SC

# 平成31年度　春期
# 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 |

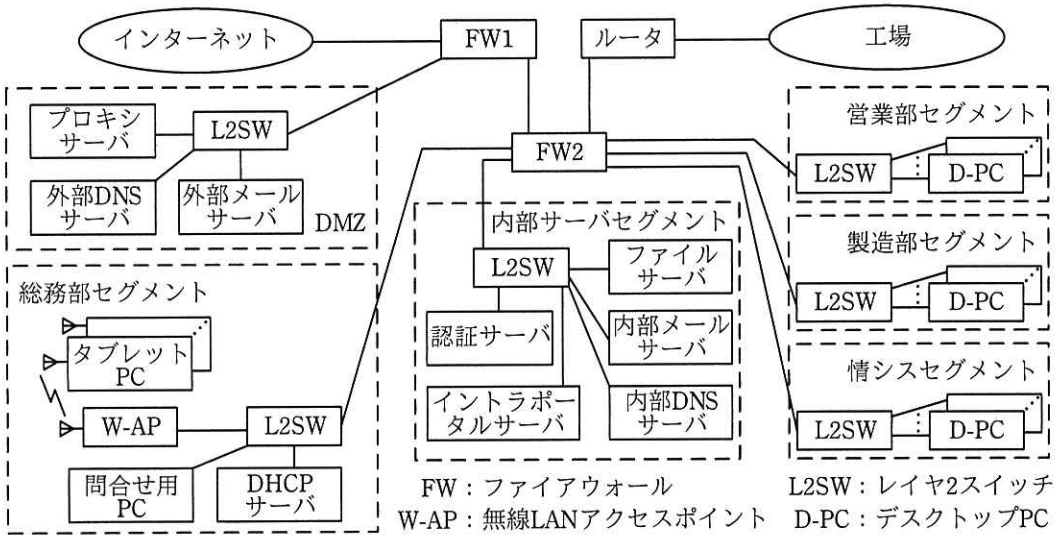
5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。2問とも○印で囲んだ場合は，はじめの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〕


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　マルウェア感染と対策に関する次の記述を読んで，設問1～6に答えよ。

N社は，従業員数5,000名の化学メーカであり，総務部，営業部，製造部及び情報システム部（以下，情シスという）がある。また，国内に工場がある。N社のLAN構成を図1に示す。




注記1　DMZのサーバには，グローバルIPアドレスが割り当てられている。

注記2　DMZ以外のセグメント及び工場の各機器には，プライベートIPアドレスが割り当てられている。

注記3　タブレットPCには，DHCPサーバによって動的にIPアドレスが割り当てられ，それ以外の機器には，固定IPアドレスが割り当てられている。

図1　N社のLAN構成

N社では，全従業員に一つずつ利用者IDが割り当てられ，その利用者IDとパスワードが認証サーバに登録される。タブレットPC，問合せ用PC及びD-PC（以下この三つを併せて，社内PCという）へのログオン時並びに内部メールサーバ及びファイルサーバへのアクセス時には，認証サーバを使用して認証が実施される。イントラポータルサーバは，認証サーバと連携して，ベーシック認証を使用している。

総務部では，無線LAN接続型のタブレットPCを導入している。無線LANの暗号化では，WPA2を使用している。W-APでは，不正な端末の接続を防ぐための対策として，次の機能を使用している。

・登録済みMACアドレスをもつ端末だけを接続可能とする接続制御

・総務部に所属する従業員の利用者IDだけに接続を許可するIEEE 802.1X認証

IEEE 802.1X認証では，認証サーバと連携して，利用者IDとパスワードを使用している（EAP-PEAP）。

プロキシサーバでは，各機器からの全てのアクセスについて，アクセスログを取得している。

N社では，クラウドサービスを利用して，会社情報や製品情報を公開するWebサイトを運用している。Webサイトには，訪問者からの問合せを受け付けるためのフォームが用意されており，訪問者が問合せ内容を入力すると，その内容が電子メール（以下，メールという）でN社の特定のメールアドレス宛てに送信される。フォームにはファイルを添付する機能はないので，問合せメールにファイルが添付されることはない。万一，このフォーム以外から，この特定のメールアドレス宛てにメールが届いた場合は，そのメールは破棄される。問合せ用PCは，問合せメールを受信するための専用のD-PCで，他の用途には使用していない。また，問合せメールを他の社内PCで受信することはない。問合せ用PCから回答メールを返信する場合，回答メールの送信元メールアドレスには送信専用のメールアドレスを使用している。

FW1のルールを表1に，FW2のルールを表2に示す。

表1　FW1のルール

| 項番 | 送信元 | 宛先 | サービス | 動作 | ログ取得 |
|---|---|---|---|---|---|
| 1 | インターネット | 外部DNSサーバ | DNS | 許可 | する |
| 2 | インターネット | 外部メールサーバ | SMTP，SMTPS | 許可 | する |
| 3 | 外部DNSサーバ | インターネット | DNS | 許可 | する |
| 4 | 外部メールサーバ | インターネット | SMTP，SMTPS | 許可 | する |
| 5 | 外部メールサーバ | 内部メールサーバ | SMTP | 許可 | する |
| 6 | 内部メールサーバ | 外部メールサーバ | SMTP | 許可 | する |
| 7 | 内部IP[1)] | プロキシサーバ | 代替HTTP | 許可 | する |
| 8 | プロキシサーバ | インターネット | HTTP，HTTPS，FTP | 許可 | する |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 15 | 全て | 全て | 全て | 拒否 | する |

注記1　SMTPSは，SMTP over TLSを，HTTPSは，HTTP over TLSを示す。

注記2　項番が小さいルールから順に，最初に合致したルールが適用される。

注[1)]　N社内で使用している全てのプライベートIPアドレスを示す。

表 2　FW2 のルール

| 項番 | 送信元 | 宛先 | サービス | 動作 | ログ取得 |
|---|---|---|---|---|---|
| 1 | 内部 IP | インターネット | 全て | 拒否 | する |
| 2 | 内部 IP | プロキシサーバ | 代替 HTTP | 許可 | する |
| 3 | 内部 IP | 内部メールサーバ | SMTP，POP3 | 許可 | する |
| 4 | 内部 IP | 内部 DNS サーバ | DNS | 許可 | する |
| 5 | 内部 IP | 認証サーバ | LDAP，LDAP over TLS | 許可 | する |
| 6 | 問合せ用 PC | 全て | 全て | 拒否 | する |
| 7 | 外部メールサーバ | 内部メールサーバ | SMTP | 許可 | する |
| 8 | 内部メールサーバ | 外部メールサーバ | SMTP | 許可 | する |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 22 | 全て | 全て | 全て | 拒否 | する |

注記　項番が小さいルールから順に，最初に合致したルールが適用される。

FW1 と FW2 は，ステートフルパケットインスペクション型である。FW1 には，ペイロードの内容に基づきアプリケーション層での通信の挙動を分析し，マルウェアの動作に伴う不正な通信を検出して遮断できる機能（以下，L7FW 機能という）がある。

〔インシデント発生〕

4 月 12 日 13:00 頃，セキュリティ情報共有団体から，“ある C&C（Command and Control）サーバを調査していたところ，そのサーバに対する N 社からの通信記録を発見した。”との連絡が届き，その通信に関して，表 3 の情報が提供された。

表 3　提供された情報（抜粋）

| | |
|---|---|
| 送信元 IP アドレス | aaa.bbb.ccc.ddd [1)] |
| 宛先 IP アドレス | C&C サーバの IP アドレス |
| 宛先 TCP ポート番号 | 443 |
| 通信が開始された時刻 | 4 月 10 日 14:00:00 |

注 [1)]　aaa.bbb.ccc.ddd は，図 1 中のプロキシサーバの IP アドレスである。

情報提供を受けて，N 社の CSIRT メンバが招集された。N 社の CSIRT のリーダである R 課長は，メンバの P 君に対して，情報処理安全確保支援士（登録セキスペ）である W 主任の支援を受けながら，直ちに状況を確認するよう指示した。P 君は，表 3 の情報の真偽を確かめるために，まず［ a ］のログを確認して N 社から当

該通信が発信されていたとの確証を得た後，通信を開始した端末を特定するために［ b ］のログを確認した。その結果，問合せ用 PC から C&C サーバに向けて HTTPS と思われるセッションが確立していたことが確認できた。

〔問合せ用 PC の調査〕

状況の報告を受けた R 課長は，問合せ用 PC の調査を指示した。P 君は，決められたインシデント対応手順に従い，まず問合せ用 PC の HDD のコピー（以下，複製 HDD という）を作成した。コピーは①ファイル単位ではなくセクタ単位で全セクタを対象とした。原本である HDD はそのまま保全した。次に，予備の D-PC を新たな問合せ用 PC として設定して，問合せメールへの回答業務を継続できるようにした。

〔感染経路の調査〕

P 君が，複製 HDD の中に残っていた直近 6 か月分の問合せメールについて調査したところ，本文に URL が記載されたメールが幾つかあった。その全ての URL のサイトを調査したが，どのサイトも改ざんの報告はなく，閲覧したとしてもマルウェアに感染するおそれがないサイトだった。

問合せメールによるマルウェア感染が C&C サーバとの通信の原因である可能性は低いと考えた P 君は，調査方針を W 主任に相談し，複製 HDD 内のログ及び関連機器内のログを調査することにした。その結果，図 2 の調査結果が得られた。

(1) 複製 HDD 内のログを調査したところ，4 月 10 日 10:00 に，ある IP アドレス（以下，被疑 IP という）から問合せ用 PC へのリモートデスクトップログオンが成功していた。そのログオンには，総務部の B さんの利用者 ID が使用されていた。
(2) DHCP サーバ内のログを調査したところ，被疑 IP は，4 月 10 日 9:30 から 11:30 までの間，ある PC（以下，被疑 PC という）に割り当てられていた。
(3) W-AP 内のログを調査したところ，4 月 10 日 9:30 に，被疑 PC が発信元である，B さんの利用者 ID を用いた IEEE 802.1X 認証要求が成功していた。
(4) 認証サーバ内のログを調査したところ，4 月 10 日 9:30 及び 10:00 に，B さんの利用者 ID の認証成功の記録があった。一方，4 月 10 日 10:00 から 2 月 1 日まで遡って確認したが，B さんの利用者 ID で認証失敗した記録はなかった。
(5) B さんに話を聞いたところ，4 月 10 日は休暇を取得していたとのことだった。念のために，タブレット PC のログを調査したが，4 月 10 日に使用された形跡はなかった。

図 2　調査結果

この調査結果から，P 君は，攻撃者が B さんの利用者 ID とパスワードを入手し，それらを利用して無線 LAN 経由で問合せ用 PC に不正にログオンしたと判断した。

そこで，W 主任は，不正な PC を W-AP に接続させないための対策として，IEEE 802.1X 認証の方式を EAP-TLS に変更する案を提案した。

また，複製 HDD の分析を続けたところ，マルウェアと思われるファイルが残っており，実行されていた痕跡があった。

〔無線 LAN の脆弱(ぜい)性〕

P 君は，総務部の W-AP は，MAC アドレスによる接続制御をしているのに，攻撃者がなぜ接続できたのか疑問に思い，W 主任に聞いてみた。W 主任は，②WPA2 を使用していても，無線 LAN の通信が傍受されてしまうと B さんが利用しているタブレット PC の MAC アドレスを攻撃者が知ることができることと，③攻撃者が，自分の無線 LAN 端末を総務部の W-AP に接続可能にする方法を P 君に説明した。

また，IEEE 802.1X 認証で使用する B さんの利用者 ID とパスワードを攻撃者が入手する方法について，次のように話した。

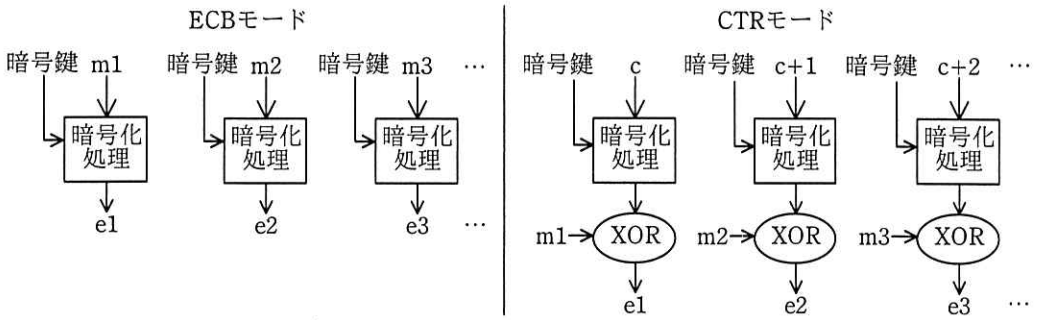
W 主任：最近，KRACKs と呼ばれる WPA2 への攻撃手法が報告され，攻撃用のサンプルコードも公表されている。この攻撃を高い確率で成功させるためには，攻撃者は不正な W-AP を設置し，正規の W-AP と端末との間の中間者として動作させる必要がある。この攻撃が成功すると，WPA2 で暗号化したパケットを解読されるおそれがある。N 社は，4 月 10 日より前に，この攻撃に遭っていながら，攻撃に気付かなかったのではないか。

P 君は，KRACKs について調べてみた。その結果，KRACKs は，攻撃者が特定の通信に介入することによって，WPA-TKIP 及び WPA2 が使用する AES-CCMP というプロトコルの暗号を解読するものであることが分かった。解読の手段は，AES-CCMP の場合，CTR モードにおける初期カウンタ値を強制的に再利用させるものであった。AES-CCMP は，AES というブロック暗号と CTR モードという暗号モードをベースとしている。

〔暗号モード〕

P 君は，暗号モードについても調べてみた。ブロック暗号を利用して長い平文を暗号化するには，平文をブロックに分割し，各ブロックに対して暗号化処理を適用する必要がある。ブロック暗号の適用方法を暗号モードと呼ぶ。最も単純な暗号モードは ECB モードである。

暗号モードのうち，ECB モードと CTR モードの仕組みを図 3 に示す。




注記 1　m1，m2，m3，…はブロック長に分割した平文（以下，平文ブロックという）を，e1，e2，e3，…は平文ブロックを暗号化した暗号文（以下，暗号ブロックという）を，c は初期カウンタ値を表す。

注記 2　XOR は，排他的論理和演算を行うことを示す。

図 3　ECB モードと CTR モードの仕組み

一般的なブロック暗号のブロック長は，64～128 ビット程度なので，暗号化のため TCP/IP パケットをヘッダも含めて平文ブロックに分割すると，④パケットがもつある特徴から，同一端末間の異なるパケットにおいて，同一の平文ブロックが繰り返して現れることが想定される。そのため，その平文の内容は高い確率で推測可能である。仮に TCP/IP パケット全体を ECB モードで暗号化した場合，［　c　］が繰り返して現れることになり，暗号の解読が容易になるおそれがある。

CTR モードでは，暗号ブロックは，［　d　］と［　e　］の排他的論理和である。無線 LAN の場合，攻撃者は暗号化されたパケットを入手可能であるので，その暗号化されたパケットに対応する［　d　］が推測できた場合，［　e　］は容易に算出できる。これらを踏まえると CTR モードでは，初期カウンタ値の再利用の強制によって，同一の［　e　］を使用して異なるパケットの暗号文を作成してしまう可能性がある。

ここまで調べた P 君は，イントラポータルサーバへのアクセスは HTTP であり，かつ，ベーシック認証を使用しているので，WPA2 の通信を解読されると利用者 ID とパスワードの流出に直結してしまうことに気付いた。

〔不審な W-AP の発見と対策〕

無線 LAN 経由で侵入された可能性のある時期には，タブレット PC は KRACKs への対策がされていなかったので，P 君は，KRACKs による攻撃を受けた可能性を調査する必要があると考えた。そこで P 君は，W 主任に相談して，攻撃者が不正な W-AP を設置していないか，N 社の周囲の無線状況を調査した。その結果，総務部の W-AP と同一の SSID が設定された不審な W-AP が，N 社敷地外にあることを発見し，KRACKs による攻撃を受けたと結論付けた。

そこで，W 主任は，KRACKs によって WPA2 の通信が解読された場合でも被害を防ぐ対策として，イントラポータルサーバへのアクセスを HTTPS に変更する案を提案した。

〔L7FW 機能の実効性の確認〕

一方，R 課長は，FW1 には L7FW 機能があることを思い出した。しかし，今回のインシデントでは，FW1 が，マルウェアによる通信を不正な通信として検出した形跡はなく，通過させていた。この件について，R 課長は P 君に調査を指示した。

P 君が，［ b ］のログを分析したところ，4 月 10 日の 10:00 以降，問合せ用 PC が発信元である HTTPS と思われる通信が，通常よりも大幅に増加していた。これらの通信の大半は，表 3 の C&C サーバの IP アドレスを含む不審な IP アドレスへの通信であったことから，マルウェアによるものと推測された。一方，問合せ用 PC が発信元である HTTP 通信は，ほとんどなかった。

続いて P 君が，FW1 の機能の設定状態を確認したところ，L7FW 機能は有効化されていたが，HTTPS 通信によって送受信されるデータを復号する機能（以下，HTTPS 復号機能という）はライセンスがないので有効化されていなかった。この状態では，HTTPS 通信に対して L7FW 機能は効果がないことも分かった。P 君は，これら一連の内容を R 課長に報告した。

R 課長は，インシデントの調査を終了し，W-AP の IEEE 802.1X 認証の方式を

EAP-TLS に変更する案と，イントラポータルサーバへのアクセスを HTTPS に変更する案を実施するとともに，残りの対策の検討に移ることにした。

〔未知マルウェア対策の改良〕

R 課長は，今後，HTTPS 通信を利用するマルウェアが増えると思われるので，社内 PC について，何らかの対策を打つ必要があると考え，W 主任に検討を指示した。

W 主任は，追加の費用が発生しない範囲で実施できる対策として，プロキシサーバがもつ，特定の URL への接続を禁止するブラックリスト機能の適用を検討した。HTTP 通信の場合，プロキシサーバでは内容を［ f ］ことができる。しかし，HTTPS 通信の場合，社内 PC からプロキシサーバに CONNECT メソッドによって接続要求を送る時点では平文で Web サーバの［ g ］名とポート番号が渡されるが，社内 PC と Web サーバの間で TLS セッションが成立して暗号通信路が確立した後は，プロキシサーバでは内容を［ f ］ことはできない。そのため，HTTPS 通信の場合，実質的にブラックリストに登録できるのが，URL の［ g ］部とポート番号部だけであり，［ h ］部は指定できないことや，そもそもブラックリストに登録すべき URL 情報が必要なタイミングで入手できないことから効果が期待できないとの結論となった。

そこで，追加の費用の発生も視野に入れた対策として，W 主任は，ライセンスの購入による HTTPS 復号機能の有効化（以下，対策 1 という）及び社内 PC のマルウェア対策の強化（以下，対策 2 という）の二つを考えた。それぞれの対策の内容は，表 4 のとおりである。

表 4　検討した対策の内容

| 項目 | 対策 1 | 対策 2 |
|---|---|---|
| 概要 | FW1 の HTTPS 復号機能のライセンスを購入し，同機能を有効にする。 | 未知のマルウェアを検出するソフトウェアを購入し，社内 PC に導入する。 |
| 期待する効果 | HTTPS 通信であっても，FW1 の L7FW 機能を用いて，マルウェアによる不正通信を検出できる。 | （省略） |
| 考慮すべき点 | HTTPS 復号機能によって，FW1 の性能低下のおそれがある。<br>HTTPS 以外の暗号通信には効果がない。 | （省略） |

W 主任は，⑤マルウェアが窃取した情報を社内 PC から社外に送信する経路が FW1 を経由した HTTPS 以外にもあり，対策 1 と L7FW 機能だけでは全ての経路を検査することはできないので，対策 2 を併せて実施する必要があると考え，P 君に対策 1 及び対策 2 の検討を指示した。

〔対策 1 と対策 2 の検討〕

P 君が，対策 1 と対策 2 の検討に当たり，HTTPS 復号機能の動作の詳細を確認したところ，N 社の LAN では図 4 に示す通信の流れになることが分かった。

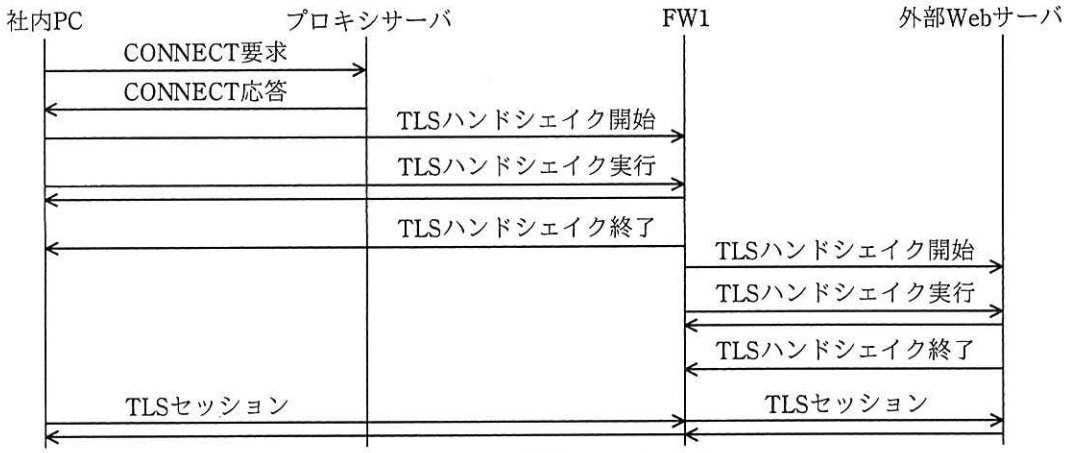



図 4　HTTPS 復号機能の通信の流れ

また，HTTPS 復号機能は，図 5 のとおりになることが分かった。

1. 事前準備
(1) FW1 が発行した自己署名証明書を［　i　］として全ての社内 PC に登録する。
2. HTTPS 復号機能による外部 Web サーバのディジタル証明書の取扱い
(1) FW1 が，外部 Web サーバへの HTTPS リクエストを検出した際に，宛先 IP アドレスを変換し，FW1 を終端として社内 PC との間で TLS セッションの確立を開始する。
(2) FW1 は，ディジタル証明書及び対応する秘密鍵を作成する。
(3) FW1 は，作成したディジタル証明書及び対応する秘密鍵を利用して社内 PC と FW1 の間で TLS セッションを確立する。
(4) FW1 は社内 PC との TLS セッションの確立とほぼ同時に，クライアントとして外部 Web サーバとの TLS セッションも確立する。
(5) 双方の TLS セッションが確立したら，FW1 はその間で通信内容の転送を行う。
(6) 片方の TLS セッションの確立に失敗した場合は，もう片方の TLS セッションも終了する。

図 5　HTTPS 復号機能の概要

P 君が FW1 の製造元に対策 1 の実施を検討している旨を伝えたところ，無料で 30 日間だけ同機能を利用できる評価用ライセンスの発行を提案されたので，早速，評価用ライセンスを適用し，CSIRT メンバの D-PC から発信される通信で評価してみた。その結果，HTTPS 復号機能には，通信の種類によっては制約があることが分かった。通信の種類と制約を表 5 に示す。

表 5　HTTPS 復号機能における通信の種類と制約（抜粋）

| 項番 | 通信の種類 | 制約の内容 | 制約の原因 |
|---|---|---|---|
| 1 | j | （省略） | 図 4 の流れの中で，FW1 は，社内 PC がもっているクライアント証明書に対応した秘密鍵を利用することができない。 |
| 2 | 外部 Web サーバのサーバ証明書に軽微な不備がある場合に，利用者が不備を無視してアクセスする。 | （省略） | 外部 Web サーバごとにサーバ証明書の検証条件を変更するということができない。 |
| 3 | k | （省略） | FW1 には，FW1 の製造元によって安全性が確認された CA のディジタル証明書だけが，信頼されたルート CA のディジタル証明書としてインストールされている。 |

P 君は，これらの制約の回避方法を運用手順に含めることにした。表 5 の項番 1 の場合は，FW1 の HTTPS 復号機能の例外リストに外部 Web サーバを追加することにした。例外リストに Web サーバを追加すると，例外的に復号機能を適用せず社内 PC と Web サーバの間で直接 HTTPS 通信を行うことができる。例外とする場合には，業務上の必要性があること，及び正当な Web サーバであることを所定の手順で確認することにした。表 5 の項番 2 及び 3 の場合も，必要な内容を運用手順に含めた。

続いて，P 君は，対策 2 の検討を行い，具体策をまとめた。W 主任は，P 君の報告を受けて，対策 1 と対策 2 の実施案をまとめた。実施案は，R 課長から CSIRT 責任者である情シス担当取締役に報告され，承認の上で実施された。以後，N 社では，マルウェアによるインシデントは発生していない。

設問1　本文中の［ a ］，［ b ］に入れる最も適切な機器名を，図1の中から選び答えよ。

設問2　本文中の下線①について，P君がこのようにコピーしたのは，何をどのような手段で調査することを想定したからか。調査する内容を20字以内で，調査の手段を25字以内で具体的に述べよ。

設問3　〔無線LANの脆弱性〕について，(1)，(2)に答えよ。

(1)　本文中の下線②について，知ることができる理由を，30字以内で述べよ。

(2)　本文中の下線③について，具体的な方法を，55字以内で述べよ。

設問4　〔暗号モード〕について，(1)，(2)に答えよ。

(1)　本文中の下線④について，TCP/IPパケットの特徴を，40字以内で述べよ。

(2)　本文中の［ c ］～［ e ］に入れる適切な字句を，それぞれ15字以内で答えよ。

設問5　〔未知マルウェア対策の改良〕について，(1)~(3)に答えよ。

(1)　本文中の［ f ］に入れる適切な字句を，10字以内で答えよ。

(2)　本文中の［ g ］，［ 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　インデックス　　イ　サブジェクト　　ウ　シーケンス

エ　ネットワーク　　オ　パス　　カ　ホスト

(3)　本文中の下線⑤について，マルウェアが窃取した情報を社外に送信する方法が複数考えられる。そのうち二つを挙げ，それぞれ35字以内で具体的に述べよ。

設問6　〔対策1と対策2の検討〕について，(1)~(3)に答えよ。

(1)　図5中の［ i ］に入れる適切な字句を，20字以内で答えよ。

(2)　表5中の［ j ］に入れる適切な字句を，40字以内で述べよ。

(3)　表5中の［ k ］に入れる適切な字句を，65字以内で述べよ。

問2　情報セキュリティ対策の強化に関する次の記述を読んで，設問1～7に答えよ。

A社は，従業員数200名の金型加工業者である。新潟市内の同じ敷地に本社と工場が，大阪市に営業拠点がある。本社には，管理部，設計部及び製造部がある。管理部には，総務係，営業係及びシステム係がある。営業係は，営業拠点を管理する。製造部は，工場を管理する。

A社の金型加工技術は，評価が高く，大企業から金型加工を請け負うことがある。請け負うときは，金型加工に必要な情報を収めたファイル（以下，設計情報ファイルという）を，DVD-R又は電子メール（以下，メールという）を使って，発注元との間でやり取りする。

A社では，最新技術の情報収集を目的として，取引先が参加している複数のメーリングリストに，営業係員及び設計部員が参加している。

〔営業秘密の取扱い〕

A社では，自社の営業秘密が不正競争防止法で保護されるようにするために，不正競争防止法及び経済産業省が公表している営業秘密管理指針（平成27年1月28日全部改訂）を参考にして，表1に示す営業秘密に関する管理規則を定めている。

表1　営業秘密に関する管理規則（概要）

| 要件名 | 管理規則（概要） |
|---|---|
| a 性 | ・営業秘密を含む文書は，全てのページにA社秘密情報と記載すること<br>・閲覧できる者を，A社の業務上必要な従業員に制限すること |
| b 性 | ・A社で開発し，A社の事業に必要な金型加工技術の情報を，営業秘密とすること |
| c 性 | ・営業秘密は，一般的に知られた状態にならないように，業界誌などの刊行物に掲載しないこと |

〔A社のネットワーク構成〕

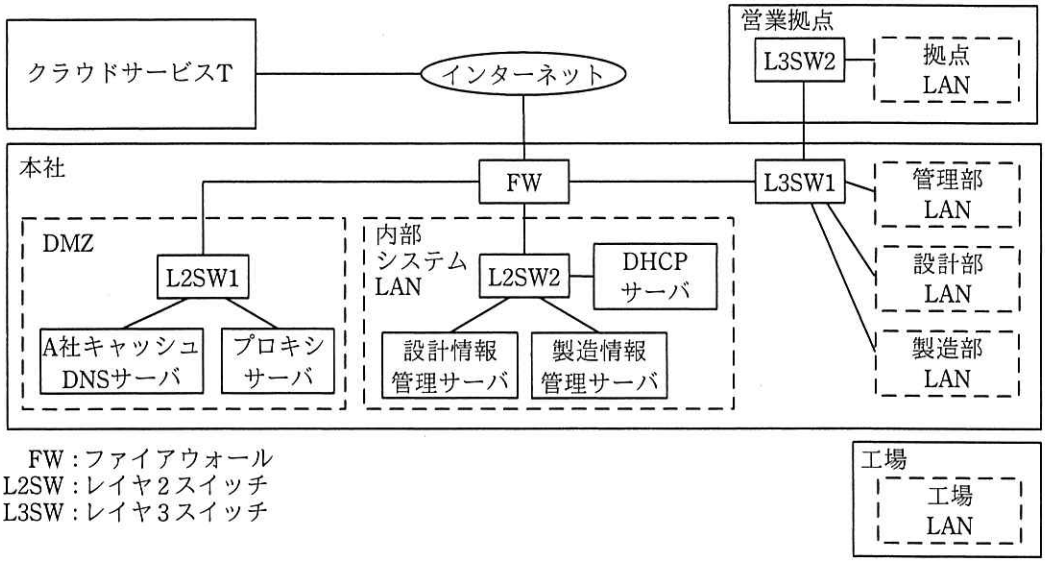
A社では，デスクトップPC（以下，DPCという）を，全ての従業員に貸与している。DPCの社外への持出しは，禁止されている。

A社は，クラウドサービスTを利用している。クラウドサービスTの機能とA社での利用方法の概要を表2に示す。

表2　クラウドサービスTの機能とA社での利用方法の概要（抜粋）

| サービス名 | IPアドレス | 機能名 | 機能と利用方法の概要 |
|---|---|---|---|
| 権威 DNS サービス | x2.y2.z2.2, x2.y2.z3.4 | ドメイン名登録及び提供機能 | ・インターネット向けのA社ドメイン名の情報を登録し，提供する。 |
| キャッシュ DNS サービス | x2.y2.z2.3 | DNS キャッシュ機能 | ・インターネット上のドメイン名の名前解決を行う。<br>・オープンリゾルバ対策として，クラウドサービス T上のサーバからの名前解決だけを許可する。 |
| メールサービス | x2.y2.z2.17 | メール転送機能 | ・SMTP を使用し，インターネットとの間でメールを転送する。<br>・迷惑メールの踏み台として使われないよう，［ d ］対策として，インターネットから転送されてきたメールのうち，宛先メールアドレスのドメイン名がA社ドメイン名のメールだけを受信する。 |
| | | マルウェア対策機能 | ・送受信時にメールのマルウェアスキャンを行い，マルウェアが検知されたメールを隔離する。 |
| | | Web メール機能 | ・DPC とメールサービスとの間は，HTTP over TLS を使用する。 |
| | | Web メール接続元制限機能 | ・A社のネットワークからの利用だけが可能となるよう，①特定のネットワークからの接続だけを許可している。 |

A社のネットワーク構成を図1に，A社のネットワーク一覧を表3に示す。




注記 1　工場 LAN は，閉じたネットワークである。

注記 2　工場 LAN に接続されている工作機械及び管理サーバの記載は省略している。

注記 3　拠点 LAN，管理部 LAN，設計部 LAN 及び製造部 LAN に接続されている DPC の記載は省略している。

注記 4　内部システム LAN 上のサーバ及び DPC からのインターネットアクセスは，プロキシサーバ経由で行われる。

図 1　A 社のネットワーク構成

表 3　A 社のネットワーク一覧

| ネットワーク名 | ネットワークアドレス |
|---|---|
| DMZ | x1.y1.z1.16/29 |
| 内部システム LAN | 192.168.1.0/24 |
| 管理部 LAN | 192.168.16.0/24 |
| 設計部 LAN | 192.168.19.0/24 |
| 製造部 LAN | 192.168.21.0/24 |
| 工場 LAN | 192.168.32.0/24 |
| 拠点 LAN | 192.168.64.0/24 |

〔A 社の情報システム〕

DMZ 上のサーバには，グローバル IP アドレスを割り当てている。DMZ 上のサーバの概要を表 4 に示す。

表 4　DMZ 上のサーバの概要（抜粋）

| サーバ名 | IP アドレス | 機能名 | 機能と利用方法の概要 |
|---|---|---|---|
| A 社キャッシュ DNS サーバ | x1.y1.z1.17 | DNS キャッシュ機能 | ・インターネット上のドメイン名の名前解決を行う。<br>・オープンリゾルバ対策として［ e ］からの名前解決だけを許可する。 |
| | | 時刻同期機能 | ・国立研究開発法人情報通信研究機構がインターネット上で公開している［ f ］サーバと時刻同期を行う。 |
| プロキシサーバ | x1.y1.z1.18 | URL フィルタリング機能 | ・接続元 IP アドレスごとに，接続できる URL を制限する。 |

内部システム LAN 上のサーバの概要を表 5 に示す。

表 5　内部システム LAN 上のサーバの概要（抜粋）

| サーバ名 | IP アドレス | 機能名 | 機能と利用方法の概要 |
|---|---|---|---|
| DHCP サーバ | 192.168.1.2 | DHCP 機能 | ・IP アドレスを割り当てる DPC の MAC アドレスをあらかじめ登録しておく。<br>・登録済み MAC アドレスの DPC に IP アドレスを割り当てる。 |
| 設計情報管理サーバ | 192.168.1.3 | 設計情報管理機能 | ・利用者は，Web インタフェースを用いて，設計情報ファイルのアップロード，ダウンロード及び検索を行うことができる。<br>・利用者 ID とパスワードで利用者認証を行う。<br>・パスワードは 10 字以上とし，英数字及び記号を使用できる。<br>・設計部のサーバ管理者が，利用者 ID と初期パスワードを登録する。<br>・フォルダごとにアクセス権限を設定できる。現在は，利用者 ID ごとに割り当てられたフォルダ配下のファイルにアクセスできる。 |
| | | アクセス制限機能 | ・接続元の IP アドレスによってアクセスを制限する。アクセスを許可する IP アドレスには，A 社で利用するプライベート IP アドレスを登録する。 |
| 製造情報管理サーバ | 192.168.1.4 | 製造情報管理機能 | （省略） |

A 社では，全ての従業員に個別のメールアドレスを割り当てており，従業員は，メールサービスを用いてメールを送受信している。

従業員のメールアドレス以外に同報用のメールアドレスがあり，このアドレスに届いたメールは，登録された従業員のメールアドレスに同報される。

従業員は，第三者に秘匿したい電子ファイルをメールに添付し，金型加工の発注元との間で送受信する場合には，ZIP 形式で圧縮している。メール添付する際の圧縮ファイルの取扱いについては，次のルールを定めている。

・発注元ごとの打合せで取り決めた，12 字以上の英数字及び記号で構成されるランダムな文字列から成るパスワードから生成した鍵を用いて暗号化する。
・暗号化アルゴリズムは，［ g ］を用いる。［ g ］は，［ h ］が選定した，電子政府における調達のために参照すべき暗号リスト（平成 30 年 3 月 29 日版）でも利用が推奨されている共通鍵暗号である。［ h ］は，暗号技術の適切な実装法や運用法の調査及び検討を行う国内のプロジェクトである 。

設計情報管理サーバの利用者は，設計部員及び製造部員である。利用者 ID は，利用者のメールアドレスである。初期パスワードには，メールアドレスと同じ文字列を登録し，利用者に通知する。利用者は，自身でパスワードを変更することができる。

FW，プロキシサーバ，内部システム LAN 上のサーバ，及び全ての DPC は，A 社キャッシュ DNS サーバとの間で［ f ］を用いて時刻同期を行っている。

DPC の IP アドレスは，DHCP サーバの DHCP 機能及び L3SW の DHCP リレーエージェント機能によって，動的に割り当てられる。

A 社では，DMZ 上及び内部システム LAN 上にあるサーバの名称と IP アドレスの対応を DPC の hosts ファイルに設定している。

DPC，DMZ 上のサーバ及び内部システム LAN 上のサーバは，導入時に，OS，アプリケーションソフトウェア及びマルウェア対策ソフト（以下，これらを併せて A 社標準ソフトという）に脆弱(ぜい)性修正プログラムを適用し，マルウェア対策ソフトはマルウェア定義ファイルを導入時点での最新版に更新している。

導入後は，プロキシサーバ経由で A 社標準ソフトの各ベンダのサイトに毎月末に自動で接続し，それぞれの脆弱性修正プログラムを適用している。

DPC 及びサーバ上のマルウェア対策ソフトは，起動時及び起動後 2 時間おきにプロキシサーバ経由でマルウェア対策ソフトベンダのサイトからマルウェア定義ファ

イルをダウンロードし，更新している。マルウェア対策ソフトでは，ファイルを読み書きするときにマルウェアスキャンする機能（以下，リアルタイムスキャンという）を有効にするとともに，全てのファイルをマルウェアスキャンする機能（以下，フルスキャンという）を，毎週火曜日 12 時に実行している。フルスキャン実行時，CPU の負荷を減らすために，圧縮ファイルは対象外としている。

〔情報漏えいの発生〕

6月7日，金型加工業者B社のL氏から，設計情報管理サーバの管理者である設計部のJさんに，A社の情報が漏えいしているおそれがあると連絡があった。Jさんは，設計部長及び管理部のE部長に報告した。Jさんの報告内容を，次に示す。

・L氏が，検索サイトで金型技術情報を検索したところ，A社とB社が共同で展示会に出品する金型（以下，共同出品金型という）の設計情報ファイル（以下，ファイルSという）と同じ名称のファイルが，ある Web ページに掲載されていることを発見した。

・ファイルSは，DVD-R に保存し，6月1日にJさんからL氏に手渡している。（以下，当該 DVD-R を DVDS という）

・L氏が，掲載されていたWebページを確認したところ，ファイルSと同じ名称をもつファイルの更新日付は6月4日と表示されていた。

・L氏は，掲載されていたファイルがファイルSと同一であるかどうかの確認及びB社における設計情報ファイルの管理状況の調査を，B社のセキュリティ担当者に依頼した。

・B社のセキュリティ担当者は，同一ファイルであることを確認するためファイルの［ i ］を調べた。その結果，DVDS 中のファイルSの［ i ］と同じであったので，同一ファイルであることが確認された。

・B社では，全ての設計情報ファイルを，設計室の閉じたネットワークにだけ接続された PC 及びサーバで利用しており，インターネットに漏えいする可能性は低い。

・B 社では，DVD-R などの外部記録媒体の持込み，持出し及び使用を管理している。管理記録によれば，DVDS に関する記録は，設計室内への持込み及び設計室内での使用だけであった。

・L氏は，A社から漏えいした可能性があるとして，A社に調査を求めてきた。

E部長は事態を重くみて，ファイルSの漏えいについての調査，及び必要であればその対処，並びにA社全体としての情報セキュリティ対策強化案の検討をシステム係のFさんに指示した。さらに，A社の情報システムの導入及び運用を支援しているシステム会社と一緒に調査することにし，システム会社のG氏が協力することになった。

Fさん及びG氏は，まず，情報漏えいの調査及び一時的な対処を実施し，その後に，A社全体としての情報セキュリティ対策強化案を検討することにした。

〔情報漏えいの調査及び一時的な対処〕

Fさんは G氏の協力を受けて，FW，DMZ上のサーバ及び内部システムLAN上のサーバの調査を開始した。Fさんと G氏は，設計情報管理サーバからファイルSが取り出された可能性が高いと考え，設計情報管理サーバのアクセスログを調査した。その結果，ファイルSを作成するためにJさんが設計情報管理サーバに登録した利用者ID kyoudou@a-sha.co.jp（以下，ID-Kという）による不審なアクセスが6月1日に発生していたことが判明した。設計情報管理サーバの6月1日のアクセスログのうち，利用者IDがID-Kのものを表6に示す。

表6　設計情報管理サーバのアクセスログ

| 項番 | 接続元IPアドレス | 日時 | 利用者ID | ログ項目 |
|---|---|---|---|---|
| 1 | 192.168.19.8 | 6/1 11:40:30 | kyoudou@a-sha.co.jp | ログイン成功 |
| 2 | 192.168.19.8 | 6/1 11:41:40 | kyoudou@a-sha.co.jp | kyoudousyuppin.zipをアップロード |
| 3 | 192.168.19.8 | 6/1 11:42:50 | kyoudou@a-sha.co.jp | ログアウト |
| 4 | 192.168.64.3 | 6/1 16:50:00 | kyoudou@a-sha.co.jp | ログイン失敗 |
| 5 | 192.168.64.3 | 6/1 16:50:05 | kyoudou@a-sha.co.jp | ログイン失敗 |
| 6 | 192.168.64.3 | 6/1 16:50:09 | kyoudou@a-sha.co.jp | ログイン失敗 |
| 7 | 192.168.64.3 | 6/1 16:50:13 | kyoudou@a-sha.co.jp | ログイン成功 |
| 8 | 192.168.64.3 | 6/1 16:50:20 | kyoudou@a-sha.co.jp | ファイルの一覧表示 |
| 9 | 192.168.64.3 | 6/1 16:51:30 | kyoudou@a-sha.co.jp | kyoudousyuppin.zipをダウンロード |

Fさんが，ID-Kについて Jさんに確認したところ，ID-Kは，共同出品金型の設計に携わっているJさん及び2名の設計部員（以下，3名を併せて，共同出品担当メンバという）が利用していた。

さらに，表6の接続元IPアドレスに記録されたDPCを特定するために，DHCPサーバのログを調査することにした。DHCPサーバの6月1日のIPアドレス割当ログのうち，割り当てたIPアドレスが192.168.19.8又は192.168.64.3であるものを表7に示す。

表7　DHCPサーバのIPアドレス割当ログ

| 項番 | 対象DPC | 日時 | ログ項目 |
|---|---|---|---|
| 1 | Jさんの DPC | 6/1 08:30:00 | IPアドレス 192.168.19.8 を割り当てた。 |
| 2 | 営業係Kさんの DPC | 6/1 11:30:00 | IPアドレス 192.168.64.3 を割り当てた。 |
| 3 | Jさんの DPC | 6/1 11:50:30 | IPアドレス 192.168.19.8 を解放した。 |
| 4 | 営業係Kさんの DPC | 6/1 17:30:20 | IPアドレス 192.168.64.3 を解放した。 |

Fさんは，②サーバのログの調査だけでは操作者を特定するには不十分なので，当事者へのヒアリング及びDPCの動作ログの調査が必要であると判断した。ヒアリング及び調査の結果を図2に示す。

(1) 共同出品担当メンバへのヒアリング及び調査の結果
・6月1日の行動
08:30 3人とも，出勤し，DPCを起動した。
08:35 共同出品金型の設計をJさんが始めた。
11:40 設計を終え，設計情報管理サーバにID-Kでログインし，ファイルSをアップロードした。アップロード後，ログアウトした。
11:45 ファイルSをDVDSに保存した。
11:50 3人とも，DPCをシャットダウンした。
13:00 B社との打合せ及びDVDSの手渡しのために，3人でB社に向かった。
13:30 3人とも，B社に到着し，L氏にDVDSを手渡し，打合せを始めた。
17:30 3人とも，打合せを終え，B社から直接帰宅した。
・6月4日の行動
3人とも，社外の研修に終日参加していた。
(2) Kさんへのヒアリング及び調査の結果
・6月1日の行動
11:30 外出先から戻り，DPCを起動した。
11:35 取引先向け資料の作成を始めた。
16:30 取引先向け資料に関する打合せを上司と始めた。
17:30 上司との打合せを終えて，DPCをシャットダウンした。
18:00 帰宅のため会社を出た。
・6月4日の行動
08:30 出勤し，DPCを起動した。
08:35 提案資料の作成を始めた。
17:25 提案資料を保存し，DPCをシャットダウンした。
17:30 帰宅のため会社を出た。
・設計情報管理サーバへのアクセス
Kさんには設計情報管理サーバの利用者IDの割当てはなく，アクセスできない。

図2 ヒアリング及び調査の結果

ヒアリング及び調査の結果，Fさんは，③表6の項番4から項番9のアクセスは，共同出品担当メンバの操作ではなく，Kさんの DPC がマルウェアに感染し，マルウェアによってファイルSが漏えいした可能性があると判断した。Fさんは，E部長に報告するとともに，調査のために，KさんのDPCを回収し，予備のDPCをKさんに貸与した。

さらに，ID-Kは不正ログインに使用されたので，Fさんは，Jさんに，④ID-Kへの一時的な対処を依頼した。

Fさんは，G氏のアドバイスを受けながら，JさんとKさんへの追加のヒアリング及び調査を行った。それらの結果を図3に示す。

(1) Jさんへの追加ヒアリング結果
・4月に，共同出品金型用の同報用メールアドレス kyoudou@a-sha.co.jp を登録してもらった。同報先には，共同出品担当メンバを登録してもらった。
・kyoudou@a-sha.co.jp は，共同出品関係者とのメールのやり取りにおいて Cc の宛先としている。社外のメーリングリスト宛てにメールを送信した時に，kyoudou@a-sha.co.jp を Cc に指定したこともある。
・Jさんがファイル S を作成するために，4月に ID-K を設計情報管理サーバに登録した。
・ID-K のパスワードは，初期パスワードのまま変更していなかった。
(2) Kさんへの追加ヒアリング結果
・5月21日9時，DPC からメールサービスにアクセスした。
・送信者が運送会社のメールアドレスになっており，かつ，ZIP 形式のファイルが添付されたメールが届いた。
・添付ファイルを DPC にダウンロードし，保存した。
・保存した添付ファイルを展開したところ，PDF ファイルがあり，ファイル名が“送付状”であったので開いた。身に覚えがない内容だったので，PDF ファイルを削除した。
・6月5日9時，上記添付ファイルを誤って再び展開したところ，リアルタイムスキャンによって，PDF ファイルがマルウェア X として検知され，PDF ファイルを削除したとのメッセージが DPC に表示された。直ちに，PC 上の上記添付ファイルを削除した。マルウェアの対処は完了したものと判断した。
・6月5日13時，フルスキャンによって別のファイルがマルウェア Y として検知され，削除された。
(3) マルウェア X に関する情報
・ダウンローダ型のマルウェアであり，攻撃者が用意した C&C（Command and Control）サーバの URL が内部に保持されている。C&C サーバからマルウェア Y をダウンロードし実行する。
・PDF 閲覧ソフトの脆弱性を悪用して PC に感染する。5月16日にリリースされた PDF 閲覧ソフトの脆弱性修正プログラムが適用されていれば，マルウェア Y をダウンロードしない。
(4) マルウェア Y に関する情報
・PC の hosts ファイルを用いて，Web サーバを探索する。
・Web サーバが見つかると，C&C サーバから取得した利用者 ID とパスワードのリストを用いてログインを試みる。ログインが成功すると，クローリングしてファイルを一つずつダウンロードし，攻撃者が用意したサーバにアップロードする。
(5) マルウェア対策ソフトベンダの対応
・5月28日10時，マルウェア X に対応したマルウェア定義ファイルをリリースした。
・6月5日10時，マルウェア Y に対応したマルウェア定義ファイルをリリースした。
(6) フルスキャン実施
・6月8日10時，F さんは，マルウェア対策ソフトで圧縮ファイルをフルスキャンの対象とするように一時的に設定を変更した後，最新のマルウェア定義ファイルに更新し，フルスキャンを行うように全ての従業員に指示した。このフルスキャン実施では，マルウェアは検知されなかった。
(7) 他のサーバの調査
・製造情報管理サーバのログを調査したところ，不審なログインの記録はなかった。

図3　追加のヒアリング及び調査の結果

G氏は，図3の(2)について，マルウェア対策ソフトでマルウェアが検知されたにも

かかわらず，報告がなかったので，A 社としての対策がとれなかったことへの改善が必要であると指摘した。F さんは，図 3 及び G 氏の指摘を踏まえ，（あ）～（え）の作業計画を作成した。

（あ）設計部長に報告するために，情報漏えいの経緯をまとめる。

（い）類似のマルウェア感染を防止する対策を検討する。

（う）設計情報管理サーバへの不正ログイン対策を検討する。

（え）サーバ及び DPC それぞれの，マルウェア対策ソフトの状態と脆弱性修正プログラムの適用状況を集中管理する仕組みを導入する。

F さんは，（あ）～（え）の作業計画を E 部長に報告し，実施についての了承を得た。

（あ）について，F さんは，情報漏えいの経緯をまとめ，E 部長が設計部長に報告した。

（い）について，F さんは，類似のマルウェア感染を防止する対策として，今回の感染の経緯と類似のマルウェアへの注意点を社内に周知した。

さらに，圧縮ファイル中のマルウェアが検知されなかったことについて，F さんは，平常時も圧縮ファイルをフルスキャンの対象とすべきかを G 氏に相談した。G 氏は，平常時の運用では，圧縮ファイルをフルスキャンの対象にしなくても DPC がマルウェアに感染するリスクは変わらないと答え，⑤その理由を F さんに説明した。F さんは，圧縮ファイルをフルスキャンの対象外とするという設定は変えないことにした。

〔設計情報管理サーバへの不正ログイン対策の検討〕

（う）について，F さんは，設計情報管理サーバへの不正なログインの経緯及び設計情報管理サーバの利用状況を踏まえ，⑥設計情報管理サーバへのアクセスを制限する設定変更案及び⑦パスワードに関する運用方法の見直し案を作成し，J さんに提案した。J さんは，F さんの提案どおりに設定の変更及び運用方法の見直しを実施することにした。

さらに，F さんと G 氏は，ID-K のように利用者 ID を共用する限り，パスワードの管理は不十分になると考えた。そこで，利用者 ID の共用は全て禁止し，フォルダへのアクセス権限を利用者 ID ごとに設定する案を作成した。

Fさんは，検討結果をE部長に説明し，了承を得てJさんに実施を依頼した。

〔集中管理の仕組みの導入〕

（え）について，Fさんは，次の機能を備えた集中管理サーバの導入案を作成した。

・マルウェア定義ファイルを配信し，配信状況を管理する機能
・マルウェアの検知を［ j ］する機能
・脆弱性修正プログラムを配信し，配信状況を管理する機能

Fさんは集中管理サーバの導入案を，E部長に説明した。E部長は，役員会で集中管理サーバの導入を提案し，集中管理サーバの導入費用が次年度の設備導入予算に組み込まれることになった。E部長は，一連の対処及び施策を設計部長に報告した。

設問1　表1中の［ a ］～［ c ］に入れる適切な字句をそれぞれ5字以内で答えよ。

設問2　〔A社のネットワーク構成〕について，(1)，(2)に答えよ。

(1)　表2中の［ d ］に入れる適切な字句を10字以内で答えよ。

(2)　表2中の下線①について，接続を許可するネットワークアドレスを答えよ。

設問3　〔A社の情報システム〕について，(1)～(4)に答えよ。

(1)　表4中の［ e ］に入れる適切なIPアドレスを答えよ。

(2)　表4及び本文中の［ f ］に入れる適切なプロトコル名を英字5字以内で答えよ。

(3)　本文中の［ g ］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　AES　　イ　DES　　ウ　HMAC　　エ　MD5　　オ　ZipCrypto

(4)　本文中の［ h ］に入れる適切な字句を英字10字以内で答えよ。

設問4　本文中の［ i ］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　サイズ　　イ　作成者の利用者ID　　ウ　作成日時　　エ　ハッシュ値

設問５　〔情報漏えいの調査及び一時的な対処〕について，(1)～(5)に答えよ。

(1)　本文中の下線②について，不十分な理由を 55 字以内で述べよ。

(2)　本文中の下線③のように判断した根拠を 50 字以内で具体的に述べよ。

(3)　本文中の下線④について，一時的な対処を 15 字以内で答えよ。

(4)　図 3 中の(6)について，フルスキャンを実施した目的は何か。40 字以内で述べよ。

(5)　本文中の下線⑤について，理由を 50 字以内で述べよ。

設問６　〔設計情報管理サーバへの不正ログイン対策の検討〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑥について，設定変更の内容を 50 字以内で具体的に述べよ。

(2)　本文中の下線⑦について，見直し後の運用方法を 40 字以内で具体的に述べよ。

設問７　本文中の［　j　］に入れる適切な字句を 10 字以内で答えよ。

〔 メ モ 用 紙 〕

〔 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。