

資料1 教育情報セキュリティポリシーに関するガイドラインの要求事項（技術的対策）に対する対応方針

#	教育情報セキュリティポリシーに関するガイドライン要求事項		三重県現状	提案依頼要件NO	想定する対応方針
	技術的対策	内容説明、実現方法等			
1	教職員の個人認証強化	校務系情報を扱う端末へは二要素認証（生体認証、物理認証の併用）を導入する	ID／パスワードによるAD認証	①	校務系情報を扱う端末（1人1台パソコン4650台）へ二要素認証を導入
2	学習系システムから校務系システムへのアクセス防止及び校務系システムのインターネットリスクからの分離	<ul style="list-style-type: none"> ・学習系システム・校務系システム間の通信経路を論理的または物理的に分離する ・校務系システム・校務外部接続系システム間の通信経路を論理的または物理的に分離する ・校務系システム・校務外部接続系システム間で通信が必要な場合は通信の無害化を行う（例：校務用と校務外部接続用の端末を仮想デスクトップ環境で分ける） 	学習系システム・校務系システム間の通信経路の論理的な分離について対応済	②	校務系・校務外部接続系の通信経路を論理的または物理的に分離
				③	校務系及び校務外部接続系の間で通信をする際は、通信の無害化を図る
3	校務外部接続系サーバ及び学習系サーバへ機微な個人情報を保管するケースに応じたセキュリティ対策	<ul style="list-style-type: none"> ・校務外部接続系サーバ及び学習系サーバ上に保存された機微情報は暗号化する ・学習系システムへ機微情報の保管は原則行わない ・やむなく学習系システムへ機微情報を保管した場合への備えが必要であり、学習系システムに保存した情報は暗号化する等の対策を実施する 例) サーバ上の特定フォルダ内に格納されたファイルは自動暗号化する	—	④	校務外部接続系サーバへ機微情報を保管する場合の暗号化
				⑤	<ul style="list-style-type: none"> ・学習系サーバへ機微情報を保管する場合の暗号化 ・学習系システムで作成した機微情報を校務系サーバへ保管する運用も検討
				⑥	校務系サーバへの機微情報保管にあたっての暗号化
4	セキュリティレベルの異なるシステム間での無害化処理の実施	メール無害化、ファイル無害化等により、インターネット接続を前提としたシステム（学習系システム・校務外部接続系システム）から校務系システムへのウイルス感染を防ぐ	—	⑦	メール無害化の実装
				⑧	ファイル無害化の実装