

令和7年度 霧島市立国分北小学校情報セキュリティポリシー

1 目的

この情報セキュリティポリシーは、霧島市立国分北小学校における児童、保護者、教職員等の個人情報及び学校運営上の重要な教育情報等の機密性、完全性、可用性を守るために必要なルールを定めたものである。

※機密性(confidentiality)

情報の機密を守ることを意味する。(許可されていない人が勝手に情報を見たり変更したりできないようにする必要がある。)

※完全性(integrity)

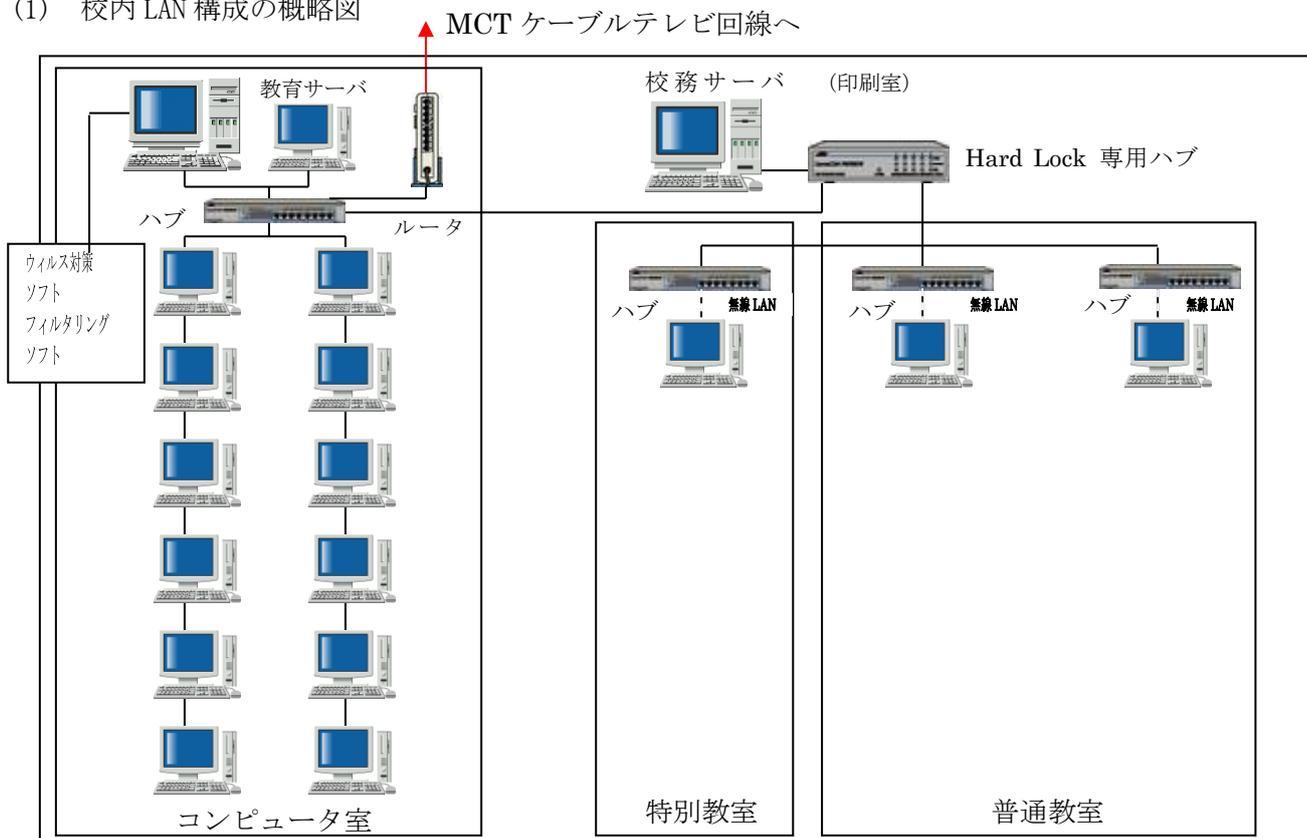
情報が改ざんなどされずに正しい状態であることを意味する。

※可用性(availability)

許可された利用者が必要なとき情報に確実にアクセスすることを意味する。

2 学校のネットワークシステム

(1) 校内 LAN 構成の概略図



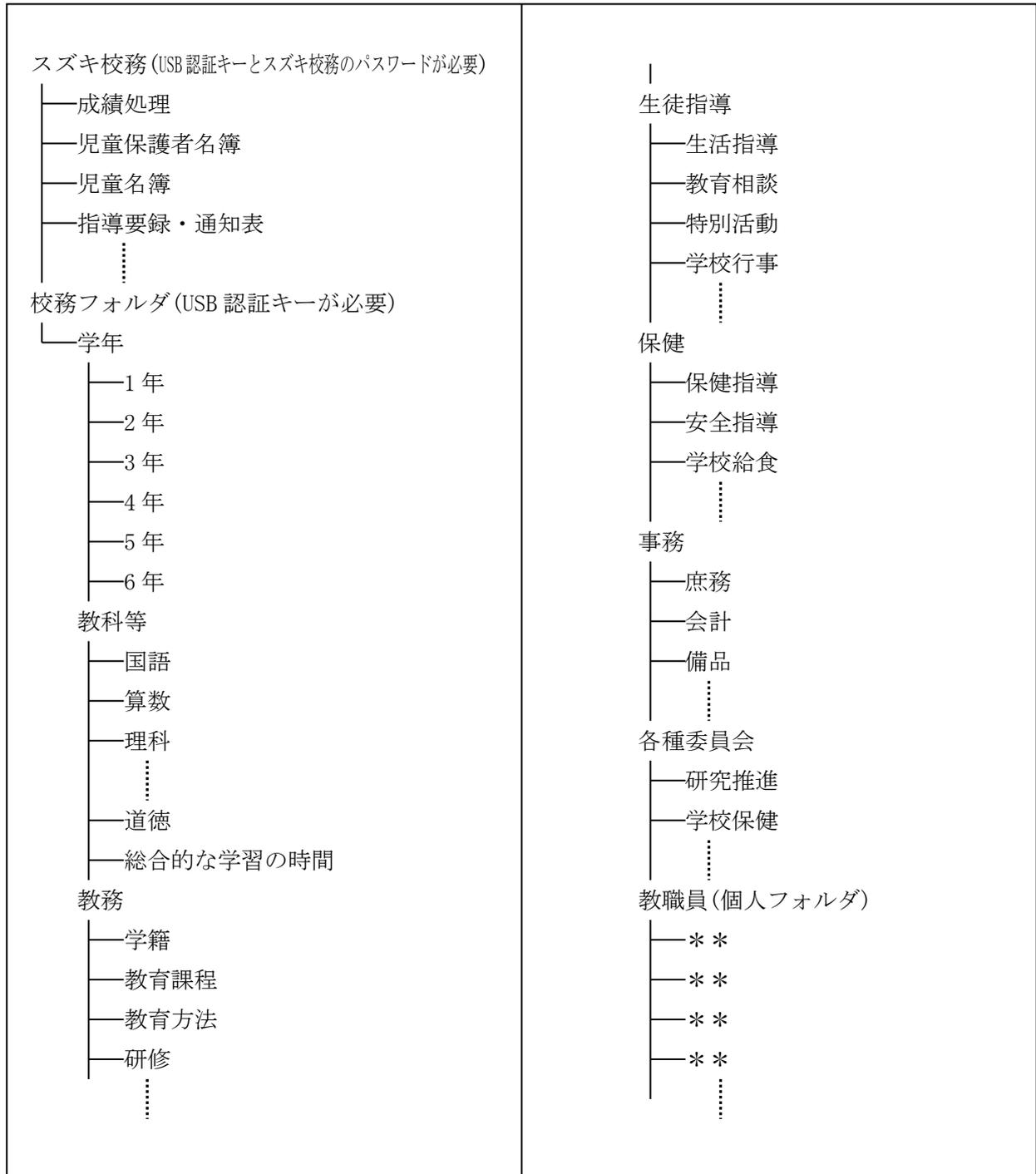
- コンピュータ室にタブレットパソコン（キーボード外付け）と教育用サーバコンピュータ、普通教室と特別教室には、児童用のパソコンは整備されていないが、移動式の教師用の教育用ノートパソコンと移動式のタブレットパソコンが数台整備されており、印刷室に校務用サーバコンピュータが整備されている。
- 全てのコンピュータは LAN(ローカルエリアネットワーク)で接続されており、コンピュータ室内のルータを通じて MCT ケーブルテレビ回線に接続されており、インターネット接続が可能である。ウイルス対策ソフトおよびフィルタリングソフトによりウイルス及び有害情報対策を行っている。

- 校内のすべてのコンピュータにはグループウェアソフト（霧島ネット）がインストールされており、校内でインターネット形式での情報通信が可能である。
- 校務サーバには、USB 認証システム Hard Lock 専用ハブを通じてコンピュータが接続されており、USB 認証キーを利用した場合のみ、校務サーバに接続して、個人情報や教育情報へアクセスできる。

3 電子データ情報資産の管理

(1) 霧島市立国分北小学校における教育情報として管理する電子データ情報は下記のとおりである。

※ HardLock y で管理する電子データには、スズキ校務による指導要録や成績や児童名簿等のデータと、校務フォルダ内の機密情報とその他の校務分掌のデータがある。



(2) 電子データの情報資産を取扱う手順と注意点

- ① 認証 USB キーを挿してパスワード(PIN 番号)を入力する。
スズキ校務を起動する際は、さらにスズキ校務のパスワードを入力する。
- ② 教育情報を保管する校務サーバの校務フォルダ (Z ドライブ) が見えるようになり、インターネット接続はできなくなる。
- ③ 教育情報の取扱いが終了したときには、認証 USB キーを抜くこと。
- ④ 教育情報の取扱いが途中であっても席を離れる場合は、認証 USB キーをぬくこと。または、画面ロックの操作 (ウインドウズキー+L) をする (パソコンの起動パスワードが児童に知られていないことが前提) こと。
- ⑤ 認証 USB キーを使用しないときは、机の引出しなど他人の目につかないところに保管すること。
- ⑥ 認証 USB キーを紛失した場合は、すみやかに情報管理者に報告する。

参考 USB キーの単価は、3 万程度

(3) 機密情報の取扱い方法

原則として機密情報に指定された電子データ情報は、認証 USB キーが必要な HardLocky で管理する指定されたフォルダにのみ保管する。紙媒体や電子データを印刷した書類は、鍵のかかる書庫・金庫に保管する。

各種取扱いについて具体的な遵守事項は次のとおりである。

機密情報の取扱い方法	電子データ	書類 (紙媒体)	注意事項
校外へのメール	原則禁止	/	添付する場合も含む。 ※インターネットメールは第三者に読まれてしまう可能性がある。
校内へのメール (グループウェア)	制限なし	/	教職員間に限る。
FAX 送信	/	禁止	※誤送信による情報漏えいを防ぐため
送付 (郵便・宅配)	受領が確認できる方法で送付すること	受領が確認できる方法で送付すること	※届いていない場合に追跡できるようにするため
保管	校務サーバの指定したフォルダに保管すること	鍵付きの書庫・金庫に保管すること	個人機器のハードディスクに保管することは禁止する。
保存媒体への保存	学校所有の媒体に保存し、鍵付きの書庫・金庫に保管する。	/	個人所有の保存媒体への保管は禁止する。
携行 (校外)	管理職の許可を得た上、必要最低限の情報だけを携行すること	管理職の許可を得た上、必要最低限の情報だけを携行すること	データを携行する場合は、データの暗号化もしくはパスワードをかけて保存すること。パソコン自体を携行する場合も同様とする。
コピー	バックアップコピーを除き原則禁止	原則禁止	

廃棄処分	物理的に破壊	シュレッダー処分	
------	--------	----------	--

(4) 機密情報以外の電子データ教育情報の取扱い

- ・ 授業で使う教材データ等の機密情報以外の電子データは、認証 USB キーが必要な Hard Locky で管理する指定されたフォルダでなく、校務サーバ内の共有教材フォルダに保存してもよい。一般に公開されていない情報については、取扱いに十分注意すること。
- ・ 個人機器に校務のデータを保存したままにせず、校務サーバに保存して情報資産として共有するようにする。
- ・ データの作成にあたっては、学校の情報資産として共有して多年度にわたり活用することを前提に、校内 LAN に導入されたソフトウェア（ワードやエクセル等）で作成し保存することとする。

4 校内 LAN の利用

- (1) 校務処理を行うコンピュータは、校内 LAN に接続されたコンピュータで行う。また、データは全て校務サーバの指定されたフォルダに保存する。個人機器の校内 LAN への接続は禁止。
- (2) 一時的に USB メモリ等の保存媒体を使用する場合は、ウイルス対応ソフトがインストールされているパソコンに限り使用できる。(USB メモリはデータ書き換え回数の上限や、衝撃や静電気によるデータの破壊、アクセス中の抜き差しによるデータの破壊等があるため、扱いには十分注意する。)
- (3) 校内 LAN の円滑な運用のため、メールのモニタリングや各種履歴(ログ)の調査を行う場合がある。
- (4) 校内で使用している個人機器や保存媒体について、監査を行う場合がある。

5 コンピュータウイルス対策

- (1) 校務処理を行う個人機器には、ウイルス対策ソフトをインストールするとともに、ウイルス対策ソフトは、常駐設定をし、パターンファイルを常に最新に保つこと。
- (2) メールに添付されてきたファイルは、安全性が確認できないものは原則として開いてはならない。
- (3) OS(Windows)には、最新のパッチを当てていること。

6 パスワード管理

- (1) 自己が利用しているパスワード・ID は、適切に管理する。
- (2) パスワードを入力するときは、児童や部外者から見られないように留意する。
※ パスワードは、記憶しておくことが基本であるが、忘れないよう記録する場合は、落としてしまうようなメモ用紙や付せんではなく、教務用ノート等に記録するようにする。

7 著作権の保護

- (1) 校内 LAN にインストールするソフトウェアは、正規のライセンスを有するものに限る。
- (2) 校内 LAN にソフトウェアをインストールする際は、事前に教育委員会に申請書を出し許可を得なければならない。借用、サンプル、フリーソフトの場合でも同様とする。

8 インターネット、メールの利用

- (1) インターネットの利用については、教育活動のための情報検索などに限定し、公私混同のないように注意すること。

- (2) メールの利用については、教育活動に限定し、職務上関係ないメールマガジンなどは許可しない。
- (3) 送信後にメールの取り消しはできないので、メールアドレスの入力には細心の注意を払い間違いないようにすること。
- (4) 複数へのメール送信時に、「キュート連絡網」を使用せずに、windows 付属メールソフト「Outlook express」を使用して複数の送信先に一斉送信する場合は、送信メールの送信先を「宛先」「Cc」を使用せずに「Bcc」を使用すること。
※ 「Bcc」では他の人のメールアドレスが送信されることはない。

9 注意事項

- (1) 長時間の離席時には、パソコンの電源を切るか、画面のロック、または、ログアウトすること。また、書類は伏せておくとともに、風で飛ばされたり落ちたりしないようにすること。
- (2) 認証 USB キーの取扱いには細心の注意を払い、紛失しないようにするとともに、使用しないときは、机の引出しなど他人の目につかないところに保管すること。

10 学校情報セキュリティ緊急時の対応

セキュリティポリシーに基づき、校内 LAN を運用していれば、トラブルが起こることは少ないと考えられるが、万一生じた場合の緊急時は、霧島市立国分北小学校教育情報セキュリティ緊急時対応計画の手順で対応する。