学校法人菅原学園
情報セキュリティ対策基準

学校法人　菅原学園

令和７年　４月１日（制定）

令和７年　４月１日（発行）

（第１版）

承　　認	作　　成
令和７年３月２７日	令和７年３月２７日

目　　次

学校法人菅原学園情報セキュリティ対策基準

Ｉ．目的

この基準は、『学校法人菅原学園総合システムセキュリティ基本規程』（基本－Ｉ－２６）第６条に定める、セキュリティ対策について、その目標達成のため次の基本項目毎にその対策基準を定めるものである。

１　ネットワーク構築基準

２　サーバ等におけるセキュリティ対策基準

３　ＰＣなどにおけるセキュリティ対策基準

４　媒体の取り扱いに関する基準

５　法人内ネットワーク利用基準

６　ユーザ認証に関する基準

７　マルウェア対策基準

８　電子メールサービス利用基準

９　Ｗｅｂサービス利用基準

10　ＳＮＳ利用に関する基準

11　プライバシーに関する基準

12　システム維持に関する基準

13　セキュリティ監視に関する基準

14　セキュリティインシデント報告、対応基準

15　セキュリティ教育に関する基準

16　第三者契約に関する基準

Ⅱ．対策基準

１　ネットワーク構築基準

本基準は、学校法人菅原学園（以下「法人」という。）のネットワーク構築をする際に必要なセキュリティに関して記述するもので、インターネット接続環境、法人内 LAN 環境、法人内 VPN 環境においてネットワーク機器及び各種サーバの構築の条件、運用・管理の実施方法の遵守事項を規定する。

１．１　全般規定

ネットワーク構築の全般規定を次に示す。

（１）ネットワーク環境は、次に示す三つの環境とする。

・インターネットと接続をするインターネット接続環境

グローバルアドレスを利用したネットワークとする。

・法人内に設置する LAN を利用した法人内 LAN 環境

プライベートアドレスを利用したネットワークであり、サーバゾーン、各フロアゾーン及び各部門の３つとする。

・専用線（VPN 接続を含む）を利用した法人内 VPN 環境

プライベートアドレスを利用したネットワークであり、本法人の設置する各学校間の接続を可能にする。

（２）ネットワーク構築のための機器は、次に示す機器とする。

・ネットワーク機器

ルータ、ハブ、スイッチングハブなど。

・サーバ類（NAS を含む）

ファイアウォールサーバ、インターネットサーバ、メールサーバなど。

（３）インターネット接続環境に接続する機器は、ルータ、スイッチングハブ、インターネットサーバとする。

（４）インターネット接続環境には、不正アクセスを防止および監視するための仕組みを設置し、不正アクセスを検出した場合には速やかにシステム管理担当部署に報告しなければならない。

（５）主要な機器には、ログ採取とネットワーク監視を実施しなければならない。

（６）パスワードの設定が可能な機器は、『６ ユーザ認証に関する基準』に準拠しなければならない。

（７）アクセス制御の設定が可能な機器には、特定の機器からの接続のみ可能な設定をしなければならない。

（８）各機器は、設置場所・接続機器状況・管理者を明確にしなければならない。

（９）主要なサーバ（インターネットサーバ・イントラネットサーバ）は、サーバ専用セグメントに接続しなければならない。

１．２　インターネット接続環境規定

インターネット接続環境の規定を次に示す。

（１）ネットワーク接続構成

・ルータによりインターネットプロバイダ接続とし、プロバイダ側のネットワークはグローバルアドレスを利用しなければならない。
・プロバイダと本法人の境界には、ファイアウォールサーバ（ルータを含む）を設置し、不正アクセス防止対策を実施しなければならない。
・インターネット接続環境に接続できる機器は、インターネットサーバとする。
・ファイアウォールサーバには DMZ を用意し、インターネットサーバを利用できるようにしなければならない。
・ファイアウォールサーバでは、グローバルアドレスとプライベートアドレスの変換を行うことが望ましい。
・外部とのメールの送受信は、最新のパターンデータでマルウェア感染チェックすると共にトロイの木馬などの不正中継対策を実施しなければならない。
・インターネットサーバには、システム管理担当部署が指示する OS 及び更新プログラムを適用し、常に最新のセキュリティ対策を実施しなければならない。

（２）利用できるサービス
・法人外ユーザ向けの WWW サービス（情報公開）
・法人内ユーザ向けの WWW サービス（情報収集）
・メールの送受信サービス
・ドメインネームサービス
・ファイル転送サービス

１．３　法人内 LAN 環境規定

法人内 LAN 環境の規定を次に示す。

（１）ネットワーク接続構成
・法人内 LAN では、IP 通信のみの利用を許可する。
・スイッチングハブとハブを使用し、構内のネットワークとする。
・ネットワークセグメント間は、通信サービス毎のアクセス制限を実施し不正アクセス防止対策を実施しなければならない。
・主要な場所に設置するネットワーク機器は、ネットワーク監視対象としなければならない。
・接続できる機器は、各種サーバ（NAS を含む）と PC（スマートデバイス等）とプリンタとする。
・使用するアドレスは、プライベートアドレスを利用しなければならない。

（２）利用できるサービス
・WWW サービス
・法人内業務システム
・ファイル共有サービス
・プリンタ共有サービス
・メールの送受信サービス
・クラウド型業務システム

（３）IP アドレスの管理

IP アドレスは各学校等のシステムセキュリティ管理担当者が管理し、IP アドレス台帳を更新しなければならない。

１．４　法人内 VPN 環境規定

法人内 VPN 環境の規定を次に示す。

（１）接続構成

・専用線（VPN 接続を含む）をルータに接続し、接続先は各学校校舎とする。
・ネットワークセグメント間は、通信サービス毎のアクセス制限を実施し不正アクセス防止対策を実施しなければならない。
・ネットワーク機器には、ネットワーク監視を実施しなければならない。
・ネットワークアドレスには、プライベートアドレスを利用しなければならない。

（２）利用できるサービス

・インターネット
・法人内各業務システム
・ファイル共有サービス
・メールの送受信サービス
・クラウド型業務システム

１．５　ネットワーク管理規定

ネットワーク内に設置するネットワーク機器は、次に示す手順で管理を行う。

（１）設置許可申請

ネットワーク機器を設置する場合、設置許可申請書（様式１）をシステム管理担当部署に提出しなければならない。

なお、申請にあたってはワークフローを利用すること。

（２）機器の設定

システムセキュリティ管理担当者は、設置予定のネットワーク機器に関して、システムセキュリティ責任者の指示するセキュリティ対策が施されるように、機器の設定を行わなければならない。

（３）設置

システムセキュリティ管理担当者は、設置許可申請書のとおりに設置しなければならない。

（４）切り離し

設置されたネットワーク機器で発見された問題点の程度によっては、システムセキュリティ責任者の判断により、問題点の処置が完了するまでネットワークから切り離なさなければならない。

２　サーバ等におけるセキュリティ対策基準

本基準は、各サーバの OS を含めたソフト、ハード及び運用を規定し、サーバに格納されている情報の保護を目的とする。

２．１　導入時の規定

（１）各学校等に設置するサーバは、システムセキュリティ管理担当者がサーバ管理者として以下の管理を行う。

・対象システムを安全な場所に設置する。

・サーバを設置する際に、サーバ設置申請書（様式２）を作成し、システムセキュリティ責任者の認可を受けなければならない。

なお、申請にあたってはワークフローを利用すること。

・サーバ設置申請書の申請時に、そのシステム構成を明確にしなければならない。

（２）本基準が適用される以前に設置された既存サーバについては、すみやかに本基準に適合するようにしなければならない。なお、本基準に適合しない場合には、システムセキュリティ責任者は情報の公開を強制的に停止させることができる。

２．２　環境設定の規定

サーバ管理者は、以下の内容の環境設定を行わなければならない。

（１）サーバで使用する OS 及び、ソフトウェア（マルウェア対策ソフトを含む）は、システムセキュリティ責任者が認めたものを使用しなければならない。

（２）サーバで使用されるソフトウェアは常に最新の OS、最新のアプリケーション及び最新の更新プログラムを適用し、不要なサービスの削除を行わなければならない。

（３）OS のアクセス制御、ファイルのアクセス制御、アプリケーション、サービスのアクセス制御に関して、厳密にアクセス権を設定しなければならない。

（４）ユーザ、Web アクセスなどに使用する匿名ユーザアカウントを含む全てのアカウントのアクセス権限に対して、適切なアクセス権限を設定しなければならない。

（５）サーバの目的、用途に応じた必要最低限のアプリケーション・サービス以外をインストールしてはならない。

（６）サーバには、推測困難なパスワードを設定しなければならない。特にサーバ管理者又はサーバ管理者に類する権限を持つアカウントのパスワードは、厳重に管理されなければならない。

２．３　運用時の規定

サーバ管理者は、以下の内容で運用を行わなければならない。

（１）サーバで使用されるソフトウェアは常に最新の OS、最新のアプリケーションを維持し、最

新の更新プログラムの適用、不要なサービスの削除を常に行わなければならない。

（２）マルウェア対策として常にマルウェア定義ファイル、マルウェア対策システムが最新のものとなるよう情報を収集し、更新があった場合には、直ちに反映させ、サーバのウイルスチェックを行わなければならない。

（３）サーバのパスワードを定期的に変更しなければならない。

（４）次の内容を検査すること。

・「サーバ設置申請書」と実際の設置機器との整合性

・不要なアクセス権が存在しない事

・不要サービスの起動が存在しない事

・不要なアカウントが存在しない事

・推測可能なパスワードが設定されていない事

（５）検査によりセキュリティの不備が発見された場合には、直ちに不備を是正し、不備の内容と対策状況をシステムセキュリティ責任者に報告する。

（６）セキュリティ侵害が発生した場合には、『13 セキュリティ監視に関する基準』に従って対応しなければならない。また、セキュリティ侵害の状況を、できるだけ速やかに、システムセキュリティ責任者に報告しなければならない。システムセキュリティ責任者は、前述の報告を受けた後、各行政機関への通報を含めて迅速に対応しなければならない。

（７）万が一、想定外のセキュリティ侵害が発生し、セキュリティ侵害時の対応手順のみでは状況の改善が見込めない場合には、即座にシステムセキュリティ責任者に報告しなければならない。

３　ＰＣなどにおけるセキュリティ対策基準

本基準は、PC 上の機密性・完全性を確保し、発生しうる各種問題を未然に防ぐことを目的とする。

３．１　PC の使用

（１）教職員が法人の業務を遂行するために使用できる PC は、法人が支給・貸与した PC と『PC 利用申請書』（様式３）によりシステム管理担当部署へ申請した PC のみとする。

なお、申請にあたってはワークフローを利用すること。

（２）教職員は、いかなる場合でも、法人システム環境に無断で PC を接続・利用してはならない。

（３）学生所有の PC 及びスマートデバイス等は、公開 Wi-Fi 環境のみに接続できる。

３．２　PC に導入するソフトウェア

（１）法人の業務を遂行するために使用する PC には、指定したソフトウェアを導入することとする。したがって、それ以外のソフトウェアを導入してはならない。

（2）（1）にて指定したソフトウェア以外で、業務上やむを得ず導入しなければならないソフトウェアは、システム管理担当部署に申請し、許可を得なければならない。

（3）導入したソフトウェアは、常に最新の状態で使用することとし、システム管理担当部署が提供するソフトウェア情報をもとに修正プログラムなどを導入しなければならない。

３．３　PC の他者への利用の制限

（1）席を離れる場合には、第三者が無断で PC を利用できないように、パスワード付きスクリーンセーバーなどによる防止策を講じなければならない。

（2）『６　ユーザ認証に関する基準』に従い、PC に対するパスワード管理を徹底しなければならない。

３．４　PC での情報の取り扱い

（1）PC で機密情報を長期期間利用する場合には、万一の漏洩に備え、パスワードの設定や暗号化などの対策を実施しなければならない。

（2）PC で一時的に機密情報を取り扱う場合には、取り扱い後には、不必要となった情報を削除し、いつまでも保持してはならない。

３．５　マルウェア対策の徹底

（1）PC を利用する上でマルウェア対策を徹底しなければならない。

（2）『７　マルウェア対策基準』に規定されている遵守事項を徹底しなければならない。

３．６　PC の移設

（1）PC を勝手に移設してはならない。

（2）PC の移設が必要な場合には、システム管理担当部署に申請し、許可を得なければならない。

３．７　ノート PC の利用上の注意事項

（1）法人外にノート PC を持ち出す場合には、『11 プライバシーに関する基準』で定められた個人データ管理責任者の許可を得なければならない。また、盗難・窃盗・情報の盗み見に注意し利用しなければならない。

３．８　PC の廃棄

（1）PC を廃棄する場合には、『４　媒体の取り扱いに関する基準』に従って廃棄しなければならない。

４　媒体の取り扱いに関する基準

本基準は、機密性の高い情報を保存する PC(以下 PC と呼ぶ)などの修理時、並びにハードディスク及び USB メモリ等の媒体廃棄時に関するルールを定め、機密性の高い情報の漏洩を未然に防ぐことを目的とする。

４．１　法人が貸与した PC（IT 製品）の修理

（１）機密性の高い情報が読み出し可能な状態で保管されていないことを確認した上でシステム管理担当部署を通して修理を依頼しなければならない。システム管理担当部署は、代替品を準備し、必要に応じて貸し出しを行う。その他の修理は、各学校等から直接修理を依頼するものとする。

（２）外部業者が法人内に立ち入って修理を行う場合には、システム管理担当部署又はシステムセキュリティ管理担当者の立会いの下に行わなければならない。

４．２　媒体の保管

（１）機密性の高い情報を媒体に保存する者は、権限のない者が保管された情報にアクセスできないよう、暗号化を行うか、媒体を鍵のかかる場所に保管し、鍵は容易に持ち出しが出来ない場所に保管しなければならない。

４．３　媒体の移動

（１）機密性の高い情報を保管した媒体を、『11 プライバシーに関する基準』で定められた個人データ管理責任者の許可なく法人外へ持ち出してはならない。

（２）特定の教職員にのみアクセス権限を限定している情報が保管された媒体を、各学校等間でやりとりしてはならない。

（３）開示範囲を法人内に限定している情報が保管された媒体を、郵送、宅配便またはメールなどで送付してはならない。各学校等間でのやりとりは、セキュリティが確保された手段で送付しなければならない。

４．４　媒体の再使用

（１）機密性の高い情報が保存されている媒体を再利用する前に、保存されていた情報を再生できない方法で消却しなければならない。

４．５　PC（IT 製品）と媒体の廃棄

（１）廃棄を行う者は、機密性の高い情報が保管されたハードディスクなどを取り外してから、指定された場所に廃棄しなければならない。取り外したハードディスクなどは、システム管理担当部署が指定する場所に持ち込まなければならない。

（２）機密性の高い情報が保管された媒体の廃棄を行う者は、システム管理担当部署が指定する場所に持ち込まなければならない。

（３）機密性の高い情報が保管されているかどうかが確認できない場合には、機密性の高い情報が保管されているものとして取り扱わなければならない。

（４）システム管理担当部署は、機密性の高い情報が保管されたハードディスクなどの媒体を、再生不能な状態に破壊して廃棄しなければならない。

５　法人内ネットワーク利用基準

本基準は、機密保持及び情報資産の保護、有効利用を目的に法人内ネットワークの利用管理を行う。

５．１　法人内ネットワーク及びインターネットの業務目的以外の利用禁止

（１）法人内ネットワーク及びインターネットの利用において、業務目的以外の使用を禁止する。

（２）システムセキュリティ責任者の許可無く、法人内ネットワーク上に、電子メールサーバや、Web サーバ、FTP サーバなどを構築してはならない。

（３）他人の利用者 ID を用いて、法人内ネットワーク及び、法人内のネットワーク、インターネット上のサイトへアクセスしてはならない。

（４）故意又は不注意を問わず、法人内ネットワーク及び法人外ネットワーク、インターネット上のサーバに対して、許可されたアクセス権限以上のアクセスを行ってはならない。

５．２　ネットワークを利用した機密情報の送受信

（１）法人の事業に関わる情報や、学生や教職員のプライバシーに関わる情報などの機密性の高い法人内の情報が法人外へ漏洩することを防ぐため、機密性の高い情報のアップロードや法人外への送信を禁止する。

（２）出所が不明なファイルや内容に確証の持てないファイルをダウンロードや実行してはならない。

（３）業務上やむを得ず機密情報を法人外へ送信又は法人外から受信する場合には、システムセキュリティ責任者の指示に従い、内容に応じてパスワードを付けるか暗号化するなどの処置を施さなければならない。パスワードや暗号解除のキーワードは必ず口頭で伝え、メモなど記録に残るものは使ってはならない。

５．３　インターネットで利用可能なサービス

（１）インターネットの利用において、電子メール、Web 閲覧及び認められた Web サービス以外を使用してはならない。

（２）Web サービスの利用については、『９　Web サービス利用基準』を遵守しなければならない。

（３）電子メールの利用については、『８ 電子メールサービス利用基準』を遵守しなければならない。

５．４ 法人内ネットワークで利用可能なサービス

（１）法人サーバゾーンにて管理されるシステムへのアクセスは、許可された利用者以外利用してはならない。

（２）機密情報について業務上やむを得ずネットワークを介して扱う場合には、システムセキュリティ責任者の指示に従い、内容に応じてパスワードを付けるか暗号化などの処置を施さなければならない。

（３）法人内ネットワークにおいて、ネットワークモニターなどの、ネットワーク上を流れるパケットを盗聴できる機器及びソフトウェアを使用してはならない。ただし、システムセキュリティ責任者が承認した調査及び監視目的のネットワークモニターなどの利用はできることとする。

（４）法人内ネットワークサーバへのアクセス用の ID、パスワード及び証明書は適切に管理しなければならない。特にパスワードの選択及び使用については、『６ ユーザ認証に関する基準』に基づいたものを利用しなければならない。

５．５ 法人内ネットワークへの接続時の注意事項

（１）ネットワーク利用者は、自宅や、他組織のネットワークに接続した PC について、ウイルス検査とセキュリティ検査を実施し、異常が発見されなかったことを各学校等のシステムセキュリティ管理担当者が確認した後でなければ、法人内ネットワークに接続してはならない。

（２）与えられた IP アドレス以外の IP アドレスを使用してはならない。

（３）法人内ネットワークに接続中のコンピュータを、システムセキュリティ責任者の許可の無い電話回線、携帯電話、無線 LAN、専用線などを利用して、法人外のネットワークへ直接接続してはならない。

５．６ リモートアクセスサービス利用基準

５．６．１ 利用申請

業務上リモートアクセスサービスの利用が必要な者は、各学校長等の承認を得、システム管理担当部署に申請しなければならない。

５．６．２ 使用機器に関する遵守事項

（１）利用者は、法人外から法人内ネットワークへのアクセスにおいて、システム管理担当部署が指定した機器を利用しなければならない。

（２）利用者は、インターネットから法人内ネットワークへの接続手段を、システム管理担当部

署の許可を得ることなく設置してはならない。

（3）その他法人内 LAN 環境への接続にあたり、利用機器は、本規程に基づいて設定されなければならない。

（4）リモートアクセスで使用する PC は、盗難に遭わない様に、また紛失しない様に、利用者が管理を行わなければならない。

５．６．３ 物理セキュリティ遵守事項

（1）リモートアクセスで使用する PC や Wi-Fi ルータは、所有者の目に届く範囲内で管理できるようにし、使用しない時には、セキュリティが確保できる場所に保管しなければならない。

６　ユーザ認証に関する基準

本基準は、情報を守るために使用されるユーザ認証に関して、セキュリティを確保しつつ利便性を実現する運用を目的として記述する。

６．１　ユーザ認証を用いたセキュリティ確保

法人システムに接続する機器は、ユーザ認証機能を装備していなければならない。また、必ずユーザ認証を行うように設定しなければならない。

６．２　対象システムによる認証システムの選定

システム管理担当部署は、対象システムが関わる重要性と、セキュリティを実現する手法の難易度を勘案してユーザ認証システムを構築しなければならない。システム管理担当部署は、ユーザ認証の仕組みには、パスワードを用いて情報システムを構築しなければならない。

６．３　パスワード

（1）８文字以上で大・小英字、数字、記号を組み合わせることが望ましい。

（2）一般に使われている単語や本人の個人属性（氏名、生年月日、住所など）、趣味などから、他人に推測されやすいパスワードを使用してはならない。

（3）パスワード変更が可能なシステムでは、３ケ月に一度を目安にパスワードを更新することが望ましい。

（4）パスワードは原則として利用者が生成して管理を行うものとする。設定したパスワードは紙などに書き留めてもよいが、対象システムが特定できたり、パスワードの文字列そのものを「あらわに」書き留めたりしてはならない。

（5）パスワードを口外したり、ヒントとなるような物品を身の回りに置いておいてはならない。

６．４　初期設定のパスワード

（1）利用者が最初に使用する初期設定のパスワードは、システム管理担当部署が発行し、口頭

もしくは書面で当該利用者に通知する。

（２）初期設定のパスワードは、職員番号などの規則性のある予測できるものに設定してはならない。

（３）利用者がパスワード変更できるシステムでは、パスワードが発行された後速やかに自らログインしパスワードを変更しなければならない。

６．５　パスワードを忘れた場合の処置

（１）パスワードを忘れた場合には、システム管理担当部署に新規パスワード発行の申請を行わなければならない。

（２）システム管理担当部署は、申請してきた利用者が本当に本人自身であることを何らかの方法で確認しなければならない。本人確認後、速やかに新規パスワードを発行して、利用者に通知しなければならない。

７　マルウェア対策基準

本基準は、ウイルス・ワーム等のマルウェアによって引き起こされる情報漏洩やシステムの破壊を未然に防ぐことを目的とする。

７．１　マルウェア対策ソフトの導入

（１）本法人は、システム管理担当部署が認めたマルウェア対策ソフトを、PC およびサーバ上に導入しなければならない。

（２）導入するマルウェア対策ソフトには、次の機能が含まれていなければならない。

・定義ファイルの自動更新機能

・常時スキャン機能（ファイルシステム、電子メール）

７．２　マルウェア対策ソフトの利用

（１）PC に導入されたマルウェア対策ソフトを常駐設定し、ファイルへのアクセスおよび電子メールの受信時には、常時スキャンできるように設定しなければならない。

（２）常時スキャンだけではなく一週間に一度、ファイル全体に対するスキャン（フルスキャン）を実施しなければならない。

（３）インストール時には、定義ファイルを毎日一度は更新するように設定しなければならない。

７．３　PC およびサーバ上のソフトウェアのセキュリティ対策

（１）PC に導入されているソフトウェアを『３　PC などにおけるセキュリティ対策基準』に従って、最新状態に維持しなければならない。

（２）サーバに導入されているソフトウェアを『２ サーバ等におけるセキュリティ対策基準』に従って、最新状態に維持しなければならない。

７．４　PC における電子メールを介してのマルウェア被害の防止

（１）メールの受信にあたっては、電子メール保護機能を有効にしなければならない。

（２）送信元不明のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審な添付ファイルは操作してはならない。

（３）「なりすましメール」の可能性も考え、添付されたファイルやメール本文内のリンクの操作には注意する。

（４）ファイルを添付してメールを送信する場合には、当該ファイルがマルウェアに感染していないことを必ず確認しなければならない。

（５）電子メールサービスを利用中に、マルウェアや、マルウェアと思われる症状を発見した場合は、『14 セキュリティインシデント報告、対応基準』に基づき対応しなければならない。

７．５　システム管理担当部署におけるマルウェア被害に対する対応

（１）法人内のマルウェア被害を迅速に収拾しなければならない。

（２）法人内のマルウェア被害状況を掌握し、問題発生時の一時対応を実施する。

７．６　マルウェア対策ソフトがマルウェアを検知した場合

（１）マルウェア対策ソフトの駆除機能を使用してマルウェアを駆除しなければならない。

（２）サーバ上で検知した場合には、同様に駆除し、システム管理担当部署に報告しなければならない。

７．７　マルウェアに感染した場合

（１）次の症状が発生した場合には、PC を直ちにネットワークから切り離す。その後、システム管理担当部署又はシステムセキュリティ管理担当者に報告し、対応方法について指示を受けなければならない。

・マルウェア対策ソフトから警告が出た。

・マルウェアに感染したメールが送られたとの連絡があった。

・突然、PC の動作が重くなったり、不審な画面が表示された。

・ファイルを開こうとしたら、マクロの警告ポップアップが出た。（このポップアップが何を意味しているのかを把握できているなら、報告の必要はない）

（２）連絡を受けたシステム管理担当部署又はシステムセキュリティ管理担当者は、PC からネットワークを切り離したことを確認しなければならない。

（３）システム管理担当部署又はシステムセキュリティ管理担当者は、当該 PC 上のマルウェア対

策ソフトの定義ファイルがいつ更新されているかを確認しなければならない。最新であれば、PC のフルスキャンを実行し、マルウェアが検知されるかを確認しなければならない。最新でない場合には、被害の程度に応じて、適切な復旧措置を実施しなければならない。

（4）システム管理担当部署又はシステムセキュリティ管理担当者は、マルウェアが検知された場合には、そのマルウェアの特性上どのような挙動を示すかを予測し、影響範囲を特定しなければならない。マルウェアが検知されない場合には、ログを確認し、怪しいログが残っていないかどうかを確認するなどして、原因を特定しなければならない。

（5）システム管理担当部署は、マルウェア被害の影響範囲が法人外にまで至っていることが判明した場合、『14 セキュリティインシデント報告、対応基準』に従って、問題の解決を図らなければならない。

8　電子メールサービス利用基準

本基準は、電子メールで受け渡される情報の安全性を確保し、電子メール利用に当たって発生しうる各種の問題を未然に防ぐことを目的とする。

8．1　電子メールサービス利用端末機器のセキュリティ

（1）電子メールの送受信にあたって、システムセキュリティ責任者が認めた電子メールソフトウェアを用いなければならない。また、システムセキュリティ責任者の指示に従い、当該ソフトウェアのバージョンアップを行わなければならない。

（2）上記ソフトウェアを使用する PC は、『３　PC などにおけるセキュリティ対策基準』に基づいたセキュリティ対策を施したものでなければならない。

8．2　電子メールで送受信される情報の保護

（1）法人の事業に関わる情報や、学生、教職員のプライバシーに関わる情報などの機密情報を、原則として電子メールを用いて送信してはならない。ただし、暗号化、電子署名などの処置を施した場合は、その限りではない。

（2）電子メールの送信にあたって、送信先のメールアドレスに間違いがないか、確認の上送信しなければならない。

（3）１通の電子メールで同報送信する場合は、場合に応じて、受信者間でメールアドレスが閲覧できる CC（カーボンコピー）か、受信者間でメールアドレスが閲覧できない BCC（ブラインドカーボンコピー）で送信しなければならない。

8．3　電子メールサービスとネットワーク保護

（1）業務目的以外に電子メールサービスを利用してはならない。

（2）スパムメールを受信した場合は、これを転送してはならない。スパムメールを受信したと

考えた場合には、これをシステムセキュリティ責任者に報告しなければならない。

（3）法人より発行されたメールアドレスを利用して、法人外のメーリングリストに参加する場合は、当該メーリングリストの信頼性、および業務への必要性を充分考慮した上で参加しなければならない。また、参加意義の無くなった場合には、直ちに脱退しなくてはならない。メーリングリストでの発言は、『８．２ 電子メールで送受信される情報の保護』を遵守しなければならない。それとともに公序良俗に反する発言をしてはならない。

（4）電子メールの送信にあたっては、送信するメールサイズを考慮しなければならない。送信可能なメールサイズの上限は２メガバイト程度とする。

（5）その他、無用な電子メールを送受信することにより、ネットワークに負荷をかけてはならない。また、HTML メールにて送信しないように、電子メールソフトウェアを設定しなければならない。

８．４　電子メールを介してのマルウェア被害の防止

（1）メールの受信にあたっては、『７ マルウェア対策基準』に基づき、電子メール保護機能を有効にしなければならない。

（2）送信元不明のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審な添付ファイルに対しては操作を加えてはならない。

（3）「なりすましメール」の可能性も考え、添付されたファイルやメール本文内のリンクの操作には注意する。

（4）ファイルを添付してメールを送信する場合には、当該ファイルのマルウェア感染が無いことを必ず確認しなければならない。

（5）電子メールサービスを利用中に、マルウェアやマルウェアと思われる症状を発見した場合には、『14 セキュリティインシデント報告、対応基準』に基づき対応しなければならない。

８．５　電子メールの監視

（1）システムセキュリティ責任者は、電子メールの利用状況を監視する。

９　Ｗｅｂサービス利用基準

本基準は、Web ブラウザを使用し、法人内外のサイトを利用するに当たって発生しうる各種の問題を未然に防ぐことを目的とする。

９．１　業務目的以外の利用禁止

（1）法人内及びインターネット上の Web サーバには、業務上必要な場合のみアクセスできる。

（2）信頼できない Web サーバにアクセスしてはならない。

（3）情報の発信（SNS や掲示板などへの書き込み）に関しては、業務上必要な場合のみとする。

このとき、情報の正確性を確保し、必要最小限の範囲で発信するものとする。また、次に該当する情報の発信は禁止する。情報の閲覧に関しても同様である。

・著作権、商標、肖像権を侵害するおそれのあるもの
・プライバシーを侵害するおそれのあるもの
・他者の社会的評価にかかわる問題に関するもの
・他者の名誉・信用を傷つけるおそれのあるもの
・法人の信用・品位を傷つけるおそれのあるもの
・性的な画像や文章に該当するおそれのあるもの
・不正アクセスを助長するおそれのあるもの
・差別的な内容を含むもの
・虚偽な内容を含むもの
・法人内の機密情報
・その他公序良俗に反するおそれのあるもの

（４）法人内外の Web サーバに対して、攻撃など不正なアクセスを行ってはならない。また、攻撃、不正なアクセスを目的として法人内外のシステムを利用してはならない。

（５）法人内外の Web サーバに対して、他人のユーザ ID やパスワードなどを利用してアクセスしてはならない。

９．２　Web ブラウザ利用端末機器のセキュリティ

（１）Web ブラウザの利用にあたって、当該ソフトウェアのバージョンアップ及び更新プログラムの適用を行わなければならない。

（２）上記ソフトウェアを使用するコンピュータ（スマートデバイス等を含む）は、『３ PC などにおけるセキュリティ対策基準』に基づいたセキュリティ対策を施したものでなければならない。

９．３　インターネット上の Web サーバへのアクセス

（１）署名の無い ActiveX や Java、JavaScript、VBScript などのコードは実行してはならない。ただし、信頼できるサイトに登録されていない場合でも、システムセキュリティ管理担当者より通知があったときは、実行してもよい。

（２）システムセキュリティ管理担当者の許可のないソフトウェアもしくはファイルをインターネット上からダウンロードして、実行、閲覧してはならない。

（３）リンクをクリックするとき、リンク先を確認してからクリックしなければならない。リンク先が信頼できない URL である場合は、クリックしてはならない。また、バナー広告についても同様で、業務上必要のないバナー広告はクリックしてはならない。

（４）システム管理担当部署の許可を得ないで他学校等へ情報を公開する目的の Web サーバを立

ち上げてはいけない。不審な Web サーバを発見した場合は、速やかにシステム管理担当部署に報告しなければならない。

（５）各学校等のサーバ（NAS を含む）において業務上必要な情報を公開する場合には、情報自体のアクセス権限を明確にし、IP アドレス、ID 及びパスワードなどを利用したアクセス制御を必ず行わなければならない。ファイルやアプリケーションをアップロードする場合には、必ずウイルスチェックを実施しなければならない。

（６）業務上不必要なファイル、ソフトウェア及び不審なファイルなどを、ダウンロードしてはならない。必要なファイルやソフトウェアであっても、Web サイト上で実行せず、必ずダウンロードし、ウイルスチェックを実施してから表示、実行しなければならない。

９．４　Web サイトの閲覧状況の監視

システムセキュリティ責任者は、Web サイトの閲覧状況を監視する。

１０　ＳＮＳ利用に関する基準

本基準は、教職員が SNS を利用するに際し、企業情報の漏洩を防止するとともに、本法人の信用失墜を防止することを目的とする。

１０．１　業務目的での利用

（１）業務を目的に SNS を利用する者は、事前に、利用目的、利用 SNS、作成予定利用アカウント名(作成したアカウント名が異なった場合は、作成後報告のこと)等をを SNS 公式アカウント登録申請書（様式４）により各学校長等に申請し承認を得ること。

なお、申請にあたってはワークフローを利用すること。

（２）SNS に記述する内容は、『９ Web サービス利用基準』に準ずる。

（３）SNS 利用において、他利用者からのクレーム、中傷、炎上等がある場合は、各学校長等に報告すること。

１０．２　業務目的外（私的利用）での利用

（１）教職員が SNS を利用する場合、本法人の非公開情報、法律、公序良俗に違反する記載をしてはならない。

（２）教職員が取引先と SNS 上で私的に交流する場合、双方の立場をわきまえ、社会人として良識の範囲で交流すること。

（３）教職員は SNS のセキュリティ設定の問題により、SNS のアカウントが乗っ取られ、悪用される可能性のあることに注意すること。

（４）教職員は使用デバイス(PC、スマートフォン、タブレット)と SNS の設定により、使用デバイス上のデータ、写真、位置情報と SNS が自動連携され、自分のプライバシーデータ、写真、

位置情報が予期せず公開される可能性のあることに注意すること。

（５）教職員は SNS の予期せぬ設定変更、機能追加によりセキュリティ制限レベルが変わり、情報がより一般に公開される可能性のあることに注意すること。

（６）教職員は SNS 利用において、本法人の非公開情報の漏洩の可能性、他利用者からのクレーム、中傷、炎上等により本法人の信用失墜がある可能性がある場合は、各学校長等に報告すること。

１１　プライバシーに関する基準

本基準は、教職員及び学生等の個人情報を取り扱う（収集・維持・廃棄）際に注意すべき事項をまとめ、発生しうる問題を未然に防ぐことを目的とする。

１１．１　個人データ管理責任者の設置

（１）個人データの収集・維持・廃棄を行う個人データ管理責任者を置く。

（２）上記（１）の個人データ管理責任者は、大学においては事務局長、専門学校においては副校長又は教頭、幼稚園及び保育園においては副園長又は教頭、法人本部においては総務部長とする。

１１．２　個人情報保護方針の公開

（１）個人データを広く一般から収集する場合、法人の Web サイトや広告などに法人の個人情報保護方針を公開しなければならない。

１１．３　個人データの収集

（１）個人データの収集を行う者は、『個人情報保護規程』第２章を遵守しなければならない。

１１．４　個人データの維持

（１）職員は、個人データに対する登録・参照・変更・削除の実施においては、細心の注意を払って行わなければならない。

（２）個人データを利用する場合には、正確な情報を利用しなければならず、そのための保護策を実施しなければならない。

（３）個人データのバックアップを実施しなければならない。バックアップした媒体は、個人データと同様の管理策を設けなければならない。

（４）当該個人の個人データに関する開示・訂正・削除の要求があった場合には、『個人情報保護規程』第５章に基づいて対応しなければならない。

（５）個人データを第三者に提供又は預託する場合には、『個人情報保護規程』第 18～20 条に基づいて対応しなければならない。

１１．５　個人データの破棄

（１）個人データを破棄する場合、『個人情報保護規程』第 26 条に基づいて破棄しなければならない。

（２）電子媒体などの破棄においては、『４　媒体の取り扱いに関する基準』に基づいて実施しなければならない。

１１．６　クレーム処理

（１）法人の業務において個人データに関するクレームを受けた場合には、速やかに対応しなければならない。

（２）個人データが漏洩してしまったなど必要がある場合、システムセキュリティ責任者は法人の見解を迅速に明確にしなければならない。

（３）どのようなクレームが発生した場合でも、第一報をシステムセキュリティ管理担当者へ 12 時間以内に報告し、その後の対応状況に関しても適宜連絡しなければならない。

１２　システム維持に関する基準

本基準は、本法人のシステムセキュリティレベルを維持するための更新プログラム等の適用ルール、バックアップルールについて規定する。

１２．１　更新プログラム適用のルール

（１）システム管理担当部署より配信された更新プログラム適用の指示に対して、自分が管理または使用している全てのマシンに対して速やかに更新プログラムを適用しなければならない。

（２）更新プログラム適用作業によるサービスの停止など他のシステムへの影響が大きく、速やかに（１）の更新プログラムが適用出来ない場合、その旨システム管理担当部署に連絡しなくてはならない。

（３）システムセキュリティ管理担当者は、（１）の更新プログラムが指示通り適用されたことをシステム管理担当部署へ報告する。

１２．２　更新プログラムの取得及び配布方法

（１）システムセキュリティ管理担当者は、OS 関連更新プログラムの取得方法を利用者に指示し、各 PC にインストールさせる。

（２）システムセキュリティ管理担当者は、各アプリケーションの更新プログラムの取得方法を利用者に指示し、各 PC にインストールさせる。

（３）システム管理担当部署は、ネットワーク機器の更新プログラムをベンダより取得し、インストールする。

１２．３　マルウェア定義ファイルの更新

（1）『7 マルウェア対策基準』に基づいてマルウェア定義ファイルを更新しなければならない。

１２．４　サーバのバックアップについて

（1）業務上重要なサーバ（Web サーバ、メールサーバ、DB サーバ等）については、そのデータ及びログを定期的にバックアップしなければならない。

（2）更新プログラムの適用など、サーバのシステムに対して何らかの変更を行う場合には、事前にサーバのシステムバックアップを取らなければならない。

（3）更新プログラムの適用など、サーバのシステムに対して何らかの変更を行った場合には、安定動作確認後にサーバのシステムバックアップを取らなければならない。

（4）バックアップ作業は業務に影響が及ばないように作業時間は十分に配慮しなければならない。

１２．５　バックアップ媒体の取り扱いについて

（1）過去２回分のバックアップデータを保持することが望ましい。

（2）バックアップに使用する媒体は、鍵付きの保管場所に置くなど、サーバ管理者が責任をもって管理しなければならない。

（3）バックアップに使用した媒体の破棄については、『４ 媒体の取り扱いに関する基準』に基づいて処理をしなければならない。

１２．６　システムの監視について

（1）システムセキュリティ管理担当者及びシステム管理担当部署は、システム障害などの兆候をいち早く見つけるために、サーバ及びネットワークの監視を行わなければならない。監視については『13 セキュリティ監視に関する基準』に基づいて行わなければならない。

１３　セキュリティ監視に関する基準

本基準は、本法人の情報システムの監視について規定し、システム障害、不正アクセスの兆候をいち早く検知し、それらの原因究明が円滑に行われることを目的とする。

１３．１　対象システムのログによる監視

（1）システム管理担当部署は、将来起こりうる調査やアクセス制御の監視に役立てるため、対象システムに関して次のログを取得し、一定期間保管しなければならない。

取得対象：・サーバ
・ファイアウォール
・主要なネットワーク機器

取得内容：・ログオン・ログオフの記録
・発信元アドレス／ポート番号
・宛て先アドレス／ポート番号

（２）システム管理担当部署は、許可された処理だけが実行されていることを確認するために、ログを定期的に解析しなければならない。解析の結果、次のような事象が確認された場合には、システムセキュリティ責任者に報告しなければならない。

・連続したアクセスの失敗
・連続した認証の失敗
・大量のデータの送受信
・権限外の処理の試み

（３）システム管理担当部署は、（２）の事象が不正アクセスによってもたらされた疑いがある場合には、『14 セキュリティインシデント報告、対応基準』に基づいて、原因究明、再発防止計画の作成など、適切な対応を実施しなければならない。

（４）システム管理担当部署は、（１）で取得するログの時間情報を適切に保ち、ログの証拠としての有効性を高めるため、NTP（時刻同期）サーバなどを用いてシステム間の時刻同期をとらなければならない。ただし、その場合には、NTP サーバ自身のセキュリティ対策にも十分配慮しなければならない。

（５）システム管理担当部署は、（１）で取得するログのバックアップを『12 システム維持に関する基準』に基づいて、一定期間、適切に保管しなければならない。

１３．２　不正侵入検知システムによる監視

システム管理担当部署は、不正侵入を監視するため、以下の対策を行う。

（１）法人のグローバルゾーンのネットワークに、ネットワーク監視型不正侵入検知システムを導入し、不正アクセスの発生状況を常時監視しなければならない。

（２）法人のグローバルゾーンに設置されている DNS サーバ、WWW サーバ、Mail サーバなどに、ホスト監視型不正侵入検知システムを導入し、不正アクセスの発生状況を常時監視しなければならない。

（３）（１）、（２）の監視によって不正アクセスの兆候が検知された場合には、『14 セキュリティインシデント報告、対応基準』に基づいて、速やかに対応しなければならない。

（４）不正侵入検知システムのログを定期的に分析し、結果をシステムセキュリティ責任者に報告しなければならない。

（５）不正侵入検知システムのログを『12 システム維持に関する基準』に基づいて、一定期間、適切に保管しなければならない。

１４　セキュリティインシデント報告・対応基準

本基準は、セキュリティインシデント（事件）が発生した場合に迅速に対応し、円滑に業務が継続されることを目的とする。

１４．１　平時の準備

（１）業務上利用するすべてのコンピュータについて、『７ マルウェア対策基準』に基づき、適切にウイルス検査を実行しなければならない。

（２）ノート PC・機密資料などの情報資産を紛失しないように十分、注意しなければならない。

（３）重要なシステムに対して UPS を使用し、停電時には自動でシャットダウンを行うように設定しなければならない。

（４）システム管理担当部署は、以下の内容を日常的に行う。

・『13 セキュリティ監視に関する基準』に基づいて、ログの取得・バックアップの取得、システム及びネットワークの監視、セキュリティ情報の収集を行い、適切な対策を実施しなければならない。

・起こり得るインシデントに適切に対応し、インシデント対応手順書を作成しなければならない。

１４．２　セキュリティインシデント発生時

（１）法人ではセキュリティインシデントを被害の深刻度に応じて、次のようにレベル分けする。

①レベル１（深刻度：低）：問題の発生原因・被害の範囲とも法人内に限定される場合

②レベル２（深刻度：中）：法人外の第三者からのセキュリティ侵害により、法人が被害者となる場合

③レベル３（深刻度：高）：法人外に対して、法人が加害者となる場合

（２）全ての利用者は、マルウェア感染被害や不正アクセスの被害に気づいた場合には、直ちに対象システムをネットワークから切り離し後、各学校等のシステムセキュリティ管理担当者に報告し、指示を仰がねばならない。

（３）システムセキュリティ管理担当者は、報告のあったすべてのインシデントについてシステムセキュリティ責任者に報告するとともに、システムセキュリティ責任者の指示のもとに、必要な措置を講じなければならない。

（４）システムセキュリティ責任者は、ログ、監視レポート、関係者へのヒアリングなどに基づいて、速やかに、被害状況を把握し、対策にあたらなければならない。

（５）システムセキュリティ責任者は、被害状況を把握するにあたり、次の事項を確認しなければならない。

①セキュリティインシデントの種類

②被害を受けた日時

③原因と対処方法（作業記録を含む）

④被害の拡大範囲

（６）システム管理担当部署は、侵害原因が解消された後、速やかにバックアップ媒体を用いてシステムを正常な状態に復旧しなければならない。

（７）全ての利用者は、マルウェア感染などが原因で OS、アプリケーションの入れ替えが必要になった場合には、適切な媒体を使用して速やかに再インストールを実施しなければならない。

１４．３　再発防止計画

（１）セキュリティインシデントへの対応が完了した後、システムセキュリティ責任者およびシステム管理担当部署は、調査した被害状況をもとに再発防止計画を作成しなければならない。再発防止計画作成時には、技術的側面と組織的（制度的）側面の両方に留意しなければならない。

（２）システムセキュリティ責任者は、作成された再発防止計画を、全ての利用者に周知し、適切に実施しなければならない。

（３）システムセキュリティ責任者は、セキュリティインシデントの発生から再発防止計画作成までの一連の記録を管理、保管しなければならない。

１５　セキュリティ教育に関する基準

本基準は、セキュリティ教育に関する事項を規定する。

１５．１　教育の実施

（１）システム管理担当部署及び各学校等のシステムセキュリティ管理担当者は、コンピュータに携わるすべての人に対し、次の教育内容について、教育資料を使用し、セキュリティの教育を実施しなければならない。

教育内容

・情報セキュリティ問題のもつ意味を理解

・組織や個人の情報セキュリティの重要性

・セキュリティ対策

・情報セキュリティ計画

・データ所有者の責任

・モラル教育

・禁止行為に関しての教育他

・啓発

１６　第三者契約に関する基準

本基準は、本法人の業務を外部の業者に委託し、実施する場合の契約における問題及び業務作業時の問題を未然に防ぐことを目的とする。

１６．１　委託契約に盛り込むべき事項

（１）委託業者との窓口となる者は、委託業務の仕様以外に次の契約事項を盛り込まなければならない。

・機密保持に関する事項

・情報管理に関する事項

・その他、必要性のある事項

１６．２　機密保持に関する事項

（１）委託業者は、本法人の業務で知り得た情報を第三者に開示してはならない。

１６．３　情報管理に関する事項

（１）委託業者は、本法人の業務を行うにあたって窓口となる情報管理責任者を明確にしなければならない。

（２）委託業者は、本法人の業務を行うにあたって入手した情報を適切に管理しなければならない。

（３）委託業者は、入手した情報をリストアップし、常に授受の状況を明確にしなければならない。

（４）委託業者は、入手した情報を閲覧・利用できる者を特定し、明示しなければならない。

（附則）

１．この基準は、令和７年４月１日から実施する。

２．この基準制定に伴い、情報セキュリティ対策基準（平成１７年７月１日制定）は廃止する。

制定　令和７年　４月　１日

（様式１）

ネットワーク機器設置許可申請書

殿

以下の機器をネットワークに接続するため設置許可を申請いたします。

申　請　年　月　日	年　月　日
申　請　区　分	１．新規　２．変更　３．取り消し （２、３の場合は現在の IP アドレスを記入　　）
申請者の所属、氏名、連絡先電話及びメールアドレス	所属 氏名
	e-mail 内線
設　置　場　所	
製品名（メーカー・機種）	
ウ イ ル ス 対 策 ソ フ ト	
利　用　目　的	（システムで接続される場合は、構成図を添付して下さい。）

年　月　日

殿

長

上記の申請を許可いたします。

（様式２）

サーバ設置申請書

殿

サーバを設置したいので次のとおり申請いたします。

申　請　年　月　日		年　月　日
申　請　区　分		１．新規　２．変更　３．取り消し （２、３の場合は現在の IP アドレスを入　）
申請者の所属、氏名、連絡先電話及びメールアドレス		所属 氏名
		e-mail 内線
サーバに関する事項	OS の名称	
	サーバ名	
	バージョン	
	機器の型名	
	メーカー	
	IP アドレス	
	変更	
	設置場所	
	用途、目的	（システム構成図を添付して下さい。）
サーバとして供するソフトウェア（該当のものを○で囲む、または下に記載）		
リモートデスクトップ ｈｔｔｐｄ　ｄｎｓ　ｓｅｎｄｍａｉｌ　ｐｏｐ３　ｉｍａｐ４		
その他システムの DNS やファイアウォールに記述する事項		

年　月　日

殿

長

上記の申請を許可いたします。

（様式３）

PC 利用申請書

殿

以下の PC をネットワークに接続するため利用許可を申請いたします。

申　請　年　月　日	年　月　日
申　請　区　分	１．新規　２．変更　３．取り消し
申請者の所属、氏名、連絡先 電話及びメールアドレス	所属 氏名
	e-mail 内線
利　用　者　の　範　囲	
Ｐ Ｃ　利　用　場　所	
利　用　Ｐ　Ｃ	メーカー　機種
	OS　バージョン
	PC 名

（注）複数の PC を使用する場合は、その都度この「利用申請書」を提出して下さい。

年　月　日

殿

長

上記の申請を許可いたします。

（様式４）

SNS 公式アカウント登録申請書

殿

SNS 公式アカウント登録について、下記の通り申請します。

記

1. 申請種別

☐ 新規登録

☐ 登録情報の変更 → ☐管理責任者の変更 ☐運用担当者の変更 ☐その他（　　）

☐ 登録情報の削除

2. 管理責任者（申請者）

氏　　名		
所　　属		
連　絡　先	e-mail	内線電話

3. 運用担当者

氏　　名		
所　　属		
連　絡　先	e-mail	内線電話

4. 詳細

利用 SNS	☐ Facebook　☐ X　☐ LINE　☐ YouTube	
	☐ その他（　　）	
利用組織名		
利用目的		
アカウント名		
U　R　L		
利用期間	開始　年　月　日	終了　年　月　日
学園章、紋章の使用	学園章・紋章の使用を　☐希望する　☐希望しない	

年　月　日

殿

長

上記の申請を許可いたします。