問2　セキュリティインシデントへの対応に関する次の記述を読んで，設問 1～5 に答えよ。

A 社は，玩具を製造販売する従業員数 1,500 名の企業である。A 社の組織図を図 1 に示す。

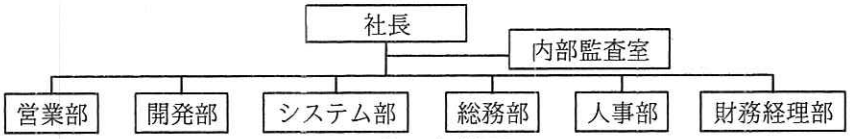
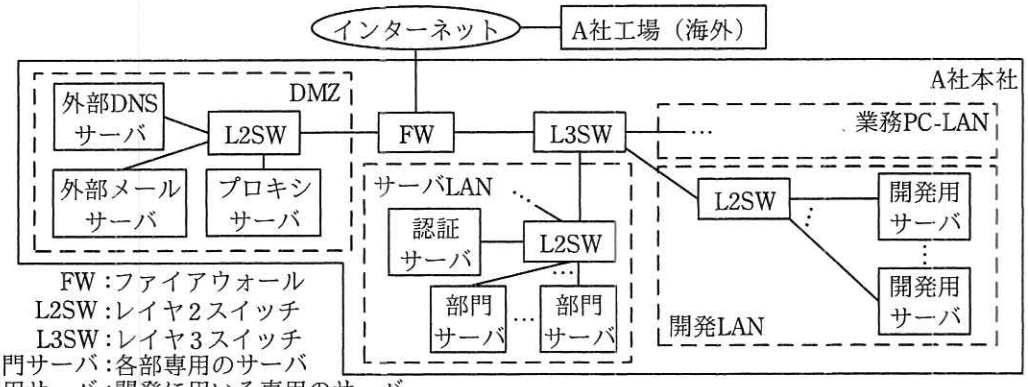


図 1　A 社の組織図

A 社は，情報セキュリティ基本方針を定めており，これに従い，情報セキュリティ委員会を設けている。情報セキュリティ委員会は，A 社の情報セキュリティについて意思決定する。情報セキュリティ委員会の委員長は社長，委員は各部の部長であり，事務局は総務部が担当する。情報セキュリティ委員会は，下部組織として，セキュリティインシデント（以下，インシデントという）に対応する非常時対応チームをもつ。非常時対応チームには，各部の代表者が参加する。ただし，非常時対応チームが取り扱うべきインシデントの範囲や，具体的な活動内容は明文化されていない。これまでのところ，非常時対応チームの活動実績は極めて少ない。

〔ネットワーク構成〕

A 社は，国内に本社を置き，海外に工場をもつ。A 社のネットワーク構成を図 2 に示す。



注記 1　個別の PC の記載は省略している。
注記 2　開発業務に用いる PC は開発 LAN に接続し，ほかの PC は業務 PC-LAN に接続している。

図 2　A 社のネットワーク構成（概要）

A 社本社のネットワークに接続する機器には，サーバ，ネットワーク機器及び PC がある。各部は，必要に応じて部門サーバをサーバ LAN に設置し，業務に利用している。各部の部門サーバは，各部が管理している。開発部は，開発部の部門サーバに加えて，開発用サーバを設置し，管理している。部門サーバと開発用サーバ以外のサーバ，全てのネットワーク機器及び全ての PC は，システム部が管理している。各部でシステム管理者を任命し，そのシステム管理者が適切に機器を管理するというのが A 社の機器管理方針である。

DMZ に設置されたサーバにはグローバル IP アドレスが付与され，インターネットとの間で通信できる。DMZ 以外に設置された機器には固定のプライベート IP アドレスが付与され，インターネットとの間の直接の通信は FW によって禁止されている。ただし，業務 PC-LAN に接続された PC は，プロキシサーバを介してインターネットにアクセスできる。プロキシサーバは直近 60 日分のログを保存している。開発 LAN から DMZ への通信は，FW によって禁止されている。

〔情報漏えいの発生〕

2018 年 9 月 11 日，A 社において，インシデント（以下，本インシデントをインシデント P という）が発覚した。この日，A 社の商品問合せ窓口に，A 社の発売前の新製品 α の操作説明書（以下，漏えい文書 X という）がインターネットの掲示板 U に投稿されている旨の通報が寄せられた。開発部の担当者が確認したところ，投稿されていたのは間違いなく A 社のもので，開発過程で作成された文書であることが分かった。

情報セキュリティ委員会は，インシデント P への対応方法を議論した。同委員会は，次の理由から，非常時対応チームではなく，当該文書を所管する開発部がインシデント P に対応することを決定した。

・個人情報及び重要な秘密情報の漏えいは見つかっておらず，緊急度及び重要度は低い。
・社内での調査活動について，非常時対応チームの権限及び調査手順が明確に定められておらず，調整が必要である。
・非常時対応チームのメンバの多くは，本来の業務のため，対応する時間の確保が難しい。

開発部は，急きょ，インシデント P に対応するためのチーム（以下，開発部対応チームという）を立ち上げ，対応を開始した。同チームの調査結果と措置状況を図 3 に示す。

(1) 開発部対応チームの調査活動の目的
・インシデント P の原因を調べて，必要な措置を講じること
(2) 調査の範囲
・検討の結果，次の機器を主な調査対象とした。
開発用サーバ及び開発部の部門サーバ
(3) 調査によって判明したこと
・漏えい文書 X は，開発部の部門サーバに保管されていた文書 Y と内容が同じだった。文書 Y は，8 月 29 日前後に作成された。
・文書 Y が保管されていた部門サーバは，開発部のメンバなら誰でもアクセスでき，文書を閲覧及び複製できる状態だった。文書 Y へのアクセスのログは取得されていなかった。
・開発部の商品企画第 2 チームは，委託先事業者である V 社と共同で新製品 α の操作説明書を執筆しており，V 社とのデータ交換に利用した USB メモリ（以下，USB メモリ R という）を紛失していた。USB メモリ R に文書 Y が格納されていた可能性があることから，USB メモリ R が情報漏えいの経路と考えられる。
(4) 調査で分からなかったこと
・文書 Y を流出させた者
・文書 Y 以外のデータの漏えいの有無，及びそのほかの被害の範囲
(5) 措置
・掲示板事業者に対する漏えい文書 X の公開中止の要請（状況：要請済み）
・USB メモリの管理方法の見直し（状況：システム部が近々見直す予定）
・本件の通報者へのお礼と対処した旨の報告（状況：担当部署を調整中）
(6) 開発部対応チームの活動時に認識された課題
次のように，会社としてのインシデント対応能力が不足している。
a. インシデント対応についての各部の責任や役割が曖昧で協力を得にくい場面があった。
b. インシデント対応についての作業手順が明確になっておらず，手探りの作業となった。このため，掲示板事業者への要請といった措置の着手が遅れた。
c. インシデント対応の経験をもつ者又はスキルをもつ者がおらず，非効率な作業になった。
d. ログが少なく調査が難航した。開発部はログ取得を定めた規程をもたず，開発部が管理する機器のうちログを取得していたものは少数だった。また，取得していたログの種類や保存期間にはばらつきがあった。

図 3　開発部対応チームの調査結果と措置状況（概要）

開発部対応チームの調査結果と措置状況は情報セキュリティ委員会に報告された。報告を受けて，委員会では，図 3 中の(5)に挙げられた一連の措置の完了をもってインシデント P への対応を終了することが了承された。また，インシデント対応能力の向上を目指すことを決め，システム部の G 部長に対応を指示した。

〔早期に取り組むべき事項のとりまとめ〕

G 部長は，情報セキュリティ委員会の承認の下，情報セキュリティに関わるコンサルティングサービスを提供する E 社に支援を依頼した。

E 社のコンサルタントである F 氏は，A 社がインシデント対応能力の向上のために早期に取り組むべき事項を図 4 のとおりまとめ，G 部長に報告した。

1. インシデント対応ポリシの策定
インシデント対応のための基本的な方針として，インシデント対応ポリシを定める。
インシデント対応ポリシに記載する項目の例として，NIST の文書 SP 800-61 Rev. 2 に挙げられているものを図 5 に示す。
2. インシデント対応のための体制整備
インシデントに迅速に対応することを目的に，インシデント対応チームを整備する。インシデント対応チームは，次の役割を担う。
・インシデントが発生した時点での対応活動
・インシデント対応に関係する他のサービスの提供
インシデント対応チームが提供するサービスの例として，NIST SP 800-61 Rev. 2 は，[a]，脆弱性や脅威についてのアドバイザリの配信，[b]，及び社内外での情報共有の推進を挙げている。
インシデント対応チームの母体として，非常時対応チームを活用することもできる。
3. 取得するログの見直し
（省略）

図 4　A 社が早期に取り組むべき事項（概要）

・[c] の責任表明
・本ポリシの目的と目標
・本ポリシの適用範囲
・[d] と関連用語の定義
・組織構造，並びに役割，責任及び権限レベルの定義
・[d] についての [e] 又は深刻度評価
・パフォーマンス測定
・報告と連絡の様式

図 5　インシデント対応ポリシに記載する項目の例

〔インシデント対応能力の向上への取組み〕

G 部長は，図 4 の事項の具体化を，F 氏の支援を受けながら進めることにした。

インシデント対応ポリシの適用範囲は全社とした。非常時対応チームは，A 社におけるインシデント対応のための組織横断チーム（以下，A-CSIRT という）として，再編成することにした。インシデント対応ポリシでは，A-CSIRT 及び各部の役割，

責任及び権限レベルを規定した。A-CSIRT は，従来の非常時対応チーム同様，各部の代表者で構成することにした。ただし，インシデントへの迅速な対応を可能にするため，各部で人選を見直し，更にシステム部所属のメンバを増やした。A-CSIRT のリーダは G 部長が務めることにした。メンバのスキルを高めるため，定期的に勉強会を開催し，外部の研修などにも積極的に参加してもらう方針を立てた。

ログについては，ログの管理に関する規程（以下，ログ管理ポリシという）を作成することにした。ログ管理ポリシの適用対象は，社内の全ての機器であり，システム部が管理する機器，部門サーバ及び開発用サーバも含まれる。ログ管理ポリシでは図 3 中の(6) d に挙げられたログに関わる課題を解決できるように，次の要件を定める。

要件 1　取得するログについての要件

・[f] について

・[g] について

要件 2　取得したログについての要件

・[h] について

・バックアップの作成について

・アクセス制御について

要件 3　各機器の時計を同期するとともに，各機器が出力するログに記録する時刻情報の [i] を [j] するという要件

情報セキュリティ委員会は，各部に対して，それぞれが管理する機器について，早急に，ログ管理ポリシに従った運用を開始するよう指示した。また，システム管理者に対して，①管理する機器について，通常時のネットワークトラフィック量や日，週，月，年の中でのその推移などの情報（以下，通常時プロファイルという）の把握に努めるよう指示した。

〔マルウェアについての通知〕

マルウェアを配布していたサイト（以下，サイト M という）に A 社の機器のうち 1 台がアクセスし，遠隔操作の機能をもつ，“new3.exe” というファイル名のマルウェア K をダウンロードした可能性がある旨の通知が，10 月 10 日に，ある民間組織か

らA社に対してあった。伝えられたサイトMのIPアドレスはA社管理外のものであり，サイトMのログに残っていたアクセス元のIPアドレスはA社のプロキシサーバのものだった。この通知はA-CSIRTに伝えられ，インシデント対応ポリシに照らして判断した結果，A-CSIRTが，インシデント（以下，本インシデントをインシデントQという）として直ちに対応を開始することになった。

A-CSIRTのメンバであるシステム部のCさんが，外部のインシデント対応研修に参加して得た知識を基に手順を手探りしながらも調査したところ，次のことが分かった。

・9月4日14時30分頃，②業務PC-LANに接続されているPCであるPC-Aがサイト M にアクセスし，“new3.exe”をダウンロードした。

・PC-Aの利用者は開発部のDさんである。

・プロキシサーバのログに，上記のダウンロードの直後，③PC-Aが特定のサイトにアクセスし，その後頻繁に同じサイトにアクセスを繰り返す様子が記録されていた。プロキシサーバのログのうち，送信元がPC-Aであるものを図6に示す。

```
 1: [04/Sep/2018:14:23:34 +0900] "GET http://xxxx/ HTTP/1.1" 200 57028 "-" "▲▲"
 2: [04/Sep/2018:14:28:42 +0900] "GET http://zzzz/2018/ne/bunrei.html HTTP/1.1" 200 14252
  "http://zzzz/2018/ne/topics.html" "▲▲"
 3: [04/Sep/2018:14:29:22 +0900] "GET http://xxxx/news/2018_3325.html HTTP/1.1" 200 22177
  "http://xxxx/" "▲▲"
 4: [04/Sep/2018:14:31:15 +0900] "GET http://yyyy/dl/samplebun.zip HTTP/1.1" 200 89331
  "http://zzzz/2018/ne/bunrei.html" "▲▲"
 5: [04/Sep/2018:14:31:23 +0900] "GET http://xxxx/news/2018_3353.html HTTP/1.1" 200 24555
  "http://xxxx/" "▲▲"
 6: [04/Sep/2018:14:34:20 +0900] "GET http://IPm/ HTTP/1.1" 200 563 "-" "▽▽"
 7: [04/Sep/2018:14:35:31 +0900] "GET http://IPm/dl/new3.exe HTTP/1.1" 200 143623 "-" "▽▽"
 8: [04/Sep/2018:14:37:06 +0900] "GET http://IPn/news.php HTTP/1.1" 200 5429 "-" "▽▽"
 9: [04/Sep/2018:14:37:32 +0900] "POST http://IPn/login/pro.php HTTP/1.1" 200 646 "-" "▽▽"
10: [04/Sep/2018:14:37:32 +0900] "POST http://IPn/login/pro.php HTTP/1.1" 200 35621 "-" "▽▽"
11: [04/Sep/2018:14:37:37 +0900] "GET http://IPn/admin/g.php HTTP/1.1" 200 563 "-" "▽▽"
12: [04/Sep/2018:14:37:47 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
13: [04/Sep/2018:14:37:52 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
14: [04/Sep/2018:14:37:58 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
15: [04/Sep/2018:14:38:04 +0900] "GET http://IPn/login/pro.php HTTP/1.1" 200 563 "-" "▽▽"
16: [04/Sep/2018:14:38:09 +0900] "GET http://IPn/admin/g.php HTTP/1.1" 200 563 "-" "▽▽"
17: [04/Sep/2018:14:38:14 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
18: [04/Sep/2018:14:38:19 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
```

図6　プロキシサーバのログのうち，送信元がPC-Aであるもの

```
（省略）
19: [05/Sep/2018:16:43:51 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
20: [05/Sep/2018:16:43:56 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
21: [05/Sep/2018:16:44:01 +0900] "POST http://IPn/login/pro.php HTTP/1.1" 200 35614 "-" "▽▽"
22: [05/Sep/2018:16:44:05 +0900] "GET http://IPn/admin/g.php HTTP/1.1" 200 563 "-" "▽▽"
（省略）
23: [06/Sep/2018:20:12:33 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
24: [06/Sep/2018:20:12:39 +0900] "GET http://IPn/admin/g.php HTTP/1.1" 200 563 "-" "▽▽"
25: [06/Sep/2018:20:12:44 +0900] "GET http://IPn/admin/g.php HTTP/1.1" 200 563 "-" "▽▽"
26: [06/Sep/2018:20:12:48 +0900] "POST http://IPn/news.php HTTP/1.1" 200 451 "-" "▽▽"
（省略）
27: [08/Sep/2018:03:39:04 +0900] "GET http://IPn/login/pro.php HTTP/1.1" 200 563 "-" "▽▽"
28: [08/Sep/2018:03:39:04 +0900] "POST http://IPn/admin/g.php HTTP/1.1" 200 35618 "-" "▽▽"
29: [08/Sep/2018:03:39:08 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
30: [08/Sep/2018:03:39:12 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
```

注記1　インシデントQとの関係が疑われるエントリを示す。

注記2　プロキシサーバが取得したログのうち，日時，リクエストのメソッド，リクエストのURL，リクエストのプロトコルとバージョン，要求元PCに送信したレスポンスのHTTPステータスコード，要求元PCに送信したレスポンスメッセージのサイズ，リクエストのRefererヘッダの値，及びリクエストのUser-Agentヘッダの値を示す。

注記3　図中のxxxx，yyyy，zzzzは，それぞれ，A社以外の特定のFQDNを示す。

注記4　図中のIPmはサイトMのIPアドレス，IPnはIPmとは異なる特定のIPアドレスを示す。

注記5　図中の▲▲及び▽▽は，それぞれ，特定のユーザエージェントを表す文字列を示す。

図6　プロキシサーバのログのうち，送信元がPC-Aであるもの（続き）

Cさんは，直ちに④PC-Aをネットワークから切断して回収した。また，ここまでに分かったことを基に，［　k　］を調査して，マルウェアKがほかの機器にも感染している可能性を簡易的に確認した。

その後，Cさんは，試行錯誤しながら更に詳しく調査を進め，図7に示す調査結果を得た。

Dさんは業務で複数の機器を利用している。そのうち，PC-A及び開発用のPC-BがインシデントQに関係していることが強く疑われる。

(1) PC-Aについて

・PC-Aは，Windows PCであり，業務PC-LANに接続されている。IPアドレスは192.168.70.131である。

・Dさんのユーザフォルダ内で“new3.exe”が見つかった。当該ファイルのプロパティ情報における作成日時は9月4日14時35分であった。

・Dさんのユーザフォルダ内で，アイコンを文書ファイルのアイコンに偽装した実行形式のファイルWが見つかった。

ファイルWの情報：
ファイル名“samplebun.docx␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣.exe”
プロパティ情報における作成日時　8月20日16時31分

・“new3.exe”及びファイルWをマルウェア対策ソフトベンダであるY社に提供してファイル解析を依頼し，表1の情報を得た。

(2) PC-Bについて

・PC-Bは，Linux PCであり，開発LANに接続されている。IPアドレスは192.168.75.245である。Dさんは，PC-Bを主にPC-Aからリモートログインして利用している。

・9月5日10時35分から45分までに，PC-Aから，⑤Dさんの利用者IDでのログイン試行が複数あり，一部は失敗し，一部は成功していた。PC-B上でのlast及びlastbコマンドの実行結果を，図8と図9にそれぞれ示す。lastはログイン履歴を，lastbはログイン失敗の履歴を出力するコマンドである。図中の“d0325”は，Dさんの利用者IDである。

・PC-Bのディレクトリ“/tmp/20xx/”に次のファイルが置かれていた。

  ・新製品αの設計資料
  ・文書Yを含む新製品αの操作説明書の草稿
  ・そのほかのファイル
  ・上記のファイルを格納したアーカイブファイル（以下，ファイルAという）

ファイルAの所有者はDさんであり，作成日時は9月7日4時15分であった。規則では，設計資料及び操作説明書のファイルはそのアーカイブファイルも含めてサーバ上にだけ保管することになっている。

(3) Dさんへのヒアリングによって得た情報

・Dさんは，サイトMにアクセスした記憶はない。

・Dさんは，9月4日午後にPC-AのWebブラウザを用いてインターネットで挨拶文例を検索し，見つけたZIP形式のファイル“samplebun.zip”をダウンロードした。Dさんは，このファイルを展開した上で，中にあったファイルWをダブルクリックし参考にした。

・Dさんは，出張のため9月5日から7日までオフィスに来ておらず，PC-Aを利用していない。この間，PC-AとPC-Bの電源は入ったままで，PC-Bはリモートログインできる状態だった。

・Dさんは，利用している機器について，それぞれの利用者IDとパスワードをファイルに記録し，PC-Aに保管していた。

・Dさんは，PC-Bの“/tmp/20xx/”ディレクトリ及びその下に置かれていたファイルについて，心当たりがない。

注記　ファイル名の“␣”は空白文字を示す。

図7　調査結果（抜粋）

表1　ファイルについての情報

ファイル	説明
new3.exe	遠隔操作の機能をもつマルウェア K である。実行されると，IPn のサイトにアクセスして，そのレスポンスに従って動作する。また，指定されたファイルを，HTTP の POST メソッドを用いて IPn のサイトに送信する機能をもつ。
ファイル W	ダウンローダの機能をもつマルウェア L である。サイト M からプログラムをダウンロードし，実行する。また，これらの処理と並行して文書作成ソフトを起動し，特定の文書を表示する。

```
d0325    pts/0    192.168.70.131   Fri Sep  7 01:33 - 09:40 (08:06)
d0325    pts/0    192.168.70.131   Wed Sep  5 10:45 - 22:13 (11:27)
d0325    pts/0    192.168.70.131   Wed Sep  5 10:41 - 10:43 (00:01)
d0325    pts/0    192.168.70.131   Tue Sep  4 11:20 - 13:45 (02:24)
d0325    pts/0    192.168.70.131   Mon Sep  3 09:35 - 20:23 (10:47)
```

注記　last コマンドの実行結果のうち，9 月 1 日から 7 日までの期間における利用者 ID “d0325” に関わる全ての行を抽出した。

図8　last コマンドの実行結果

```
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:44 - 10:44 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:44 - 10:44 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:43 - 10:43 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:40 - 10:40 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:37 - 10:37 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:37 - 10:37 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:37 - 10:37 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:36 - 10:36 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:36 - 10:36 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:35 - 10:35 (00:00)
d0325    ssh:notty  192.168.70.131   Mon Sep  3 09:34 - 09:34 (00:00)
```

注記　lastb コマンドの実行結果のうち，9 月 1 日から 7 日までの期間における利用者 ID “d0325” に関わる全ての行を抽出した。

図9　lastb コマンドの実行結果

次は，これまでの調査結果についての，C さんと G 部長との会話である。

C さん：PC-A が攻撃者によって遠隔操作されたことは間違いないと思います。また，PC-B は，少なくとも，D さんがオフィスに来ていなかった 9 月 5 日に攻撃者に遠隔操作されていたようです。

G 部長：PC-B で見つかったファイル A については，どのように考えればよいか。

Cさん：ファイル A は，情報を社外に送信するために攻撃者が作成したと考えればよいと思います。しかし，PC-B はインターネットにアクセスできないので，情報は社外に送信されなかったと思われます。

G部長：そうだろうか。例えば，ほかの機器を経由して送信された可能性はないのか。

Cさん：ほかの機器もいろいろと調査しましたが，ファイル A と同じ名前のファイルは見つかりませんでした。

G部長：ファイル名が同じとは限らない。ファイルが既に削除されている可能性もある。そういった可能性も考えて調査を続けてほしい。

Cさんは，Dさんが利用している機器について，フォレンジックツールを用いて，ファイル A のファイルサイズと [1] をキーにしてファイルを検索した。その結果，PC-A において，9月8日3時35分に，ファイル名は異なっていたものの，ファイル A と同じ内容のファイルが作成されていたことが分かった。また，プロキシサーバのログから，⑥当該ファイルが社外に送信された可能性があることが分かった。

加えて，C さんがインターネット検索をしたところ，ファイル A に格納されていた複数のファイルが，掲示板 U に，インシデント P のときと同じ投稿者によって投稿されていたことが分かった。これらのファイルのうち幾つかは，USB メモリ R に格納されたことはないと考えられるものだった。

〔インシデント Q のタイムラインと措置〕

G 部長は，調査結果の確認及び対応措置の検討について F 氏の支援を受けるよう C さんに指示した。F 氏の支援を受けて C さんが作成したインシデント Q のタイムラインを表2に示す。

表2　インシデントQのタイムライン

No.	日時	事象
1	ア	Dさんは，PC-AのWebブラウザで社外のサイトにアクセスし，ファイルWを格納したZIP形式のファイルをダウンロード
2	9/4 14:XX	Dさんは，No.1でダウンロードしたファイルをPC-A上で展開してファイルWを取り出した上で，これをダブルクリックし，m を実行
3	9/4 14:35	m は，n にアクセスし，“new3.exe”をダウンロード
4	9/4 14:XX	m は，o を実行
5	イ	o は，IPnのサイトとの頻繁な通信を開始 攻撃者による p が始まったと推測
6	9/5 10:35	攻撃者はPC-Bへのログインの試行を開始
7	ウ	攻撃者はPC-Bへのログインに初成功
8	～9/7 4:15	攻撃者は，漏えいが疑われるファイルのコピーと q を，r のローカルディスクに作成
9	9/8 3:35	攻撃者は，q と同じ内容のファイルを s のローカルディスクに作成
10	不明	No.9で作成されたファイルがIPnのサイトに送信された可能性

注記　XXは，正確な時刻が不明であることを示す。

また，F氏による追加調査の結果，社内の文書Zが，9月22日までの間に，攻撃者によって社外に送信されていたことが確認された。文書Zは，それまでに漏えいしたものとは別の新製品βの設計書である。

Cさんは，F氏の支援を受け，インシデントの封じ込め，根絶及び復旧のための措置を検討した。マルウェアLとマルウェアKについては，Y社から，これらを検知するためのマルウェア定義ファイルの提供を受け，全てのサーバ及びPCに適用することにした。Cさんは，そのほか必要と思われる措置をまとめて，G部長に提案した。G部長は，Cさんの提案を承認し，承認された措置が実施された。

〔インシデント対応のレビュー〕

インシデントQの対応が一段落した後，インシデント対応ポリシに従い，インシデントQの対応についてレビューが開催された。レビューにおいて，最初にG部長から，インシデントPとインシデントQは一連の攻撃だと推定されるという報告があった。次にインシデントQの対応が報告された。インシデントQの対応は，イン

シデント P の対応に比べて大幅に改善されたとの評価を受け，インシデント対応能力が向上してきていると判断された。最後に，⑦インシデント対応能力について未対応の課題を解決するための措置がまとめられ，順次実施されていくことになった。

設問１　〔早期に取り組むべき事項のとりまとめ〕について，(1)，(2) に答えよ。

(1)　図 4 中の［ a ］，［ b ］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　ISO/IEC 15408 の PP の作成　　イ　教育と意識向上

ウ　情報セキュリティポリシの管理　　エ　侵入検知

オ　内部統制基準の作成　　カ　ネットワーク機器の保守

(2)　図 5 中の［ c ］～［ e ］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　CVSS v3 基本値　　イ　SIEM　　ウ　インシデント

エ　受付窓口　　オ　個人情報　　カ　情報公開

キ　情報システム部門　　ク　ポリシ　　ケ　マネジメント層

コ　優先順位付け　　サ　ログと証跡

設問２　〔インシデント対応能力の向上への取組み〕について，(1)～(3) に答えよ。

(1)　本文中の［ f ］～［ h ］に入れる適切な字句を，それぞれ 12 字以内で答えよ。

(2)　本文中の［ i ］，［ j ］に入れる適切な字句を，それぞれ 8 字以内で答えよ。

(3)　本文中の下線①について，取得した通常時プロファイルの利用方法を 35 字以内で具体的に述べよ。

設問３　〔マルウェアについての通知〕について，(1)～(7) に答えよ。

(1)　本文中の下線②について，サイト M にアクセスした PC を特定した方法を，60 字以内で具体的に述べよ。

(2)　本文中の下線③について，このアクセスによってマルウェアが何を行っていたと考えられるか。HTTP リクエストと HTTP レスポンスによってマルウ

ェアが行っていた活動を，HTTP リクエストによる活動は 30 字以内で，HTTP レスポンスによる活動は 20 字以内でそれぞれ具体的に述べよ。

(3) 本文中の下線④について，調査の観点から見たときの問題は何か。40 字以内で具体的に述べよ。また，この問題を軽減するために本文中の下線④を実行する前に行うべき措置を，30 字以内で具体的に述べよ。

(4) 本文中の［ k ］に入れる適切な調査内容を，40 字以内で具体的に述べよ。

(5) 図 7 中の下線⑤について，D さんの利用者 ID を用いた PC-B へのログインに最初に成功するまでに，攻撃者が何回ログインに失敗したことが記録されているか。記録されている失敗の回数を答えよ。

(6) 本文中の［ l ］に入れる適切な字句を，8 字以内で答えよ。

(7) 本文中の下線⑥について，ファイルの社外への送信の可能性を示す記録を図 6 中から選び，行番号で答えよ。また，プロキシサーバ又は FW が取得できる情報のうち，当該記録と併せて見ることによってファイル送信の有無を判断するのに役立つ情報を 35 字以内で答えよ。ただし，送信元の IP アドレス及び図 6 中に示された情報は対象外とする。

設問 4 〔インシデント Q のタイムラインと措置〕について，(1)，(2) に答えよ。

(1) 表 2 中の［ ア ］～［ ウ ］に入れる適切な日時を答えよ。

(2) 表 2 中の［ m ］～［ s ］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア “samplebun.zip”	イ C さん	ウ D さん
エ IPn のサイト	オ PC-A	カ PC-B
キ SQL インジェクション	ク WHOIS サービス	ケ 遠隔操作
コ サイト M	サ 総当たり攻撃	シ ファイル A
ス フィッシング	セ プロキシサーバ	ソ マルウェア K
タ マルウェア L		

設問 5 本文中の下線⑦について，図 3 中の(6)に示された課題 a ～ d の中から，この時点で未対応の課題を選び，記号で答えよ。また，その課題を解決するための措置を，25 字以内で具体的に述べよ。