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）

（令和６年４月）

柏市教育委員会 指導課

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）

目次

１　実施手順

学校（柏市立小学校，中学校，高等学校。以下同じ。）において，柏市教育情報ネットワーク（以下「教育情報ネットワーク」という。）を利用するにあたり，柏市教育情報セキュリティ対策基準（以下「対策基準」という。）に従い，情報セキュリティ対策を実行するために，各教職員が行動する手順（以下「本実施手順」という。）を定める。

柏市では，GIGA スクール構想を受け，柏市 GIGA スクールとして１人１台の端末及び高速大容量の通信環境の整備を含めた柏市教育情報システムの再構築を行ったところである。

今後積極的な活用を進めるためには，安全で安心な情報教育システムの運用が要であり，セキュリティ対策を講じる必要がある。

本実施手順の策定にあたっては，GIGA スクール構想の下で整備された１人１台端末の運用への対応，および GIGA 端末が持ち帰りにより積極的に活用される観点から １ 人 １ 台端末の利用にあたり保護者等との間で確認・共有すべき事項も規定する。

２　教育情報セキュリティ管理者

⑴ 任免

教育情報用ネットワークを利用する各学校長を，教育情報セキュリティ管理者とする。

⑵ 責任

ｱ. 教育情報セキュリティ管理者（校長）は，各学校の教育情報セキュリティ対策に関する権限と責任を有する。

ｲ. 教育情報セキュリティ管理者（校長）は，当該学校において，情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合は，教育情報セキュリティ責任者，統括教育情報セキュリティ責任者及び CISO へ速やかに報告を行い，指示を仰がなければならない。

３　情報管理者

⑴ 任免

ｱ. 情報管理者は，教育情報用ネットワークを利用する各学校の副校長又は教頭をもって充てる。

ｲ. 情報管理者（副校長又は教頭）は，教育情報セキュリティ管理者（校長）が不在の場合，その職を代わって務めることができる。

⑵ 責任

ｱ. 情報管理者（副校長又は教頭）は，教育情報セキュリティ管理者（校長）を補佐し，教育情報用ネットワーク内における教育情報セキュリティに関する連絡体制を構築する。

ｲ. 情報管理者（副校長又は教頭）は，教育情報用ネットワーク内において教育情報セキュリティ対策を講ずるものとし，情報資産に対する侵害や情報漏洩，又はそのおそれがある場合は，教育情報セキュリティ管理者（校長）へ速やかに報告し，指示を受けなければならない。

ｳ. 情報管理者（副校長又は教頭）は，定められた研修に参加し教育情報セキュリティについての最新情報を把握・習得するものとする。

ｴ. 情報管理者（副校長又は教頭）は，職員に対して実施する研修等を通じて習得した最新情報を提供し，啓発を行うものとする。

4　教職員

教職員は，研修等を通じ教育情報セキュリティに関する事項を理解し，教育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。教職員は情報セキュリティに関する意識を高め，教職員一人一人が重要な情報資産を扱っているという意識を持つこと。

5　教育情報ネットワーク環境

柏市 GIGA スクールにおける学習系ネットワークと校務系ネットワークをそれぞれ下記及び別添資料１及び２に示す。

(1) 学習系ネットワーク（別添資料１）

- 学習者用端末：iPad 及び Chromebook
- 教師端末：iPad 及び Chromebook
  家庭など学校外に持ち帰って使う場合のネットワークの利用の違いについては別添資料１を参照
- アクセスポイント：WiFi アクセスポイント，各教室に設置され学習者用端末が接続する無線 LAN 用の装置
- コンテンツフィルタリング：校内で使用するときや，学習者用端末を持ち帰り学習するときにコンテンツフィルタリングを通してインターネットに接続される。インターネットとの間でやり取りされる情報を監視し，許可されていないウェブサイトへの接続を防止する
- Google 学習系アプリ：Google の学習用クラウドサービス。Google Drive，Classroom など。

(2) 校務系ネットワーク（別添資料２）

- 校務用端末：校務系ネットワークに接続可能な校務系業務に使用する

端末は，原則，教育委員会が導入した，登録され認証を経たパソコン，モバイル端末，プリンタ，のみとする。

- NAS：学校に設置される校務系ネットワーク接続ファイルサーバ
- LAN：学校内に敷設されている有線 LAN
- クラウド校務支援システム
- クラウドファイルサーバ（校務系サーバ）
- デジタル採点システム
- Microsoft365 のアカウントで使用できるものなど
- 学校契約クラウドサービス：教育委員会の承認のもと学校が個別に利用するクラウドサービス
- 学校公開 HP：学校ごとに公開している HP
- コンテンツフィルタリングリスクサイトへのアクセス利用

(3) 学習系ネットワークと校務系ネットワークの共通部分

- L2 スイッチ，L3 スイッチ：学校内の LAN ネットワーク装置
- ルータ，ONU：WAN 接続用ルータ，光回線終端装置
- WAN：１Gbps 帯域網，教育委員会が契約する広域ネットワーク
- DC：データセンタ。教育委員会が契約する GIGA スクール用のデータセンタ。DC 内のファイアウォールから SINET に接続され，SINET からインターネットに接続される

(4) 学習系ネットワークから校務系ネットワークへのアクセス

学習系ネットワーク上の学習者用端末から校務系ネットワークへのアクセスはできない構造となっている。校務系ネットワーク上の校務用端末から学習系ネットワークへのアクセスは，クラウドサービスに対してアカウントを有している場合はアクセスできる

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「２情報資産の分類」で定められた重要性分類の定義に応じ，対策基準の「３　情報資産の管理」で定められた保存場所に保存するものとする。

重要性分類Ⅰ・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（校務系サーバ），デジタル採点システム）に保存すること。

重要性分類Ⅲ・Ⅳの情報資産を紙媒体ではなくデータで保存する場合は，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。ただし，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。

(1) 情報資産の重要性分類

ｱ. 重要性分類

重要性分類
Ⅰ セキュリティ侵害が教職員又は児童生徒の生命，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	情報資産の例示
Ⅰ	【校務系】 ・指導要録原本 ・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】 該当なし 【公開系】 該当なし
Ⅱ	【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

Ⅱ	○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，それを教師が採点したもの） ・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

Ⅱ	○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，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） ○健康関係 ・健康診断表 ・歯の検査表 ・心臓管理等医療情報 ・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 ○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 ・指導要録作成システム等，データの入っていない帳票

Ⅱ	【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 【公開系】 該当なし
Ⅲ	【校務系】 ○児童生徒の氏名 ・出席簿 ・各列表 ・座席表 ・児童生徒委員会名簿 ○学校運営関係 ・卒業アルバム ・学校行事や部活動の児童・生徒の写真 【学習系】 ○学校運営関係 ・授業用教材 ・教材研究資料 ・生徒用配付プリント ○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，学習中の助言等） ・授業内の学習活動の記録（動画，写真等） 【公開系】 該当なし

Ⅳ	【校務系】 該当なし 【学習系】 該当なし 【公開系】 〇学校運営関係 学校紹介パンフレット，PTA 資料など 〇学校活動の記録 ※保護者の承諾がある場合，以下は公開可能 ・学校行事や部活動の児童・生徒の写真や動画 ・授業内の学習活動の記録

(2) 重要性分類ごとの情報資産の保管場所

市が導入している基本的なシステムやサービスごとに，保存して良い情報資産は決められている。次の表を参考に，適切な場所で情報資産を扱うこと。

	重要性分類	Ⅰ	Ⅱ	Ⅲ	Ⅳ
校務	クラウド校務支援システム	〇	〇	〇	〇
	クラウドファイルサーバ （校務系サーバ）	〇	〇	〇	〇
	デジタル採点システム	×	〇	〇	×
	Microsoft365のアカウントで使用するもの （例：teams,Forms,One Drive,Outlook, Word,Excel,PowerPoint）	×	×	〇	〇
	NAS（学校内設置，動画・画像専用）	×	×	〇	〇
	学校が契約したクラウドサービス	×	×	×	〇
	学校公開 Webサーバ	×	×	×	〇
授業	Google workspace	×	×	〇	〇

7　情報資産の取扱い

(1) 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（校内や，市が契約している重要性分類Ⅰ・Ⅱを取り扱うことができると定めるシステムやサービス内も含む）から外部へ（内部で定義した範囲外）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Ⅲ・Ⅳの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。
ただし，バックアップのための複製は可とする。

ｲ. 必要に応じ学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。

(2) 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，利用目的を保護者に示し，利用目的以外に使用しないことを定めた上で保護者の承諾を得るなど慎重な取り扱いが求められる。

(3) 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，利用目的を保護者に示し，利用目的以外に使用しないことを定めた上で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・Ⅱと指定がありましたが削除）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。FAX による情報送信は，限定されたアクセスの措置（アクセス制限や通信経路の暗号化）が不可能であること，FAX による誤送信のリスクがあることから，送信相手が FAX 受信を指定してきた場合のみ利用することが望ましい。

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

(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，原則として教育委員会が導入した，校務用・学習用の端末及び 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。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が，個人で購入したもの，法人ではなく個人で契約する個人アカウントの使用は禁止する。
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。

１０　１人１台端末の運用への対応

１人１台端末の円滑な運用に向けて，教育情報セキュリティ管理者（校長）及び情報管理者（教頭）は，下記事項について確認しなければならない。

ｱ. GIGA スクール構想で整備される端末の管理台帳に基づき，問合せ先，管理・運用上のルールを明確に示しておくこと。

ｲ. 共同作業において円滑にクラウドサービスを利用できるよう，発行されたアカウント（ID）を正しく管理すること。

ｳ. 学校等において，ICT 端末とインターネットが効率的かつ安全・安心に活用されるよう準備すること。

ｴ. １人１台端末を活用することの意義やその方法・留意点等について，教職員への研修や家庭・保護者等への情報提供を十分に行うこと。

ｵ. 学校や教師が孤立しないよう，１人１台端末の活用を含む教育の情報化を推進するための組織・支援体制を構築すること。

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

１人１台端末を積極的に活用していく観点から，児童生徒が安心して端末を使用できるようにするため，教育情報セキュリティ管理者（校長）及び情報管理者（教頭）は，下記事項について保護者等との間で啓発・共有しなければならない。

ｱ. 児童生徒が端末を扱う際のルール

ｲ. 健康面への配慮

ｳ. 端末・インターネットの特性と個人情報の扱い方

ｴ. トラブルが起きた場合の連絡や問合せ方法の情報共有の仕組み

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

(1) クラウドサービスの利用

学校が学習内容の補強，又は保護者等外部とのコミュニケーションの推進の一環としてクラウドサービスを利用する場合は，対策基準 9 項クラウドサービスの利用に従い，教育情報セキュリティ責任者の承認により利用する。

ｱ. クラウド事業者の選定にあたっては，第三者認証等の安全性など，クラウド事業者の情報セキュリティの実態が確認できる資料等をクラウド事業者から徴収し，教育情報セキュリティ責任者に報告すること。

ｲ. クラウドサービスの利用にあたっては，クラウド事業者に当該クラウドサービスのログインに関わる認証機能の提供を求め，サービス提供定款又は契約書面上で確認又は合意すること。

(2) 重要性Ⅰ・Ⅱの情報を扱うクラウドを利用した校務系システムの利用

ｱ. 教職員がクラウドを利用した校務系システムにアクセスする場合は，校務系ネットワークに接続された校務用端末から利用しなければならない。

ｲ. 教職員が，ｱの方式以外の方式で校務系システムにアクセスする場合は，教育委員会により校務系システムへのアクセスを可能とした認証方式を備えたパソコンを利用しなければならない。

１３　Web 会議サービスの利用のための運用手順

Web 会議サービスを利用する場合は，以下の運用手順による。

(1) 教育情報セキュリティ責任者による Web 会議サービスの指定

ｱ. 教育情報セキュリティ責任者は，推奨利用する Web 会議サービスを指定する。教職員等は，可能な限り指定された Web 会議サービスを利用する。

ｲ. 教育情報セキュリティ責任者は，Web 会議サービスを指定するにあたり，重要性分類Ⅲ以上の情報を取り扱うことを前提にエンドツーエンド（E2E）の暗号化を備えたサービスを指定する。

ｳ. 教育情報セキュリティ責任者は，教職員に対して，重要性分類Ⅲ以上の情報を取り扱う場合は，E2E の暗号化が適用されない機能（例えば議事録作成機能，自動翻訳機能等）については可能な限り使用しないことを勧告する。

(2) 教職員等によるサービスを利用するにあたっての運用手順

ｱ. 原則として，教育委員会が導入した端末を利用すること。

ｲ. 利用する Web 会議サービスのソフトウェアが最新の状態であることを確認すること。
ｳ. 音声を扱う場合は，ヘッドホンを使用するなど，内容が周囲に漏れないよう注意すること。
ｴ. 教職員等は，Web 会議を主催する場合，会議に無関係の者が参加できないよう，会議室にアクセスするためのパスワード等をかけると伴に，会議の参加者にパスワード等を通知する際は第三者に知られないよう安全な方法で通知すること。
ｵ. 教職員等は，Web 会議が相手側からの招待で実施される場合には，原則として重要性分類Ⅲ以上の情報を当該 Web 会議で取り扱わないこと。

１４　緊急時の対応

(1) 教育情報セキュリティ管理者（校長）及び情報管理者（教頭）は，次の緊急時案が発生した場合は，直ちに教育情報セキュリティ管理者（校長）を通じて教育情報セキュリティ責任者に報告し，その指示に従わなければならない。
ｱ. 教育情報セキュリティ管理者（校長）又は情報管理者（副校長又は教頭）が，情報資産の漏えいの恐れがある，又は漏えいしたと認知した時。
ｲ. 教職員等から，情報資産の漏えいの恐れがある，又は漏えいしたとの通知を受けたとき。
ｳ. 住民等外部から，教職員を通じ又は直接，情報資産の漏えいの恐れがある，又は漏えいしたとの通知を受けたとき。

(2) 教育情報セキュリティ管理者（校長）及び情報管理者（副校長又は教頭）は，次の緊急時案が発生し，情報資産の防護のためにネットワークの切断が必要な場合は，ネットワークを切断する措置を講ずるものとし，直ちに教育情報セキュリティ管理者（校長）を通じて教育情報セキュリティ責任者に報告し，その指示に従わなければならない。
ｴ. 異常なアクセスが継続しているとき又は不正アクセスが判明したとき。
ｵ. コンピュータウィ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。
ｶ. 委員会公用 USB を紛失したとき。
ｷ. その他情報資産に係る重大な被害が想定されるとき。

(3) 教育情報セキュリティ管理者（校長）及び情報管理者（副校長又は教頭）は，緊急時案に係る証拠保全を実施するとともに，当該事案の分析と再発

防止にための暫定措置，日頃発生するアラート等の対応について検討するものとする。

１５　法令等の遵守

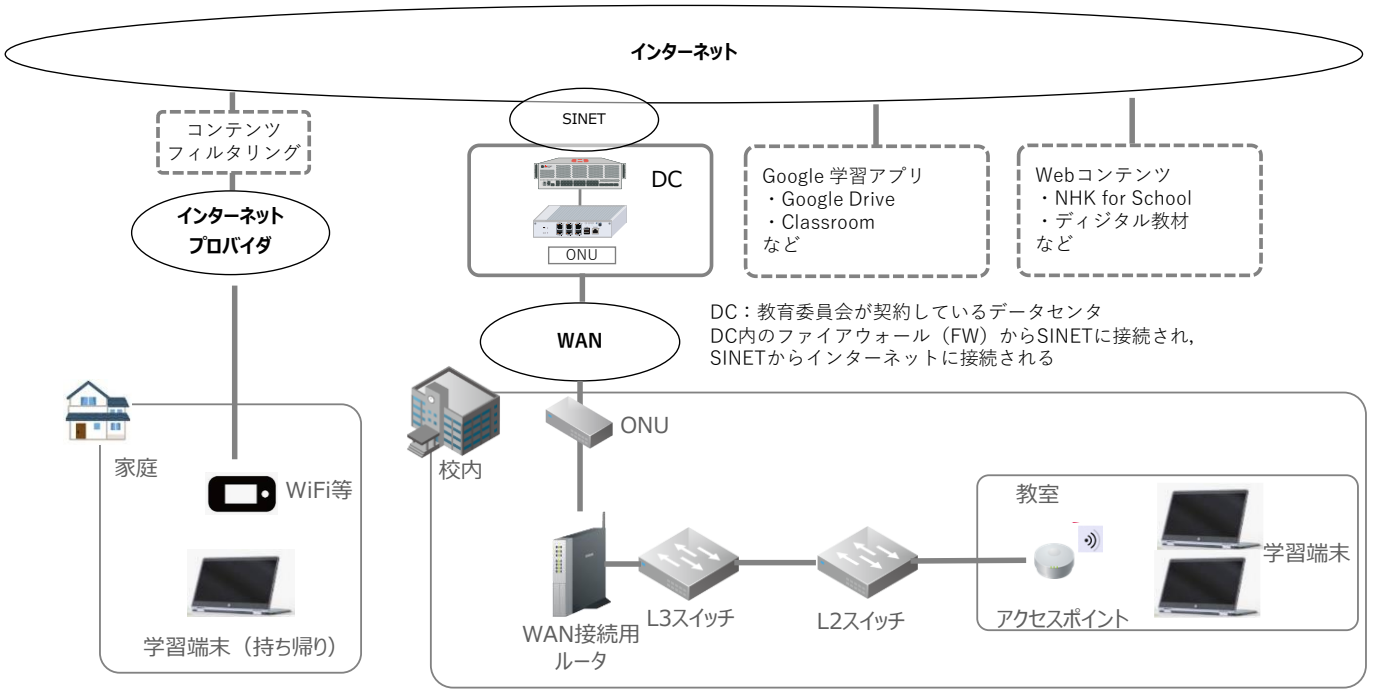
利用者は，職務上使用する情報資産について，不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号），著作権法（昭和 45 年法律第 48 号），千葉県個人情報保護条例（平成 5 年千葉県条例第 1 号），柏市電子計算機処理に係る個人情報保護条例８平成 16 年柏市条例第 11 号），その他関係法令を遵守しなければならない。

１６　見直しの実施

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，本基準の見直しを適宜行うものとする。

別添資料１

■GIGAスクール　学習系ネットワーク

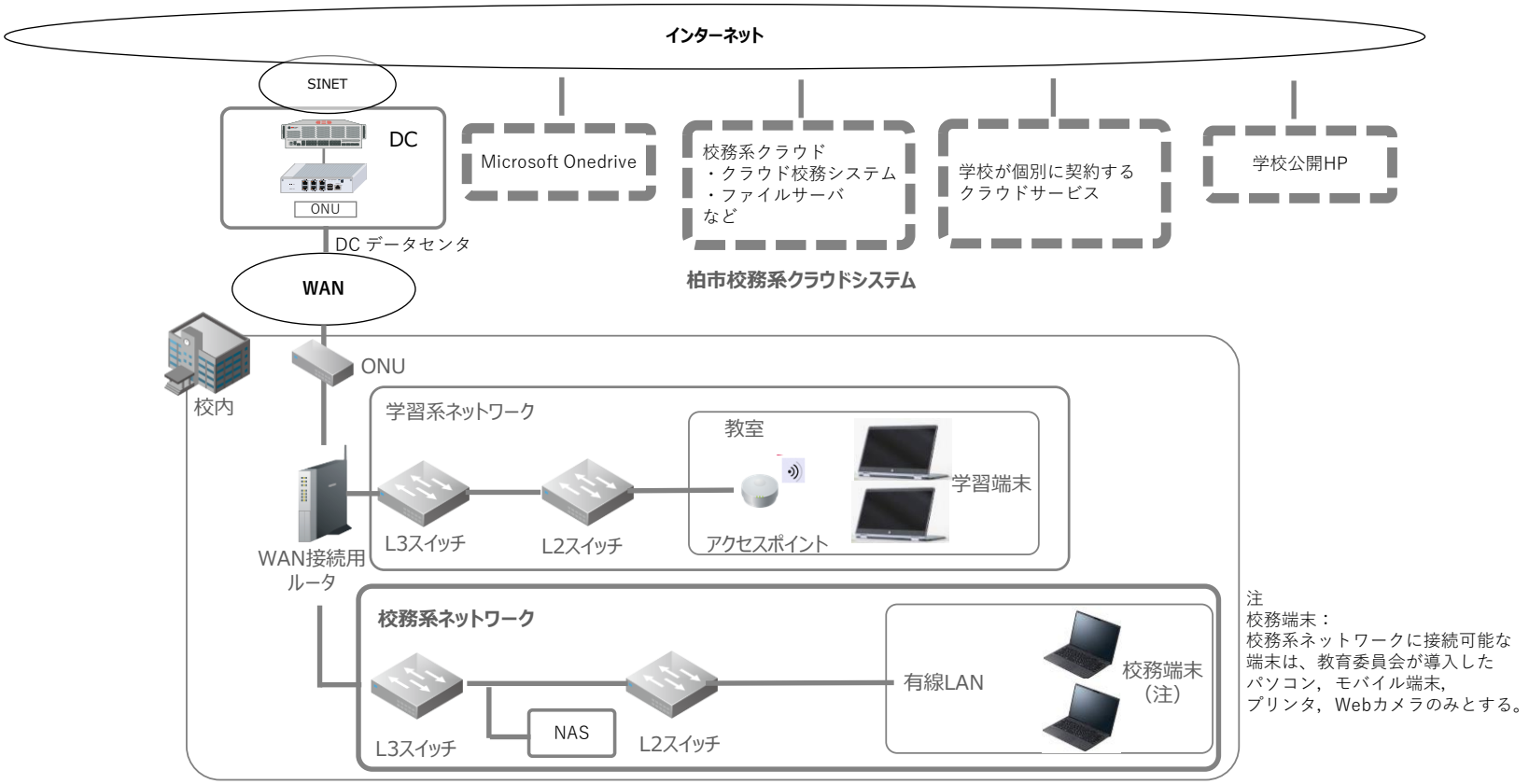


WiFi等：
家庭にネットワーク環境がない場合は教育委員会が準備した
モバイルルータを貸与して持ち帰り学習をする

コンテンツフィルタリング；
インターネットとの間でやり取りされる情報を監視し、
許可されていないウェブサイトへの接続を防止する

別添資料２

■GIGAスクール　校務系ネットワーク　（WAN及びDCは学習系ネットワークと共同利用）



注
校務端末：
校務系ネットワークに接続可能な
端末は、教育委員会が導入した
パソコン，モバイル端末，
プリンタ，Webカメラのみとする。