

高専情報環境に係る情報セキュリティ対策業務 加点項目

評価項目(要求要件)	評価点	評価観点
4. 情報セキュリティに関する要件		
3. 脆弱性診断		
(1) 対象システムで利用するOSやソフトウェアにおいて新たに確認された脆弱性や未対応の脆弱性が残存していないか等、脆弱性診断や脆弱性情報の収集等により脆弱性に対する対応状況を、構築時及び契約期間中に1回以上実施すること。	10	10
6. Webシステムの対策		
(2) webアプリケーションに対する脆弱性については、以下の既知の脆弱性を排除すること。それ以外の脆弱性を排除する場合は加点する。 <ul style="list-style-type: none"> ・ SQL インジェクション脆弱性 ・ OS コマンドインジェクション脆弱性 ・ ディレクトリトラバーサル脆弱性 ・ セッション管理の脆弱性 ・ クロスサイトスクリプティング脆弱性 ・ クロスサイトリクエストフォージェリ脆弱性 ・ クリックジャッキング脆弱性 ・ HTTP ヘッダインジェクション脆弱性 ・ バッファオーバーフロー及び整数オーバーフロー脆弱性 上記項目以外にも、システムへ影響を及ぼしかねない脆弱性を検出・認知した場合には、機構担当者へ速やかに報告を行うこと。	10	10
7. 対象システムの監視		
(6)対象 システムの安定稼働や利用者または対象システムの要保護情報に対する重大侵害行為を検知した場合には、直ちに、機構担当者へ連絡を行い、必要かつ推奨する対応について助言を行うこと。必要な対応作業を受注者側で行う場合は加点する。	10	10
5.3 提案内容のプレゼンテーション		
プレゼンテーションにより、情報セキュリティ対策業務の実施体制について評価する。	20	1位20点、2位15点、3位10点、4位以下5点
		評価観点 ・情報セキュリティ対策業務の実施体制や実施上の工夫について評価する。
		50