＜問２＞　工場のセキュリティ

●設問１

［試験センターによる解答例］

(1) User-Agent ヘッダフィールドの値が A 社で利用している Web ブラウザを示す値であるケース（47 字）

(2) a：エ

(3) b：ア

(4) c：サイト U（4 字）

(1) User-Agent ヘッダフィールドには、HTTP リクエストにおいて、ブラウザの名称やバージョン情報などが入る。User-Agent ヘッダフィールドは攻撃者によって詐称される場合も多いが、プロキシサーバのログ中に会社の標準的なブラウザ環境とは異なる値がないかを監視することで、内部に侵入したマルウェアによる C&C サーバとの不正な通信等を検知できる可能性がある。その反面、User-Agent ヘッダフィールドの値が A 社で利用している Web ブラウザを示す値である場合には、上記の監視をしていてもマルウェアによる通信であると判定するのは困難である。

(2) CAD-V の脆弱性への対策であるから、解答群で該当するのは脆弱性修正プログラムである「パッチ」である。

(3) ランサムウェアに感染し、一部のファイルが暗号化されてしまった PC-S は、「初期化」した上で、図 3 の項番 9(2)～(4)にあるような復旧作業を行う必要がある。

(4) 図 3 の項番 2、5 にあるように、ファイル T はランサムウェアであり、サイト U にアクセスし、自身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ことがわかっている。したがって、ファイル T を配布していた Web サイトとともに、サイト U に対する A 社内からのアクセスを FW によって遮断する必要がある。

●設問２

［試験センターによる解答例］

(1) d：カ
　　e：キ
　　f：オ

(2) 活動 1：1
　　活動 2：7
　　活動 3：3

(1) d：マルウェアが“おとり”として偽装する正常なファイルであるから、解答群の中で該当するのは「ドキュメント」である。

e：侵入に成功した攻撃者が、その後も長期にわたり侵入を継続できるように設置するのは「バックドア」である。

f：マルウェアが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受け取り、それに従って動作するものであるから、該当するのは「攻撃者の指示」である。

(2) 活動 1：SNS でターゲット組織を調査する活動であるから、該当するのは 1（偵察）である。

活動 2：ターゲット組織のファイルサーバにアクセスし、秘密情報を盗む行為であるから、該当するのは 7（目的の実行）である。

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入り口付近に置いておく行為であるから、該当するのは 3（配送）である。

●設問３

［試験センターによる解答例］

g：電波を傍受（5 字）
h：MAC アドレス（7 字）

MAC アドレスによる認証は、かつては無線 LAN 環境における端末認証として広く使用されていたが、MAC アドレスはネットワーク中を平文で流れるため、攻撃者が電波を傍受して同アドレスを入手することで容易に AP に接続できてしまう。そのため、認証方式として採用する場合にはそうしたリスクを認識しておく必要がある。

●設問４

［試験センターによる解答例］

(1) 攻撃者の操作指示が FA 端末に伝えられない。(21 字)

(2) i：イ
j：ウ
k：ア

(3) USB メモリをマルウェア対策ソフトでスキャンする。(25 字)

(1) 表 3 のデータダイオード方式の説明にあるように、この方式では 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。FA 端末が APT 攻撃を受け、表 1 の番号 5 までのステップ（インストール）までが成功した場合、番号 6 のステップ(コマンドとコントロール)で FA 端末に侵入したマルウェアは、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、その後の操作指示を受け取ろうとする。しかし､データダイオード方式では､A-NET 側から F-NET 側への通信は遮断されるため、攻撃者からの操作指示を FA 端末に伝えることができなくなる。

(2) データ転送の即時性で FW 方式、中継用 PC 方式、データダイオード方式を比較した場合、中継 PC 方式は担当者による操作を必要とする。したがって解答群の中でデータ転

送の即時性が△であるウに該当するのは中継 PC 方式である。中継 PC 方式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が、中継用 PC に侵入したマルウェアが F-NET に接続された機器に感染を拡大するリスクがある。
また、FW 方式とデータダイオード方式はいずれもデータ転送の即時性は○であるが、FW 方式では、F-NET に接続された FA 端末から A-NET 側へのアクセスとその応答に相当する通信を中継するため、マルウェアに感染するリスクがある。それに対し、データダイオード方式では、F-NET 側から A-NET 側へのデータの転送を許可されるものの、その逆方向は全ての通信が遮断されるため、マルウェアに感染するリスクは FW 方式より低い。
したがって、FW 方式がイ、中継用 PC 方式がウ、データダイオード方式がアとなる。

(3) USB メモリを介して FA 端末がマルウェアに感染するリスクを低下させるために接続前に行うべき措置としては、当該 USB メモリをマルウェア対策ソフトでスキャンすることである。

●設問５

［試験センターによる解答例］

(1) 事務 LAN 用：(い)
センサ NET 用：(か)

(2) 事務 LAN とセンサ NET は F-NET と分離されており、AP に不正接続しても FA 端末を攻撃できないから（50 字）

(1) 事務 LAN 用の認証サーバを設置する場所については図 1 の(あ)と(い)から選択する。(あ)は DMZ の L2SW、(い)は全社サーバ LAN の L2SW に接続されているが、事務 LAN は A 社の内部ネットワークであるため、認証サーバは(い)に設置すべきである。
続いてセンサ NET 用の認証サーバを設置する場所について図 5 の(う)、(え)、(お)、(か)から選択する。センサ NET は A 社のネットワークであるが、事務 LAN や F-NET とは切り離されている。したがって、認証サーバはセンサ NET の L2SW である(か)に設置すべきである。

(2) 問題文の〔見直し実施の方針〕にあるように、プロジェクト W は、サイバー攻撃などによる生産設備への停止を防ぐことを目的としている。図 5 で、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、F-NET は、事務 LAN 及びセンサ NET から切り離された独立ネットワークである。そのため、攻撃者が事務 LAN の AP やセンサ NET の AP に不正接続しても、FA 端末を攻撃することはできない。このことから、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。

●設問６

［試験センターによる解答例］

(1) イ

(2) ・当該脆弱性に対応したパッチを適用する。(19 字)
・脆弱性をもつソフトウェアの利用を禁止する。(21 字)

(1) 脆弱性の深刻度を評価するのに用いられるのは CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）である。CVSS は、IT 製品の脆弱性に対するオープンで汎用的な評価手法であり、ベンダに依存しない共通の評価方法を提供している。CVSS には、次の三つの基準がある。

基本評価基準（Base Metrics）
脆弱性そのものの特性を評価する基準。機密性、完全性、可用性に対する影響を評価し、CVSS 基本値（Base Score）を算出する。

現状評価基準（Temporal Metrics）
脆弱性の現状の深刻度を評価する基準。攻撃コードの出現有無や対策情報が利用可能であるかといった基準で評価し、CVSS 現状値（Temporal Score）を算出する。

環境評価基準（Environmental Metrics）
製品利用者の利用環境も含め、最終的な脆弱性の深刻度を評価する基準。攻撃による被害の大きさや対象製品の使用状況といった基準で評価し、CVSS 環境値（Environmental Score）を算出する。

上記の中で、下線④に該当するのは CVSS 環境値である。

(2) 図 5 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は、第一に当該脆弱性に対応したパッチの有無を確認し、提供されている場合には直ちに適用することである。パッチが提供されていない場合、もしくはパッチを適用することが難しい場合は、脆弱性をもつソフトウェアの利用を禁止することが確実な対策となる。

●設問 7

［試験センターによる解答例］

(1) **【図 4】 工場 LAN：エ**
標準 PC：エ
FA 端末：ア

【図 5】 事務 LAN：エ
F-NET：ア
センサ NET：ア
標準 PC：エ
FA 端末：ア

(2) **・各部門が定めた管理・維持のための措置（18 字）**
・リスクアセスメントの結果（12 字）

(1)

【図 4】

・注記 1 にあるように、工場 LAN は A-NET の一部であるため、システム部が管理する
・図 2 にあるように、標準 PC はシステム部が管理する
・FA 端末はα工場の部門機器であるため、α工場が管理する

【図 5】

・表 2 にあるように、事務 LAN は A-NET の一部であるため、システム部が管理する
・表 2 にあるように、F-NET とセンサ NET はα工場の部門 NET であるため、α工場が管理する
・図 2 にあるように、標準 PC はシステム部が管理する
・FA 端末はα工場の部門機器であるため、α工場が管理する

(2) 図 2 の 7 では、各部門が部門機器又は部門 NET を A-NET に接続する際のシステム部への申請において、書面に記載する事項として、「接続の目的」「接続に必要な技術情報」「管理者と連絡先」があるが、これに追加すべき二つの事項を考察する。
問題文の〔セキュリティ規程の見直し〕にあるように、C さんは、これまでの経緯を踏まえ、各部門に対し、次の事項を実施することをセキュリティ規程に追加しようとしている。

・部門機器又は部門 NET を適切に管理・維持するための措置
・部門機器又は部門 NET と A-NET との接続についてリスクアセスメントを実施

したがって、各部門が A-NET への接続申請をする際には、従前の事項のほかに、「各部門が定めた管理・維持のための措置」と「リスクアセスメントの結果」についても記載すべきである。