問1　ソフトウェアの脆弱性対策の監査について

近年，ソフトウェアの脆弱性，すなわち，ソフトウェア製品及びアプリケーションプログラムにおけるセキュリティ上の欠陥を悪用した不正アクセスが増えている。ソフトウェア製品とは，アプリケーションプログラムの開発及び稼働，並びに情報システムの運用管理のために必要なオペレーティングシステム，ミドルウェアなどをいう。

ソフトウェアの脆弱性によっては，それを放置しておくと，アクセス権限のない利用者が情報を閲覧できるなど，アクセス権限を越えた操作が可能になる場合もある。例えば，不正アクセスを行う者が，この脆弱性を悪用して攻撃を仕掛け，情報の窃取，改ざんなどを行ったり，情報システムの利用者に，本来は見えてはいけない情報が見えてしまったりする。

ソフトウェアの脆弱性対策では，開発段階で，ソフトウェア製品及びアプリケーションプログラムの脆弱性の発生を防止するとともに，テスト段階で脆弱性がないことを確認する。しかし，テスト段階で全ての脆弱性を発見し，取り除くことは難しい。また，ソフトウェアのバージョンアップの際に新たな脆弱性が生じる可能性もある。したがって，運用・保守段階でも継続的に脆弱性の有無を確認し，適切な対応を実施していくことが必要になる。

システム監査人は，ソフトウェアの脆弱性を原因とした情報セキュリティ被害を防止するために，ソフトウェアの脆弱性対策が適切に行われるためのコントロールが有効に機能しているかを確認する必要がある。

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システムの概要，及びその情報システムにおけるソフトウェアの脆弱性によって生じるリスクについて，800 字以内で述べよ。

設問イ　設問アに関連して，ソフトウェアの脆弱性対策について，開発，テスト，及び運用・保守のそれぞれの段階において必要なコントロールを，700 字以上 1,400 字以内で具体的に述べよ。

設問ウ　設問イで述べたコントロールの有効性を確認するための監査手続について，確認すべき監査証拠を含めて 700 字以上 1,400 字以内で具体的に述べよ。