平成１９年度　春期　テクニカルエンジニア（情報セキュリティ）　午後Ｉ問題

問１　プログラム開発におけるセキュリティ対策に関する次の記述を読んで，設問 1～3 に答えよ。

A 社は，従業員数 1,000 名の中堅広告代理店である。A 社では，契約書，顧客向けの企画書や広告原稿などの文書を，部署ごとに作成，管理している。これらの様々な文書を一括管理するために文書管理システムを開発することになり，開発チームによるプロジェクトを立ち上げた。

文書管理システムは，機密性の維持と原本性の確保が必要な文書を取り扱うので，特にセキュリティに配慮することが重要な開発要件となっている。

〔プログラム作成時の脆弱性対策〕

A 社では，文書管理システムを開発するに当たり，開発の生産性や品質の向上のために，開発標準ルールを作成することにした。次は，開発標準ルールの作成を担当することになった S 主任と T 君の会話である。

S 主任：開発標準ルールでは，開発チームが脆弱性のないプログラムを作成するためのコーディングルールを示すとともに，なぜそうすべきかを理解させるようにしたいね。

T 君　：はい，同感です。プログラマに対して，コーディングの悪い例を示す際に，脆弱性が悪用される仕組みについても解説しましょう。システムが攻撃される仕組みを理解できれば，プログラマも納得すると思います。

S 主任：そうだね。さらに，一般的に言われているプログラム作成上の基本的な注意事項を守ることも，セキュリティ対策になることを強調したいね。開発に使用するプログラム言語やプログラムの稼働環境によって対策が異なってくるので，まずは，文書管理システムで使用される C++言語から取り組んでみよう。

T 君　：C 言語や C++言語のように，配列の範囲チェックを自動で行わないプログラム言語を使用する場合は，バッファオーバフローを防ぐ必要があります。

S 主任：そのために，まず，どのような手段でバッファオーバフローを悪用した攻撃が行われるのか検討してみよう。

T 君　：この脆弱性による影響には幾つかのタイプがあるようです。その一つを含む，図 1 のプログラムを作成してみました。このプログラムの本来の意図は，実行時に最初のコマンドライン引数として文字列を受け取り，その文字列を表示した後，特定のファイル（ファイル名“somefile”）の内容を表示することです。

```
001: #include <fstream>
002: #include <iostream>
003:
004: using namespace std;
005:
006: int main(int argc, char *argv[])
007: {
008:   char val1[256] = "somefile";          // 操作対象ファイル名格納変数
009:   char val2[128];                       // コマンドライン引数の値格納用バッファ
010:   char val3[1024];                      // 出力用バッファ
011:
012:   if(argc > 1) {                      // コマンドライン引数の数の確認
013:     strcpy(val2, argv[1]);            // 最初のコマンドライン引数を val2 にコピー
014:     cout << "-- " << val2 << end1;   // コンソールに val2 の値を表示
015:   } else {                            // コマンドライン引数が指定されていない場合,
016:     return 1;                         // 終了
017:   }
018:
019:   ifstream fin(val1);               // 名前が val1 のファイルを入力ファイルとして開く
020:   if (!fin) {                                  // ファイルが開けない場合,
021:      cout << "open error " << val1 << end;  // エラーメッセージを表示して終了
022:      return 2;
023:  }
024:
025:   fin.getline(val3, 1024);            // ファイルから 1 行読み取り, val3 に格納
026:   while( !fin.eof() ) {               // ファイルの最後まで繰り返す
027:     cout << val3 << endl;             // コンソールに val3 の値を表示
028:     fin.qetline(val3, 1024);          // ファイルから 1 行読み取り, val3 に格納
029:   }
030:
031:   fin.close();
032:
033:   return 0;
034: }
```

図１　脆弱性のあるプログラム例

S 主任：具体的に確認してみよう。

T 君　：はい。このプログラムでは，バッファオーバフローの結果，［　a　］領域に確保された変数の値が，意図に反して書き換えられる可能性があります。私がこのプログラムを実行して確認したところ，変数 val1 がメモリ上に展開されたときの先頭アドレスは 0xbffffa60 で，同様に変数 val2 では 0xbffff9e0，変数 val3 では 0xbffff5e0 でした。このとき，コマンドライン引数として一定バイト数以上の長さの文字列が与えられると，変数［　b　］がバッファオーバフローを起こして，変数［　c　］の値が書き換えられてしまいます。

S 主任：そうだね。しかし，もっと重大なセキュリティ問題に結び付くことを示したいね。

T 君　：分かりました。前提条件として，このプログラムの実行環境は UNIX とします。ファイル

“somefile”の所有者はOSのシステム管理者で，所有者にだけread/write属性が付けられているものとします。また，実行ファイルの所有者はシステム管理者ですが，一般利用者でもファイル“somefile”の内容を見ることができるように，setuid属性が付けられているものとします。攻撃者はシステム管理者ではない一般利用者の権限をもっているものとします。さらに，攻撃対象のファイル“afile”の所有者はシステム管理者で，所有者にだけread/write属性が付けられているものとします。これらの前提条件の下で，①攻撃者が，図2のコマンドライン引数を与えて，図1のプログラムを実行すると，ファイル“afile”の内容が表示されてしまいます。

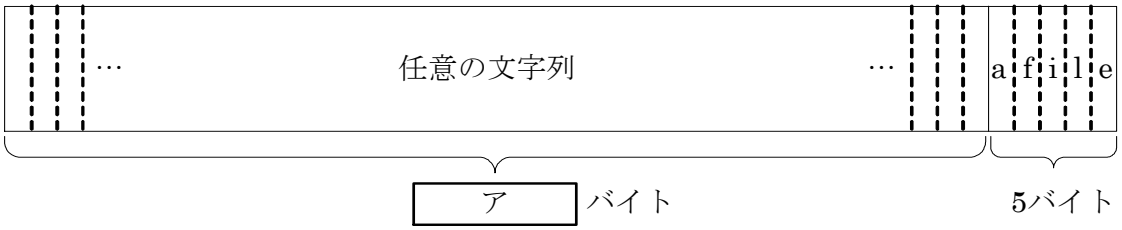


図２　コマンドライン引数

S主任：これは重大な問題だな。setuid属性が付けられている実行ファイルは，ファイル所有者の権限で実行される。これは，システム管理者の権限の乗っ取りにつながる［ d ］の脅威も抱えているから取扱いに注意しなければいけないな。加えて，［ a ］領域には，［ e ］のパラメタや戻りアドレスなどが格納されるので，その［ e ］の戻りアドレスが書き換えられてしまうことがある。そうなると，悪意のあるプログラムに制御を移すことができるから，特に注意が必要だ。

T君　：はい，そうですね。脆弱性を最小限に抑えるために，プロセスの権限については，プログラムの設計段階で考慮すべきだと思います。

S主任：図1のプログラムにはないようだが，malloc関数などによって［ f ］領域に確保された変数についてのバッファオーバフローの脆弱性も，よく知られているね。

T君　：そうですね。ただ，［ a ］領域と［ f ］領域に確保された変数については，どちらもプログラム作成上の対策は同じと考えてよいと思います。

S主任：そのとおりだが，バッファオーバフローを防ぐ根本的な対策は，ループ文の中で配列への書込みを行う場合や，組込み関数を使う場合などで方法が異なるから，それぞれについて示すことにしよう。また，プログラムコードのレビューや検証作業を行うことで，コーディングルールに違反したプログラムを検出し，修正することの重要性も強調すべきだな。

T君　：これまで検討してきたコーディングルール以外にも，［ e ］の戻りアドレスが変更されて，悪意のあるプログラムが実行されることを防ぐ方法があります。例えば，②戻りアドレスの改ざんを検知する方法，戻りアドレスが［ a ］領域上の場合に実行を禁止する方法，バッファオーバフローの脆弱性をもつ組込み関数に対して，バッファオーバフローの検知と防御の仕組みが加えられた実行時ライブラリに置き換える方法などがあります。

S主任：だが，それらの方法ではバッファオーバフローの問題をすべて解決することはできないので，

補完的な対策であることを強調して，開発標準ルールに記載しておこう。また，バッファオーバフローの脆弱性以外にも，競合条件による脆弱性や一時ファイルの消去忘れによる情報漏えいなどの対策を考慮した，プログラム作成上の注意事項についても述べることにしよう。

S 主任と T 君は，開発標準ルールをまとめ，開発チームに提供した。A 社では，このルールを基に，安全性の高い文書管理システムが開発され，無事，本番稼働を迎えることができた。

設問１　本文中 [a] ～ [f] に入れる適切な字句を，[e] は 6 字以内，その他は 4 字以内で答えよ。

設問２　図 1 のプログラムに関するバッファオーバフローの脆弱性について，(1)～(3) に答えよ。

(1) 図 2 中の [ア] に入れる適切な数値を答えよ。

(2) 本文中の下線①について，ファイル“afile”の内容が表示されてしまうことによって，セキュリティ上どのような問題が生じるといえるか。40 字以内で述べよ。

(3) この脆弱性を排除するために，図 1 のプログラムの 12 行目だけを変更したい。どのように変更すればよいか。50 字以内で述べよ。

なお，解答は，変更の内容を文章で説明する方法と，変更後のプログラムコードを示す方法のどちらでもよい。

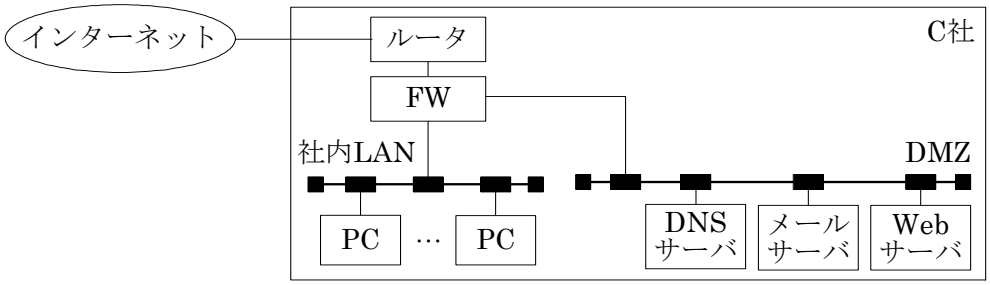
設問３　本文中の下線②について，戻りアドレスが改ざんされていないことを確認する方法を，70 字以内で具体的に述べよ。

問２　ネットワークのセキュリティに関する次の記述を読んで，設問 1～3 に答えよ。

B 社は，顧客のネットワークやシステムの構築を主要業務とするシステム開発会社である。今回，顧客である C 社から，オフィスの移転を機に DMZ を含むネットワークの再構築を依頼された。C 社は，従業員数 200 名の経営コンサルタント会社である。コストを抑えるために既存のサーバ類は移設するが，ファイアウォール（FW）は更新し，ネットワーク型の侵入検知システム（IDS）又は侵入防止システム（IPS）を新規に導入する計画である。B 社のシステム開発部では，J 主任をリーダとしてプロジェクトチームを編成し，C 社のネットワーク再構築を進めることにした。プロジェクトチームでは，メンバの K 君が FW のフィルタリングルールの設計と，IDS 又は IPS の導入の検討を行うことになった。

〔FW のフィルタリングルールの設計〕

C 社のネットワークについては，図に示す構成で設計を進めている。



注　IDS 又は IPS は，図では省略している。

図　C社のネットワーク構成

K 君は FW のフィルタリングルールの設計案を作成した段階で，セキュリティに詳しい J 主任に意見を求めた。

K 君　：C 社の FW には，パケットフィルタリング方式を採用する方針です。フィルタリングルールの設計案は表 1 に示すとおりですが，この案について，セキュリティ面で何か問題があるでしょうか。

J 主任：表 1 のルール 10 は，セキュリティに配慮した定石どおりの設定になっているし，ルール 1 は，社内外へのウイルス感染を防止するために設定していることは分かる。しかし，ルール 7 を設定した特別な理由はあるのか。

表１　ＦＷのフィルタリングルールの設計案

項目名 / ルール	送信元	あて先	ポート番号	動作
1	a	b	135，137～139，445	拒否
2	任意	DNS サーバ	53	許可
3	DNS サーバ	任意	53	許可
4	任意	メールサーバ	25	許可
5	メールサーバ	任意	25	許可
6	任意	Web サーバ	80，443	許可
7	任意	Web サーバ	23	許可
8	DMZ	社内 LAN	任意	許可
9	社内 LAN	任意	任意	許可
10	任意	任意	任意	c

注　上から順に，最初に一致したルールが適用される。

K 君　：C 社の要求事項に，“Web サーバの緊急対応用に，Web 管理者の自宅から telnet で接続できること”という項目があるので設定しました。

J 主任：telnet は，①パスワードを流出させるおそれがある。例えば，ポート番号が 22 の［　d　］などの安全なプロトコルに変更した方がよいと思うが。

K 君　：分かりました。要求事項のこの項目につては，telnet から［　d　］に変更すべきであることを，C 社に提案します。

J 主任：それから，ルール 8 には，セキュリティ上の問題がある。このままでは，②インターネットから社内 LAN に不正にアクセスされるおそれがある。

K 君　：分かりました。このルールを削除して，DMZ から社内 LAN へのアクセスは最小限の運用にするよう，C 社に提案します。

K 君は，J 主任の助言に従って FW のフィルタリングルールを修正して，設計を完了し，続いて IDS 又は IPS の導入の検討を実施した。

〔IDS 又は IPS の導入〕

数日後，J 主任は K 君の検討結果を基に，IDS 又は IPS の導入に関して，C 社の L 氏と打合せを行った。

L 氏　：IDS 又は IPS を導入する必要性について，説明してください。

J 主任：③FW のフィルタリングルールの設定だけでは，Web サーバに対するバッファオーバフロー攻撃などを防御できません。こうした攻撃への対策として，IDS 又は IPS の導入や，サーバにセキュリティパッチを適用することが考えられます。しかし，御社では，セキュリティパッチ適用時のサーバの動作確認や，適用前のデータのバックアップ採取を行う必要があり，すぐにセキュリティパッチを適用することはできません。そこで，IDS 又は IPS の導入をお勧めした次

第です。

L氏　：分かりました。では，IDS，IPSには，どのような機種を選定したらよいでしょうか。

J主任：IDS及びIPSの候補機種について比較した結果を，表2に示します。

表２　IDS及びIPSの候補機種の比較（抜粋）

比較項目＼機種名	P	Q
IDS又はIPS	IDS	IPS
検知方式	シグネチャ型＋アノマリ型	シグネチャ型
⋮	⋮	⋮
防御方式	FWとの連携	パケットの破棄
相対価格	100	120

J主任：検知方式には，シグネチャ型とアノマリ型があり，シグネチャ型は，既知の攻撃パターンに基づく情報とマッチングすることによって攻撃を検知し，例えば，サーバの既知の脆弱性を突いた攻撃を防ぐことができます。一方，アノマリ型は，RFCのプロトコル仕様などと比較して異常なパケットや，トラフィックを分析して［　e　］的に異常なパケットを攻撃として検知します。

L氏　：では，サーバにセキュリティパッチを適用して既知の脆弱性をなくしておけば，シグネチャ型のIDSやIPSは不要なわけですね。

J主任：いえ，そうでもありません。一部のDoS攻撃などについては，セキュリティパッチの適用では防御できませんが，シグネチャ型のIDS又はIPSで検知又は防御できる場合があるので，やはりIDS又はIPSを導入した方がよいでしょう。

L氏　：分かりました。それでは，そのほかに機種Pと機種Qの違いは何ですか。

J主任：機種Qは，インライン接続で通信路上に挿入され，検知した攻撃については防御することができるので，運用負荷が軽くなります。機種Pは，基本的には，通信をモニタリングし，攻撃を検知すると警告を発するだけです。機種Pにも，④FWとの連携によって攻撃を防御する機能がありますが，完全なものとは言えません。

L氏　：機種Qには問題点はないのですか。

J主任：機種Qの場合は，処理能力が不足していると，それがボトルネックになり，通信のスループットが低下する可能性があります。しかし，御社の回線速度を考慮すると，機種Qの処理能力なら問題ありません。

L氏　：運用面で注意することはありますか。

J主任：一般に，IDS及びIPSには，⑤フォールスポジティブや，⑥フォールスネガティブというエラーが存在します。IPSは，攻撃と判断した通信パケットを自動的に破棄するので，前者のエラーから受ける影響は，IDSよりも大きくなります。しかし，機種Qは，自動的な学習によって，これらのエラーを極力少なくする機能をもっています。

L氏　：それでは，価格は多少高いですが，運用負荷が軽いので，機種Qの導入を前提として具体的な案を作成してください。

B 社は，C 社に機種 Q を含む再構築案を提出し，了承を得た。その後，C 社のネットワーク再構築は順調に進み，運用を開始することができた。

設問１　表 1 中の［ a ］～［ c ］について，(1)，(2) に答えよ。

(1) ウイルス拡散を防ぐためには，［ a ］，［ b ］をどのように設定すればよいか。それぞれ 6 字以内で答えよ。

(2) ［ c ］に入れる適切な字句を，“許可”又は“拒否”のいずれかで答えよ。

設問２　〔FW のフィルタリングルールの設計〕について，(1) ～ (3) に答えよ。

(1) 本文中の［ d ］に入れる適切な字句を，5 字以内で答えよ。

(2) 本文中の下線①のおそれがある理由を，プロトコルの特徴に着目して，20 字以内で述べよ。

(3) 本文中の下線②のおそれは，どのような攻撃を想定しているか。40 字以内で述べよ。

設問３　〔IDS 又は IPS の導入〕について，(1) ～ (4) に答えよ。

(1) 本文中の［ e ］に入れる適切な字句を，3 字以内で答えよ。

(2) 本文中の下線⑤，下線⑥とはどのようなエラーか。それぞれ 30 字以内で述べよ。

(3) 本文中の下線③について，FW のパケットフィルタリングルールだけでは攻撃を防御できない理由を，30 字以内で述べよ。

(4) 本文中の下線④について，FW との連携によって攻撃を防御する機能が完全でない理由を，60 字以内で述べよ。

問３　監査ログの設計に関する次の記述を読んで，設問 1～3 に答えよ。

D 社は，従業員数 5,000 名の飲料製造会社である。最近は，企業経営の透明性が強く求められていることから，経営陣から，社内の情報システムの運用状況，特に内部統制に必要な機構が適切に動作しているかを再確認せよとの指示があった。これを受けて，D 社の電算室の責任者である X 氏，社外コンサルタントの Y 氏, 及び D 社のシステム構築を担当している E 社の Z 主任が確認作業を開始した。次は，X 氏と Y 氏の確認作業に関する会話である。

Y 氏 : IT による内部統制の確保で必要なこととして，企業活動にかかわる情報システムの利用者認証機構やアクセス制御機構が正しく動作していることを，監査時に監査ログを基にして第三者が確認できることがあります。御社では，営業管理システムが企業活動に大きな役割を果たしていますね。この営業管理システムの利用状況，利用者認証の仕組みを説明してください。

X 氏 : 当社の営業管理システムは 3 年前に稼働を始めました。受注情報，入金情報，出荷情報，検収情報やこれらの統計情報といった営業管理情報に，営業部員が毎日のようにアクセスし，登録，参照，更新を行っています。ピーク時には，1 時間に 5,000 件程度のトランザクションが発生します。①利用者認証には，ワンタイムパスワード方式を利用しているので，一定期間固定で利用されるパスワードよりも安全です。

続いて X 氏は，営業管理システムのアクセス制御の仕組みについて，Y 氏に次のように説明した。

X 氏 : 営業管理システムでは，営業部員に“役割”が割り当てられます。“役割”には，“権限”が割り当てられます。“権限”は，アクセス対象の営業管理データと，参照，更新，追加などの許可された操作との集合によって定義されています。営業部員が営業管理システムにアクセスする際，営業部員に割り当てられた役割にアクセス対象情報への操作権限が割り当てられていれば，その操作が許可される仕組みになっています。

Y 氏 : なるほど。この仕組みは［　a　］アクセス制御といわれるものですね。この営業管理システムは，どのようなログを採取していますか。

X 氏 : 利用者認証の失敗や権限のないアクセス要求が発生したとき，ログを採取しています。このログを監査ログとして使いたいのですがどうでしょうか。

Y 氏 : ログ採取については，改善が必要ですね。現状の営業管理システムのログでは，監査時に②監査ログとしての役割を十分には果たせません。

Y 氏から，監査ログの役割について説明を受けた X 氏と Z 主任は，営業管理システムのログ処理には改善が必要であることを理解し，営業管理システムに対してどのような追加開発が必要なのか検討を始めた。

〔監査ログに関する検討〕

Z 主任 : 監査ログレコードとして，時刻，利用者名，アクセス対象に関する情報，操作，失敗などを示すアクセス結果などを採取すればよいと思います。また，アクセス制御機構の動作を検証可能

とするために，受注などの営業業務の操作だけでなく，［ b ］及び［ c ］の定義と設定，利用者の登録についても監査ログを採取します。

X氏　：その監査ログにセキュリティ対策は必要ですか。

Y氏　：はい，必要です。監査ログへのセキュリティ対策の機能は，JIS X 5070（ISO/IEC 15408）にも記述されています。例えば，監査ログファイルの安全な管理，改ざんや破壊への対策が必要ですね。

Z主任：なるほど。セキュリティ対策についても，これから検討します。

Z主任は，まず，営業管理システムのアクセス制御部分において，監査ログファイルの閲覧を限定するために必要な，［ b ］及び［ c ］を適切に定義し，設定することにした。次に，図に示すように，監査ログファイル管理レコードと監査ログレコードなどから成る監査ログファイルのフォーマットを設計した。監査ログレコードは，ログを採取する監査イベントに対応して記録されるもので，監査ログデータ LD_i と図に示す計算によって得られるハッシュ値 C_i から構成されている。Z主任は監査ログファイルのフォーマットについて，Y氏に次のように説明した。

監査ログファイル管理レコード	C_0
LD_1	C_1
LD_2	C_2
⋮	⋮
LD_n	C_n
終端データ	C_{n+1}

（C_1～C_n：監査ログレコード）

$M(\alpha, s)$：データ α に対する鍵(s)付きハッシュ関数
LD_1～LD_n：監査イベントを記録した監査ログデータ
C_0 ＝ M(ファイル名 | ファイル初期化日時，s)
C_i ＝$M(C_{i-1} | LD_i, s)$，　i ＝ 1～ n
C_{n+1} ＝ $M(C_n | 終端データ, s)$

注　監査ログファイル管理レコードには，ファイル名，記録開始日時，ファイル初期化日時などが含まれる。
|：データの連結を示す。

図　監査ログファイルのフォーマット

Z主任：監査ログファイルに記録されている情報の正当性を確保するために，何らかの不正があったときでも③なるべく多くの監査ログデータの内容の正当性を証明できるようにセキュリティ対策を考えました。

Y氏　：なるほど，よく考えられていると思います。では，監査ログファイルの領域の管理はいかがでしょうか。ここで留意すべき点は，監査ログが採取されない状況を避けることです。

Z主任：はい。運用者の指示によって定期的にバックアップすることが可能です。監査ログの保存には，あらかじめ作成した二つのファイルを使います。監査ログを一方のファイルに書き込み，設定したサイズに達するともう一方のファイルに書き込み始めると同時に，満杯になったファイルをバックアップし，運用者に通知することとします。バックアップ後，満杯になったファイルは初期化され，監査ログファイル管理レコードと項目 C_0 が書き込まれます。項目 C_i（i ＝ 0 ～

n＋1)の作成に使用した鍵 s は，安全に保管します。領域のサイズについては，現状のアクセス件数と将来予想を考慮して設定します。

Y 氏　：D 社のルールでは，営業管理情報の保存期間は 8 年間と決められています。したがって，営業管理システムの監査ログファイルのバックアップファイルにも，長期にわたって安全に保管するための対策が必要です。バックアップファイルの保管に関する運用ルールの策定を計画に含めてください。

〔タイムスタンプ技術の検討〕

X 氏：この監査ログが実現すれば，営業管理システムの監査可能性は十分でしょうか。

Y 氏：いいえ，十分ではありません。タイムスタンプ技術を利用することをお勧めします。まず，バックアップファイルの［ d ］を計算して［ e ］に送信します。次に，［ e ］で作成されたタイムスタンプトークンを取得し，バックアップファイルとともに保存します。これによって，④図に示した監査ログファイルに新たな証拠能力を付加することができます。

そこで，X 氏は，Z 主任に対し，バックアップの際にタイムスタンプ技術を利用することを依頼した。また，これらの検討結果を経営陣に報告し，営業管理システムの改善指示を受けた。その後，Z 主任は，D 社からの指示を受けて，営業管理システムに関して監査ログの採取システムを開発した。

設問１　営業管理システムの利用者認証とアクセス制御について，(1)，(2) に答えよ。

(1) 本文中の［ a ］に入れる適切な字句を 8 字以内で答えよ。

(2) 本文中の下線①で安全であると述べている理由を，想定する攻撃を含めて 25 字以内で述べよ。

設問２　監査ログファイルのフォーマット設計について，(1) ～ (3) に答えよ。

(1) 本文中の下線②で示す，営業管理システムにおける監査ログの役割を，45 字以内で具体的に述べよ。

(2) 本文中の［ b ］，［ c ］に入れる適切な字句を，それぞれ 2 字で答えよ。

(3) 本文中の下線③が示す正当性の証明について，図に示す監査ログレコードの項目 C_i（i ＝ 1 ～ n）は監査ログデータ（LD_i）に関して何を証明しているか。また，項目 C_{i-1}（i ＝ 1 ～n＋1）を利用して項目 C_i を作成することは，複数の監査ログレコードに関して何を証明するか。それぞれ 25 字以内で述べよ。

設問３　タイムスタンプ技術について，(1)，(2) に答えよ。

(1) 本文中の［ d ］，［ e ］に入れる適切な字句を，［ d ］は 8 字以内，［ e ］は 15 字以内で答えよ。

(2) 本文中の下線④において，Y 氏が付加できるとしている新たな証拠能力を，40 字以内で具体的に述べよ。

問４　アンケートシステムの構築に関する次の記述を読んで，設問 1～3 に答えよ。

F 社は，様々なシステム構築を受注する，従業員数 500 名のソフトウェア開発業者である。昨年，従業員数 10,000 名の G 社から，公開鍵基盤（PKI）を利用した社内りん議システムの構築を受注した。その実績もあって，今回，G 社が社内アンケートを実施するためのシステム（以下，Q システムという）の構築を受注した。そこで，F 社のシステム部主任の N 氏とその部下の R 君が，Q システムを設計することになった。次は，そのときの N 氏と R 君のやり取りである。

〔Q システムの要件確認〕

N 氏：まず，G 社から出されている要件を確認しよう。

R 君：はい。アンケートは 1 か月に一度実施され，原則として，全従業員が回答することになっています。従来は，表計算ソフトを用いて作成したアンケート用紙を人数分印刷して，配布していました。人事担当者がアンケート内容を作成するので，今後とも，操作が容易な表計算ソフトを使いたいと考えているようです。また，全従業員を対象とするので，オンラインでアンケートを配布して，コスト削減を図り，さらに，1 人 1 回答というルールを守りつつ匿名で回答できるようにしたいそうです。アンケートの回答内容は，限られた集計担当者が集計し，それ以外の従業員に回答内容が漏れないようにしなければなりません。提出漏れをチェックできるように，各部門の担当者が，所属する従業員の回答を取りまとめ，集計担当者に提出する方式を考えているようです。また，回答後の内容変更は，認めないとのことです。

N 氏：従業員対象のアンケートだから，総数は決まっているが，別の従業員になりすまして回答を提出したり，回答内容を途中で改ざんしたりするなどの不正をチェックできるようにする必要がある。G 社の要望をよく考慮して設計を進めてくれ。また，各従業員の公開鍵は，以前に構築した G 社 PKI を利用して安全に取得できるから，これをうまく活用しよう。

R 君は，G 社の要望を考慮して Q システムの設計を行った。

〔Q システムの設計〕

R 君：G 社の要望を考慮して設計した Q システムの処理フローを，図 1 に示します。アンケートの実施方法ですが，表計算ソフトを使用して作成されたアンケートファイルを，アンケート配布システムがアンケート回答者（以下，回答者という）に電子メールで送付して回答してもらう仕組みがよいと思います。回答者には，アンケートファイルに回答を記入し，マクロ処理によってアンケート提出ファイル（以下，提出ファイルという）を出力してもらいます。そして，出力された提出ファイルを，電子メールで各部門の担当者あてに送付してもらいます。部門の担当者は，送付された提出ファイルを基に回収プログラムで提出漏れのないことをチェックした後，アンケート集計用ファイル（以下，集計用ファイルという）にまとめて，集計担当者あてに電子メールで送付します。

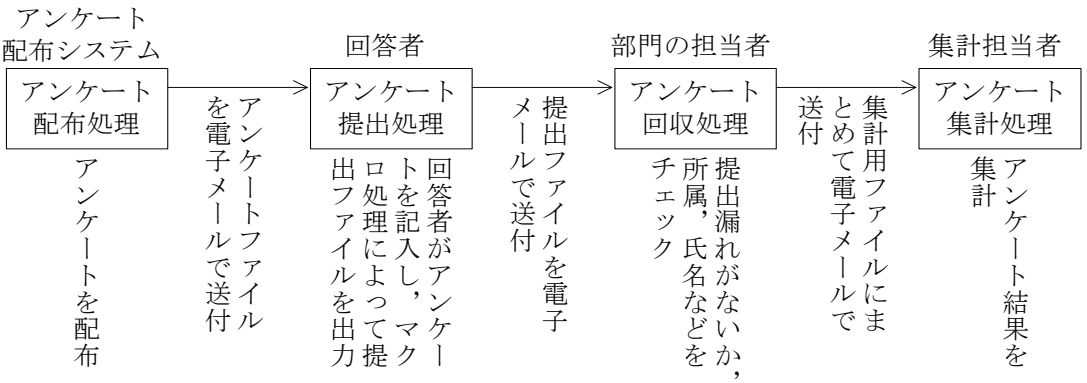


図１　Ｑシステムの処理フロー

N 氏：処理フローは分かった。提出ファイルを作成する方法を説明してくれないか。

R 君：はい。まず，アンケートの回答内容を［　a　］するため，マクロ処理によって集計担当者の公開鍵を使って暗号化します。公開鍵暗号アルゴリズムには，以前使用したことがあるアルゴリズム S を使おうと思います。回答者には，暗号化した回答内容を提出ファイルとして，各部門の担当者あてに電子メールで送付してもらいます。

N 氏：①その方法では，回答内容が漏えいするおそれがあるだろう。アルゴリズム S は，同じ平文に対して，同じ暗号文を出力するので，例えば，“はい”，“いいえ”のいずれか一方で答える質問が 3 問あるアンケートの場合，［　b　］種類の暗号文しか出力されない。同じ平文に対しても毎回異なる暗号文が出力されるアルゴリズム V を使用する方法もある。匿名で回答できるアンケートを実施したいという G 社の要望も併せて考慮して，再度検討してみてくれ。

R 君は，N 氏からの指摘を考慮して設計の見直しを行った。次は，その結果を基に設計のレビューを行ったときの N 氏と R 君のやり取りである。

〔Q システムの設計レビュー〕

R 君：設計の見直しを行った Q システムについて説明します。提出ファイルは，アンケート集計を行う集計担当者の公開鍵と，部門の担当者の公開鍵で，二重に暗号化します。また，アンケートファイルには，シリアル番号と，シリアル番号に対する署名を含めます。この署名は，アンケート配布システムがもつ秘密鍵を用いて計算します。以前に使用したことがあるシリアル番号は再使用しません。図 2 に，アンケート提出方式の概要を示します。

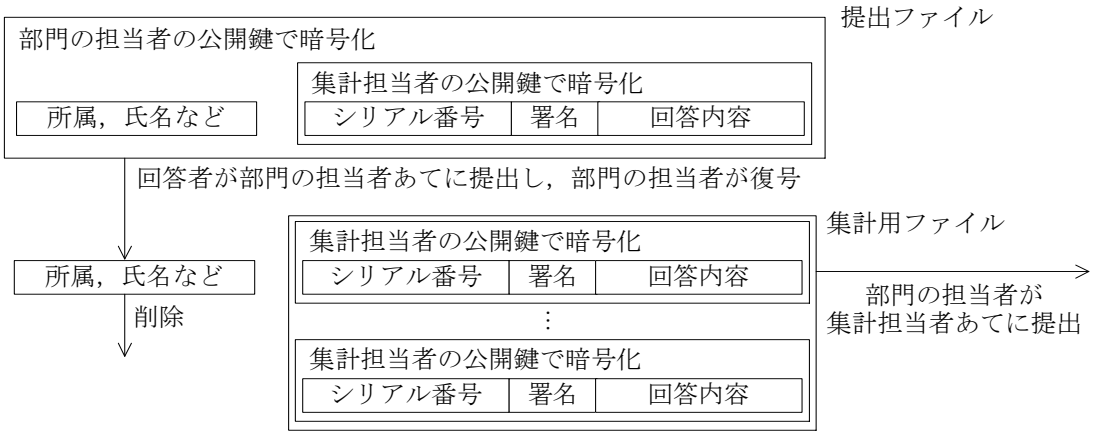


図２　アンケート提出方式の概要

R 君：まず，アンケート配布システムは，あらかじめ人数分のアンケートファイルを作成しておきます。個々のアンケートファイルはすべて異なるシリアル番号をもっています。そして，②この中から，無作為に一つアンケートファイルを選択し，回答者あてに回答者の公開鍵で暗号化して送付します。アンケート配布システムは，1 件のアンケートを送付するごとに送付したアンケートファイルを直ちに削除することで，重複して送付しないようにします。また，回答者が提出ファイルを作成する際には，シリアル番号とシリアル番号に対する署名を，マクロ処理によって，回答内容とともに集計担当者の公開鍵で暗号化し，所属，氏名などとともに提出ファイルに格納します。暗号化されているシリアル番号とその署名及び回答内容は集計用ファイルにまとめて，集計担当者に提出されます。集計担当者には，③シリアル番号に関する不正をチェックするプログラムも提供します。

N 氏：なるほど，この方式であれば，G 社の要望を満足できそうだ。ところで，なぜ，シリアル番号を付け，アンケートファイルを回答者の公開鍵で暗号化して送付する必要があるのかね。

R 君：そうしないと，④出張などで不在の従業員に代わって，別の従業員が勝手に回答を提出できるからです。また，部門の担当者が自分で提出ファイルを作成し，回答者からの提出ファイルとすり替えて，勝手に回答を変更してしまうことも可能になります。

N 氏：確かにそのとおりだな。それでは Q システムの構築を進めよう。

R 君と N 氏は，検討した結果に従って設計を行い，Q システムの構築を完了した。

設問１　暗号方式の検討について，(1)，(2) に答えよ。

(1) 本文中の［　a　］に入れる適切な字句を答えよ。また，［　b　］に入れる適切な数値を答えよ。

(2) 本文中の下線①において，回答内容だけをアルゴリズム S で暗号化した場合，暗号化された回答内容から攻撃者が回答内容を知る方法を，40 字以内で述べよ。

設問２　アンケートの匿名化について，(1)，(2) に答えよ。

(1) 図 2 で示した提出方式によって実現された G 社の要件を二つ挙げ，それぞれ 35 字以内で述べよ。

(2) 本文中の下線④の不正行為を防止できる理由を，50 字以内で述べよ。

設問３　アンケートの集計について，(1)，(2) に答えよ。

(1) 本文中の下線②において，アンケートファイルを無作為に選択している理由を，回答者の匿名性確保の観点から 35 字以内で述べよ。

(2) 本文中の下線③において，不正をチェックするプログラムがシリアル番号の署名検証のほかに行うべき処理を，35 字以内で述べよ。