

MENETにおいて扱う情報の保護に関する規則

平成28年10月1日 前橋市教育委員会

(目的及び定義)

1 本規則の目的

本規則は、前橋市個人情報保護条例及び前橋市情報セキュリティポリシー、前橋市教育情報ネットワーク運用規程（以下「運用規程」という）第9条及び第10条に基づき、前橋市教育情報ネットワーク（以下「MENET」という）・MENETにおいて提供される各種サービス（以下「MENETサービス」という）・MENETに接続された機器（以下「MENET機器」という）を利用する際に扱う情報の保護を徹底するために、全ての利用者が遵守すべき事項を定めたものである。

2 定義

本規則における情報とは、MENET・MENETサービス・MENET機器で扱われるデジタル化された情報であり、情報の保護とは、利用者の故意や過失による廃棄、削除、破壊、流出、第三者による不正な持ち出し、改竄、消去等を防止するために以下の(1)～(4)に示したセキュリティ対策のことである。

(1) 情報の分類

個人情報の有無等を考慮して情報を分類した上で、その重要度に応じた利用者、利用手段、利用場所、保存場所等を明確にし、そのルールに基づいた利用を徹底する。

(2) 物理的セキュリティ対策

MENET機器の管理及び利用について制限を設けるなど、物理的な対策を講じる。

(3) 技術的セキュリティ対策

MENET機器やデータ等に対して、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(4) 人的セキュリティ対策

運用規程第8条に基づき、セキュリティに関し職員等が遵守すべき事項を定めるとともに、十分な教育や啓発を行い、人的な対策を講じる。

(組織)

1 管理責任者

MENETに接続されている前橋市立の各学校園及び教育関係機関（以下「各拠点」という）における情報の保護に関する管理責任者（以下、「管理者」という）は、運用規程第3条に基づき、所属長が務める。

2 管理者の業務

管理者は、以下の(1)～(3)の業務にあたり、個人情報保護及びセキュリティレベルの保持に努める。

(1) 規則遵守の徹底

管理者は、所属内の利用者に対し本規則の遵守を徹底しなければならない。遵守しない利用者に対しては、MENET・MENETサービス・MENET機器の利用停止もしくは、

利用を制限する権限を有する。

(2) セキュリティ委員会の設置

管理者は、所属内の情報の保護のための具体的方策の検討を行う「セキュリティ委員会」を設置する。各学校園においては、構成員を校（園）長、教頭、教務主任、情報教育主任、その他必要と認められる者とし、その他の教育関係機関においては、所属長及び所属長が指名する職員とするが、運用規程第4条で規定されている内部M E N E T運用委員会の組織と兼ねることができる。

(3) 運用担当者の任命

管理者は、所属内の情報を保護するために、具体的な方策を実行する運用担当者（以下、「運用者」という）を任命し、その実務に当たらせることができる。

3 運用者の業務

運用者は、以下の(1)～(4)の業務にあたり、情報の保護に努める。なお、(1)～(3)の業務の管理・運用要領は別に定める。

- (1) 拠点内M E N E T（拠点内有線・無線L A N）及び構成機器類の管理
- (2) 教職員用P C及び授業用P C（指導者用タブレットP C・児童生徒用P C）の管理
- (3) M E N E Tサービス利用時に扱うデータの管理
- (4) 利用者に対するウィルス情報、アップデート情報等の提供及び対策支援

（ネットワークの分類）

拠点内M E N E Tは扱う情報及び接続可能な機器を分別管理するために、次の2種類に分類し設置する。

1 職員系ネットワーク

主に業務（校務）での利用を目的としたネットワークで、利用者は教職員のみとする。各学校園で、校長室、職員室、保健室、事務室等に敷設された有線ネットワーク。

2 児童生徒系ネットワーク

主に授業での利用を目的としたネットワークで、利用者は児童生徒及び教職員とする。教室、特別教室、体育館等に敷設された有線及び無線ネットワーク。尚、災害時の避難場所として学校を提供する場合は、一時的に地域住民も利用することができる。

(情報の分類)

MENET・MENETサービス・MENET機器で扱う情報を、次のA～Dの4種類に分類する。

A プライバシー性が非常に高く、情報が漏洩した場合、非常に大きな信用を失う情報
 児童生徒の学籍や成績、健康診断の記録など守秘義務を要する重要な個人情報が含まれている情報

学籍情報・学校経営・その他	生徒指導関係	成績関係・学習関係
<ul style="list-style-type: none"> ○指導要録（学籍に関する記録） ○出席簿 ○卒業証書授与台帳 ○転入出受付（整理）簿 ○就学児童生徒異動報告書 ○教科用図書給付児童生徒名簿 ○児童生徒一覧表（住所、電話番号、家族構成等を含むもの） ○教職員個人調査票 ○教職員一覧表 	<ul style="list-style-type: none"> ○事故報告書・記録 ○生徒指導・特別指導等記録 ○児童生徒個人調査票 ○児童・生徒の個人写真（氏名を併記したもの） 	<ul style="list-style-type: none"> ○指導要録（指導に関する記録） ○評定一覧表 ○進級・卒業認定会議資料 ○通知票 ○定期考査素点表 ○成績に関する個票等 ○成績一覧表 ○高校入試関連資料（合否判定資料等含む）
進路関係	教務関係・保健関係	事務関係
<ul style="list-style-type: none"> ○卒業生進路先一覧等 ○進路希望調査 ○進路指導記録簿 ○調査書 ○推薦書 ○受験報告書 	<ul style="list-style-type: none"> ○健康診断に関する表簿・歯の検査表 ○定期健康診断結果 ○保健日誌 	<ul style="list-style-type: none"> ○要・準要保護児童生徒認定台帳 ○その他校内就学援助関係書類 ○給与関係書類 ○手当関連書類 ○監査調書 ○特学奨励費関係書類 ○マイナンバー関係書類

B プライバシー性が高く、情報が漏洩した場合、大きな信用を失う情報
 学習指導案や校務分掌で使用するデータ、児童生徒の個人が特定できる写真や氏名などを含む情報

学籍情報・学校経営・その他	生徒指導関係	成績関係・学習関係
<ul style="list-style-type: none"> ○児童生徒名簿 ○職員会議資料（個人情報含） ○各校務分掌のデータ（個人情報含） 	<ul style="list-style-type: none"> ○指導データ（児童生徒等理解カード） ○教育相談・面接の記録 ○個別の教育支援計画 ○個別の指導計画 ○自転車等通学生徒一覧表 ○児童・生徒の個人写真 	<ul style="list-style-type: none"> ○テストの解答 ○個人の学習履歴（PC内でのテスト等） ○学習指導案（児童生徒の実態や対応が記載されているもの）

進路関係	教務関係・保健関係	事務関係
	<input type="checkbox"/> 週ごとの指導計画 (個人情報が含まれるもの) <input type="checkbox"/> 児童・生徒等健康調査票 (宿泊行事前, 長期休み明けの健康調査など) <input type="checkbox"/> 身体測定の結果・個票	<input type="checkbox"/> 各種証明書関係書類 <input type="checkbox"/> 収入調定書 <input type="checkbox"/> 旅行関係書類 <input type="checkbox"/> 各種点検報告書 <input type="checkbox"/> 休暇承認簿等の服務管理関連書類

C 配布または公開されることがある情報のうち、個人情報を含む可能性のあるもの
 学年, 学級通信, 学校行事のしおりなど

学校運営・学校経営・その他	生徒指導関係	成績関係・学習関係
<input type="checkbox"/> 学校要覧 <input type="checkbox"/> 学校紹介パンフレット <input type="checkbox"/> 学級(学年)通信 <input type="checkbox"/> PTA資料 <input type="checkbox"/> 学校行事のしおり (修学旅行・キャンプ・合宿等) <input type="checkbox"/> 集合写真等 <input type="checkbox"/> 不審者対策等マニュアル <input type="checkbox"/> 職員会議資料 <input type="checkbox"/> 各校務分掌のデータ <input type="checkbox"/> 学年学級会計簿(個人情報の含まれないもの)	<input type="checkbox"/> 生徒指導計画や 生徒指導のしおり等	<input type="checkbox"/> 授業用ワークシート <input type="checkbox"/> 作品・作文・レポート <input type="checkbox"/> 学習指導案(児童生徒の実態以外)
進路関係	教務関係・保健関係	事務関係
	<input type="checkbox"/> 週ごとの指導計画 <input type="checkbox"/> 保健たより <input type="checkbox"/> 保健指導のワークシート(実施後) <input type="checkbox"/> 学校保健委員会の感想等	

D 配布または公開されてもよい情報のうち、個人情報を含まないもの

学籍情報・学校経営・その他	生徒指導関係	成績関係・学習関係
<input type="checkbox"/> ホームページの バックアップデータ等		<input type="checkbox"/> 授業用教材 <input type="checkbox"/> 教材研究資料
進路関係	教務関係・保健関係	事務関係
<input type="checkbox"/> 進路のしおり等 <input type="checkbox"/> 動画等		

(物理的セキュリティ対策)

1 PC等の端末の分類

PC等の端末を以下の(1)～(3)に分類し、利用できる情報等の条件を個別に設ける。

- (1) 職員系ネットワークに接続でき、教職員が事務処理に利用するPC【赤シール端末】
(例：校長室、職員室、保健室、事務室（共同実施室を含む）に固定設置されているPC)
- (2) 児童生徒系ネットワークのみ接続でき、教職員が授業で利用するPC【黄シール端末】
(例：指導者用タブレットPC)
- (3) 児童生徒系ネットワークのみ接続でき、児童生徒が授業で利用するPC【緑シール端末】
(例：PC室の児童生徒用PC、図書室用PC、教室設置のリースアウトPCなど)

2 情報をPC等の端末で扱う場合の利用条件

PC等の端末については、分類毎に、利用場所・利用用途・保存先を、下表のとおり具体的に定める。ただし、管理者の許可を受ければ、これ以外の条件でも利用することができる。

学校で扱う情報の分類及びPC等の端末で扱う場合の条件										
学校で扱う情報の分類			PC等の端末で扱う場合の条件							
重要度	情報の特性	取り扱う情報の例	端末の使用条件と扱える情報				保存先			
			用途	校務用	授業用		端末本体	データセンター	職員室サーバー	PC室サーバー
					指導者用	学習者用				
			本体シール	赤	黄	緑				
			使用可能者	教職員	教職員	教職員 児童生徒				
端末移動	×	校地内のみ ○	校地内のみ ○							
接続可能NW /方法	職員系 /有線	児童生徒系 /有線・無線	児童生徒系 /有線・無線							
A	プライバシー性が非常に高く、情報が漏洩した場合、非常に大きな信用を失う情報	<ul style="list-style-type: none"> ・指導要録 ・出席簿 ・健康診断簿 ・個人調査票 ・通知票 等	○	×	×	×	○	×	×	
B	プライバシー性が高く、情報が漏洩した場合、大きな信用を失う情報	<ul style="list-style-type: none"> ・学習指導案 ・記入済テスト、ワークシート ・校務分掌で使用するデータ ・個人を特定できる写真や動画 等	○	×	×	×	○	×	×	
C	配布または公開されてもよい情報のうち、個人情報を含む可能性があるもの	<ul style="list-style-type: none"> ・学年、学級通信 ・学校要覧 ・ホームページのデータ ・学校行事のしおり 等	○	○	×	×	○	○	○	
D	配布または公開されてもよい情報のうち、個人情報を含まないもの	<ul style="list-style-type: none"> ・授業用教材及び資料 ・教材研究用資料 ・未記入のワークシート ・個人を特定できない写真や動画 等	○	○	○	×	○	○	○	

3 利用条件の例外

(1) 指定場所以外での利用

黄シール端末を管理台帳の指定場所以外で利用する場合には、管理職へ報告（口頭も可）してから移動する。ただし、教室等で利用した場合には、そのまま放置することのないようにし、利用後はその都度必ず管理台帳に記載された場所に戻す。

また、黄シール端末及び緑シール端末を遠足や社会科見学等の校外学習で使用する場合は、市内教育関係団体・PTA等の各種事業に使用する場合は、データ持ち出し時と同様に、遵守事項を守り、管理者の許可を得れば、所属校の校外であっても使用することができる。

(2) 例外的に緑シール端末で扱える情報

Cの情報のうち、教材として教師から提示されたもの、ホームページ等で一般に公開されているもの、本人が作成中の作品・作文・レポート・ワークシート等については、緑シール端末でも扱うことができる。

(3) PC等の端末本体への一時保存

データ作成後の利用方法を考慮し、必要な場合には一時的に本体に保存してもよいこととするが、利用が終わり次第速やかに移動しなければならない。

(4) データ持ち出し時の遵守事項

A・Bのデータの持ち出しは禁止とする。なおC・Dのデータについても原則として禁止とするが、どうしても必要な場合に限り、次の①～⑦の事項を遵守し管理者に許可を得れば持ち出すことができる。

- ① 個人情報に記載されている場合は、該当する部分をすべて削除すること。
- ② データを複製した外部記録媒体を持ち出す際は、常に身につけ、盗難や紛失のないよう十分な管理を行うとともに、自宅に持ち帰る場合は寄り道をせず直接帰るようにする。
- ③ データを複製した外部記録媒体は、私用のデータを保存してある外部記録媒体と分けるなどして、十分な管理を行う。
- ④ 自宅等でデータを使用する場合は、複製したデータがインターネット等を通して漏洩することがないように、使用するコンピュータのセキュリティを教育用PCと同等以上に保持すること。特に、ファイル交換ソフトのインストールされているコンピュータやウイルス対策ソフトが最新版に更新されていないコンピュータでの使用は禁止する。
ただし、自宅等でデータを使用する場合は、個人所有PCとする。
- ⑤ 自宅等でデータを更新した場合、データは自宅等のコンピュータ等に保存しない。
自宅等で更新したデータを学校に戻した場合、外部記録媒体から速やかにデータを削除する。
- ⑥ データを保存した外部記録媒体を廃棄する際は、物理的に破壊するか専用のソフトを用いてデータを完全に削除する。
- ⑦ 持ち出したデータが紛失したり盗難にあたりたりした場合や、インターネット等を通じて漏洩した場合は、速やかに管理者に報告し、指示を仰ぐ。

(5) インターネット上で企業が運営するストレージサーバ等の利用

インターネット上で企業が運営するストレージサーバや電子メールへの添付などについて

ても原則禁止とするが、データの持ち出し行為と同様の扱いとする。

(6) 重要なデータへの特別措置

重要な個人情報や重要なデータを作成した場合は、必要に応じて暗号化した上で、外付けハードディスクやCD-R等の外部記録媒体に保存して金庫等に保存するなど、適切な措置を講じることとする。

(技術的セキュリティ対策)

1 セキュリティレベルの保持

運用者は、情報の保護に必要な機器等のセキュリティレベルを保持するために、管理者の指示を受け、以下の項目を必要に応じて利用者に呼びかけるとともに、その実施の支援を行う。また、利用者はその際には運用者の呼びかけに応じなければならない。

(1) アップデート

利用者は、OSやソフトウェアのセキュリティアップデート等を定期的に行い、最新の状態に保つこととする。ただし、OSやソフトのバージョンは、必ずしも最新でなくてもよいこととする。

(2) ウィルス対策

利用者は、ウィルス対策ソフトウェアのパターンファイルを最新の状態に保ち、定期的にウィルスチェックを行うこととする。また、貸与されたPC以外のPCで作成したデータをデータセンターまたは職員室サーバに保存する際には、当該データのウィルス検査を必ず実施し、安全を確認しなければならない。

(3) 守秘義務

利用者は、ネットワークに接続するために必要なID、パスワード等の諸情報の機密について、守秘義務を負うものとする。

(4) 緊急時の対応

利用者は、ウィルス感染等の緊急時の場合、速やかに管理者に報告し、指示を仰ぐこととする。

2 機器等の初期設定の変更

機器等の設定は、業務に支障のない限り、マウスの設定の変更等、簡易な変更について認めることとする。

3 ソフトウェアのインストール

業務を円滑に進める上で必要な場合は、必要最小限かつセキュリティ上の安全性が証明されているソフトウェアのみ、貸与されたPCにインストールすることができる。この場合、管理者の許可を受け、管理台帳に記載しなければならない。さらに、当該ソフトの使用許諾契約に反しない方法でインストールすることとし、当該ソフトの著作権を遵守することとする。

4 周辺機器の追加

貸与されたPCへの周辺機器の追加は、原則禁止する。ただし、業務を遂行する上で必要な場合は、必要最小限かつセキュリティ上の安全性が証明されている周辺機器のみ、管理者

の許可を受けて追加することができる。この場合、管理台帳に記載しなければならない。

(人的セキュリティ対策)

1 定期的なデータ管理

運用者は、データセンター・職員室サーバ・PC室サーバ内のデータが保存ルールに基づいて適正に保存されているか定期的に確認し、必要に応じて利用者への助言やデータ移動等の作業を行う。

2 遵守事項の確認・研修

管理者は、情報の保護のための遵守事項を書面で定期的に確認するとともに、必要に応じてそのための研修の機会を設ける。その場合は、所属内の実態を把握した上で、最もリスクが高いと考えられる事故等を具体的に扱うなど、利用者の誤った認識を改善できる内容となるよう配慮する。

3 禁止事項の徹底

管理者は、情報の保護のため、利用者以下(1)～(3)の禁止事項を徹底させるとともに、運用者は禁止行為を発見した場合、速やかに管理者に報告し、指示を仰ぐものとする。

(1) 私的利用の禁止

職務に関係のないWebページの閲覧やSNS等のインターネットサービスの利用、私有メールアドレスの利用及び私的メールの送受信、私的データの保存等、MENE Tサービスの私的利用は禁止する。

(2) 違法ソフト等のインストールの禁止

正規ライセンスを所有していない違法ソフト及び校務処理ソフト、利用目的に関係のないソフトをインストールすることは禁止する。

(3) 個人所有コンピュータ等の持ち込み禁止

個人が所有しているコンピュータ等(以下「個人所有PC」という)を校内に持ち込む行為は禁止する。

ただし、個人所有PCの持ち込みが、業務遂行上、必要であると管理者が認めた場合は、以下の事項を遵守すれば使用することができる。

① 個人所有PCを校内LANに接続しないこと。

② 個人所有PCを校内で使用する際は、本規程のデータ持ち出し時の遵守事項に準じ、一度外部記録媒体等を経由すること。

(評価・見直し)

1 セキュリティ監査及び自己点検の実施

本規則で定めたセキュリティ対策の遵守状況を検証するためには、必要に応じて自己点検又は監査を実施する。

2 本規則の見直し

自己点検又は監査の結果等により、本規則の見直しが必要となった場合及びセキュリティに関する状況の変化に対応するために新たな対策が必要となった場合には、本規則を見直す。

(附 則) 本利用規程は、平成28年10月1日から施行する。