問1　スマートフォンに関する次の記述を読んで，設問1～4に答えよ。

K社は，従業員数5,000名の情報システム会社である。K社では，モバイルPCに加えて，スマートフォン（以下，スマホという）から，従業員が電子メールやグループウェアなどの社内システムへアクセスできるシステム環境（以下，Bシステムという）を昨年導入した。Bシステムの利用に先立ち，従業員が電子メール用やグループウェア用のアプリケーションソフトウェア（以下，アプリケーションソフトウェアをアプリという）をスマホにインストールする。また，Bシステムの導入に当たっては，スマホを遠隔で管理するシステム（以下，Mシステムという）を追加で導入し，スマホのOSやアプリのバージョンなどの構成情報の管理や，スマホの紛失時のデータ消去などのセキュリティ対策を実現した。さらに，“個人の所有物であるスマホからBシステムを利用する際は，事前に，利用者の氏名に加えてスマホの製品名や電話番号といった情報をK社に申請すること”などを定めたスマホ利用規程を策定した。

Bシステムの導入から1年が過ぎたので，K社では，セキュリティ対策及びスマホ利用規程が有効であったかについて確認することにした。その際に，スマホに関するセキュリティ対策を改めて議論することにした。

〔ルート特権の利用について〕

スマホのルート特権を利用者が利用できる状態にする行為（以下，ルート特権化という）について，セキュリティ上の問題がないかを検討することになった。スマホの多くは，利用者がルート特権をもたず一般利用者の権限だけで利用することを前提にしている。そのため，ルート特権をもつ個人のPCと違い，OSの設定の一部を自由に変更できないという制約や，スマホのベンダによってあらかじめインストールされているアプリを削除できないという制約などがある。そのような制約を嫌う利用者の中には，ベンダが想定していない手段で，ルート特権化を自ら行う者もいる。

K社で調査したところ，ルート特権化は，主に，バッファオーバフロー攻撃を用いて実現されることが分かった。

〔バッファオーバフロー攻撃の詳細と対策について〕

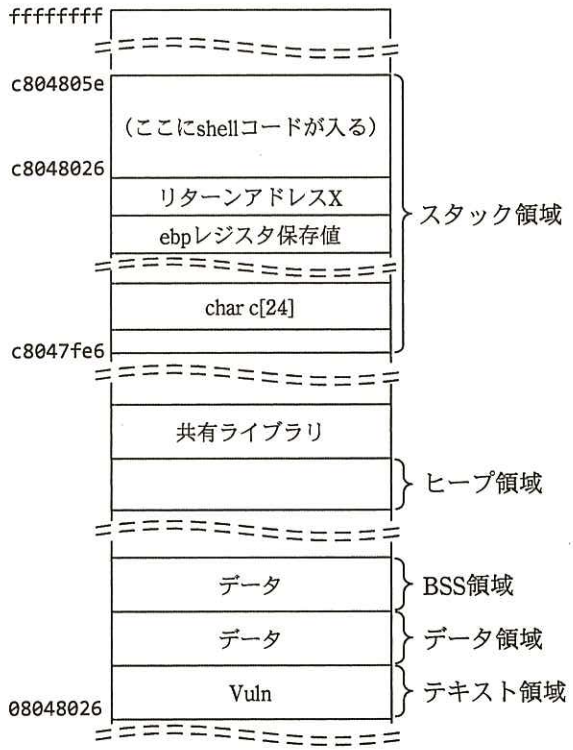
バッファオーバフロー攻撃に関するセキュリティホールは，スマホ用の OS だけではなく，PC 用 OS やサーバ用 OS においても報告されている。通常，OS やライブラリのセキュリティホールが公表された場合，PC やサーバを管理する者は，開発元から提供される［ a ］の適用やソフトウェアの更新によって，セキュリティホールに対処する。他方，Web サーバにおいては，［ a ］の適用やソフトウェアの更新をしなくても，①通信路上に IPS や WAF を設置することによって，インターネットから Web サーバへのバッファオーバフロー攻撃を防止することもできる。

バッファオーバフロー攻撃としては，スタックバッファオーバフロー攻撃，［ b ］バッファオーバフロー攻撃や，静的メモリ領域を対象としたバッファオーバフロー攻撃が知られている。いずれのバッファオーバフロー攻撃も，主に C や C++で作成されたプログラムが狙われる。スタックバッファオーバフロー攻撃は，スタック領域を破壊するので，スタック破壊攻撃とも呼ばれる。スタック破壊の挙動をプログラム実行時に検知して停止する機能（以下，スタック破壊検知機能という）を含むコードを生成するコンパイラも普及している。

図 1 は，スタックバッファオーバフロー攻撃に対して脆弱（ぜい）なプログラム（以下，Vuln という）である。図 2 は，関数 foo が呼び出された後のメモリ配置である。ここで，図 2 中の shell コードは，攻撃者がスタックバッファオーバフロー攻撃によってメモリ上に配置するものである。スタック破壊検知機能を含めずにコンパイルした Vuln においては，攻撃を成立させるために挿入するデータ（以下，インジェクションベクタという）を変数 a に与えることによって，shell コードにプログラムの制御が移ってしまう。ここでは，図 3 が Vuln に対するインジェクションベクタである。その際，Vuln が実行時に②一定の条件を満たせば，あらゆる命令の実行が shell コードで可能となる。

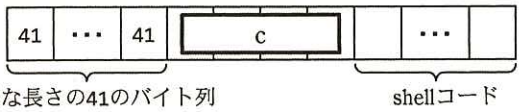
```
 1: (省略)
 2: int main(int argc, char *argv[]) {
 3:    char *a;
 4: (省略, ここで a がポイントする領域にインジェクションベクタが挿入される。)
 5:    foo(a);
 6: (省略, ここでその他の必要な処理をする。)
 7: }
 8: int foo(char *b) {
 9:    char c[24];
10: (省略)
11:    strcpy(c, b);
12: (省略, ここで c を利用する。)
13:    return 0;
14: }
```

図１　スタックバッファオーバフロー攻撃に対して脆弱なプログラム Vuln




注記　メモリアドレスは 4 バイトの 16 進数表記である。

図２　関数 foo が呼び出された後のメモリ配置




注記　表記は 16 進数である。

図３　Vuln に対するインジェクションベクタ

このスタックバッファオーバフロー攻撃を防止するため，指定されたメモリ領域でのコードの実行を禁止する機能（以下，データ実行防止機能という）が登場した。これは，CPU の機能を用いて実現されている。

しかし，プログラム実行時に共有ライブラリがメモリ上にロードされていることを利用して，データ実行防止機能を回避する新たな攻撃法が登場した。これは，共有ライブラリ内の関数であって，かつ，任意のプログラムを実行できる関数を，スタックバッファオーバフロー攻撃時に利用するものである。libc 共有ライブラリを利用する場合，この攻撃は［ d ］攻撃と呼ばれる。

最近の OS では，こういった攻撃が成功することを抑制するため，アドレス空間配置ランダム化技術が実装されている。アドレス空間配置ランダム化技術を用いると，スタック破壊検知機能を含めずにコンパイルしたプログラムであっても，スタックバッファオーバフロー攻撃の成功を抑制することができる。

〔K 社での対策〕

K 社の調査の結果，スマホの OS のあるバージョン（以下，バージョン V という）以降ではデータ実行防止機能及びアドレス空間配置ランダム化技術が実装されていることが分かった。また，バージョン V 以降では，その他様々な点でセキュリティ対策が強化されていることも分かった。

その上で，ルート特権化されたスマホから B システムを利用することについて改めて検討したところ，ルート特権化されたスマホは，ベンダの保守サポートの対象外になること，及び M システム用のアプリや B システム用のアプリが動作しなくなることが分かった。さらに，ルート特権化されていないスマホと違い，ルート特権化されたスマホでは，“データを盗み出すタイプのマルウェア”が侵入してしまうと，それがルート特権を取得して，③スマホ内に保存されているアプリのデータを不正に読み出してしまうリスクが高まることも分かった。そのため，K 社では，スマホ利用規程で，ルート特権化されたスマホからの B システムの利用を禁止することにした。

しかしながら，④それだけでは，従業員がスマホ利用規程を守ったとしても，“意図しないルート特権化”のリスクが残存する。K 社は，B システムのセキュリティを確保するために，スマホでは，バージョン V 以降の OS を利用することが必要であるとの結論に至った。そのため，⑤スマホの OS のバージョンを K 社が確認する運用策を実施することにした。

**設問1**　本文中の［ a ］，［ b ］，［ d ］に入れる適切な字句を，［ a ］は15字以内で，［ b ］は5字以内で，［ d ］は20字以内でそれぞれ答えよ。

**設問2**　Vulnへのスタックバッファオーバフロー攻撃とその対策について，(1)～(3)に答えよ。

(1)　図2のメモリ配置について，スタックバッファオーバフロー攻撃を防止するには，データ実行防止機能をどのメモリ領域に適用すればよいか。図2中の用語を用いて答えよ。

(2)　図3中の［ c ］に入れる適切なバイト列を解答群の中から選び，記号で答えよ。ただし，バイトオーダはリトルエンディアンとする。

解答群

ア　068004c8　　イ　08048026　　ウ　26800408　　エ　268004c8

オ　5e8004c8　　カ　c8048006　　キ　c8048026　　ク　c804805e

(3)　アドレス空間配置ランダム化技術は，攻撃者のどのような行為をできないようにすることによって，図3のインジェクションベクタによるスタックバッファオーバフロー攻撃が成功することを抑制するか。25字以内で具体的に述べよ。

**設問3**　バッファオーバフロー攻撃について，(1)，(2)に答えよ。

(1)　本文中の下線①にある，インターネットからWebサーバへのバッファオーバフロー攻撃の対策として，IPSやWAFではどのような処理をするか。25字以内で具体的に述べよ。

(2)　本文中の下線②の条件を20字以内で述べよ。

**設問4**　〔K社での対策〕について，(1)～(3)に答えよ。

(1)　ルート特権化されていないスマホでは，本文中の下線③の不正な読出しを，OSのファイルシステムがどのような仕様で制限しているか。40字以内で述べよ。

(2)　本文中の下線④について，意図しないルート特権化がどのような状況で起こり得るか。25字以内で述べよ。

(3)　本文中の下線⑤について，確認方法を具体的に20字以内で述べよ。