柏市教育情報セキュリティ対策基準に係る実施手順（学校版の抜粋）

柏市教育情報セキュリティ対策基準に係る実施手順（学校版）の項目は次のとおりです。

１　実施手順
２　教育情報セキュリティ管理者
３　情報管理者
４　教職員
５　教育情報ネットワーク環境
６　情報資産の分類と保管場所
７　情報資産の取扱い
８　情報の漏洩に対する対策
９　教育情報ネットワークへの外部からの脅威の侵入に対する対策
１０　１人１台端末の運用への対応
１１　１人１台端末の利用にあたり保護者等との間で確認・共有事項
１２　クラウドを利用した学習系および校務系のシステム利用
１３　Web 会議サービスの利用のための運用手順
１４　緊急時の対応
１５　法令等の遵守
１６　見直しの実施

アミカケ箇所は特に重要です。
重点的に確認してください。

この中で特に確認いただきたい,「６　情報資産の分類と保管場所」「７　情報資産の取り扱い」「８　情報の漏洩に対する対策」「９　教育情報ネットワークへの外部からの脅威の侵入に対する対策」について，抜粋し記載します。

６　情報資産の分類と保管場所

学校で取り扱う教育情報セキュリティにおける情報資産は, 対策基準の「３情報資産の分類と管理方法　(1)　情報資産の分類」で定められた重要性分類の定義に応じた保存場所に保存するものとする。重要性分類ⅠとⅡは必ず，校務系システム（クラウド校務支援システム，クラウドファイルサーバ（AZURE））に保存すること。

重要性分類Ⅰ Ⅱ以外の情報資産をインターネットによる外部ストレージ上に保存する場合は，教育委員会が契約しているクラウドストレージ又はクラウドファイルサーバのみとすること。

(1) 情報資産の重要性分類

ｱ. 重要性分類

Ⅰ セキュリティ侵害が教職員又は児童生徒及び保護者の生命，財産，プライバシー等へ重大な影響を及ぼす

Ⅱ セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす

Ⅲ セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす

Ⅳ 影響をほとんど及ぼさない

ｲ. 重要性分類ごとの情報資産の例示

■重要性分類Ⅰの情報資産の例示	
校務系	・指導要領原本 ・教職員の人事情報 ・入学者選抜問題 ・教育情報システム仕様書
学習系／公開系	該当なし
■重要性分類Ⅱの情報資産の例示	
校務系	○学籍関係 卒業証書授与台帳，転退学受付（整理）簿，転入学受付（整理）簿，就学児童・生徒異動報告書，休学・退学願等受付（整理）簿，教科用図書給付児童・生徒名簿，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 ○成績関係 通知表，評定一覧表，進級・卒業認定資料，定期考査・テスト等の答案用紙（児童・生徒が記入したもの），定期考査素点表，成績に関する個票等 ○指導関係 事故報告書・記録簿，生徒指導・特別指導等記録簿，児童・生徒等の個人写真・集合写真，指導記録・指導カード（児童・生徒等理解カード），教育相談・面接の記録・カード等，個別の教育支援計画（学校生活支援シート），個別指導計画，家庭訪問記録・個別面談記録，教務手帳，週ごとの指導計画（個人情報が含まれるもの） ○進路関係・調査書 推薦書，公立高校入学者選抜に係る成績一覧表，入学者選抜に関する表簿（願書等），私立高校入試に係る事前相談資料，卒業生進路先一覧等，進路希望調査，進路判定会議資料，進路指導記録簿 ○児童・生徒に関する個人情報 生活歴，心身の状況，財産状況等の情報，電話番号，メールアドレス，住所，生

	年月日，性別等の基本情報を含むもの ○学校教職員に関する個人情報 病歴，心身の状況，収入等の情報，メールアドレス，住所，生年月日，性別等の基本情報を含むもの ○健康関係 健康診断表，歯の検査表，心臓管理棟医療情報，学校生活管理指導票，児童・生徒等健康調査票，児童・生徒の健康保険等被保険者証の写，健康診断に関する表簿，就学時健康診断表 ○教職員に割り当てた機密性の高い情報 情報システムログイン ID/PW 管理台帳，情報端末ログイン ID/PW 管理台帳 ○その他 給食関係書類，寄宿関係書類，校内就学援助関係書類 ○名簿等 児童生徒名簿，保護者緊急連絡網，児童生徒の住所録，PTA 会員名簿，職員緊急連絡網・職員住所録，委員会名簿，PTA 役員連絡網 ○各種帳票ファイル 指導要領作成システム等，データの入っていない帳票
学習系／公開系	□学習系 ○児童生徒の学習系情報 学習システムログイン ID/PW 管理台帳，学習用端末ログイン ID/PW 管理台帳
■重要性分類Ⅲの情報資産の例示	
校務系	○児童生徒の氏名 出席簿，名列表，座席表，児童生徒役員会名簿帳 ○学校運営関係 卒業アルバム，学校行事等の児童・生徒の写真
学習系／公開系	□学習系 ○学校運営関係 授業用教材，生徒用配布プリント ○児童生徒の学習系情報 児童生徒の学習記録（確認テスト，ワークシート，レポート，作品等），・学習活動の記録（動画・写真等）
■重要性分類Ⅳの情報資産の例	
校務系	
学習系／公開系	□公開系 ○学校運営関係 学校・学園要領，学校紹介パンフレット，使用教科書一覧，教育課程編成表，学

	校設定科目の届出書，特色紹介冊子原稿，学校徴収金会計簿，学校行事実施計画，保護者への配布文書文例，各種届雛形，校務分掌表，PTA 資料，学園・学校・学年・学級だより，学校・学園ホームページ掲載情報，学校行事のしおり ○学校活動の記録（保護者の承諾がある場合，以下は公開可能） 学校行事等の児童生徒の写真，学習活動の記録，動画・写真・作品等）

(2) 重要性分類ごとの情報資産の保管場所

◎　主として保管する場所
○　保管しても良い場所
×　保管が禁止される場所
－　該当なし

重要性分類	Ⅰ		Ⅱ		Ⅲ		Ⅳ	
	校務	－	校務	学習	校務	学習	－	公開
クラウド校務支援システム	◎	－	◎	◎	◎	○	－	○
クラウドファイルサーバ（AZURE）	○	－	○	○	○	○	－	○
Office，　Teams	×	－	×	×	○	○	－	○
NAS	×	－	×	×	○	○	－	○
OneDrive	×	－	×	×	○	○	－	○
学校契約クラウドサービス	×	－	×	×	－	○	－	○
学校公開 Web サーバ	×	－	×	×	×	×	－	◎
Google workspace（Google 学習アプリ等）	×	－	×	×	○	◎	－	○

7　情報資産の取扱い

(1) 組織内部の定義

情報資産を，組織内部から外部に持ち出す場合は重要性分類に従った規定に従うこと。組織内部とは，校務系ネットワーク（別添資料２）で示される以下の範囲とする。

- 校務用端末
- クラウド校務支援システム
- クラウドファイルサーバ（AZURE）
- Microsoft Office365
- NAS
- 学校契約クラウドサービス
- 学校公開 WEB サーバ

(2) 重要性分類Ⅰ及びⅡの取扱い

重要性分類Ⅰ及びⅡのデータは，原則として組織内部から外部への持ち出しを禁止する。業務上の必要性により外部へ持ち出す場合は，規定の手続きによること。

重要性分類Ⅰ又はⅡでない情報であっても個人情報が含まれる場合は，重要性分類Ⅰ又はⅡに準じた取扱いとすること。

ｱ. 複製・配布にあたっては必要以上の複製及び配布を禁止する。

ｲ. 必要に応じ本校外に情報を持ち出す際には，対策基準を準拠していることを確認した上で，教育情報セキュリティ管理者（校長）の判断で持ち出しを可能とする。

原則，情報をメール等で本校外へ送信してはならない。用意されたク　ラウドストレージ等を利用すること。

(3) 重要性分類Ⅲの取扱い

重要性分類Ⅲのデータは，児童生徒の名簿や学校運営関係の情報であり，組織内部から外部への持ち出し等の運用は教育情報セキュリティ管理者（校長）の包括的承認で可とする。ただし児童生徒の写真等に関する個人情報を含む場合は，保護者の承諾を得るなど慎重な取り扱いが求められる。

(4) 重要性分類Ⅳの取扱い

重要性分類Ⅳのデータは，学校から保護者等一般に公開している情報であり，一般の公開を可とする。ただし児童生徒の写真等に関する個人情報を含む場合は，保護者の承諾を得るなど慎重な取り扱いが求められる。

８　情報の漏洩に対する対策

情報資産の持ち出しは，情報の漏えいに対し十分な注意を払うこと。

(1) 委員会公用 USB による持ち出し

ｱ. 原則，USB フラッシュメモリによる情報の持ち出しは避ける。ただし，教職員が，職務遂行の必要性により，本校の個人情報を含む情報を止むを得ず本校外に持ち出す場合には，教育委員会が貸与する公用 USB フラッシュメモリ（以下「委員会公用 USB」という。）を使用しなければならない。

ｲ. 委員会公用 USB は，施錠可能な場所に保管するものとし，持ち出しの際には，次に掲げる手続を経なければならない。

① 持ち出す個人情報について，あらかじめ校長の許可を得ること。

② 記録簿等にその記録を残すこと。

③ 委員会公用 USB に情報を格納する際は，パスワードをかけ，及び情報（データ）の暗号化等を行い，情報漏洩への対策を施すこと。

ｳ. 委員会公用 USB を使用した教職員は，使用終了後直ちに委員会公用 USB を次に掲げる手順により返却しなければならない。

① 使用した委員会公用 USB に格納した情報を消去すること。

② 消去を教育情報セキュリティ管理者（校長）と共に確認すること。

③ 記録簿等に記録すること。

ｴ. 委員会公用 USB を含む外部記録媒体等をやむを得ず修理等により本校外に持ち出す場合は，電子情報を消去し，記録簿により管理するものとし，電子情報の消去が難しい場合は委託業者に対し秘密を守ることを契約に定めなければならない。

ｵ. 委員会公用 USB を含む外部記録媒体等を処分する場合，当該媒体に含まれる電子情報は，初期化又は専門業者に委託するなどして復元できない措置を取ったうえで廃棄するものとする。

(2) 電子メールでの持ち出し

重要性分類Ⅰ及びⅡの情報を外部送信する際には，必要に応じクラウド上の共有ドライブで適切なアクセス権限を設定し，そのリンクを送信する方法で行うこと。

(3) 印刷等での持ち出し

重要性分類Ⅰ及びⅡの情報を印刷又は FAX する場合，印刷物は物理的な暗号化が困難であり，FAX による送信も受信トレイに放置されるなど，不特定多数の目に触れる可能性が高いため，利用後の処理は 2 人体制でお互いにチェックしながら行うなど，特に留意して適切な管理を行うこと。

9　教育情報ネットワークへの外部からの脅威の侵入に対する対策

教育情報ネットワークは，サーバ・ネットワーク・利用端末にそれぞれセキュリティ対策を講じ，外部からの脅威の侵入を総合的に防御している。教職員は，教育情報ネットワークへのマルウェア感染防止の対策について理解し遵守しなければならない

マルウェアの不安があるとき，ソフトウェア「ApexOne」を使って調べることができます。最後の【別添資料】をご参照ください。

(1) 端末の管理

1. 教育情報ネットワーク内のネットワークに接続できる装置は，原則として教育員会が導入した，校務用の端末及び NAS，プリンターのみとする。
2. 学校の購入によるプリンタ，チャイム等（以下「各学校購入プリンタ等」という。）を教育情報ネットワーク内のネットワークに接続する際には，教育情報セキュリティ責任者の許可を得なければならない。この場合において，教育委員会への申請を行うとともに教育委員会からの指示に従い接続者負担によるセキュリティソフトの導入等，教育委員会整備パソコン等の設定と同等のセキュリティ対策を行うこと。
3. 教育委員会整備パソコン等又は各学校購入パソコン等以外の職員個人のパソコン，モバイル端末（以下「個人所有パソコン等」という。）を教育情報ネットワーク内のネットワークに接続することを禁止する。
4. 教育委員会整備パソコン等に，ファイル共有ソフト及び同様の外部とのデータを同期するソフトをインストールし，教育情報ネットワーク内のネットワークに接続することを禁止する。
5. 教育委員会整備パソコン等の各学校外への持ち出しは，公務での利用に限り，委員会公用 USB の持ち出しに準じ，あらかじめ教育情報セキュリティ管理者（校長）の許可を得て行わなければならない。
6. 教育委員会整備パソコン等及び各学校購入パソコン等の設定及び設置場所の変更を行わないこと。それらの設定及び設置場所の変更を行う場合は教育委員会への申請を行い，教育情報セキュリティ責任者の許可を得ること。
7. 職員は，原則として事前の申請がない場合は，教育委員会整備パソコン等及び各学校購入パソコン等に無許可ソフトウェアを導入してはならない。ただし，業務上やむを得ない緊急の場合は事後申請を行うものとする。
8. 職員は，業務用の必要がある場合は，統括教育情報セキュリティ責任

者及び教育情報システム管理者の許可を得て，ソフトウェアを導入することができる。なお導入する際は，教育情報セキュリティ管理者（校長）は，ソフトウェアのライセンスを管理しなければならない。

9. 職員は，不正にコピーしたソフトウェアを利用してはならない。

(2) 各種パスワードの管理

ｱ. パスワードは秘密にし，他人に教えたり他人の目にふれたりしないよう，管理を徹底すること。

ｲ. パスワードは十分な長さとし，文字列は想像しにくいものにしなければならない。

ｳ. パスワードが流出したおそれがある場合には，教育情報セキュリティ責任者及び教育情報セキュリティ管理者（校長）に速やかに報告し，パスワードを速やかに変更しなければならない。

(3) コンピュータウィルスへの対応

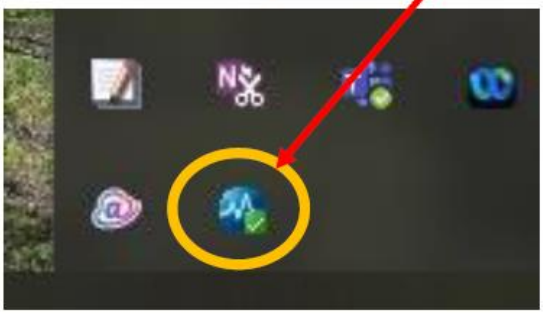
ｱ. 教育委員会整備パソコン等及び各学校購入パソコン等は，最新のセキュリティ対策ソフトウェアが導入され，最新のセキュリティ対応状況に更新されていなければならない。セキュリティ対策ソフトウェアによりセキュリティ検査を定期的に実施し，異常がある場合は，直ちに利用を停止し，情報管理者（教頭）に報告しなければならない。

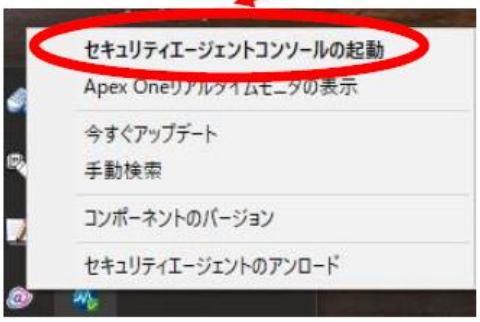
ｲ. 委員会公用 USB を個人所有パソコン等に接続する場合は，接続する個人所有パソコン等は最新のセキュリティ対策ソフトウェアが導入されており，また，OS，ソフトウェアを最新のセキュリティ対応状況に更新しておかなければならない。

【別添資料】マルウェアの不安があるときの ApexOne の利用

R5,4,11

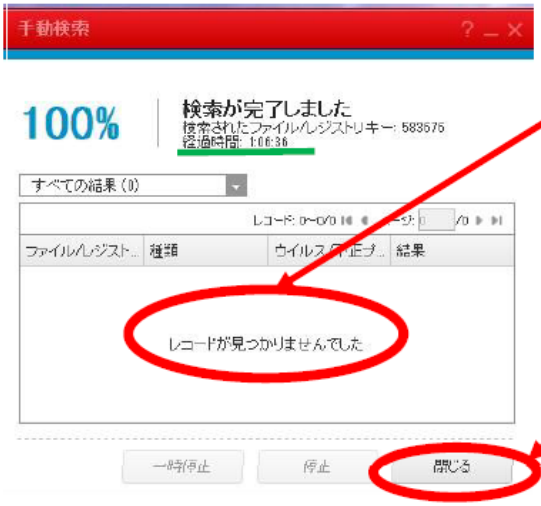
1 タスクトレイの △ をクリックして 「ApexOne」のアイコンを右クリックし、「セキュリティエージェントコンソールの起動」 を選びます。





2 コンソールで、「検索」を選び、検索するフォルダで「マイコンピュータ」 を選び、「検索」を開始します。

3 終了まで待ちます。



この場合　1 時間 6 分かかっています。

レコードに、何か表示されれば、マルウェアが検知されていますので、その内容をお知らせください

何もなければ「閉じる」で終了します。