令和7年7月定例教育委員会議案

中津市教育委員会

令和7年7月定例教育委員会提出案件

（令和7年7月25日提出）

（議案事項）

議第24号

津民小学校廃校に伴う関係条例及び規則の改正について

上記について、別紙のとおり提案いたします。

令和7年7月25日提出

中津市教育委員会

教育長　古　口　宣　久

小学校の設置に関する条例の一部改正する条例の概要

１一部改正の理由

児童数の減少に伴い地元から中津市立津民小学校閉校についての要望書が提出され、令和７年６月の臨時教育委員会に於いて同校の閉校が承認されたことにより、同校を廃校（城井小学校への統合）とするため。

２一部改正の内容

別表中津市立津民小学校の項を削る。

３施行期日

令和８年４月１日

【参考】

○津民小学校の現況（R7.5.1 現在）

・位　　置　　中津市耶馬溪町大字大野 1072 番地２
・設 立 年　　明治７年　大野校舎（初等小学校）創設
・学校長名　　山香　昭
・施設概要　　校地面積 12,303 ㎡(うち学校敷地 4,008 ㎡、運動場 4,703 ㎡)
・児童・学級数　　２人・１学級（複式 1 学級 3･6 年）
・児童・学級数の推移

年度	H17	H18	H19	H20	H21	H22	H23	H24	H25	H26
児童数	31	29	28	21	19	14	18	16	17	19
学級数	4	4	4	4	4	4	4	4	4	4
複式	2	2	2	2	2	2	2	2	2	2

年度	H27	H28	H29	H30	R1	R2	R3	R4	R5	R6
児童数	18	16	10	5	5	5	3	3	3	3
学級数	4	3	3	3	3	3	2	2	2	2
複式	2	2	2	1	1	1	1	1	1	1

○城井小学校の現況（R7.5.1 現在）

・位　　置　　中津市耶馬溪町大字平田 1399 番地
・設 立 年　　明治８年　平田小学校　開設
・学校長名　　山口　善子
・施設概要　　校地面積 11,382(うち学校敷地 6,431 ㎡、運動場 4,951 ㎡)
・児童・学級数　　２９人・４学級（複式 2 学級 2･3 年、4･5 年）

議第　　号

小学校の設置に関する条例の一部改正について

小学校の設置に関する条例の一部を改正する条例を次のように定める。

令和　７年　８月２６日提出

中津市長　　奥　　塚　　正　　典

記

小学校の設置に関する条例の一部を改正する条例

小学校の設置に関する条例（昭和３９年中津市条例第２６号）の一部を次のように改正する。

別表中津市立津民小学校の項を削る。

附　則

この条例は、令和８年４月１日から施行する。

説　明

中津市立津民小学校を廃校するため、本案のように改正いたしたく提出する。

新旧対照表

○小学校の設置に関する条例

<table>
<tr><th>改正後</th><th>改正前</th></tr>
<tr><td>別表（第２条関係）<table><tr><th>名称</th><th>位置</th></tr><tr><td>略</td><td>略</td></tr><tr><td colspan="2">（削る。）</td></tr><tr><td>略</td><td>略</td></tr></table></td><td>別表（第２条関係）<table><tr><th>名称</th><th>位置</th></tr><tr><td>略</td><td>略</td></tr><tr><td>中津市立津民小学校</td><td>中津市耶馬溪町大字大野1072番地２</td></tr><tr><td>略</td><td>略</td></tr></table></td></tr>
</table>

中津市立学校管理規則等の一部改正する規則の概要

１．一部改正の理由

津民小学校の廃校（城井小学校への統合）に伴い、関係規則の一部改正をおこなうもの。

２．一部改正の内容

○中津市立学校管理規則（第１条）

・第１学校支援センターが管轄する学校から、津民小学校を削るもの。

○中津市立小・中学校通学区域設定規則（第２条）

・城井小学校の通学区域に、津民小学校の通学区域（耶馬溪町大字栃木（うち小川内を除く。）耶馬溪町大字中畑　耶馬溪町大字大野　耶馬溪町大字川原口）を加えたものに改め、津民小学校の通学区域を削るもの。
・耶馬溪中学校の通学区域から津民小学校通学区域を削るもの。
・併せて小学校通学区域の文言の修正を行うもの。

○中津市立学校体育施設の開放に関する規則（第３条）

・学校施設の開放を行う学校から津民小学校を削るもの。

○中津市立学校給食共同調理場管理規則（第４条）

・本耶馬渓共同調理場が管轄する学校から津民小学校を削るもの。

３．施行期日等

令和８年４月１日

中津市立学校管理規則等の一部を改正する規則をここに公布する。

令和７年　　月　　日

中津市教育委員会

中教規則第　　号

中津市立学校管理規則等の一部を改正する規則

（中津市立学校管理規則の一部を改正する規則）

第１条　中津市立学校管理規則（昭和３３年中教規則第１号）の一部を次のように改正する。

別表第３連携校の欄中「中津市立津民小学校」を削る。

（中津市立小・中学校通学区域設定規則の一部を改正する規則）

第２条　中津市立小・中学校通学区域設定規則（平成１５年中教規則第８号）の一部を次のように改正する。

別表第１小楠小学校の項中「牛神の一部　一ツ松の一部」を「牛神（一部を除く。）一ツ松（一部を除く。）」に改める。城井小学校の項中「耶馬溪町大字栃木（小川内）」を「耶馬溪町大字栃木　耶馬溪町大字栃木　耶馬溪町大字中畑　耶馬溪町大字大野　耶馬溪町大字川原口」に改め、同表津民小学校の項を削り、同表２耶馬溪中学校の項中「　津民小学校通学区域」を削る。

（中津市立学校体育施設の開放に関する規則の一部を改正する規則）

第３条　中津市立学校体育施設の開放に関する規則（昭和５９年中教規則第７号）の一部を次のように改正する。

別表施設の欄中「中津市立津民小学校」を削る。

（中津市立学校給食共同調理場管理規則の一部を改正する規則）

第４条　中津市立学校給食共同調理場管理規則（昭和４６年中教規則第５号）の一部を次のように改正する。

第３条第１項の表市内義務教育諸学校の欄中「津民小学校」を削る。

附　則

この規則は、令和８年４月１日から施行する。

新旧対照表

○中津市立学校管理規則（第１条関係）

改正後

別表第３（第25条関係）

名称	拠点校	連携校
第１学校支援センター	中津市立豊陽中学校	中津市立鶴居小学校 中津市立大幡小学校 中津市立三保小学校 中津市立今津小学校 中津市立沖代小学校 中津市立樋田小学校 中津市立上津小学校 中津市立城井小学校 中津市立下郷小学校 （削る。） 中津市立緑ヶ丘中学校 中津市立今津中学校 中津市立本耶馬渓中学校 中津市立耶馬溪中学校
略	略	略

改正前

別表第３（第25条関係）

名称	拠点校	連携校
第１学校支援センター	中津市立豊陽中学校	中津市立鶴居小学校 中津市立大幡小学校 中津市立三保小学校 中津市立今津小学校 中津市立沖代小学校 中津市立樋田小学校 中津市立上津小学校 中津市立城井小学校 中津市立下郷小学校 中津市立津民小学校 中津市立緑ヶ丘中学校 中津市立今津中学校 中津市立本耶馬渓中学校 中津市立耶馬溪中学校
略	略	略

○中津市立小・中学校通学区域設定規則（第２条関係）

改正後

別表（第２条関係）

１　小学校通学区域

学校名	通学区域

改正前

別表（第２条関係）

１　小学校通学区域

学校名	通学区域

改正後	
略	略
小楠小学校	牛神（一部を除く。）　一ツ松（一部を除く。）　宮夫　東浜　西大新田　東大新田　下池永（字古附142番地先から字葱手211番地先水路及び錆矢堂、新田線（市道牛神舞手川線まで）の以西を含む。）　上池永の一部
略	略
城井小学校	耶馬溪町大字平田　耶馬溪町大字小友田　耶馬溪町大字三尾母　耶馬溪町大字福土　耶馬溪町大字戸原　耶馬溪町大字冠石野（柚木）　耶馬溪町大字多志田（中川原）　耶馬溪町大字柿坂　耶馬溪町大字大島（杉畑）　耶馬溪町大字栃木　耶馬溪町大字中畑　耶馬溪町大字大野　耶馬溪町大字川原口　耶馬溪町大字山移（うち無浅、上長谷を除く。）　耶馬溪町大字深耶馬
略	略
（削る。）	（削る。）
略	略

2　中学校通学区域

学校名	通学区域
略	略
耶馬溪中学校	城井小学校通学区域　下郷小学校通学区域
略	略

改正前	
略	略
小楠小学校	牛神の一部　一ツ松の一部　宮夫　東浜　西大新田　東大新田　下池永（字古附142番地先から字葱手211番地先水路及び錆矢堂、新田線（市道牛神舞手川線まで）の以西を含む。）　上池永の一部
略	略
城井小学校	耶馬溪町大字平田　耶馬溪町大字小友田　耶馬溪町大字三尾母　耶馬溪町大字福土　耶馬溪町大字戸原　耶馬溪町大字冠石野（柚木）　耶馬溪町大字多志田（中川原）　耶馬溪町大字柿坂　耶馬溪町大字大島（杉畑）　耶馬溪町大字栃木（小川内）　耶馬溪町大字山移（うち無浅、上長谷を除く。）　耶馬溪町大字深耶馬
略	略
津民小学校	耶馬溪町大字栃木（うち小川内を除く。）　耶馬溪町大字中畑　耶馬溪町大字大野　耶馬溪町大字川原口
略	略

2　中学校通学区域

学校名	通学区域
略	略
耶馬溪中学校	城井小学校通学区域　下郷小学校通学区域　津民小学校通学区域
略	略

○中津市立学校体育施設の開放に関する規則（第３条関係）

改正後

別表（第４条、第７条関係）

施設		単位	金額
略	略	略	略
中津市立城井小学校 中津市立下郷小学校 （削る。）	体育館	１時間当たり	中学生以下　200円
			一般　410円
	運動場夜間照明施設	１時間当たり	中学生以下　270円
			一般　550円
	運動場		無料
略	略	略	略

備考

略

改正前

別表（第４条、第７条関係）

施設		単位	金額
略	略	略	略
中津市立城井小学校 中津市立下郷小学校 中津市立津民小学校	体育館	１時間当たり	中学生以下　200円
			一般　410円
	運動場夜間照明施設	１時間当たり	中学生以下　270円
			一般　550円
	運動場		無料
略	略	略	略

備考

略

○中津市学校給食共同調理場管理規則（第４条関係）

改正後

（業務を行う学校等）

第３条　共同調理場が業務を行う市内義務教育諸学校は、次の表のとおりとする。

共同調理場	市内義務教育諸学校
略	略
中津市学校給食本耶馬渓共同調理場	樋田小学校　上津小学校　城井小学校　本耶馬渓中学校
略	略

２　略

改正前

（業務を行う学校等）

第３条　共同調理場が業務を行う市内義務教育諸学校は、次の表のとおりとする。

共同調理場	市内義務教育諸学校
略	略
中津市学校給食本耶馬渓共同調理場	樋田小学校　上津小学校　城井小学校　津民小学校　本耶馬渓中学校
略	略

２　略

議第25号

財産の取得について

上記について、別紙のとおり提案いたします。

令和7年7月25日提出

中津市教育委員会

教育長　古　口　宣　久

議第　　号

財産の取得について

記

１　取得する物　　①iPad
②キーボードケース
③電源アダプタ
④音声接続端子

２　配置場所　　中津市立小学校２１校、中学校１０校

３　数量　　①７，３８４台
②７，３８４個
③７，３８４個
④７，３８４個

４　取得の方法　　随意契約（大分県による一般競争入札で落札した業者）

５　取得価格　　４９３，８４１，９２０円（消費税込）

６　取得の相手方　大分市東春日町１７番５７号
株式会社オーイーシー
代表取締役社長　加藤　健

説　明

効率的に情報教育に取り組むことができるよう児童生徒が使用する授業用 iPad、教員が使用する iPad 及びその周辺機器を取得いたしたく提出する。

議第26号

和解及び損害賠償の額を定めることについて

上記について、別紙のとおり提案いたします。

令和7年7月25日提出

中津市教育委員会

教育長　古　口　宣　久

議第　　号

和解及び損害賠償の額を定めることについて

記

１　事故概要　令和２年７月１８日、市立中学校の生徒が、野球部マネージャーとして練習試合前のノック練習を補助していたところ、部活動顧問のスイングしたバットが額に当たり挫創する事故が発生した。

この事故により、通院治療したが、前額部に長さ 4.5 ㎝、幅 3㎜ の瘢痕が残った。

２　事故当事者　　甲　学校設置者　中津市豊田町１４番地３　中津市長 奥塚 正典

部活動顧問　市立中学校教諭

乙　当　事　者　■■　■■（保護者■■　■■）

３　和解内容の要旨

（１）甲は損害賠償金として、乙に対して１１，０００，０００円を支払う。

（２）今後本件事故に関し、双方とも異議の申し立て、訴訟は一切行わない。

４　過失割合　　甲　１００％　　乙　０％

５　損額賠償の額　１１，０００，０００円（損害賠償については全額保険で対応）

議第27号

中津市立小・中学校通学区域の変更等に関する取扱要綱の一部
改正について

上記について、別紙のとおり提案いたします。

令和7年7月25日提出

中津市教育委員会

教育長　古　口　宣　久

中津市立小・中学校通学区域の変更等に関する取扱要綱の一部改正概要

１　一部改正の理由

通学区域の変更において、教育委員会が相当と認める事項について通常変更が認められる事例を追加し、手続きを行う保護者及び意見書等必要書類を作成する学校の負担を軽減するもの。

２　一部改正の内容

別表の一部を改正するもの

〇次の２つの事項を追加するもの。

・指定校変更の承認を受けた児童・生徒の兄弟・姉妹が同一校の就学を希望する場合

・小学校の指定校変更の承認を受けた児童が中学校に入学する場合において、在籍する小学校を通学区域とする中学校を希望する場合

〇その他文言の修正をあわせて行うもの。

３　施行期日等

公示の日から施行する。

教育委員会学校教育課
学校教育係
折元
（内線　＊６４９５）

新旧対照表

○中津市立小・中学校通学区域の変更等に関する取扱要綱

改正後

別表

事項		変更申請内容	変更期間	必要書類等
転居に関わる事項	（１） 学年途中	学年途中に転居し、通学において支障がない場合（保護者が責任を負うとした場合も含む。）	小・中学校とも卒業までの申請期間	不要
	略	略	略	略
	（３） 公共事業及び災害	ア 公共事業により校区外へ転居せざるを得ない場合（自己都合を除く。）	ア 小・中学校とも卒業までの申請期間	ア 当該事業主体者の証明書
		イ 災害による仮移転の場合	イ 住居が確定するまで。ただし、仮設住宅等以外の住居に移転した場合は１年未満とする	イ 公的機関から出される証明書 (ア)被災証明 (イ)仮移転を証する書類
		ウ 公共事業による一時立ち退きの場合	ウ 再転居するまでの期間	ウ 当該事業主体者の証明書
教	略	略	略	略

改正前

別表

事項		変更申請内容	変更期間	必要書類等
転居に関わる事項	（１） 学期途中	学期途中に転居し、通学において支障がない場合（保護者が責任を負うとした場合も含む。）	小・中学校とも卒業までの＿＿期間	不要
	略	略	略	略
	（３） 公共事業及び災害	ア 公共事業により校区外へ転居せざるを得ない場合（自己都合を除く。）	ア 小・中学校とも卒業までの＿＿期間	ア 当該事業主体者の証明書
		イ 災害による仮移転の場合	イ 住居が確定するまで。ただし、仮設住宅等以外の住居に移転した場合は１年未満とする	イ 公的機関から出される証明書 (ア)被災証明 (イ)仮移転を証する書類
		ウ 公共事業による一時立ち退きの場合	ウ 再転居するまでの期間	ウ 当該事業主体者の証明書
	略	略	略	略

改正後				
育上の配慮	（５） 特別支援教育推進に関する理由	ア 指定校に特別支援学級がなく、特別支援学級のある学校に通学する場合 イ 特に教育的配慮が必要な場合	ア 通常の学級に編入できるまでの期間 イ 必要な期間	ア 就学指導委員会等による意見書面談 イ 学校長の意見書
	（６） 生徒指導に関する理由	ア 不登校等、生徒指導上特に教育的配慮が必要な場合 イ 同一小学校から分かれて中学校に就学する際において、教育的配慮が必要な場合（当該中学校へ就学する児童数が当該小学校卒業見込児童数の２割に満たない状況にある場合に限る。）	ア 必要な期間 イ 中学校卒業までの申請期間	ア 学校長の意見書面談 イ 面談
	略	略	略	略

改正前				
	（５） 特別支援教育推進に関する理由	ア 指定校に障害児　学級がなく、障害児学級のある学校に通学する場合 イ 特に教育的配慮が必要な場合	ア 通常の学級に編入できるまでの期間 イ 必要な期間	ア 就学指導委員会等による意見書面談 イ 学校長の意見書
	（６） 生徒指導に関する理由	ア 不登校等、生徒指導上特に教育的配慮が必要な場合 イ 同一小学校から分かれて中学校に就学する際において、教育的配慮が必要な場合（当該中学校へ就学する児童数が当該小学校卒業見込児童数の２割に満たない状況にある場合に限る。）	ア 必要な期間 イ 中学校卒業までの　期間	ア 学校長の意見書面談 イ 面談
	略	略	略	略

改正後				
	（８） 安全に関する理由	ア 保護者が共働き等から、昼間留守家庭となり、帰宅後監督者がいない場合（小学生に限る。）	ア 小学校卒業までの必要な期間	ア 保護者の勤務証明書又は営業（自営）を証する書類及び身元引受け承諾に関する確認書
		イ 通学路の安全に関し保護者責任においての申立てがあった場合	イ 小・中学校とも卒業までの申請期間	イ 確約書 面談
家庭の事情	（９） 兄弟姉妹関係	指定校変更の承認を受けた児童・生徒の兄弟・姉妹で同一校の就学を希望する場合	小・中学校とも卒業までの申請期間	不要
	(10) 指定校変更児童の中学校入学	指定校変更の承認を受けた児童が中学校に入学する場合において、在籍する小学校を通学区域とする中学校を希望する場合	中学校卒業までの申請期間	不要 面談
	(11) 保護者の入院等	保護者の入院等で一時的に親族等へ預けられた	保護者と生活ができるまでの期間	(ア)医師の証明書等 (イ)身元引受け承

改正前				
	（８） 安全に関する理由	ア 保護者が共働き等から、昼間留守家庭となり、帰宅後監督者がいない場合（小学生に限る。）	ア 小学校卒業までの必要な期間	ア 保護者の勤務証明書又は営業（自営）を証する書類及び身元引受け承諾に関する確認書
		イ 通学路の安全に関し保護者責任においての申立てがあった場合	イ 小・中学校とも卒業までの　期間	イ 確約書 面談
	（新設）	（新設）	（新設）	（新設）
	（新設）	（新設）	（新設）	（新設）
家庭の	（９） 保護者の入院等	保護者の入院等で一時的に親族等へ預けられた	保護者と生活ができるまでの期間	(ア)医師の証明書等 (イ)身元引受け承

改正後				
		場合		諾に関する確認書
	(12)　精神的不安定	保護者の死亡、離婚、失踪等の理由及び転校回数が多い（小・中学校３回程度を目安）等の理由により、家庭環境の急激な変化が児童生徒に精神的に著しい影響があり、不安定と認められた場合	必要な期間	学校長の意見書又は医師の診断書
	(13)　住民票の異動ができない	家庭の事情で居住地に住民登録ができない場合	住民票の異動届出ができるまでの期間	自治委員等の居住を証する書類
	(14)　児童相談所等による措置	児童相談所等による措置を受けた場合（中学生に限る。）	必要な期間	関係機関との協議による意見書
帰国児童生徒	(15)　帰国児童生徒	ア　外国生活が長い帰国児童生徒の内、日本語の指導が必要な場合 イ　外国生活が	ア　帰国時に限り特別に日本語指導を行っている学校へ必要な期間 イ　帰国時に限	不要 面談

改正前				
事情		場合		諾に関する確認書
	(10)　精神的不安定	保護者の死亡、離婚、失踪等の理由及び転校回数が多い（小・中学校３回程度を目安）等の理由により、家庭環境の急激な変化が児童生徒に精神的に著しい影響があり、不安定と認められた場合	必要な期間	学校長の意見書又は医師の診断書
	(11)　住民票の異動ができない	家庭の事情で居住地に住民登録ができない場合	住民票の異動届出ができるまでの期間	自治委員等の居住を証する書類
	(12)　児童相談所等による措置	児童相談所等による措置を受けた場合（中学生に限る。）	必要な期間	関係機関との協議による意見書
帰国児童生徒	(13)　帰国児童生徒	ア　外国生活が長い帰国児童生徒の内、日本語の指導が必要な場合 イ　外国生活が	ア　帰国時に限り特別に日本語指導を行っている学校へ必要な期間 イ　帰国時に限	不要 面談

改正後				
及び外国人の就学		長い帰国児童生徒で日本の生活になじみにくいと認められる場合	り知人等がいる学校へ必要な期間	
	(16)　外国人の就学	日本語が理解できない外国人が就学を希望する場合	入国時の就学に限り同国籍の児童生徒がいる学校又は特別に日本語指導を行っている学校へ必要な期間	住民票の写し及び面談
略		略	略	略

略

改正前				
及び外国人の就学		長い帰国児童生徒で日本の生活になじみにくいと認められる場合	り知人等がいる学校へ必要な期間	
	(14)　外国人の就学	日本語が理解できない外国人が就学を希望する場合	入国時の就学に限り同国籍の児童生徒がいる学校又は特別に日本語指導を行っている学校へ必要な期間	住民票の写し及び面談
略		略	略	略

略

議第28号

中津市教育情報セキュリティポリシーの策定について

上記について、別紙のとおり提案いたします。

令和7年7月25日提出

中津市教育委員会

教育長　古　口　宣　久

中津市教育情報セキュリティポリシー

中津市教育委員会

目次

教育情報セキュリティポリシー

本基本方針は、本市立小学校、中学校（以下「学校」という）教育委員会が保有する情報資産の機密性、完全性及び可用性を維持するため、学校における情報セキュリティ対策について基本的な事項を定めることを目的とする。

１．対象範囲及び用語説明

（１）行政機関等の範囲

本対策基準が適用される行政機関等は、教育委員会及び学校とする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①教育ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体

②教育ネットワーク及び教育情報システムで取り扱う情報（これらを印刷した文書を含む。）

③情報システムの仕様書及びネットワーク図等のシステム関連文書

（３）用語説明

本対策基準における用語は、以下のとおりとする。

用語	定義
校務系情報	児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報
校務外部接続系情報（公開系情報）	校務系情報のうち、保護者メールや学校ホームページ等インターネット接続を前提とした校務で利用される情報
学習系情報	児童生徒のワークシート、作品など、学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ当該情報に教員及び児童生徒がアクセスすることが想定されている情報
校務用端末	校務系情報にアクセス可能な端末
校務外部接続用端末	校務外部接続系情報にアクセス可能な端末
学習者用端末	学習系情報にアクセス可能な端末で、児童生徒が利用する端末
指導者用端末	学習系情報にアクセス可能な端末で、教員のみが利用可能な端末
校務系システム	校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム及び、校務系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
校務外部接続系システム	校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（CMS）及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム
学習系システム	学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成

	される学習系情報を取り扱うシステム及び、学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称合わせた総称
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	校務外部接続系情報を取り扱うサーバ
学習系サーバ	学習系情報を取り扱うサーバ

２．組織体制

（１）構成員

役職名	役職者	役割
最高情報セキュリティ責任者（CISO:Chief Information Security Officer、以下「CISO」という。）	教育長	①CISO は、本市における全ての教育ネットワーク、教育情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。 ②CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。
統括教育情報セキュリティ責任者	教育部長	①統括教育情報セキュリティ責任者は、CISO を補佐しなければならない。 ②統括教育情報セキュリティ責任者は、本市の全ての教育ネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。 ③統括教育情報セキュリティ責任者は、本市の全ての教育ネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。 ④統括教育情報セキュリティ責任者は、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者及び教育情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。 ⑤統括教育情報セキュリティ責任者は、本市の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に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。 ⑥統括教育情報セキュリティ責任者は、本市の共通的な教育ネットワーク、教育情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

		⑦統括教育情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。 ⑧統括教育情報セキュリティ責任者は、緊急時にはCISOに早急に報告を行うとともに、回復のための対策を講じなければならない。
教育情報セキュリティ責任者	学校教育課長	①教育情報セキュリティ責任者は、本市の教育情報セキュリティ対策に関する統括的な権限及び責任を有する。 ②教育情報セキュリティ責任者は、その所管する部局等において所有している教育情報システムにおける開発、設定の変更、運用、見直し等を行う際の情報セキュリティに関する統括的な権限及び責任を有する。 ③教育情報セキュリティ責任者は、本市において所有している教育情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び教職員等(学校現場に勤務するすべての職員（臨時的任用又は非常勤の職にあるものを含む）をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。
教育情報セキュリティ管理者	校長	①教育情報セキュリティ管理者は、当該学校の情報セキュリティ対策に関する権限及び責任を有する。 ②教育情報セキュリティ管理者は、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には、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。
教育情報システム管理者	学校教育課長	①教育情報システム管理者は、所管する教育情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。 ②教育情報システム管理者は、所管する教育情報システムにおける情報セキュリティに関する権限及び責任を有する。 ③教育情報システム管理者は、所管する教育情報システムに係る情報セキュリティ実施手順の維持・管理を行う。
教育情報システム担当者	学校教育課員	①教育情報システム担当者は、教育情報システム管理者の指示等に従い、教育情報システムの開発、設定の変更、運用、更新等の作業を行う。

（２）中津市教育情報化推進委員会

①本市の情報セキュリティ対策を統一的に実施するため、中津市教育情報化推進委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

②中津市教育情報化推進委員会は、必要に応じ、本市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

（３）兼務の禁止

①情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

②監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

（４）情報セキュリティに関する統一的な窓口の設置

①CISO は、情報セキュリティの統一的な窓口の機能を有する組織を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

②CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供する。

③情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

④情報セキュリティに関して、以下の関連機関、関連業者と情報共有を行う。

関連機関・関連業者	詳細
中津市情報デジタル推進課	中津市役所関連部署
大分県教育ＤＸ推進課	大分県関連部署
大分県内市町村の教育ＩＣＴ担当課	大分県内市町村関連部署
学校ネットワーク関連保守業者	委託業者

（５）教職員等

①臨時的任用、非常勤の職にあるものを含めた、学校現場に勤務するすべての職員を教職員等と称する。

②教職員等は学校が所管する情報資産を取り扱う立場にあり、教育情報セキュリティ管理者の指導の下、情報セキュリティを遵守しなければならない。

（６）教育委員会事務局

①教育ネットワークを利用して、学校が所管する情報にアクセスできる教育委員会事務局を指す。

②教育委員会事務局職員は学校の情報資産にアクセスできる立場にあり、教育情報セキュリティ責任者の指導の下、情報セキュリティを遵守しなければならない。

３．情報資産の分類と管理方法

３．１．情報資産の分類

本市における情報資産は、機密性、完全性及び可用性の 3 つの観点から影響度を評価し、次のとおり 4 段階の重要性分類を行い、必要に応じて取扱制限を行うものとする。

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。

情報資産の分類		情報資産の例示			
重要性分類	定義	校務系		学習系	公開系
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。	・指導要録原本 ・教職員の人事情報 ・教育情報システム仕様書			
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。	○学籍関係 ・卒業証書授与台帳 ・転入学受付簿 ・転退学受付簿 ・就学児童・生徒異動報告書 ・休学退学願受付簿 ・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 ・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	○児童・生徒に関する個人情報 （生活歴、心身の状況、財政状況等の情報、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 ・健康診断票 ・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	○児童生徒の学習系情報 ・学習系システムログインID/PW管理台帳 ・学習用端末ID/PW管理台帳	

		簿 ・児童・生徒等の個人写真・集合写真 ・指導記録・指導カード ・教育相談・面接の記録・カード等 ・個別の教育支援計画 ・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 ・卒業生進路先一覧等 ・卒業生進路先一覧表 ・進路希望調査 ・進路判定会議資料 ・進路指導記録簿	・健康診断に関する表簿 ・就学時健康診断票 ○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 ・寄宿関係資料 ○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 ・職員緊急連絡網・職員住所録 ・委員会名簿 ○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		
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。	○児童生徒の氏名 ・出席簿 ・名列表 ・座席表 ・児童生徒委員会名簿	○学校運営関係 ・卒業アルバム ・学校行事等の児童・生徒の写真	○学校運営関係 ・授業用教材 ・教材研究資料 ・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)	
Ⅳ	影響をほとんど及ぼさない。				○学校運営関係 ・学校要覧 ・学校紹介パンフレット ・使用教科書一覧 ・教育課程編成表 ・学校認定科目の届け出 ・特色紹介冊子原稿 ・学校徴収金会計簿（学年費、教育振興費等） ・学校行事実施計画（避難訓練・体育祭実施計画等） ・保護者等への配布文書文例 ・各種届雛形・校務分掌表 ・学校・学級だより ・学校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）

３．２情報資産の管理

（１）管理責任

①CISO または統括教育情報セキュリティ責任者は、教育情報システムとその運用管理を定めた学校教育情報セキュリティ対策基準を策定しなければならない。

②統括教育情報セキュリティ責任者は、学校教育情報セキュリティ対策基準に基づき、学校現場での情報セキュリティ運用管理に関する実施手順ひな形を作成しなければならない。

③統括教育情報セキュリティ責任者は、学校で標準的に所管する情報資産について、分類を定義した標準情報資産台帳（以下「標準台帳」という。）を作成し、適宜更新しなければならない。

④教育情報セキュリティ管理者は、実施手順ひな形に基づき、自校の実施手順を作成しなければならない。

⑤教育情報セキュリティ管理者は、標準情報資産台帳に基づき、自校で所管する情報資産を確認し、不足内容を補完した自校向け情報資産台帳（以下「台帳」という。）を整備しなければなら

ない。

⑥教育情報セキュリティ管理者は、自校の所管する情報資産について管理責任を有する。

⑦教育情報セキュリティ管理者は、教職員等の情報資産の取扱いに際し、台帳及び実施手順に基づいた運用管理を指導しなければならない。

⑧教職員等は、台帳及び実施手順に基づき、適切に情報資産を取り扱わなければならない。

（２）情報資産の取り扱い

①情報資産の分類の表示

教職員等は、情報資産について、その分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

※情報資産の分類の表示先ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等

②情報の作成

（ア）教職員等は、業務上必要のない情報を作成してはならない。

（イ）情報を作成する教職員等は、情報の作成時に３．１の分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。

（ウ）情報を作成する教職員等は、作成途上の情報についても、取扱いを許可されていない者の閲覧や紛失・流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

③情報資産の入手

（ア）本市教職員等が作成した情報資産を入手した教職員等は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

（イ）本市教職員等が作成した情報資産を入手した教職員等は、３．１の分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。

（ウ）情報資産を入手した教職員等は、その情報資産の分類が不明な場合、教育情報セキュリティ管理者に判断を仰がなければならない。

④情報資産の利用

（ア）情報資産を利用する教職員等は、業務以外の目的に情報資産を利用してはならない。

（イ）情報資産を利用する教職員等は、情報資産の分類に応じ、適正な取扱いをしなければならない。

（ウ）情報資産を利用する教職員等は、電磁的記録媒体または保存されている領域（フォルダやサーバ）に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体または保存されている領域を取り扱わなければならない。

（３）情報資産の保管

①教育情報セキュリティ管理者又は教育情報システム管理者の措置事項

（ア）教育情報セキュリティ管理者は、資産台帳に従って、情報資産の保管先を定め、教職員等に周知しなければならない。

（イ）教育情報セキュリティ管理者又は教育情報システム管理者は、情報資産を記録した USB メモリ等の外部電磁的記録媒体を長期保管しないように管理しなければならない。

（ウ）教育情報セキュリティ管理者又は教育情報システム管理者は、情報システムのバックアップで取得したデータを記録する電磁的記録媒体を保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。なお、クラウドサービスを利用する場合はサービスの機能として自然災害対策がなされていることを確認すること。

（エ）教育情報セキュリティ管理者又は教育情報システム管理者は、重要性分類Ⅲ以上の情報を記録した電磁的記録媒体を保管する場合、耐火、耐震、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

②教職員等の遵守事項

（ア）教職員等は、教育情報セキュリティ管理者が指定した保管先にのみ情報資産を保管しなければならない。

（イ）教職員等は、児童生徒が生成する学習系情報の保管先について児童生徒に指示し、それ以外の場所に保管しないよう指導しなければならない。

（４）情報資産の外部持ち出し

①分類に応じた情報資産の外部持ち出し制限

（ア）教職員等は、重要性分類Ⅱ以上の情報資産を外部持ち出しする場合は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行い、教育情報セキュリティ管理者の個別許可を得なければならない。また、持ち出し持ち帰りの記録をつけなければならない。なお、外部持ち出しツールに限定されたアクセスの措置設定（アクセス制限や暗号化）機能を有する場合には、有効にしなければならない。

（イ）重要性分類Ⅲの情報資産については、教職員等の外部持ち出しについて、教育情報セキュリティ管理者の判断で包括的許可を可とする。なお、外部持ち出しツールに限定されたアクセスの措置設定（アクセス制限や暗号化）機能を有する場合には、有効にしなければならない。

②電子メール、外部ストレージサービスによる情報の送信

情報資産が組織内部（組織が利用するサーバやクラウドサービス等）から組織外部（家庭や地域、事業者等）に電子メール等により外部送信される場合は、情報資産分類に応じ以下を実施しなければならない。

（ア）電子メール、外部ストレージサービスにより重要性分類Ⅲ以上の情報を外部送信する者は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行わなければならない。

（イ）利用する電子メール、外部ストレージサービスは教育委員会又は学校から提供される公式サービスのみを利用し、私的に契約したサービスを利用してはならない。

③外部電磁的記録媒体を用いた情報の外部持ち出し

USB メモリ等の物理的な媒体による情報の外部持ち出しは、紛失・盗難リスクを伴うことから基本的には不可とする。

④FAX による情報の送信

FAX による情報の送信は、限定されたアクセスの措置（アクセス制限や暗号化）が不可能であること、誤送信のリスクがあることに鑑み、送信相手が FAX 受信を指定してきた場合にのみ利用することとする。

⑤情報資産の運搬

（ア）車両等により重要性分類Ⅲ以上の情報資産を運搬する場合は、必要に応じ暗号化又はパスワードの設定を行う等の安全管理措置を講じ、宛名・差出名を明記して、厳重に封印しなければならない。

（イ）重要性分類Ⅲ以上の情報資産を運搬する教職員等は、教育情報セキュリティ管理者に許可を得なければならない。

⑥情報資産の公表

（ア）教育情報セキュリティ管理者は、公開する情報が正しい内容であることを事前に確認し、誤公開を防がなければならない。

（イ）教育情報セキュリティ管理者は、住民に公開する情報資産について、改ざんや消去されないように定期的に確認しなければならない

（５）情報資産の廃棄等

①情報資産を廃棄する教職員は、重要性分類Ⅲ以上の情報が記載された紙媒体の書類を廃棄する場合には、内容が復元できないように細断、熔解またはこれに準ずる方法にて廃棄しなければならない。

②情報を記録している電磁的記録媒体を利用しなくなった場合、情報を復元できないように処置した上で廃棄しなければならない。

③情報資産の廃棄・リース返却を行う教職員等は、教育情報セキュリティ管理者の許可を得て、行った処理について、日時、担当者及び処理内容を記録しなければならない。

④業者に廃棄委託する場合、廃棄する情報資産を業者が引き取る際、教職員等が立ち会わなければならない。

４．物理的セキュリティ

４．１．サーバ等の管理

（１）機器の取付け

教育情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

（２）機器の電源

①教育情報システム管理者は、統括教育情報セキュリティ責任者及び施設管理部門と連携し、校務系サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②教育情報システム管理者は、統括教育情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

（３）通信ケーブル等の配線

①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は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

②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は、主要な箇所の通信ケーブル

及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③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は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

④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は、自ら又は教育情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更又は追加できないように必要な措置を施さなければならない。

（４）機器の定期保守及び修理

①教育情報システム管理者は、重要性分類Ⅲ以上（可用性 2A 以上）のサーバ等の機器の定期保守を実施しなければならない。

②教育情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、教育情報システム管理者は、外部の事業者に故障を修理させるに当たり、修理を委託する事業者との間で、守秘義務契約を締結するとともに秘密保持体制の確認等を行わなければならない。

（５）施設外又は学校外への機器の設置

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は、施設外又は学校外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（６）機器の廃棄等

教育情報システム管理者は、機器を廃棄又はリース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

４．２．管理区域（情報システム室等）の管理

（１）管理区域の構造等

①管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

②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は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

③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は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

④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は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（２）管理区域の入退室管理等

①教育情報システム管理者は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

②地方公共団体職員等及び外部委託事業者が、管理区域に入室を許可する場合、これらの者に身分

証明書等を携帯させ、必要に応じ、その提示を求めなければならない。

③教育情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された地方公共団体職員等が付き添うものとし、外見上地方公共団体職員等と区別できる措置を講じなければならない。

④教育情報システム管理者は、重要性分類Ⅱ以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（３）機器等の搬入出

①教育情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ地方公共団体職員又は委託した業者に確認を行わせなければならない。

②教育情報システム管理者は、情報システム室の機器等の搬入出について、地方公共団体職員またはその代理の者を立ち会わせなければならない。

４．３．通信回線及び通信回線装置の管理

（１）統括教育情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

（２）統括教育情報セキュリティ責任者は、外部へのネットワーク接続ポイント及び該当ポイントに接続される端末を正確に把握し、適切な管理を行わなければならない。

（３）統括教育情報セキュリティ責任者は、重要性分類Ⅲ以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、通信経路上での暗号化を行わなければならない。

（４）統括教育情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

（５）統括教育情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

（６）統括教育情報セキュリティ責任者は、学校運営上必要なネットワーク帯域を確保するとともに、遅延等に対する適切な対策を講じなければならない。クラウドサービス提供事業者側のサービス要件基準を満たす配慮を含めてネットワーク構成を設計する。また、運用開始前には十分検証し、利用状況に応じて定期的に改修計画を行うこと。

４．４．教職員等の利用する端末や電磁的記録媒体等の管理

（１）教育情報システム管理者は、不正アクセス防止のため、ログイン時の ID パスワードによる認証など、使用する目的に応じた適切な物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

（２）教育情報システム管理者は、校務系システム、教育情報システムへアクセスする端末へのログインパスワードの入力を必要とするように設定しなければならない。

（３）教育情報システム管理者は、端末の電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を設定しなければならない。

（４）教育情報システム管理者は、特に強固なアクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産を取り扱う端末に対し、当該データ暗号化等の措置により、不正アクセスや教員の不注意等による情報流出への対策を講じなければならない。

（５）教育情報システム管理者は、パソコンやモバイル端末におけるマルウェア感染の脅威に対し、ウイルス対策ソフトの導入等の対策を講じなければならない。なお、OS によっては標準的にウイルス対策ソフトを備えている製品、OS としてウイルス感染のリスクが低い仕組みとなっている製品などもあるため、実際に運用する端末において適切な対策を講じること。強固なアクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産を取り扱う端末に対し、当該端末の状況および通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み（ふるまい検知）等の活用を検討し、適切な対策を講じること。

（６）教育情報システム管理者は、インターネットへ接続をする場合、教職員等のパソコン、モバイル端末に対して不適切なウェブページの閲覧を防止する Web フィルタリング等の対策を講じなければならない。

４．５．学習者用端末のセキュリティ対策

（１）不適切なウェブページの閲覧防止

児童生徒が端末を利用する際に不適切なウェブページの閲覧を防止するために、フィルタリングソフト、検索エンジンのセーフサーチ、セーフブラウジングなどの対策を講じなければならない。

（２）マルウェア感染対策

学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

（３）端末を不正利用させないための防止策

端末のセキュリティ状態の監視に加えて、不適切なアプリケーションやコンテンツの利用を制限し、常に安全で児童生徒が安心して利用できる状態を維持しなければならない。

（４）セキュリティ設定の一元管理

児童生徒への端末配布後においても、端末のセキュリティ設定や OS アップデート、ウェブブラウザのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を、離れた場所からでも一元管理できることが望ましい。

（５）端末の盗難・紛失時の情報漏洩対策

児童生徒が端末を紛失しても、遠隔操作でロックをかける、あるいはワイプ（データ消去）することで第三者による不正操作や情報漏洩を防ぐ等の安全管理措置を講じなければならない。

４．６．パソコン教室等における学習者用端末や電磁的記録媒体の管理

（１）教育情報システム管理者は、盗難防止のため、教室等で利用するパソコンの保管庫による管理等の物理的措置を講じなければならない。

（２）教育情報システム管理者は、パソコン及び電磁的記録媒体について、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

（３）教育情報システム管理者は、情報システムへのアクセスにおけるログインパスワードの入力等による認証を設定しなければならない。

５．人的セキュリティ

５．１．教育情報セキュリティ管理者の措置事項

（１）情報資産の管理

①情報資産の持ち出し及び持ち込みの記録管理

教育情報セキュリティ管理者は、教職員等による情報資産の外部持ち出しについて、記録管理しなければならない。

②情報資産の廃棄管理

（ア）教育情報セキュリティ管理者は、廃棄処理を外部に委託する場合は、学校の外に委託業者が持ち出す行為に教職員等が立ち合うように指示し、誤廃棄を予防しなければならない。

（イ）教育情報セキュリティ管理者は、廃棄した情報資産を記録管理しなければならない。

（２）教職員等の情報セキュリティ意識醸成

①教育情報セキュリティ管理者は、教職員等に対して、日頃から情報セキュリティに関する話題を積極的に提供し、情報セキュリティ研修を受講させるなど、積極的にセキュリティ認識の向上を図らなければならない。

②教育情報セキュリティ管理者は、校内でセキュリティ事故につながりかねないヒヤリ・ハット事案を抑止するために、教職員等が事案を発見した際に、直ちに対処し、速やかに報告が上がるよう、教職員等に対する情報セキュリティ意識の醸成と風通しのよい関係性維持に努めなければならない。

③情報セキュリティポリシー等の閲覧容易性確保

教育情報セキュリティ管理者は、教職員等が常に教育情報セキュリティポリシー及び実施手順を閲覧・確認できるように配慮しなければならない。

（３）端末等の持ち出し及び持ち込みの記録

教育情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

（４）教職員等への情報セキュリティポリシー等の遵守指導

①教育情報セキュリティ管理者は、新規採用教職員等及び他自治体から本市に新規赴任した教職員等、及び非常勤及び臨時の教職員に対し、教育情報セキュリティポリシー等遵守すべき内容を理解・浸透するように指導を行わなければならない。

②教育情報セキュリティ管理者は、教職員等に対して、必要に応じて情報セキュリティポリシーの遵守の同意書への署名を求める。

（５）新規ソフトウェア及びコンテンツの導入・利用判断

教育情報セキュリティ管理者は、教職員等から、導入したソフトウェア・コンテンツの制限解除や、業務上新たなソフトウェア・コンテンツの導入について、事前に相談があった場合は、教育情報シ

ステム管理者に上申して、判断を仰がなければならない。

（６）インターネット接続及び電子メール利用の制限

①教育情報セキュリティ管理者は、教職員等に業務端末による作業を行わせる場合において、業務以外でのインターネット接続及び電子メールの利用をしないよう教職員等に指導しなければならない。なお Web フィルタリングの設定について、教職員等から相談があった場合は、教育情報システム管理者に上申して、判断を仰がなければならない。

②教育情報セキュリティ管理者は、パソコンやモバイル端末の機能は、教職員等の業務内容に応じて、不必要な機能については制限することが適切である。

（７）校内及び執務室での管理

教育情報セキュリティ管理者は、教職員等と協力して下記を管理しなければならない。

①来校者の氏名及び入退時刻を記録しなければならない。

②来校者には名札などを着用させ、第三者であることが識別できるようにしなければならない。

③地域住民、保護者などに校内施設を開放する場合、執務室等開放していない施設へは入場できないよう制限を設けなければならない。

（８）自己点検の実施

①教育情報セキュリティ管理者は、年１回、学校の自己点検を行わなければならない。

②教育情報セキュリティ管理者は、自己点検の結果を情報セキュリティ委員会に報告しなければならない。

５．２．教職員等の遵守事項

（１）教育情報セキュリティポリシー等の遵守

教職員等は、教育情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに教育情報セキュリティ管理者に相談し、指示を仰がなければならない。

（２）執務上での管理

①執務室の施錠管理

執務室にて教職員等が不在となる場合には、執務室を施錠しなければならない。

②来校者等への対応

来校者等を執務室に入れる場合には、教育情報セキュリティ管理者または学校情報セキュリティ担当者の許可を求めなければならない。

③机上の書類・端末等の管理

教職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は教育情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

（３）支給端末の取り扱い

①教職員等は、業務目的以外で支給端末を利用してはならない。

②教職員等は、外部のソフトウェアを無断で支給端末にインストールしてはならない。業務上必要

な場合には、事前に学校セキュリティ管理者の許可を得なければならない。

③教職員等は、支給端末の利用において、下記のカスタマイズを無断でしてはならない。

（ア）セキュリティ機能に関する設定変更

（イ）メモリ増設等の改造

④教職員等は、モバイル端末を利用する場合は、盗難・紛失リスクに備えての安全管理をしなければならない。

⑤業務端末から離れる時は、端末をロックするなど、他者が閲覧できないようにしなければならない。

⑥業務終了後と外出時には、電源を落とさなければならない。

（４）支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

①教職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、教育情報セキュリティ管理者の許可を得て利用することができる。

②教職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、教育情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

（５）モバイル端末や電磁的記録媒体等の持ち出し及び教育委員会・学校が構築・管理している環境（本ガイドラインが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境）の外部における情報処理作業の制限

①教職員等は、学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、教育情報セキュリティ管理者の許可を得なければならない。

②教職員等は、外部で情報処理業務を行う場合には、教育情報セキュリティ管理者の許可を得なければならない。

（６）IDの取扱い

教職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。

①自己が利用しているIDは、他人に利用させてはならない。

②共用IDを利用する場合は、共用IDの利用者以外に利用させてはならない。

③教職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括教育情報セキュリティ責任者又は教育情報システム管理者に通知しなければならない。

（７）パスワードの取扱い

教職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

①パスワードは、他者に知られないように管理しなければならない。

②パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

③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。

④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管理者に直ちに報告し、パスワードを速やかに変更しなければならない。

⑤複数の教育情報システムを扱う教職員等は、同一のパスワードを複数のシステム間で用いてはならない。（シングルサインオンを除く）

⑥仮のパスワード（初期パスワードを含む）は、最初のログイン時点で変更しなければならない。
⑦サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。
⑧教職員等間でパスワードを共有してはならない（ただし、共有IDに対するパスワードは除く）。
⑨共有IDに対するパスワードは定期的に又はアクセス回数に基づいて変更しなければならない。

（８）外部電磁的記録媒体の取り扱い

①利用する外部電磁的記録媒体は教育委員会又は学校から支給された公式の媒体を使用しなければならない。その他の媒体は使用禁止とする。
②業務上やむを得ず、公式以外の電磁的記録媒体を使用する場合は、ウイルスチェックでウイルス感染がされていないことが確認でき、教育情報セキュリティ管理者の許可を得た上で使用しなければならない。
③外部電磁的記録媒体は、職員室の書庫等の鍵のかかる場所に施錠保管しなければならない。

（９）電子メールの利用制限

①教職員等は、自動転送機能を用いて、電子メールを転送してはならない。
②教職員等は、業務上必要のない送信先に電子メールを送信してはならない。
③教職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
④教職員等は、重要な電子メールを誤送信した場合、教育情報セキュリティ管理者に報告しなければならない。
⑤教職員等は、ウェブで利用できるフリーメールサービス等を統括教育情報セキュリティ責任者の許可無しに業務利用してはならない。
⑥情報ファイルを添付する場合には、パスワード設定等の対策を講じなければならない。その際、パスワードを同一メールに記載してはならない。
⑦送信時には誤送信を予防するため、送信先のメールアドレス、添付ファイルの内容を確認しなければならない。
⑧差出人、添付ファイル又は本文中のリンク先等が不審なメールを受信した場合には、添付ファイルの閲覧やリンク先（URL）にアクセスせずに、教育情報セキュリティ管理者に指示を仰がなければならない。

（１０）クラウドサービス、ソーシャルメディアサービスの利用制限

①重要性分類Ⅱ以上の情報資産を、インターネットを通信経路としたパブリッククラウドサービスで取り扱ってはならない。なお、強固なアクセス制御による対策を講じたシステム構成の場合は、その限りではない。
②私的に契約したクラウドサービスを業務利用してはならない。
③ソーシャルメディアサービスを利用して、業務上知り得た情報を公開してはならない。

（１１）不正プログラム対策に関する教職員等の遵守事項

教職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。OS及びコンピュータウイルス対策ソフトウェアが常に最新の状態に保てるようにしなければならない。自動更新される設定の場合は、自動更

新設定を変えてはならない。

②外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

③差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

④端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

⑤添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

⑥統括教育情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、直ちに教育情報セキュリティ管理者に報告し、指示を仰がなければならない。また、以下の対応を行わなければならない。

（ア）パソコン等の端末の場合

有線LANにつながる業務端末（校務用端末等）の場合は、LANケーブルの即時取り外しを行わなければならない。

（イ）モバイル端末の場合

無線LANにつながる業務端末（指導者用端末及び学習者用端末）の場合は、直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

（ウ）指示があるまでは、端末の電源は切らずに保持しなければならない。

（１３）電子署名・暗号化

①教職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、CISOが定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

②教職員等は、暗号化を行う場合にCISOが定める以外の方法を用いてはならない。また、CISOが定めた方法で暗号のための鍵を管理しなければならない。

③CISOは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

（１４）無許可ソフトウェアの導入等の禁止

①教職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

②教職員等は、業務上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、教育情報セキュリティ管理者又は教育情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

③教職員等は、不正にコピーしたソフトウェアを利用してはならない。

（１５）機器構成の変更の制限

①教職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

②教職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要があ

る場合には、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なければならない。

（１６）ネットワークの取り扱い

①教職員等は、統括教育情報セキュリティ責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

②無線アクセスポイントを増設したい場合、教育情報システム管理者に増設の可否についての判断を仰がなければならない。

③ネットワークの配線を変更する際は、教育情報システム責任者またはその代理の者の立ち会いのもと行わなければならない。

（１７）業務以外の目的でのウェブ閲覧の禁止

教職員等は、業務以外の目的でウェブを閲覧してはならない。

（１８）外部からのアクセス等の制限

①教職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、教育情報セキュリティ管理者を介して、統括教育情報セキュリティ責任者及び当該情報システムを管理する教育情報システム管理者の許可を得なければならない。

②教職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を施設内のネットワークに接続する前に、アンチウイルス等を通じて、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

（１９）児童生徒への指導事項

教職員等は、児童生徒に学習者用端末等を利用させるにあたり、以下の事項について指導を行わなければならない。

①学習用途の利用限定

学習者用端末及び学習系クラウドサービスは学習目的で利用すること。

②利用者認証情報の秘匿管理

ID及びパスワードは他の人に知られないようにすること。

③ウイルス対策ソフトウェアの管理

ウイルス対策ソフトウェアは常に最新の状態に保つこと。

④端末のソフトウェアに関するセキュリティ機能の設定変更禁止

利用する端末のセキュリティ機能の設定を、許可なく変更してはならないこと。

⑤学習系情報は学習系クラウドに保管

端末で生成した情報の保存先を学習系クラウドに指定できる機能がある場合には、この機能を利用して原則学習系クラウドに保管し、学習者用端末にローカル保存は必要最小限とすること。

⑥無断で外部ソフトウェアをインストール禁止

無断で外部ソフトウェアをインストールしないようにすること。

⑦コミュニケーションツールの利用制限

学校から許可されたコミュニケーションツール（SNS,チャット等）のみを利用すること。

⑧ウイルス感染が疑われる場合の報告

学習用端末が動かない、勝手に操作されている、いつもと異なる画面や警告が表示されるなどの

症状がでた場合、すぐに担任教員に報告すること。

⑨端末の安全な取り扱い

学習用端末は大事に取り扱い、盗難・紛失・破損等に注意すること。

⑩私物端末利用禁止

私物端末など承認されていない端末を学校に持ち込んで、学校のネットワークにつながないこと。

（２０）異動・退職時等の遵守事項

教職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産（紙情報、データの格納された端末、外部記録媒体等）を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

５．３.教育委員会事務局職員の遵守事項

教育委員会事務局職員は、教育情報セキュリティ責任者の指導の下、以下の規定を遵守しなければならない。

（１）教育情報セキュリティポリシー等の遵守

（２）業務以外の目的での使用の禁止

（３）校務用端末による外部での情報処理作業の禁止

（４）重要性分類Ⅱ以上の情報資産について校務用端末以外のパソコン、モバイル端末及び電磁的記録媒体等によるアクセスの禁止

（５）知りえた情報の秘匿

（６）業務を離れる場合の遵守事項

異動、退職等により業務を離れる場合には、利用していた情報資産をすべて返却する。また、その後も業務上知り得た情報を漏らさない。

５．４．研修・訓練

（１）情報セキュリティに関する研修・訓練

CISO は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

（２）研修計画の策定及び実施

①CISO は、教職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、情報セキュリティ委員会の承認を得なければならない。

②新規採用の教職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

③研修は、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者及びその他教職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

④CISO は、毎年度 1 回、情報セキュリティ委員会に対して、教職員等の情報セキュリティ研修の実施状況について報告しなければならない。

（３）緊急時対応訓練

CISO は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワ

ーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

（４）研修・訓練への参加

全ての教職員等は、定められた研修・訓練に参加しなければならない。

５．５．情報セキュリティインシデントの連絡体制の整備

（１）学校内からの情報セキュリティインシデントの報告

①教職員等は、情報セキュリティインシデントを認知した場合、速やかに教育情報セキュリティ管理者に報告しなければならない。

②報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者、教育情報システム管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

③教育情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じて CISO 及び教育情報セキュリティ責任者に報告しなければならない。

（２）教職員等の報告義務

①教職員等は、教育情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括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に報告を行わなければならない。

②違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括教育情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

（３）住民等外部からの情報セキュリティインシデントの報告

①教職員等は、管理対象のネットワーク及び教育情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、教育情報セキュリティ管理者に報告しなければならない。

②報告を受けた教育情報セキュリティ管理者は、速やかに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に報告しなければならない。

③教育情報セキュリティ管理者は、当該情報セキュリティインシデントについて、必要に応じて CISO 及び教育情報セキュリティ責任者に報告しなければならない。

（４）情報セキュリティインシデント原因の究明・記録、再発防止等

①統括教育情報セキュリティ責任者は、情報セキュリティインシデントについて、教育情報セキュリティ管理者、教育情報システム管理者及び情報セキュリティに関する統一的な窓口と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。

②CISO は、統括教育情報セキュリティ責任者から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

（５）支給端末の運用・連絡体制の整備

学校内外での支給端末の運用ルールを制定し、インシデント時の連絡先対応方法を各学校にて整理し、実施手順に反映しなければならない。

６．技術的セキュリティ

６．１．コンピュータ及びネットワークの設定管理

（１）文書サーバの設定等

①教育情報システム管理者は、教職員等が使用できる文書サーバの容量を設定し、教職員等に周知しなければならない。

②教育情報システム管理者は、文書サーバを学校等の単位で構成し、教職員等が他の学校等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

③教育情報システム管理者は、住民の個人情報、人事記録等、特定の教職員等しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一学校等であっても、担当職員以外の教職員等が閲覧及び使用できないようにしなければならない。

④教育情報システム管理者は、インターネット接続を前提とする校務外部接続系サーバ及び学習系サーバに保管する情報（学習系サーバにおいては、個人情報などを含む重要性が高い情報を保管する場合に限る）については、標的型攻撃等によるファイルの外部流出の可能性を考慮し、ファイル暗号化等による安全管理措置を講じなければならない。

（２）バックアップの実施

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は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、次の①及び②に基づきバックアップを実施するものとする。

①校務系情報及び校務外部接続系情報については、必要に応じて定期的にバックアップを実施しなければならない。

②学習系情報については、必要に応じて定期的にバックアップを実施しなければならない。

（３）ログの取得等

①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は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

②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は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

③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は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（４）ネットワークの接続制御、経路制御等

①統括教育情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、所管するネットワークの内部におけるファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②統括教育情報セキュリティ責任者は、不正アクセスを防止するため、所管するネットワークに適切なアクセス制御を施さなければならない。

（５）外部の者が利用できるシステムの分離等

教育情報システム管理者は、保護者等の外部の者が利用できるシステム等がある場合、重要性が高い情報、特に情報資産重要性分類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情報資産以上を扱うシステムとの論理的又は物理的な分離、もしくは各システムにおけるアクセス権管理の徹底を行うこと。

（６）外部ネットワークとの接続制限等

①教育情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括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。

②教育情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内及び学校の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

③教育情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

④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は、ウェブサーバ等をインターネットに公開する場合、教育ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

⑤教育情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括教育情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（７）重要性が高い情報に対するインターネットを介した外部からのリスク、児童生徒による重要性が高い情報へのアクセスリスクへの対応

①校務系システム及び学習系システム間の通信経路の論理的又は物理的な分離をするとともに、ウェブ閲覧やインターネットメールなどのインターネットを介した外部からのリスクの高いシステムと重要性が高い情報（特に校務系）を論理的又は物理的に分離をしなければならない。

②教育情報システム管理者は、校務系システムとその他のシステム（校務外部接続系システム、学習系システム）との間で通信する場合には、各システムにおけるアクセス権管理の徹底を行う等の適切な措置を図らなければならない。また、ネットワーク分離による対策を講じたシステム構成ではウイルス感染のない無害化通信など、適切な措置を図らなければならない。

（８）複合機のセキュリティ管理

①統括教育情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

②統括教育情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③統括教育情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（９）特定用途機器のセキュリティ管理

統括教育情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線

への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

（１０）無線 LAN 及びネットワークの盗聴対策

①統括教育情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な通信経路の暗号化及び認証技術の使用を義務付けなければならない。

②統括教育情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、通信経路の暗号化等の措置を講じなければならない。

（１１）電子メールのセキュリティ管理

統括教育情報セキュリティ責任者メールサーバの管理・制御している大分県に対し以下のように依頼をしなければならない。

①権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行う。

②大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止する。

③電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能とする。

６．２．アクセス制御

（１）アクセス制御等

統括教育情報セキュリティ責任者又は教育情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員等がアクセスできないように、システム上制限しなければならない。特に強固なアクセス制御による対策を講じたシステム構成の場合、重要な情報資産へのアクセスについては、多要素認証等のアクセスの真正性に関する要素技術を取り入れることで、当該システムへの認証強度の向上とアクセス権管理を徹底すること。

（２）外部からのアクセス等の制限

①統括教育情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

②統括教育情報セキュリティ責任者は、民間事業者等の外部組織からのシステムアクセスを認める場合、アクセスする利用者の本人確認、システムアクセスの対象となる児童生徒の本人（保護者）からの同意を得る等の措置を講じなければならない。

③統括教育情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために通信経路の暗号化等の措置を講じなければならない。

④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は、外部からのアクセスに利用するモバイル端末を教職員等に貸与する場合、モバイル端末管理（MDM）の導入等を通じて、セキュリティ確保のために必要な措置を講じなければならない。

⑤統括教育情報セキュリティ責任者は、外部から教育ネットワークに接続することを許可する場合は、利用者の ID 及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（３）ログイン時の表示等

教育情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ教職員等がログインしたことを確認することができるようシステムを設定しなければならない。

（４）特権による接続時間の制限

教育情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

６．３．システム開発、導入、保守等

（１）情報システムの調達

①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は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

②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は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（２）情報システムの開発

①システム開発における責任者及び作業者の特定

教育情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

②システム開発における責任者、作業者の ID の管理

（ア）教育情報システム管理者は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。

（イ）教育情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③システム開発に用いるハードウェア及びソフトウェアの管理

（ア）教育情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

（イ）教育情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

（３）情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

（ア）教育情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

（イ）教育情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（ウ）教育情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを

確認した上で導入しなければならない。

②テスト

（ア）教育情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

（イ）教育情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

（ウ）教育情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

（エ）教育情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

（オ）教育情報システム管理者は、運用環境への移行に先立ち、システムの脆弱性テストを行い、その結果を確認しなければならない。

（４）システム開発・保守に関連する資料等の整備・保管

①教育情報システム管理者は、システム開発･保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

②教育情報システム管理者は、テスト結果を一定期間保管しなければならない。

③教育情報システム管理者は、情報システムに係るソースコードならびに使用したオープンソースのバージョン（リポジトリ）を適切な方法で保管しなければならない。

（５）情報システムにおける入出力データの正確性の確保

①教育情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

②教育情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③教育情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（６）情報システムの変更管理

教育情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（７）開発・保守用のソフトウェアの更新等

教育情報システム管理者は、開発･保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（８）システム更新又は統合時の検証等

教育情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

６．４．不正プログラム対策

（１）統括教育情報セキュリティ責任者の措置事項

統括教育情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

①外部ネットワークから受信したファイルは、インターネットのゲートウェイなどにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

②外部ネットワークに送信するファイルは、インターネットのゲートウェイなどにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ教職員等に対して注意喚起しなければならない。

④所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑤不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

⑥不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑦業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

（２）情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

①教育情報システム管理者は、その所掌するサーバ及びパソコン等の端末を守るため、コンピュータウイルス等の不正プログラムへの対策を講じなければならない。

②不正プログラム対策は、常に最新の状態に保たなければならない。

③インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、市が管理している電磁的記録媒体以外を教職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

６．５．不正アクセス対策

（１）統括教育情報セキュリティ責任者の措置事項

統括教育情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

①使用されていないポート及びSSID（無線LANネットワーク名）を閉鎖しなければならない。

②不要なサービスについて、機能を削除又は停止しなければならない。

③不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、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へ通報するよう、設定しなければならない。

④統括教育情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

（２）攻撃の予告

CISO 及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

（３）サービス不能攻撃

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は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（４）標的型攻撃

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は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

６．６．セキュリティ情報の収集

（１）セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等

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は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（２）不正プログラム等のセキュリティ情報の収集及び周知

統括教育情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、教職員等に周知しなければならない。

（３）情報セキュリティに関する情報の収集及び共有

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は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

７．運用

７．１．情報システムの監視

（１）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は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。特に強固なアクセス制御による対策を講じたシステム構成の場合、重要な情報資産へのアクセスについては、侵入検知システム（IDS）や侵入防御システム（IPS）などの対策を講じなければならない。

（２）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は、重要なログ等を取得するサー

バの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

（３）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は、重要性分類Ⅱ以上の情報資産を格納する校務系システム及び校務外部接続系システムを常時監視しなければならない。

（４）内部からの攻撃監視

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は、教職員等及び外部委託事業者が使用しているパソコン等の端末からの所管するネットワークのサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

７．２．ドキュメントの管理

（１）システム管理記録及び作業の確認

①教育情報システム管理者は、所管する教育情報システムの運用において実施した作業について、作業記録を作成しなければならない。

②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は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

③統括教育情報セキュリティ責任者、教育情報システム管理者又は教育情報システム担当者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、2 名以上で作業し、互いにその作業を確認しなければならない。

（２）情報システム仕様書等の管理

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は、ネットワーク構成図、情報システム仕様書等について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりすること等がないよう、適切に管理しなければならない。

（３）障害記録の管理

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は、教職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（４）記録の保存

CISO 及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

７．３．教職員等の ID 及びパスワードの管理

（１）利用者 ID の取扱い

①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は、利用者の登録、変更、抹消等の情報管理、教職員等の異動、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

②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は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

（２）パスワードに関する情報の管理

①統括教育情報セキュリティ責任者又は教育情報システム管理者は、教職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

②統括教育情報セキュリティ責任者又は教育情報システム管理者は、教職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

７．４．児童生徒における ID 及びパスワード等の管理

（１）ID 登録・変更・削除

①入学/転入時の ID 登録処理

ID についてはシンプル・ユニーク（唯一無二）・パーマネント／パーシスタント（永続的な識別）な構成要素になっていることや、児童生徒の発達段階に応じた複雑性を上げたパスワードポリシーによりセキュリティ強度を上げていくなど適切な措置を講じなければならない。

ID 登録やパスワードポリシーにおいては情報セキュリティ対策として重要な要素であるため学校毎に管理するのではなく、同一の教育委員会等の組織にて一元管理することが望ましい。

②進級/進学時の ID 関連情報の更新

ID については原則として進級/進学にも変更不要とすることが望ましい。ID を変えることなく ID の属性情報（進級時の組・出席番号、進学先学校名など）の更新を行っておくことで、MDM による各種ポリシーや使用アプリケーションの変更を効率的に行うことが可能となる。

さらに統合型校務支援システム等における児童生徒の氏名と連動した ID 管理を行うことで、校務側で管理している属性情報と一体となった ID を含んだマスター管理の一元化が望ましい。

③転出/卒業/退学時の ID 削除処理

ユニークな ID は個人を識別できる可能性があるため、個人情報保護の観点から、サービス提供期間を超えて個人を特定する情報を保持しないようにする必要がある。

転出や卒業退学時に学習用ツールのサービス利用期間が終了する場合は、あらかじめ児童生徒本人によるデータ移行をサービス利用期間内に実施し、ID の利用停止後、最終的には ID 及び関連するデータの完全削除を行うこと。

ただし、本人同意や個人情報保護条例に従った適切な管理の下、一部のデータを活用することは可能である。

（２）多要素認証によるなりすまし対策

本人確認を厳格に行う必要がある場合においては児童生徒の ID/パスワードに加えて多要素認証を設定することが望ましい。

（３）学習用ツールへのシングルサインオン

学習履歴を活用したり、個人の成果物を保存するアプリケーションが増えてくると、サービス利用時に都度 ID/パスワード等の認証情報を入力したり、サービス毎のアカウント情報管理が非常に煩雑になるため、一度の認証により一定時間は各種サービスにアクセスが行えるシングルサインオ

ンの導入を行うことが望ましい。

７．５．特権を付与されたIDの管理等

（１）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は、管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理しなければならない。

（２）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特権を代行する者は、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が指名し、CISOが認めた者でなければならない。

（３）CISOは、代行者を認めた場合、速やかに統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者及び教育情報システム管理者に通知しなければならない。

（４）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は、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。

（５）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は、特権を付与されたID及びパスワードについて、その利用期間に合わせて特権IDを作成・削除する、もしくは、入力回数制限を設ける等のセキュリティ機能を強化しなければならない。

（６）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は、特権を付与されたIDを初期設定以外のものに変更しなければならない。

７．６．教育情報セキュリティポリシーの遵守状況の確認・管理

（１）遵守状況の確認及び対処

①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は、教育情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかにCISO及び統括教育情報セキュリティ責任者に報告しなければならない。

②CISOは、発生した問題について、適切かつ速やかに対処しなければならない。

③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は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

（２）パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

CISO及びCISOが指名した者は、不正アクセス、不正プログラム等の調査のために、教職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（３）業務以外の目的でのウェブ閲覧の禁止

統括教育情報セキュリティ責任者は、教職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、教育情報セキュリティ管理者に通知し適切な措置を求めなければならない。

（４）教職員等による不正アクセスの管理

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は、教職員等による不正アクセスを発見した場合は、当該教職員等が所属する学校等の教育情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

７．７．専門家の支援体制等

（１）専門家の支援体制

統括教育情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

（２）他団体との情報システムに関する情報等の交換

教育情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、統括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責任者の許可を得なければならない。

７．８．侵害時の対応等

（１）緊急時対応計画の策定

CISO 又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により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発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

（２）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

①関係者の連絡先

②発生した事案に係る報告すべき事項

③発生した事案への対応措置

④再発防止措置の策定

（３）業務継続計画との整合性確保

自然災害、大規模又は広範囲に及ぶ疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（４）緊急時対応計画の見直し

CISO 又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

７．９．例外措置

（１）例外措置の許可

教育情報セキュリティ管理者及び教育情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、学校事務及び教育活動の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、CISO の許

可を得て、例外措置を取ることができる。

（２）緊急時の例外措置

教育情報セキュリティ管理者及び教育情報システム管理者は、学校事務及び教育活動の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかにCISOに報告しなければならない。

（３）例外措置の申請書の管理

CISOは、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

７．１０．法令遵守

（１）職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

①地方公務員法（昭和25年法律第261号）

②教育公務員特例法（昭和24年1月12日法律第1号）

③著作権法（昭和45年法律第48号）

④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）

⑤個人情報の保護に関する法律（平成15年5月30日法律第57号）

⑥行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）

⑦サイバーセキュリティ基本法（平成26年法律第104号）

７．１１．懲戒処分等

（１）懲戒処分

教育情報セキュリティポリシーに違反した教職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

（２）違反時の対応

教職員等の教育情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

①統括教育情報セキュリティ責任者が違反を確認した場合は、統括教育情報セキュリティ責任者は当該教職員等が所属する学校の教育情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

②教育情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括教育情報セキュリティ責任者及び当該教職員等が所属する学校の教育情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

③教育情報セキュリティ管理者の指導によっても改善されない場合、統括教育情報セキュリティ責任者は、当該教職員等の教育ネットワーク又は教育情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括教育情報セキュリティ責任者は、教職員等の権利を停止あるいは剥奪した旨をCISO及び当該教職員等が所属する学校の教育情報セキュリテ

ィ管理者に通知しなければならない。

8．外部委託

（1）外部委託事業者の選定基準

教育情報システム管理者は、外部委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

（2）契約項目

情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・教育情報セキュリティポリシー及び教育情報セキュリティ実施手順の遵守
・外部委託事業者の責任者、委託内容、作業者、作業場所の特定
・提供されるサービスレベルの保証
・外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
・外部委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・市による監査、検査
・市による情報セキュリティインシデント発生時の公表
・教育情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

（3）確認・措置等

教育情報システム管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、（2）の契約に基づき措置しなければならない。また、その内容を統括教育情報セキュリティ責任者に報告するとともに、その重要度に応じて CISO に報告しなければならない。

（4）外部委託事業者に対する説明

教育情報システム管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

9．SaaS 型パブリッククラウドサービスの利用

9．1．SaaS 型パブリッククラウドサービスの利用における情報セキュリティ対策

（1）利用者認証

①統括教育情報セキュリティ責任者は、クラウド事業者における当該クラウドサービスを提供する情報システムの運用もしくは開発に従事する者又は管理者権限を有する者について、適切な利用者確認がなされていることをクラウド事業者に求め、サービス提供約款や契約書面上で確

認または合意しなければならない。

②統括教育情報セキュリティ責任者は、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クラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

③統括教育情報セキュリティ責任者側管理者権限を有する者の ID の管理について、「７．６．特権を付与された ID の管理等」を遵守しなければならない。

（２）アクセス制御

①統括教育情報セキュリティ責任者は、当該クラウドサービスに対して、アクセスする権限のない者がアクセスできないように、システム上制限する機能の提供をクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

②統括教育情報セキュリティ責任者は、クラウド事業者の提供するアクセス制御機能を用いて、情報資産毎に、許可されたクラウドを利用する教職員等及び児童生徒のみがアクセスできる環境を設定しなければならない。

（３）クラウドに保管するデータの暗号化

①統括教育情報セキュリティ責任者は、当該クラウドサービスへのデータの保管に際し、情報漏えい等に備えて、暗号化等の保護措置を講じられていることを、クラウド事業者にサービス提供約款や契約書面上で確認または合意しなければならない。

（４）マルチテナント環境におけるテナント間の安全な管理

①統括教育情報セキュリティ責任者は、複数の統括教育情報セキュリティ責任者がクラウドリソースを共用する環境において、特定の統括教育情報セキュリティ責任者に対して発生したセキュリティ侵害が、他の統括教育情報セキュリティ責任者に影響を与えないように対策が講じられていることを、クラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

（５）クラウドサービスを提供する情報システムに対する外部からの悪意のある脅威の侵入を想定した技術的セキュリティ対策

①統括教育情報セキュリティ責任者は、当該クラウドサービスを提供する情報システムを監視し、セキュリティ侵害を検知することを、クラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

②統括教育情報セキュリティ責任者は、当該クラウドサービスを提供する情報システムのインターネット接続境界において、統括教育情報セキュリティ責任者以外による不正な通信・侵入を防ぐ措置を講じるとともに、外部脅威の侵入を検知し、防御する対策を講ずることを、クラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

（６）情報の通信経路のセキュリティ確保

①統括教育情報セキュリティ責任者は、教育情報システムのインターネット境界から当該クラウドサービスを提供する情報システムまでの情報の通信経路において、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）をクラウド事業者に求め、合意のうえ、利用しなければならない。

②統括教育情報セキュリティ責任者は、クラウド事業者が保守運用等を遠隔で行う場合の、保守運

用拠点と管理区域間での通信回線及び通信回線装置の管理について、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準･手順等の整備、通信の暗号化等）をクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

（７）クラウドサービスを提供する情報システムの物理的セキュリティ対策

①統括教育情報セキュリティ責任者は、当該クラウドサービスのサーバ等の管理条件を「４．１．サーバ等の管理」に準じた対策をクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

②統括教育情報セキュリティ責任者は、クラウド事業者側の管理区域（サーバ等を設置）及び保守運用拠点の管理において、「４．２.管理区域情報システム室等の管理（教育委員会等のサーバ室にサーバを設置している場合)」に準じた対策をクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

③統括教育情報セキュリティ責任者は、クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）にあたり、セキュリティを確保した対応となっているかをクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

なお、当該確認に当たっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

（８）クラウドサービスを提供する情報システムの運用管理

①統括教育情報セキュリティ責任者は、クラウド事業者に対して、サービスの一時停止等クラウドを利用する教職員等に影響があり得る運用手順の有無、有る場合にはクラウドを利用する教職員等への影響範囲（時間、サービス内容)、連絡方法等について情報提供を求め、統括教育情報セキュリティ責任者が業務運営に支障がないことを確認し、合意しなければならない。また、クラウド事業者の設定不備等によるインシデント発生時にも同様の確認をしなければならい。

②統括教育情報セキュリティ責任者は、当該クラウドサービスにおけるサーバの冗長化について、「４．１．サーバ等の管理（2）サーバの冗長化」に準じた対策をクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

③統括教育情報セキュリティ責任者は、当該クラウドサービスにおけるデータバックアップ及び復旧手順について、「６．１．コンピュータ及びネットワークの設定管理（2）バックアップの実施」に準じた対策をクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

④統括教育情報セキュリティ責任者は、当該クラウドサービスにおける情報セキュリティの確保や監査に必要なログの取得について、「６．１.コンピュータ及びネットワークの設定管理（3）ログの取得等」に準じた対策をクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

（９）クラウドサービスを提供する情報システムのマルウェア対策

①統括教育情報セキュリティ責任者は、クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等について、マルウェア対策を講じることをクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

②統括教育情報セキュリティ責任者は、内部システムに侵入した攻撃を検知して対処するために、通信をチェックする等の対策を講じることをクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

（１０）統括教育情報セキュリティ責任者側のセキュリティ確保

①統括教育情報セキュリティ責任者は、クラウドサービスにアクセスするクラウドを利用する教職員等及び児童生徒側端末について、保管するデータの外部流出、改ざん等から保護するために必要な措置を講じなければならない。

②統括教育情報セキュリティ責任者は、標的型攻撃による外部からの脅威の侵入を防止するために、クラウドを利用する教職員等及び児童生徒への教育や入口対策を講じなければならない。

（１１）クラウド事業者従業員の人的セキュリティ対策

①統括教育情報セキュリティ責任者は、クラウドサービスに関わるクラウド事業者従業員に対して、クラウド事業者の情報セキュリティポリシー及び保守運用管理規程等を遵守することをクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

②統括教育情報セキュリティ責任者は、クラウドサービスに関わるクラウド事業者従業員に対して、業務に用いる ID 及びパスワードその他の個人認証に必要な情報及び媒体について、部外者及び業務に関わらない従業員に漏えいすることがないように、適切に管理することをクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

③統括教育情報セキュリティ責任者は、クラウドサービスに関わらない従業員等が統括教育情報セキュリティ責任者のデータを知り得る状態にならないよう、業務に関わるクラウド事業者従業員に対して秘匿を義務づけることをクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

④統括教育情報セキュリティ責任者は、統括教育情報セキュリティ責任者のデータ及びデータを格納した端末機器又は電磁的記録媒体の外部持ち出しについて、統括教育情報セキュリティ責任者の許可なく外部持ち出しできないこと及び外部持ち出しにおける安全管理手順をクラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

⑤統括教育情報セキュリティ責任者は、クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等に、マルウェアを侵入させないよう、クラウド事業者に求め、サービス提供約款や契約書面上で確認または合意しなければならない。

（１２）サービス終了時等のデータの廃棄及び利用者アカウント抹消について

①統括教育情報セキュリティ責任者は、サービス利用終了時等において、統括教育情報セキュリティ責任者のデータ及び利用者アカウント情報が不用意に残置されないよう、適切に破棄するための流れについてサービス提供約款や契約書面上で確認または合意しておかなければならない。

②統括教育情報セキュリティ責任者は、サービス利用終了時等におけるデータの扱いについて、スムーズに回収、次期システムへの移行等を行えるよう、その措置の流れについてサービス提供約款や契約書面上で確認または合意しておかなければならない。

③統括教育情報セキュリティ責任者は、クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

（１３）クラウドサービス要件基準を満たす配慮を含めたネットワーク設計

①統括教育情報セキュリティ責任者は、利用するクラウドサービスの要件規準を確認し、要件規準を満たすネットワークを設計しなければならない。

９．２．SaaS 型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項

（１）守秘義務、目的外利用及び第三者への提供の禁止

①統括教育情報セキュリティ責任者は、クラウド事業者と契約時に守秘義務、目的外利用及び第三者への提供の禁止条項を締結しなければならない。クラウドサービス事業者がコンテンツにアクセスできるかどうかを確認し、サービスに係る情報及び受託した情報に関する守秘義務、目的外利用及び第三者への提供の禁止条項について、サービス提供に係る契約に含めなければならない。契約には、当該条項に違反したクラウドサービス事業者に対する損害賠償規定を含める。

（２）準拠する法令、情報セキュリティポリシー等の確認

①統括教育情報セキュリティ責任者は、クラウド事業者がどのような規範に基づいてサービス提供するか開示を求め、統括教育情報セキュリティ責任者の準拠する法令、情報セキュリティポリシーを確認し、それらとの整合を確認しなければならない。（クラウド事業者の準拠する認証制度、個人情報保護指針、プライバシーポリシー、情報セキュリティに関する基本方針及び対策基準、保守運用管理規程等）

（３）クラウド事業者の管理体制

①統括教育情報セキュリティ責任者は、クラウド事業者に対して、情報セキュリティポリシー等の遵守を担保する管理体制が整備されているか、クラウド事業者の組織体制を確認し、合意しなければならない。確認すべき項目例を下記に示す。

（ア）サービスの提供についての管理責任を有する責任者の設置

（イ）情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理者）の設置

（ウ）サービスの提供に係る情報システムの運用に関する事務を統括する責任者の設置

（４）クラウド事業者従業員への教育

①統括教育情報セキュリティ責任者は、クラウド事業者に、従業員に対して個人情報保護等の関係法令、守秘義務等、業務遂行に必要な知識、意識向上のための適切な教育及び訓練を実施し、充分な知識とセキュリティ意識を醸成することを求めなければならない。

②統括教育情報セキュリティ責任者は、クラウド事業者に、従業員への上記育成計画、教育実績等の情報を提示させ、自らデータを管理する場合と同様の教育・訓練を実施しているかを確認しなければならない。

（５）情報セキュリティに関する役割の範囲、責任分界点

①統括教育情報セキュリティ責任者は、クラウド事業者の情報セキュリティに関する役割の範囲と責任分界点について開示するよう求めなければならない。

②統括教育情報セキュリティ責任者は、クラウド事業者の情報セキュリティに関する役割の範囲と責任分界点が統括教育情報セキュリティ責任者側で講ずる情報セキュリティ対策の役割の範囲と整合することを確認し、合意しなければならない。

（６）監査

①統括教育情報セキュリティ責任者は、クラウドサービスの監査状況、範囲・条件、内容等についてクラウド事業者に開示するよう求めなければならない。

②統括教育情報セキュリティ責任者は、クラウド事業者によるクラウドサービスに関する監査レポート等を根拠にして、自らの関係法令、情報セキュリティポリシーと照らし合わせ、安全性が確保されているかについて確認しなければならない。

（７）情報インシデント管理及び対応フローの合意

①統括教育情報セキュリティ責任者は、情報セキュリティインシデント管理に関する責任範囲、及びインシデント対応フローを、サービス仕様の一部として定めることについて、クラウド事業者に対して求めなければならない。

②統括教育情報セキュリティ責任者は情報セキュリティインシデント管理に関する責任範囲、及びインシデント対応フローを検証し、インシデントに備えた組織体制を整備しなければならない。

（８）クラウドサービスの提供水準及び品質保証

①統括教育情報セキュリティ責任者は、クラウドサービスの提供水準（サービス内容、提供範囲等）と品質保証（サービス稼働率、故障等の復旧時間等）を確認するとともに、それらの水準・品質が、業務遂行に求められる要求水準を満たすことを確認し、合意しなければならない。

（９）クラウド事業者の再委託先等との合意事項

①統括教育情報セキュリティ責任者は、クラウド事業者と合意したサービス履行内容及び情報セキュリティ対策について、クラウド事業者自らが実施する内容と、再委託先等に委託する内容も含めて提示することをクラウド事業者に求めなければならない。また、サプライチェーンリスク対策が適切に講じられていることをクラウド事業者に求めなければならない。

②統括教育情報セキュリティ責任者は、①の提示内容が、クラウド事業者と合意したサービス履行内容及び情報セキュリティ対策と整合していることを確認しなければならない。

（１０）その他留意事項

①統括教育情報セキュリティ責任者は、クラウド事業者がサービスを安定して提供可能な企業・団体であるかについて考慮しなければならない。

②統括教育情報セキュリティ責任者は、クラウド事業者間でのデータ形成の互換性が必ずしも保証されている訳ではないことから、事業者を変更する際のデータ移行の方法などについて、クラウド事業者にサービス提供約款や契約書面上で確認または合意しなければならない。

③統括教育情報セキュリティ責任者は、クラウド事業者に対して、クラウドサービスにおいて扱う情報資産や情報システム等について、日本の法令が適用されること及び係争等における管轄裁判所が日本国内であることを確認すること。

④統括教育情報セキュリティ責任者は、クラウド事業者において個人情報の適切な管理が行われているか確認するとともに、確認した項目については、調達時においてサービスの過剰な排除にならないよう留意した上で、契約要件等として定めなければならない。

９．３．SaaS 型パブリッククラウドサービス利用における教職員等の留意点

（1）ID・パスワード等の秘匿

①教職員等は、ID・パスワードについて秘匿管理を行わなければならない。

②教職員等は、多要素認証に必要な要素（知識、生体、物理）についても適切に管理を行わなければならない。もし該当要素が流出等したと考えられる場合には、速やかに教育情報セキュリティ管理者に報告しなければならない。

（2）モバイル端末持ち歩きリスク

教職員等は、クラウドサービスにアクセスする際に活用するモバイル端末について、紛失・盗難を避けるよう、適切に管理しなければならない。

（3）重要性分類に基づく情報管理

パブリッククラウド上で重要な情報（重要性分類 II 以上）を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じる必要がある。

（4）学校外からのパブリッククラウド利用

①教職員等は、学校外からクラウドサービスを利用する際、情報資産の取扱いをクラウドサービス上のみで行うことを原則とする。

②クラウドサービスから端末にファイルをダウンロードする際は、情報資産の外部持ち出しに基づく安全管理措置として、端末の安全性を事前に確認するとともに、作業が終わり次第当該端末から情報資産をすみやかに消去しなければならない。

（5）SaaS 型パブリッククラウドサービスの学習用途、校務用途混在リスクへの対応

①教職員等は、強固なアクセス制御による対策を講じたシステム構成にてクラウドサービスを利用している場合には、クラウドサービスを学習用途と校務用途で適切に使い分けるよう、共有先やダウンロード方法等の運用ルールについてあらかじめ確認し、適切に運用しなければならない。

②教職員等は、ネットワーク分離による対策を講じたシステム構成の場合にてクラウドサービスを利用している場合には、クラウドサービスを学習用途と校務用途で使い分けるよう、適切に運用しなければならない。

9．4．約款による外部サービスの利用

（1）約款による外部サービスの利用に係る規定の整備

①教育情報システム管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、機密性の高い情報の取扱いには十分に留意するように規定しなければならない。

（ア）約款によるサービスを利用してよい範囲

（イ）業務により利用する約款による外部サービス

（ウ）利用手続及び運用手順

（2）約款による外部サービスの利用における対策の実施

教職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

９．５．ソーシャルメディアサービスの利用

（１）教育情報システム管理者は、教育委員会又は学校が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

①本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

②パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

（２）重要性分類Ⅲ以上の情報はソーシャルメディアサービスで発信してはならない。

（３）利用するソーシャルメディアサービスごとの責任者を定めなければならない。

１０．評価・見直し

１０．１．監査

（１）実施方法

CISO は、情報セキュリティ監査統括責任者を指名し、教育ネットワーク及び教育情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

（２）監査を行う者の要件

①情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

②監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

（３）監査実施計画の立案及び実施への協力

①情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、中津市教育情報化推進委員会の承認を得なければならない。

②被監査部門は、監査の実施に協力しなければならない。

（４）委託事業者に対する監査

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、教育情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

（５）報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、中津市教育情報化推進委員会に報告する。

（６）保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

（７）監査結果への対応

CISO は、監査結果を踏まえ、指摘事項を所管する教育情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない教育情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

（８）情報セキュリティポリシー及び関係規程等の見直し等への活用

中津市教育情報化推進委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

１０．２．自己点検

（１）実施方法

①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は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

②教育情報セキュリティ責任者は、教育情報セキュリティ管理者と連携して、所管する部局における教育情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

（２）報告

統括教育情報セキュリティ責任者、教育情報システム管理者及び教育情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、中津市教育情報化推進委員会に報告しなければならない。

（３）自己点検結果の活用

①教職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

②中津市教育情報化推進委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

１０．３．教育情報セキュリティポリシー及び関係規程等の見直し

（１）中津市教育情報化推進委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

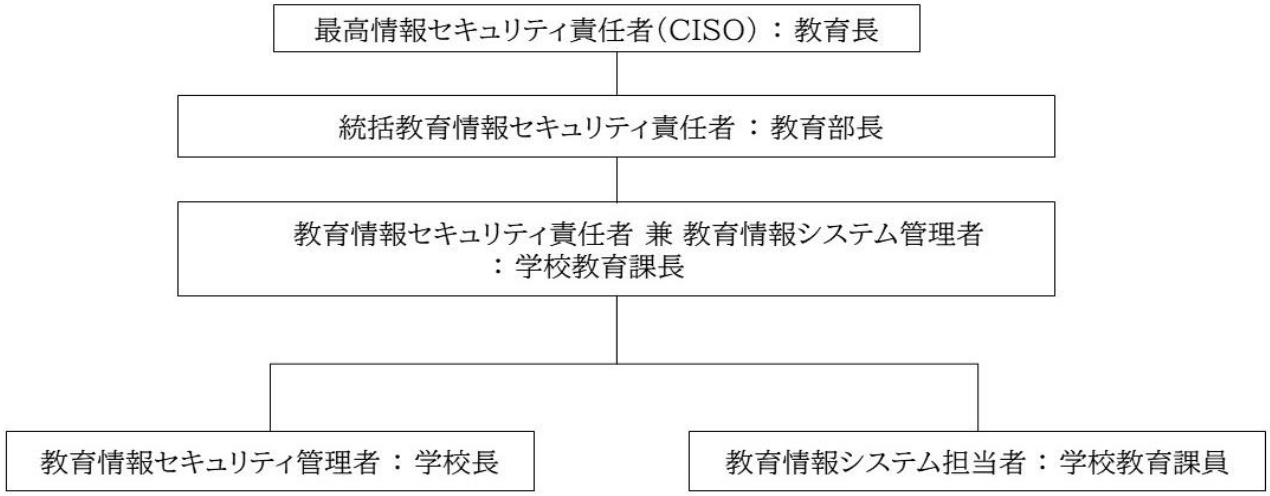
中津市教育情報セキュリティポリシー（概要版）

中津市教育委員会

1　情報資産とは

情報資産とは、業務を実施するのに必要な情報及びそれを扱う情報システムをいう。

2　組織体制



3　情報資産の分類と管理方法

（1）情報資産の分類

本教育委員会では情報資産を以下のように分類し、様々な脅威から守るための対策を実施する。

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。

（2）標準情報資産台帳の作成

学校で標準的に所管する情報資産について標準情報資産台帳を作成し、適宜更新しなければならない。

（3）情報資産の取り扱い

業務以外の目的に情報資産の利用をしてはならない。利用する場合は情報資産の分類に応じ、適正な取り扱いをしなければならない。

（4）情報資産の保管

耐火、耐震、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

（5）情報資産の外部持ち出し・送信

重要性分類Ⅲ以上の情報資産を外部に持ち出す場合、電子メール等で送信する場合は、アクセス制限や暗号化等の設定を行い、教育情報セキュリティ管理者の許可を得なければならない。

（６）情報資産の廃棄

電磁的記録媒体及び文書等が不要になった場合は、物理的に破壊するなど、情報を復元できないようにしたうえで廃棄しなければならない。

４　人的セキュリティ

（１）離席時の対応

①離席時には、パソコンやモバイル端末をロックしなければならない。また電磁的記録媒体、文書等を容易に閲覧されない場所へ保管しなければならない。

（２）端末の取り扱い

①支給された端末のみ業務で使用することができ、私物のパソコンやモバイル端末を業務で使用してはいけない。

②業務目的外で支給端末を使用することはできない。

③業務終了後と外出時には、電源を落とさなければならない。

（３）電磁的記録媒体の取り扱い

①教育委員会又は学校から支給された公式の電磁的記録媒体を使用しなければならず、私物の電磁的記録媒体を使用することはできない。

②業務上やむを得ず、公式以外の電磁的記録媒体を使用する場合は、ウイルスチェックでウイルス感染がされていないことが確認でき、教育情報セキュリティ管理者の許可を得た上で使用しなければならない。

③外部電磁的記録媒体は、職員室の書庫等の鍵のかかる場所に施錠保管しなければならない。

（４）ID・パスワードの取扱い

①自己が利用している ID・パスワードは、他人に利用させてはならない。また利用されないように管理しなければならない。

（５）電子メールの取り扱い

①複数人に電子メールを送信する場合、他の送信先の電子メールアドレスが分からないようにしなければならない。

②電子メールに情報ファイルを添付する場合、パスワード設定をする必要があり、そのパスワードを同一メールに記載してはならない。

③差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

（６）ネットワークの取り扱い

①無線アクセスポイントを増設したい場合、教育情報システム管理者に増設の可否についての判断を仰がなければならない。

②ネットワークの配線を変更する際は、教育情報システム責任者またはその代理の者の立ち会いのもと行わなければならない。

５　運用

（１）教育情報セキュリティポリシーの遵守状況の管理

教育情報セキュリティ管理者は教育情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに CISO 及び統括教育情報セキュリティ責任者に報告しなければならない。

（２）懲戒処分

教育情報セキュリティポリシーに違反した者は、その重大性や状況等に応じて、地方公務員法による懲戒処分の対象とする。

６　評価・見直し

（１）自己点検

①教育情報セキュリティ管理者は、教育情報セキュリティポリシーに沿った情報セキュリティ対策状況について、必要に応じて自己点検を行わなければならない。

②教職員等は、自己点検の結果に基づき、改善を図らなければならない。

6月21日～7月31日　教育委員会　報告

6月

日・曜	時間	催　し　物	場　所	備　考
21日（土）		学びのススメ土曜塾	各公民館、コミュニティーセンター等	
		中津市放課後子ども教室	各公民館、コミュニティーセンター等	
	14：00	美術鑑賞講座「美術のすすめ」	小幡記念図書館視聴覚室	
	18：00	中津市連合子ども会育成会協議会総会	新博多町交流センター	
22日（日）	10：00	日本語教室「あい♡ことば」	豊田公民館	
23日（月）	11：00	おはなし会(幼児向け)	小幡記念図書館	
24日（火）	9：00	八面山美術展巡回展～7/13	中津市歴史博物館	
	13：30	公民館長会議、教育コーディネーター会議、消防訓練	豊田公民館	
25日（水）	10：30	中津市学校のあり方検討委員会学校視察	国東市立志成学園・豊後高田市立戴星学園	教育長他
26日（木）				
27日（金）				
28日（土）		学びのススメ土曜塾	各公民館、コミュニティーセンター等	
		中津市放課後子ども教室	各公民館、コミュニティーセンター等	
	14：00	上映会（一般）「52ヘルツのクジラたち」	小幡記念図書館視聴覚室	
29日（日）	11：00	日曜おはなし会（幼児向け）	小幡記念図書館視聴覚室	
	13：30	日本語教室「きらきら」	如水コミュニティーセンター	
30日（月）				

7月

日・曜	時間	催　し　物	場　所	備　考
1日（火）		市教委学校訪問		
	16：00	緑ヶ丘中学校区（大幡小学校区、三保小学校区、鶴居小学校区）ネットワーク会議	鶴居コミュニティーセンター	
2日（水）				
3日（木）	18：00	職人フェスティバル第2回実行委員会	北部集会所	
4日（金）	13：30	中津市公民館運営審議会	中津市役所4階研修室	教育長他
	15：30	中津市社会教育委員会議	中津市役所4階研修室	教育長他
5日（土）		中学校統一公開日	各中学校	
		中津市放課後子ども教室	各公民館、コミュニティーセンター等	
	14：00	上映会(一般) 「ロッタちゃんとはじめてのおつかい」	小幡記念図書館視聴覚室	
6日（日）		ジュニアグローバルリーダー研修（13日まで）	グアム	
		祇園車展示（～7/20まで）	歴史博物館	
	10：00	中津市生涯を通じた障がい者の学び支援事業 まなびば	三光コミュニティーセンター	
7日（月）	11：00	おはなし会(幼児向け)	小幡記念図書館視聴覚室	

7月

日・曜	時間	催し物	場所	備考
8日（火）	10：00	大分県地域婦人団体連合会リーダー研修会	ビーコンプラザ 別府国際コンベンションセンター	
	10：30	中津市青少年健全育成市民会議叙任理事会	大幡コミュニティーセンター研修室	
	12：30	赤ちゃん絵本の読み聞かせ事業「はじめましてひらくっちゃん」	三光コミュニティーセンター	
	14：30	中津市青少年健全育成市民会議総会・研修会	大幡コミュニティーセンター集会室	市長・教育長他
9日（水）		市教委学校訪問		
	13：00	大分県教育庁 中津市生涯学習社会教育に係る行政意見交換会	中津市教育委員会事務局会議室2	
10日（木）		市教委学校訪問		
	13：00	中津地区公民館連合会公民館振興大会・第1回社会教育研究集会	宇佐市長洲公民館	
	15：30	令和7年度中津市立学校職員衛生委員会・衛生管理部会合同会議	中津下毛教育会館	教育長他
11日（金）	14：00	図書館講座「大人のペーパークラフト講座」	小幡記念図書館研修室	
	14：15	第3回定例校長会議	研修室	
	18：30	第5回中津市学校のあり方検討委員会	教育委員会室	教育長他
12日（土）		学びのススメ土曜塾	各公民館、コミュニティーセンター等	
		中津市放課後子ども教室	各公民館、コミュニティーセンター等	
	9：00	戦後80年 戦争の記憶展（～9/15まで）	歴史博物館	
	13：30	中津少年少女発明クラブ第2回講座	中津市生涯学習センター まなびん館	
	14：00	上映会(児童) 「きらきらシャンシャンおほしさま★げんきげんきノンタン」	小幡記念図書館視聴覚室	
13日（日）	13：30	日本語教室「きらきら」	如水コミュニティーセンター	
14日（月）	11：00	おはなし会(幼児向け)	小幡記念図書館視聴覚室	
	15：00	第2回教頭会議		
15日（火）	13：30	いじめ問題専門委員会		
16日（水）	10：00	あかちゃんタイム	小幡記念図書館	
	11：00	赤ちゃんおはなし会	小幡記念図書館視聴覚室	
	15：30	特別支援連携協議会		
17日（木）				
18日（金）		1学期終業式	各幼・小中学校	
19日（土）		中津市放課後子ども教室	各公民館、コミュニティーセンター等	
		学びのススメ土曜塾	各公民館、コミュニティーセンター等	
	9：00	八面山美術展巡回展～8/24	道の駅なかつ	
	14：00	上映会(一般) 「あまのがわ」	小幡記念図書館視聴覚室	
20日（日）	10：00	日本語教室「あい♡ことば」	教育福祉センター	
21日（月）				

7月

日・曜	時間	催　し　物	場 所	備 考
22日（火）	13：30	7月中津市公民館長会議	三光コミュニティーセンター	
23日（水）				
24日（木）	9：00	校長・所長面談Ⅱ	教育委員会室	
	10：00	大分県公民館連合会第2回理事会	大分県立図書館	
25日（金）	13：30	定例教育委員会	教育委員会室	教育長他
	13：40	幼保小連携に係る研修会	中津下毛教育会館	
26日（土）		学びのススメ土曜塾	各公民館、コミュニティーセンター等	
		中津市放課後子ども教室	各公民館、コミュニティーセンター等	
	13：30	中津少年少女発明クラブ第3回講座	中津市生涯学習センター まなびん館	
	14：00	上映会(児童) 「ふしぎ駄菓子屋銭天堂　10」	小幡記念図書館視聴覚室	
27日（日）				
28日（月）	9：00	教育課程研究協議会・統一部会	各会場	
	11：00	おはなし会(幼児向け)	小幡記念図書館視聴覚室	
	13：00	令和7年度第1回「地域とともにある学校」づくり連絡協議会	大分県庁舎新館133会議室	
29日（火）	9：00	校長・所長面談Ⅱ	教育委員会室	
	14：00	授業づくり研修会	大幡コミュニティーセンター	
	19：30	市子連親子ふれあい創作活動（親子で手作り花火）	鶴居コミュニティーセンター	
30日（水）		特別支援教育研修会	三光コミュニティーセンター	
31日（木）	14：00	中津市立図書館と学校図書館司書との合同研修会	小幡記念図書館研修室	
	19：00	市子連親子ふれあい創作活動（親子で手作り花火）	大幡コミュニティーセンター	

8月　教育委員会行事予定表

日・曜	時間	催　し　物	場　所	主催・担当課等	出席依頼者
1日（金）		小学生「夏休み☆本の感想文（オススメ本の紹介文）作成」（～8月22日）	三光図書館	小幡記念図書館	
	9：00	校長・所長面談Ⅱ	教育委員会室	学校教育課	
	18：30	第6回中津市学校のあり方検討委員会	教育委員会室	教育総務課	
2日（土）		学びのススメ土曜塾	各公民館、コミュニティーセンター等	社会教育課、生涯学習推進室	
		中津市放課後子ども教室	各公民館、コミュニティーセンター等	社会教育課、生涯学習推進室	
	10：00	なかはく夏休み子ども体験学習講座	歴史博物館	歴史博物館	
	10：30	小学生「夏の工作教室」 『卵パックで作る☆ビー玉落とし＆迷路』	本耶馬渓図書館	小幡記念図書館	
	13：30	中津少年少女発明クラブ第4回講座	中津市生涯学習センター　まなびん館	社会教育課、生涯学習推進室	
	14：00	上映会(児童) 「ふしぎ駄菓子屋銭天堂　12」	小幡記念図書館 視聴覚室	小幡記念図書館	
3日（日）	10：00	なかはく夏休み子ども体験学習講座	歴史博物館	歴史博物館	
	10：00	なかはく夏の手作りワークショップ	歴史博物館	歴史博物館	
	13：30	日本語教室「きらきら」	如水コミュニティーセンター	社会教育課、生涯学習推進室	
4日（月）	10：00	井上こどもメディカルスーパーバイザー研修会（養護教諭対象）	三保コミュニティーセンター	学校教育課	
	11：00	おはなし会(幼児向け)	小幡記念図書館 視聴覚室	小幡記念図書館	
5日（火）		なかはくとうろう夜（～8/31までとうろう点灯）	歴史博物館	歴史博物館	
	10：00	井上こどもメディカルスーパーバイザー研修会（教育補助員対象）	小楠コミュニティーセンター	学校教育課	
	13：30	赤ちゃん絵本の読み聞かせ事業 「はじめましてひらくっちゃん」	三光コミュニティーセンター	小幡記念図書館	
	19：00	市子連親子ふれあい創作活動 （親子で手作り花火）	沖代公民館	社会教育課、生涯学習推進室	
6日（水）					
7日（木）					
8日（金）	9：00	校長・所長面談Ⅱ	教育委員会室	学校教育課	
	13：30	小学生「夏の工作教室」 『ペットボトルを使った二つのリングのツーリング飛行機』『ストローを使って紙飛行機』	山国図書館	小幡記念図書館	
	14：00	小学生「夏の工作教室」『ワクワク万華鏡をつくろう』	小幡記念図書館 研修室	小幡記念図書館	
9日（土）		学校閉庁日（～17日まで）			
		学びのススメ土曜塾	各公民館、コミュニティーセンター等	社会教育課、生涯学習推進室	
		中津市放課後子ども教室	各公民館、コミュニティーセンター等	社会教育課、生涯学習推進室	
		なかはくナイトミュージアム（21時まで開館）	歴史博物館	歴史博物館	
	14：00	上映会(一般) 「お終活　再春！」	小幡記念図書館 視聴覚室	小幡記念図書館	
10日（日）					
11日（月）					
12日（火）					
13日（水）					
14日（木）					

8月　教育委員会行事予定表

日・曜	時間	催　し　物	場　所	主催・担当課等	出席依頼者
15日（金）					
16日（土）		中津市放課後子ども教室	各公民館、コミュニティーセンター等	社会教育課、生涯学習推進室	
	9：20	中津市各種女性団体連絡協議会大会	中津下毛教育会館	社会教育課、生涯学習推進室	市長・教育長他
	14：00	上映会(児童) 「ゴミおばけがやってきた」	小幡記念図書館 視聴覚室	小幡記念図書館	
17日（日）	10：00	日本語教室「あい♡ことば」	教育福祉センター	社会教育課、生涯学習推進室	
18日（月）	11：00	おはなし会(幼児向け)	小幡記念図書館 視聴覚室	小幡記念図書館	
19日（火）	9：20	第9回市人研大会	文化会館	学校教育課、社会教育課	
20日（水）	10：00	あかちゃんタイム	小幡記念図書館	小幡記念図書館	
	11：00	赤ちゃんおはなし会	小幡記念図書館 視聴覚室	小幡記念図書館	
21日（木）					
22日（金）	13：30	定例教育委員会	教育委員会室	教育総務課	教育長他
23日（土）		学びのススメ土曜塾	各公民館、コミュニティーセンター等	社会教育課、生涯学習推進室	
		中津市放課後子ども教室	各公民館、コミュニティーセンター等	社会教育課、生涯学習推進室	
	9：00	企画展「よしながこうたく絵本原画展」(～9/23まで)	木村記念美術館	木村記念美術館	
24日（日）	11：00	日曜おはなし会(幼児向け)	小幡記念図書館 視聴覚室	小幡記念図書館	
	13：00	北原人形芝居ワークショップ	歴史博物館	歴史博物館	
	13：30	日本語教室「きらきら」	如水コミュニティーセンター	社会教育課、生涯学習推進室	
25日（月）		2学期始業式	各小・中学校		
26日（火）	13：30	中津市公民館長会議	本耶馬渓コミュニティーセンター	社会教育課、生涯学習推進室	
	14：00	定例校長会議	大会議室	学校教育課	
27日（水）		アーカイブズ講座(～8/29まで)	新中津市学校、他	歴史博物館	
	9：00	八面山美術展巡回展～9/15	八面山荘	社会教育課、生涯学習推進室	
28日（木）					
29日（金）					
30日（土）		学びのススメ土曜塾	各公民館、コミュニティーセンター等	社会教育課、生涯学習推進室	
		中津市放課後子ども教室	各公民館、コミュニティーセンター等	社会教育課、生涯学習推進室	
	14：00	上映会(一般) 「落下の解剖学」	小幡記念図書館 視聴覚室	小幡記念図書館	
31日（日）	9：00	中津市生涯を通じた障がい者の学び支援事業　まなびば	中津市生涯学習センターまなびん館	社会教育課、生涯学習推進室	