問1　IoT システムの企画段階における監査について

近年，センサと通信機能を備えた IoT デバイスを利活用したシステム（以下，IoT システムという）の運用事例が増えてきている。例えば，IoT デバイスから位置，状態，動きなどの情報を継続的かつ大量に収集・分析して，機器の故障予測，自動車の運転制御，製造ラインの自動制御を行ったり，農作物の生産管理などに利用したりしている。また，収集した情報を活用した健康増進型保険や自動車保険のサービスなど，新たなビジネスモデルも出始めている。

IoT システムに多様かつ大量の IoT デバイスが接続されると，IoT システムの構成も変化し，アプリケーションソフトウェアの種類・機能も拡充されていく。そのため，IoT デバイスに故障，誤動作などが生じると，関連するアプリケーションシステム，サービスに様々な影響を及ぼすことが考えられる。また，IoT デバイスがサイバー攻撃の踏み台として悪用されるおそれもある。さらに，医療機器，自動車などに組み込まれた IoT デバイスが不正に遠隔操作されると，人命に危険が及ぶことも想定される。

今後，IoT システムの利活用がますます拡大していく状況を踏まえて，システム監査人には，IoT システム特有のリスクを想定した上で，IoT システムの開発，運用，保守，及びセキュリティに関わる方針・基準などが適切かどうかを，企画段階で確かめておくことが求められる。

あなたの経験と考えに基づいて，設問ア～ウに従って論述せよ。

設問ア　あなたが関係する組織において導入した IoT システム，又は導入を検討している IoT システムの概要と，IoT システムの利活用によるビジネス上のメリットについて，800 字以内で述べよ。

設問イ　設問アで述べた IoT システムにおいて，システム監査人はどのようなリスクを想定すべきか。IoT システム特有のリスクを中心に，700 字以上 1,400 字以内で具体的に述べよ。

設問ウ　設問イで述べたリスクを踏まえて，IoT システムの企画段階において，IoT システムの開発，運用，保守，及びセキュリティに関わる方針・基準などが適切かどうかを確かめるための監査手続について，700 字以上 1,400 字以内で具体的に述べよ。

問2　情報セキュリティ関連規程の見直しに関するシステム監査について

サイバー攻撃，個人情報規制，テレワーク，スマートデバイス，クラウド利用拡大などに伴って変化するリスクに，組織全体で対応するためには，情報セキュリティ関連規程（以下，関連規程という）を適時に見直すことが求められる。この関連規程には，情報セキュリティ基本方針，その詳細な管理策，実施手順などが含まれる。

また，関連規程の見直しによって，各部署で管轄するハードウェア，ソフトウェア，ネットワークなどの多くの IT 資産の管理及びその利用に大きな影響を与えることになるので，組織には，見直した関連規程を十分に周知徹底することが求められる。

関連規程を効果的で実現可能な内容に見直すためには，目的，適用時期，適用範囲，対応技術などを適切に検討する手続が必要である。さらに，見直した関連規程が適切に運用されるためには，単に社員教育だけでなく，影響する IT 資産・利用者の範囲，組織体制などを考慮した周知手続，進捗管理，適用上の課題解決などが重要である。

システム監査人は，このような点を踏まえ，関連規程の見直しが適切な手続に基づいて実施されているかどうか確かめる必要がある。また，見直した関連規程が，全ての部署に適切に周知徹底されるように計画され，実施されているかどうかについても確かめる必要がある。

あなたの経験と考えに基づいて，設問ア～ウに従って論述せよ。

設問ア　あなたが携わった情報セキュリティ関連規程の見直しの概要，その背景及び影響を与える IT 資産の管理と利用について，800 字以内で述べよ。

設問イ　設問アで述べた関連規程の見直しに関する手続の適切性を確かめるための監査手続及び留意すべき事項について，700 字以上 1,400 字以内で具体的に述べよ。

設問ウ　設問ア及び設問イを踏まえて，見直した関連規程を周知徹底するための計画及び周知徹底状況の適切性を確かめるための監査手続及び留意すべき事項について，700 字以上 1,400 字以内で具体的に述べよ。

(C) 2019 環境と習慣