。

(7) 例外措置

ア　各管理者は、教職員等以外が利用する情報システムなど、情報セキュリティ関係規定を遵守することが困難な場合は、幹事に協議の上、別途処理基準等を定めることができる。

イ　各管理者は、校務等の遂行に緊急を要し、例外措置を実施しなければ校務等の遂行に著しい支障を及ぼすことが予想される場合には、例外措置の実施後速やかに統括責任者に報告しなければならない。

8　法令遵守

(1) 教職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

ア　地方公務員法（昭和二十五年法律第二百六十一号）

イ　不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）

ウ　著作権法（昭和四十五年法律第四十八号）

エ　宮崎県個人情報保護条例（平成十四年宮崎県条例第四十一号）

(2) 情報セキュリティに関する法令等に違反した教職員等及びその監督責任者は、その重大性及び事案の状況に応じて地方公務員法第 29 条の規定により、懲戒処分の対象となり得る。

9　評価・見直し

(1) 監査

ア　幹事は、情報セキュリティ対策の実施状況について、定期的に監査を実施するものとする。

イ　監査の実施方法等については、別に定める。

(2) 自己点検

ア　学校情報セキュリティ管理者は、所属校における情報セキュリティ対策の実施状況について定期的に自己点検を行わなければならない。

イ　学校情報ネットワークシステム管理者は、学校が所管するネットワーク又は情報システムにおける情報セキュリティ対策の実施状況について定期的に自己点検を行わなければならない。

(3) 対策基準の更新

対策基準については、新たに必要な対策が発生した場合又は監査の結果及び自己点検の結果を踏まえ、必要な部分の見直しを行い更新するものとする。

附　則

この基準は、平成２４年１２月１２日から施行する。