●落札候補者選定基準（第3次佐賀県情報セキュリティクラウド構築及び運用保守業務委託）

別添6

1)技術点 満点1500点

No	大項目	中項目・小項目		評価内容	配点		評価 必須	評価 得点
1	全体の評価		提案書	・具体的かつ合理的な提案であり、実現のためのエ夫が示されているか。 ・使用されている用語・表現は、伝わりやすく、必要に応じて注釈が付けられているか。	20	10		0
2			実績	・これまでに構築したセキュリティクラウドの年間サービス稼働率はどの程度か。 なお、運用メンテナンスの停止時間は別途提示すること。		10		0
3	【別紙1】調達仕様書	9)プロジェクト管理	(1)プロジェクト体制	・プロジェクトマネージャーの資格、能力、経験等は適切であるか。 ・構成員の役割分担が明確に記述され、かつ適切であるか。	40	20		0
4			(2)プロジェクト管理	・提案されたスケジュールは適切か。 ・進捗を担保する工夫があるか。		20		0
5	【別紙2】要件定義書	3)全体構成に関する要件	(1)次期SCの構成	・機器やネットワークは冗長性及び拡張性を考慮されているか。 ・設計上やむを得ず必要となる場合、利用団体の改修想定範囲について具体的に明示されているか	170	30		0
6			(2)インターネット接続回線	・1.5Gbpsの帯域保障がされている。		30	○	0
7				・1.5Gbpsを超える帯域保障がされている。		30		0
8			(3)利用団体と次期SC間の通信回線	・接続回線の通信遅延は極力少ない方式が提案されているか。 ・利用団体毎のトラフィック状況を加味した回線仕様を具体的に示されているか。等		30		0
9			(4)実施場所	・次期SCと利用団体間の通信回線を国内のデータセンタに収容する。		20	○	0
10				・データセンタの評価		30		0
11		4)機能に関する要件	(1)Webサーバ	・仕様書要件を満たしている	580	30	○	0
12			(2)メールリレーサーバ	・仕様書要件を満たしている。		30	○	0
13			(3)プロキシサーバ	・仕様書要件を満たしている。		30	○	0
14			(4)外部DNSサーバ	・仕様書要件を満たしている。		30	○	0
15			(5)ファイアウォール	・仕様書要件を満たしている。		30	○	0
16			(6)IDS／IPS	・仕様書要件を満たしている。		30	○	0
17			(7)マルウェア対策	・仕様書要件を満たしている。		30	○	0
18			(8)通信の復号化対応	・仕様書要件を満たしている。		30	○	0
19			(9)URLフィルタ	・仕様書要件を満たしている。		30	○	0
20			(10)アンチウイルス対策／スパム対策	・仕様書要件を満たしている。		30	○	0
21			(11)振る舞い検知	・仕様書要件を満たしている。		30	○	0
22			(12)メール無害化／ファイル無害化	・仕様書要件を満たしている。		30	○	0
23			(13)WAF	・仕様書要件を満たしている。		30	○	0
24			(14)CDN	・仕様書要件を満たしている。		30	○	0
25			(15)コンテンツ改竄検知	・仕様書要件を満たしている。		30	○	0
26			(16)EDR	・仕様書要件を満たしている。		30	○	0
27			(17)機能に対する評価	・機能に関する要件（1）から（16）について、県の仕様を超えて有益で具体的な提案があるか。		80		0
28			(18)上記の他、提供可能なサービス	・仮想ブラウザ		5		0
29				・メール原本保管		5		0
30				・脆弱性診断		5		0
31				・そのほか提供可能なサービス		5		0
32		5)移行に関する要件	(1)設計・設定	・利用団体毎の現行の設計、ネットワーク構成、システム構成等を十分に把握しているか。 ・利用団体現環境に影響を与えないよう十分に留意し、設計を行う計画等が具体的に提案されているか。	120	40		0
33			(2)テスト	・各要件や設計、設定の内容を十分踏まえたテスト計画書について、作成方針等を具体的に提案されているか。 ・テスト期間の確保は十分か。		40		0
34			(3)移行	・移行に関するリスクや負担が最小限となる方法及びスケジュールについて、具体的な提案がなされているか。 ・各利用団体の移行に係る設定変更等の対応について、支援内容及び調整事項が具体的に提案されているか。		40		0
35		6)セキュリティ運用に関する要件	(1)SOC	・必要な体制、機能、認証規格、実績、体制に配置する高度な人材について具体的に提示しており、セキュリティ対策・運用上で有効だと判断できるか。	160	40		0
36			(2)マネージメントセキュリティサービス	・ログ監視、分析によるインシデントの発生を予防する方法について、具体的に提案されているか ・セキュリティインシデント発生の際に、利用団体のCSIRT等に対しての助言や問合わせへの対応方法について、具体的に提案されているか。		40		0
37			(3)ログ収集・分析	・分析ルールの作成について、作成方針等を具体的に提案されているか。		40		0
38			(4)セキュリティ管理	・セキュリティインシデントの発生を想定した訓練を年1回以上行うことが具体的に提案されているか。 ・第三者の監査を受けることが具体的に提案されているか。 ・セキュリティインシデント発生時の各団体のCSIRTへの支援方法が、具体的に提案されているか。		40		0
39	【別紙2】要件定義書	7)運用に関する要件	(1)体制・役割	・本業務を確実かつ円滑に行う為の実施体制について、具体的に提案されているか。	290	30		0
40			(2)運用業務管理者	・運用業務を円滑に行う為、運用業務管理者等の業務形態（人員配置場所や人数等）について、具体的に提案されているか。		30		0
41			(3)ヘルプデスク機能	・利用団体からの問合せや不具合の連絡及び設定変更の依頼等への対応方針は具体的に提案されているか。		30		0
42			(4)障害管理	・障害発生時の速やかな復旧のため、各種関係者（利用団体の管理者及び保守業者、公共ネットワーク保守業者等、現行セキュリティクラウド運用保守業者）との連携に関するリスクについて考慮されており、また、連携を円滑かつ密接に行う為の体制や仕組み、工夫について、具体的に提案されているか。		30		0
43			(5)維持管理	・仕様要件を満たしている。		30	○	0
44			(6)システム・サービス構成管理	・仕様要件を満たしている。		30	○	0
45			(7)バックアップとリストア	・仕様要件を満たしている。		40	○	0
46			(8)定例会議等の運営	・仕様要件を満たしている。		30	○	0
47			(9)監視業務	・仕様要件を満たしている。		40	○	0
48	【別紙3】サービスレベル定義書	3)サービスレベル	(2)サービス指標	・定義書で示している指標以上の数値で提案されているか。	60	30		0
49			(3)評価項目の管理方法	・定義書で示しているサービス指標以外で有効な指標（評価の管理方法含む）を追加で提案されているか。		30		0
50		4)結果対応	(1)サービスレベルの改善	・定義書で示している指標以上の数値で提案されているか。	60	30		0
51				・提案したサービスレベルが未達成の場合の対応方法について、具体的な提案がなされているか。		30		0
	技術点				1500			0
	価格点			・計算の結果、500点を超えるものは500点とする。	500			0
合計点				・必須項目に「×」がある場合は「失格」とする。				0

※技術点の最低基準点は900点とする