問２　サイバーセキュリティ管理態勢に関するシステム監査について

情報通信技術の進展，デジタルトランスフォーメーション（DX）の取組拡大などに伴い，デジタル環境を前提とするビジネス，サービスが増えてきている。このような環境ではインターネットなど外部ネットワークとの接続を前提とすることから，サイバーセキュリティのリスクが高まっている。

例えば，サイバー攻撃は，年々，高度化，巧妙化し，情報システムの停止，重要情報の外部流出などから攻撃があったことに気づく場合がある。また，サイバーセキュリティ対策が適切でないと，被害が拡大し，ビジネス，サービスに及ぼす影響が大きくなることも想定される。さらに，サプライチェーン上の取引先などのサイバーセキュリティ対策に脆弱性があると，取引先を経由した攻撃を受けるおそれもある。

このようにサイバーセキュリティのリスクが多様化している状況においては，特定の情報システムにおけるインシデントが発生しないように技術的な対策を実施するだけでは不十分である。また，インシデント発生時の被害を最小限に抑え，ビジネス，サービスを速やかに復旧し，継続できるように対策しておくことが重要になる。したがって，企業などの組織には，サイバーセキュリティ管理態勢を構築して，PDCA サイクルを実施することが求められる。

以上のような点を踏まえて，システム監査人は，サイバーセキュリティ管理態勢が適切かどうかを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　あなたが関係するビジネス又はサービスの概要，及びサイバーセキュリティ管理態勢が必要となる理由について，800 字以内で述べよ。

設問イ　設問アを踏まえて，サイバーセキュリティ管理態勢における PDCA サイクルの実施が適切かどうかを確かめるための監査の着眼点及び入手すべき監査証拠を挙げ，監査手続によって確かめるべき内容を，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，インシデント発生時を想定したサイバーセキュリティ管理態勢が適切かどうかを確かめるための監査の着眼点及び入手すべき監査証拠を挙げ，監査手続によって確かめるべき内容を，700 字以上 1,400 字以内で具体的に述べよ。