別表８　　セキュリティ要求項目

項番	項　目	概　要
1	システム全体	・地方公共団体情報セキュリティ管理基準（総務省）に厳格に適合した運用ができること。 ・経済産業省が策定している『クラウドサービス利用のための情報セキュリティマネジメントガイドライン』に十分留意されていること。 ・参加団体の情報セキュリティ規則を踏まえて対策を講じること。 ・資産管理やネットワーク監視等の実施が可能な統合管理ツールを使用すること。 ・不正アクセス対策を講じること。 ・サーバーに侵入して情報の盗聴、情報の不正コピー、改ざん、破壊、不正アクセスへの対策、及びDoSやDDoS、クロスサイトスクリプティング、スパムメールの不正中継アクセスなど他のネットワークへの攻撃の踏み台とされないための対策を講じること。 ・特定の参加団体からの不正または異常な通信が認められる場合には、他団体に影響することなく当該団体からの通信のみを遮断することができること。
2	ウィルス対策	・システム全体として、ウィルス対策を講じること。 ・旧来及び最新のウィルスに対する対策を講じること。
3	緊急時対策	・災害や情報流出事故等により情報資産に損害等、緊急事態が発生した場合に、被害を最小限に抑えることを第一に、迅速かつ適切な対応が可能となるような危機管理対策の整備等の対策を講じること。
4	端末利用者認証	・職員及び臨時職員が端末を利用するにあたり、職員ＩＤとパスワード入力を必須とすること。 ・二要素認証を使用できること。 ・監査証跡を残すこと。
5	ユーザ端末操作の制限 （アクセス権限管理）	・ファイルサーバー上の共有ファイルへのアクセス権設定を行い、許可された職員以外はデータアクセスができないこと。 ・監査証跡を残すこと。
6	セキュリティパッチ	・端末毎のセキュリティパッチ適用状況の監視、一元管理を行い、セキュリティパッチ未適用の端末に対し事業者が適用指示を行うこと。

7	情報漏洩の危機を防ぐ暗号化	・重要データの取り扱いについては、必要に応じデータの暗号化を行い、万一ファイルの紛失などが起こった場合も情報漏洩のリスクを軽減できるよう提案すること
8	ユーザ操作情報の収集	・ユーザ操作ログを収集でき、不正利用を抑止する効果と、万一の事故発生時の原因特定ができること。