「地方公共団体における情報セキュリティ監査に関するガイドライン（案）」に対する意見及びそれに対する考え方

番号	該当箇所	提出者	提出された意見	意見に対する考え方
1	全体	法人	1.情報セキュリティといった、安全性に特化した監査では、部分最適に陥る可能性がある。むしろ信頼性・効率性等も含めた大局高所からのシステム監査の中での、情報セキュリティ項目のチェックの方が良いのではないか。たとえばオープンソースの一部利用による、特定OSへの攻撃の被害回避や、信頼できる無料ソフト活用による費用削減等、総合的に評価を下すべきである。	本ガイドラインは、システム監査等の監査手法に関する具体的なセキュリティ対策ではなく、地方公共団体における全体的な情報セキュリティ監査について記載しております。 ご指摘につきましては、今後の参考とさせていただきます。
2	【付録】情報セキュリティ監査業務委託仕様書（例）	法人	2.自治体等の官公庁のIT関係の監査は、有資格者（システム監査技術者、公認システム監査人、CISA等）のみに限定すべきである。なお、情報セキュリティ中心の監査の場合は、電気通信主任技術者や情報セキュリティスペシャリストも選択肢に加えるべきである。	ガイドライン上は、「資格を有する者が1名以上含まれていること」と記載しており、地方公共団体の実情に応じて、適切な対策をとっていただくことを想定しております。
3	3.8.1 318 （94ページ）	法人	318 監査実施の例 意見：「日本の法令の範囲内で運用している。」を削除いただきたい。 理由：当該箇所については、本ガイドライン案の検討を行った「地方公共団体における情報セキュリティ対策の向上に関する研究会」において、「府省庁対策基準策定のためのガイドライン」（平成26年5月19日内閣官房情報セキュリティセンター）の「遵守事項4.1.1(1)(a)(ア)「委託先によるアクセスを認める情報及び情報システムの範囲」について」を参考にされたものと理解しております。内閣官房情報セキュリティセンターにおいて「府省庁対策基準策定のためのガイドライン」を改訂されるに当たっては、そのパブリックコメントの過程において、同センターは「海外法令に基づき外国政府等の第三者に情報が提供されるおそれのある場所に個人情報を置くことを不適切な管理の例として示しておりますが、設置場所を国内に限定することを条件とはしていません。」との見解を出されております。元来、機密性の高い情報の保全については、データセンターの設置場所によらず、暗号化、トークン化等の技術的な対策により講じることが望ましいと考えますので、日本国内のデータセンターでの保存を義務付ける原案は削除いただきたく存じます。	データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択することを求めており、データセンターの所在地を制限するものではありません。 ご指摘につきましては、今後の参考とさせていただきます。
4	3.8.1 318 （94ページ）	法人	該当箇所：P94　318 監査実施の例 意見：「日本の法令の範囲内で運用している。」を削除いただきたい。 理由：当該箇所については、「府省庁対策基準策定のためのガイドライン」（平成26年5月19日内閣官房情報セキュリティセンター）の「遵守事項4.1.1(1)(a)(ア)「委託先によるアクセスを認める情報及び情報システムの範囲」について」に準拠されたと拝察しております。しかし「府省庁対策基準策定のためのガイドライン」の改訂の過程で出されたパブリックコメントの回答において、同センターは「海外法令に基づき外国政府等の第三者に情報が提供されるおそれのある場所に個人情報を置くことを不適切な管理の例として示しておりますが、設置場所を国内に限定することを条件とはしていません。」との見解を出されております。本来、機密性の高い情報の保全については、データセンターの設置場所によらず、暗号化、トークン化等の技術的な対策を講じることがデータを守る上ではより重要と考えます。	データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択することを求めており、データセンターの所在地を制限するものではありません。 ご指摘につきましては、今後の参考とさせていただきます。