SC

# 令和元年度　秋期
# 情報処理安全確保支援士試験
# 午後Ⅰ　問題

| 試験時間 | 12:30 ～ 14:00（1時間30分） |
|---|---|

**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3 |
|---|---|
| 選択方法 | 2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。3問とも○印で囲んだ場合は，はじめの2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。

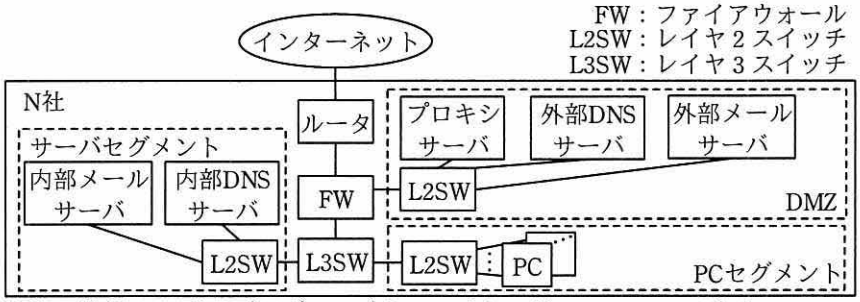
〔問1，問3を選択した場合の例〕

| 選択欄 | |
|---|---|
| 2問選択 | ○問1 |
| | 問2 |
| | ○問3 |

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　電子メールの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。

N社は，従業員数500名の情報サービス事業者である。N社の情報システムの構成を図1に示す。




注記　外部DNSサーバのグローバルIPアドレスは，x1.y1.z1.2である。

図1　N社の情報システムの構成

N社の情報システムは，情報システム部（以下，情シ部という）のQ部長とU主任を含む5名で運用している。

各PC及び各サーバは脆弱(ぜい)性修正プログラムが自動的に適用され，導入済のマルウェア対策ソフトのマルウェア定義ファイルが自動的にアップデートされる設定になっている。外部メールサーバでは，スパムメールフィルタの機能を利用している。

N社では，インターネットドメイン名n-sha.co.jp（以下，N社ドメイン名という）を取得しており，メールアドレスのドメイン名にも使用している。外部DNSサーバは，電子メール（以下，メールという）に関して図2のように設定してある。

```
n-sha.co.jp.        IN MX   10   mail.n-sha.co.jp. 1)
mail.n-sha.co.jp.   IN A    x1.y1.z1.1 2)
```

注記　逆引きの定義は省略しているが，適切に設定されている。
注1)　mail.n-sha.co.jpは，外部メールサーバのホスト名である。
2)　x1.y1.z1.1は，グローバルIPアドレスを示す。

図2　N社の外部DNSサーバのメールに関する設定

送信者メールアドレスには，SMTPの［　a　］コマンドで指定されるエンベロープの送信者メールアドレス（以下，Envelope-FROMという）と，メールデータ内のメールヘッダで指定される送信者メールアドレス（以下，Header-FROMという）

がある。送信したメールが不達になるなど配送エラーとなった場合，Envelope-FROM で指定したメールアドレス宛てに通知メールが届く。N 社では，従業員が PC からメールを送信する場合，Envelope-FROM 及び Header-FROM とも自身のメールアドレスが設定される。

昨今，メールを悪用して企業秘密や金銭をだまし取る攻撃が発生しており，N 社が属する業界団体の会員企業でも，なりすましメールによる攻撃によって被害が発生した。こうした被害を少しでも抑えるため，同団体から送信者メールアドレスが詐称されているかをドメイン単位で確認する技術（以下，送信ドメイン認証技術という）を普及させるよう働きかけがあったことから，N 社でも情シ部が中心になって送信ドメイン認証技術の利用を検討することになった。

〔送信ドメイン認証技術の検討〕

Q 部長と U 主任は，送信ドメイン認証技術の利用について検討を始めた。次は，その際の Q 部長と U 主任の会話である。

Q 部長：当社でも送信ドメイン認証技術を利用すべきだと経営陣に報告したい。まずは，どのような送信ドメイン認証技術を利用するかを検討しよう。

U 主任：送信ドメイン認証技術では，SPF，DKIM，DMARC が標準化されています。当社の外部メールサーバでは，いずれも利用が可能です。

Q 部長は，図 3 のなりすましメールによる攻撃の例を示し，送信ドメイン認証技術が各攻撃の対策となるかどうかをまとめるように U 主任に指示した。

攻撃 1　N 社の取引先のメールアドレスを送信者として設定したメールを，攻撃者のメールサーバから N 社に送信する。
攻撃 2　N 社のメールアドレスを送信者として設定したメールを，攻撃者のメールサーバから N 社の取引先に送信する。

図 3　なりすましメールによる攻撃の例

U 主任は，SPF への対応と各攻撃に対する効果の関係を表 1 にまとめ，SPF が対策となるかどうかを同表を用いて Q 部長に説明した。

表1　SPF への対応状況と各攻撃に対する効果

| 項番 | SPF への対応状況 | | | | 攻撃1に対する効果 | 攻撃2に対する効果 |
|---|---|---|---|---|---|---|
| | 外部 DNS サーバでの設定 1) | 外部メールサーバでの対応 2) | 取引先の DNS サーバでの設定 1) | 取引先のメールサーバでの対応 2) | | |
| 1 | 設定済み | 実施する | 設定済み | 実施する | ○ | ○ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 4 | 設定済み | 実施する | 未設定 | 実施しない | b | c |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 6 | 設定済み | 実施しない | 設定済み | 実施しない | d | e |
| 7 | 設定済み | 実施しない | 未設定 | 実施する | f | g |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 13 | 未設定 | 実施しない | 設定済み | 実施する | h | i |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 16 | 未設定 | 実施しない | 未設定 | 実施しない | × | × |

注記　表中の“○”は送信者メールアドレスが詐称されているかを判断可，“×”は判断不可を示す。
注 1)　SPF に必要な設定を DNS サーバに設定済みかを示す。
2)　メール受信時に，SPF に必要な問合せを実施するかを示す。

次は，その後の Q 部長と U 主任の会話である。

Q 部長：SPF に対応するには，具体的にどのような設定が必要になるのか。

U 主任：DNS サーバでの設定は，当社の外部 DNS サーバに図 4 に示す TXT レコードを登録します。

n-sha.co.jp.　IN TXT　"v=spf1 +ip4:[ j ] -all"

図 4　TXT レコード

メールサーバでの対応は，当社の外部メールサーバの設定を変更します。SPF による検証（以下，SPF 認証という）が失敗したメールは，件名に[NonSPF]などの文字列を付加して，受信者に示すこともできます。

Q 部長：なるほど。SPF の利用に注意点はあるのかな。

U 主任：メール送信側の DNS サーバ，メール受信側のメールサーバの両方が SPF に対応している状態であっても，その間で SPF に対応している別のメールサーバが Envelope-FROM を変えずにメールをそのまま転送する場合は，①メール受信側のメールサーバにおいて，SPF 認証が失敗してしまうという制

約があります。

Q部長：なるほど。それでは，DKIMはどうかな。

U主任：DKIMに対応したメールを送信するためには，まず，準備として公開鍵と秘密鍵のペアを生成し，そのうち公開鍵を当社の外部 DNS サーバに登録し，当社の外部メールサーバの設定を変更します。DKIM利用のシーケンスは，図5及び図6に示すとおりとなります。


図5　DKIM利用のシーケンス

1. DKIM-Signature ヘッダにディジタル署名を付与し，メールを送信する。
2. 受信側メールサーバは，DKIM-Signature ヘッダの d タグに指定されたドメイン名を基に，外部 DNS サーバに公開鍵を要求する。
3. 要求を受けた外部 DNS サーバは，登録されている公開鍵を送信する。
4. ②受信した公開鍵，並びに署名対象としたメール本文及びメールヘッダを基に生成したハッシュ値を用いて，DKIM-Signature ヘッダに付与されているディジタル署名を検証する。

図6　DKIM利用のシーケンスの説明

Q部長：DKIMの方が少し複雑なのだな。

U主任：はい。しかし，DKIMは，メール本文及びメールヘッダを基にディジタル署名を付与するので，転送メールサーバがディジタル署名，及びディジタル署名の基になったメールのデータを変更しなければ，たとえメールが転送された場合でも検証が可能です。SPFとDKIMは併用できます。

Q部長：分かった。両者を導入するのがよいな。それでは，DMARCはどうかな。

U主任：DMARC は，メール受信側での，SPF と DKIM を利用した検証，検証したメールの取扱い，及び集計レポートについてのポリシを送信側が表明する方法です。DMARC のポリシの表明は，DNS サーバに TXT レコードを追加することによって行います。TXT レコードに指定する DMARC の主なタグ

を表2に示します。

表2　DMARC の主なタグ（概要）

| タグ | タグの説明 | 値と説明 |
|---|---|---|
| p | 送信側が指定する受信側でのメールの取扱いに関するポリシ（必須） | none：何もしない。<br>quarantine：検証に失敗したメールは隔離する。<br>reject：検証に失敗したメールは拒否する。 |
| aspf | SPF 認証の調整パラメタ（任意） | r：Header-FROM と Envelope-FROM に用いられているドメイン名の組織ドメインが一致していれば認証に成功<br>s：Header-FROM と Envelope-FROM に用いられている完全修飾ドメイン名が一致していれば認証に成功 |
| adkim | DKIM 認証の調整パラメタ（任意） | r：DKIM-Signature ヘッダの d タグと Header-FROM に用いられているドメイン名の組織ドメインが一致していれば認証に成功<br>s：DKIM-Signature ヘッダの d タグと Header-FROM に用いられている完全修飾ドメイン名が一致していれば認証に成功 |
| rua | DMARC の集計レポートの送信先（任意） | URI 形式で指定する。 |

注記　完全修飾ドメイン名が“a-sub.n-sha.co.jp”の場合，組織ドメインは“n-sha.co.jp”となる。

これらの検討結果を経営陣に報告したところ，N 社は送信ドメイン認証技術として SPF，DKIM，DMARC を全て利用することになり，情シ部が導入作業に着手した。

〔ニュースレターの配信〕

送信ドメイン認証技術の導入作業着手から 1 週間後，N 社営業部で取引先宛てにニュースレターを配信する計画が持ち上がった。ニュースレターの配信には，X 社のクラウド型メール配信サービス（以下，X 配信サービスという）を利用する。ニュースレターは，X 社のメールサーバから配信され，配送エラーの通知メールは，X 社のメールサーバに届くようにする。Header-FROM には，N 社ドメイン名のメールアドレス（例：letter@n-sha.co.jp）を設定する。Envelope-FROM には，N 社のサブドメイン名 a-sub.n-sha.co.jp のメールアドレス（例：letter@a-sub.n-sha.co.jp）を設定する。X 社のメールサーバのホスト名は，mail.x-sha.co.jp であり，グローバル IP アドレスは，x2.y2.z2.1 である。X 社の DNS サーバのグローバル IP アドレスは，x2.y2.z2.2 である。X 配信サービスでは，SPF，DKIM，DMARC のいずれも利用が可能である。

N 社は，ニュースレターの配信についても，3 種類の送信ドメイン認証技術を利用することにした。具体的には，N 社の外部 DNS サーバに図 7 のレコードを追加する。

a-sub.n-sha.co.jp. IN MX 10 [ k ]
a-sub.n-sha.co.jp. IN TXT "v=spf1 +ip4:[ l ] -all"

注記 1　逆引きの定義は省略しているが，適切に設定されている。
注記 2　DKIM，DMARC のレコードは省略しているが，適切に設定されている。

図 7　追加するレコード

ここで，受信側で検証に失敗したメールは隔離するポリシとするため，DMARC の p タグと aspf タグの設定は表 3 のとおりとする。

表 3　DMARC のタグ設定

| タグ | 値 |
|---|---|
| p | [ m ] |
| aspf | [ n ] |

注記　ほかのタグは省略しているが，適切に設定されている。

その後，N 社と主要な取引先での送信ドメイン認証技術の導入が完了した。

設問 1　本文中の [ a ] に入れる適切な字句を答えよ。

設問 2　〔送信ドメイン認証技術の検討〕について，(1)～(4)に答えよ。

(1)　表 1 中の [ b ] ～ [ i ] に入れる適切な内容を，“○”又は“×”のいずれかで答えよ。

(2)　図 4 中の [ j ] に入れる適切な字句を答えよ。

(3)　本文中の下線①について，SPF 認証が失敗する理由を，SPF 認証の仕組みを踏まえて，50 字以内で具体的に述べよ。

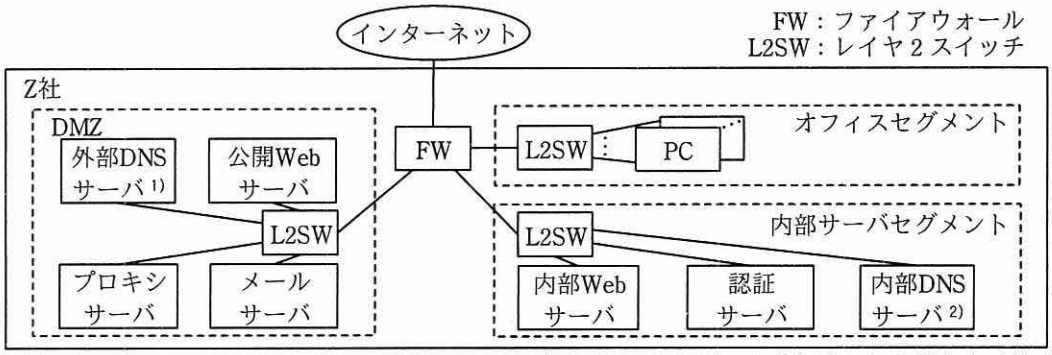
(4)　図 6 中の下線②の検証によってメールの送信元の正当性以外に確認できる事項を，20 字以内で述べよ。

設問 3　図 7 中の [ k ]，[ l ]，表 3 中の [ m ]，[ n ] に入れる適切な字句を答えよ。

設問 4　攻撃者がどのように N 社の取引先になりすまして N 社にメールを送信すると，N 社が SPF，DKIM 及び DMARC では防ぐことができなくなるのか。その方法を 50 字以内で具体的に述べよ。

問2　セキュリティインシデント対応におけるサイバーセキュリティ情報の活用に関する次の記述を読んで，設問1，2に答えよ。

Z社は，従業員数150名の金融事業会社である。事業規模は小さいが，多くの個人情報を扱っている。サイバーセキュリティ情報を共有し，サイバー攻撃への防御力を高める目的で活動する組織（ISAC：Information Sharing and Analysis Center）に最近加盟した。Z社には5名で構成されるIT部門があり，ITシステムの運用や管理を行っている。Z社のネットワーク構成を図1に示す。




注記　インターネットからZ社の公開Webサーバやメールサーバの名前解決を行う外部向け権威DNSサーバの役割は，ドメイン登録サービスが提供するDNSサービスが担っている。ドメイン登録サービスが提供するDNSサービスの記載は省略している。

注1)　外部DNSサーバは，メールサーバ又はプロキシサーバからDNSクエリを受け，インターネット上の権威DNSサーバと通信し，名前解決を行うフルサービスリゾルバとして機能する。

2)　内部DNSサーバは，PCが内部Webサーバ及び公開Webサーバにアクセスするときの名前解決を行う権威DNSサーバとして機能する。

図1　Z社のネットワーク構成

FWのフィルタリングルールを表1に，図1中に記載された機器の詳細を表2に示す。

表1　FWのフィルタリングルール

| 項番 | 送信元 | 宛先 | サービス | 動作 |
|---|---|---|---|---|
| 1 | オフィスセグメント | DMZ | HTTP，HTTPS，DNS，POP，SMTP | 許可 |
| 2 | オフィスセグメント | 内部サーバセグメント | HTTP，HTTPS，認証サービス，DNS | 許可 |
| 3 | 全て | インターネット | DNS | 許可 |
| 4 | インターネット | DMZ | HTTP，HTTPS，SMTP | 許可 |
| 5 | DMZ | インターネット | HTTP，HTTPS，SMTP | 許可 |
| 6 | 内部サーバセグメント | オフィスセグメント | 認証サービス | 許可 |
| 7 | 全て | 全て | 全て | 拒否 |

注記　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。

表2　図1中に記載された機器の詳細（抜粋）

| 記号 | 機器 | 詳細 | 取得ログ |
|---|---|---|---|
| (a) | PC | 1) 次の汎用ソフトウェアを導入している。<br>・メールソフト：社内外との電子メール（以下，メールという）の送受信に利用する。<br>・文書作成ソフト：文書ファイルの閲覧・作成・編集に利用する。<br>・表計算ソフト：表計算ファイルの閲覧・作成・編集に利用する。<br>・Web ブラウザ：Web アクセスに利用する。インターネットへの通信は全てプロキシサーバを経由するように設定され，設定は管理者だけが変更可能である。<br>2) 次のセキュリティ対策ソフトウェアを導入している。設定は管理者だけが変更可能である。<br>・マルウェア対策ソフト：メール及びファイルのリアルタイムスキャンを行う。また，1 日 2 回マルウェア定義ファイルを更新し，週 1 回フルスキャンを実行する。<br>・EDR（Endpoint Detection and Response）：PC 上のプロセスの起動・終了，ネットワーク通信，ファイル操作，実行ファイルのパスなどを記録し，検索できる。 | ・マルウェア対策ソフトによるリアルタイム検知情報とフルスキャン結果<br>・EDR による記録結果 |
| (b) | FW | ステートフルパケットインスペクション型の FW である。 | ・動作ログ |
| (c) | プロキシサーバ | PC からインターネット上の Web サイトへの HTTP 及び HTTPS 通信を中継する。PC からインターネットにアクセスするためには利用者 ID とパスワードによる BASIC 認証（以下，PC からインターネットにアクセスする際にプロキシサーバで実施される BASIC 認証をプロキシ認証という）を必須としている。プロキシ認証に必要なアカウント情報（以下，プロキシ認証情報という）は，プロキシサーバ内に保存されている。 | ・アクセスログ<br>・認証結果 |
| (d) | 外部 DNS サーバ | （省略） | なし |
| (e) | メールサーバ | 社内外とのメールの送受信に利用する。プロトコルは POP と SMTP を使用する。 | ・メールの送受信履歴 |
| (f) | 認証サーバ | 従業員が PC にログインする際に PC に入力された利用者 ID とパスワードで従業員を認証する。認証成功後に PC が利用できる。 | ・認証結果 |
| (g) | 内部 DNS サーバ | （省略） | なし |

〔ISAC からの情報提供と対応〕

20XX 年 11 月 19 日，Z 社は ISAC から，サイバーセキュリティ情報の提供を受けた。当該情報の概要を図 2 に示す。

A) 20XX 年 11 月 17 日，金融事業会社 Q 社において従業員が社内で利用している利用者 ID とパスワードが窃取され，某掲示板に掲載されるという攻撃が発見された。
B) 利用者 ID とパスワードの窃取には，マルウェア Y の亜種の一つであるマルウェア P が使用された。
C) 攻撃グループ X は，マルウェア Y とその亜種を使用することで知られており，今回の攻撃も攻撃グループ X による可能性が高い。
D) 攻撃グループ X は，当該掲示板において，マルウェアを利用して Z 社の利用者 ID とパスワードを窃取する計画を立てていた。しかし，会話は途中までしか確認されておらず，実際に計画を実行したかは不明である。
E) 攻撃グループ X の過去の活動について，次のことが確認されている。
（あ）攻撃グループ X は，メールでマルウェアを配信する。同じマルウェアを攻撃対象ごとにファイル名だけ変更して送付することもあれば，挙動は同じだが攻撃対象ごとにコードの一部とファイル名を変更したマルウェアの亜種を送付することもある。
（い）マルウェアは，侵入後，窃取する重要情報を探すため，内部ネットワークの探索を行う。窃取する情報を持ち出す際には，まず，窃取する情報を暗号化し，一定のサイズに分割する。その後，C&C（Command and Control）通信を使用して持ち出す。
（う）C&C 通信には，HTTP 又は DNS プロトコルを使用する。HTTP の場合，Web ブラウザに設定されたプロキシサーバの IP アドレスを確認し，プロキシサーバ経由で C&C サーバと通信する。DNS プロトコルの場合，パブリック DNS サービス L を経由して通信する。攻撃対象となる組織が管理する DNS サーバを経由して C&C サーバと通信する事例は報告されていない。

注記　パブリック DNS サービスとは，インターネット上に公開され，誰でも自由に利用可能なフルサービスリゾルバ型の DNS サービスのことである。

図 2　提供されたサイバーセキュリティ情報の概要

攻撃グループ X が Z 社を攻撃する計画を立てていたことを重く見た Z 社は，実際に攻撃を受けたかの調査を開始した。IT 部門の K 部長がプロジェクトリーダとなり，部下の H さんが調査した。図 3 に H さんの調査結果を示す。

A) 最新のマルウェア定義ファイルを用いてZ社の全PCをスキャンしたが，マルウェアは検知されなかった。

B) ISACから提供されたマルウェアPの情報を用いてEDRで調査したところ，1台のPC（以下，PC-Vという）がマルウェアPに感染しているのを発見した。更に調査したところ，次のことが判明した。

（あ）マルウェアPはAmX3PxvR7.exeというファイル名で，PC-Vのローカルストレージのフォルダ N に配置されていた。

（い）20XX年11月18日 11:09，PC-Vを利用している従業員が，表計算ファイルを装ったメールの添付ファイルをクリックしたことで，PC-VがマルウェアPに感染した。

（う）マルウェアPは，汎用検索サービスA及びグローバルIPアドレスMへのHTTPによる通信を試みたが，①当該通信はZ社のネットワーク環境によって遮断されていたことがプロキシサーバのログに記録されていた。

C) 追加調査から，グローバルIPアドレスMは，攻撃グループXのC&Cサーバに割り当てられたIPアドレスだと判明した。

D) Z社が導入しているEDRでは，DNSプロトコルによる通信を記録しない設定となっていたが，パブリックDNSサービスLに対してDNSプロトコルによる通信が発生すれば，［ a ］のログに記録される。当該ログを調査したところ，該当する通信がなかったことを確認した。

E) 全PCを対象にグローバルIPアドレスMとの通信の有無について，EDRを使って調査したところ，あるPC（以下，PC-Tという）のローカルストレージのフォルダ N に bV6fZq3hi.exeというファイルが配置され，グローバルIPアドレスMとの通信を試みたことを示すログを発見した。更に調査したところ，次のことが判明した。

（あ）bV6fZq3hi.exeについてセキュリティベンダの協力を仰いで調査した結果，マルウェアYの亜種の一つであるマルウェアRであった。

（い）20XX年11月18日 16:15，PC-TはPC-Vと同じ方法で感染した。

（う）マルウェアRは，汎用検索サービスA及びグローバルIPアドレスMへのHTTPによる通信を試みたが，マルウェアPの場合と同様，遮断されていた。

F) ISACから提供された情報を基に，②情報持ち出し成功時に残る痕跡を調査したが，該当する痕跡は確認できなかった。

A)～F)の調査によって，攻撃は受けたが，情報持ち出しは成功していないと判断した。

図3 Hさんの調査結果

K部長は，情報持ち出しは成功していないと判断できたことは不幸中の幸いだったとして，調査は一旦完了とした。③調査で判明した情報はISACに提供した。

〔対策の検討〕

K部長は，様々なC&C通信の手法が今後も使われるであろうと想定し，多層防御の考えに基づいて，C&C通信全般及び各手法への対策案を検討するようHさんに指示した。Hさんが検討したC&C通信全般への対策案を図4に，C&C通信の各手法への対策案を表3に示す。

| |
|---|
| ディジタル署名が付与されていない実行ファイルからの通信を EDR で遮断する。Z 社の業務で利用しているソフトウェアの実行ファイル（以下，正規実行ファイルという）には，ソフトウェア開発会社がディジタル署名を付与するか，自社で付与することができる。④ディジタル署名を検証すれば，正規実行ファイルか否かを判定できる。 |

図 4　C&C 通信全般への対策案（抜粋）

表 3　C&C 通信の各手法への対策案（抜粋）

| 項番 | C&C 通信の手法 | 対策案 |
|---|---|---|
| 1 | マルウェアが⑤プロキシ認証情報を窃取して，プロキシ認証を突破し，C&C 通信を行う。 | （省略） |
| 2 | マルウェアがパブリック DNS サービスを利用して，C&C 通信を行う。 | ⑥FW のフィルタリングルールを変更することで，C&C 通信を遮断する。 |
| 3 | 攻撃者は，あらかじめ攻撃用ドメインを取得し，［ b ］を C&C サーバとして，インターネット上に用意しておく。マルウェアが，［ c ］に攻撃用ドメインについての［ d ］を送信すると，［ c ］が C&C サーバに非［ d ］を送信する。こうして，マルウェアは C&C 通信を行う。<br>大量の情報を持ち出す場合，次の特徴が現れる。<br>・長いホスト名をもつ DNS クエリの発生<br>・［ e ］ | （省略） |

対策案は社内で承認され，対策が導入された。

設問 1　〔ISAC からの情報提供と対応〕について，(1)～(4)に答えよ。

(1)　図 3 中の下線①について，通信が遮断された理由を 20 字以内で述べよ。ここで，図 1 で示した Z 社内の機器及び攻撃グループ X の C&C サーバは正常に稼働していたものとする。

(2)　図 3 中の［ a ］に入れる適切な機器を表 2 中の(a)～(g)から一つ選び，記号で答えよ。

(3)　図 3 中の下線②について，情報持ち出しが成功した可能性が高いと Z 社が判断可能な痕跡は何か。該当する痕跡を二つ挙げ，それぞれ 30 字以内で述べよ。

(4)　本文中の下線③について，ISAC に伝えるべき情報のうち，他社が EDR などセキュリティ対策ソフトウェア又はセキュリティ機器を用いて感染端末を検出する際に有効であり，共有すべき情報を解答群の中から二つ選び，記号で答えよ。

解答群

ア　PC-V と PC-T がマルウェアに感染した日時情報

イ　マルウェア P とマルウェア R が HTTP による通信を試みたグローバル IP アドレス M

ウ　マルウェア P とマルウェア R が配置されていたフォルダ N のパス名

エ　マルウェア P に感染した PC-V のプライベート IP アドレス

オ　マルウェア P のファイル名

カ　マルウェア R に感染した PC-T のプライベート IP アドレス

キ　マルウェア R のファイル名

設問2　〔対策の検討〕について，(1)～(5)に答えよ。

(1)　図 4 中の下線④について，ソフトウェアのディジタル署名の検証に利用する証明書を解答群の中から選び，記号で答えよ。

解答群

ア　S/MIME 証明書　　イ　TLS クライアント証明書

ウ　TLS サーバ証明書　　エ　コードサイニング証明書

(2)　表 3 中の下線⑤について，プロキシ認証情報の窃取に使用できない攻撃手法を解答群の中から選び，記号で答えよ。

解答群

ア　Web ブラウザのオートコンプリート情報の窃取

イ　キーロガーによる攻撃

ウ　ゴールデンチケットの窃取

エ　総当たり攻撃

オ　偽の BASIC 認証入力フォームの表示とそのフォームへの利用者の誘導

カ　ネットワーク盗聴

(3)　表 3 中の下線⑥について，表 1 のフィルタリングルールを一つ変更することによって対応した。変更すべきフィルタリングルールを項番で答えよ。また，変更後のフィルタリングルールについて，送信元，宛先，サービス，動作を答えよ。

(4)　表 3 中の［ b ］～［ d ］に入れる適切な字句をそれぞれ 10 字以内で答えよ。

(5)　表 3 中の［ e ］に入れる適切な特徴を 30 字以内で述べよ。

問３　標的型攻撃への対応に関する次の記述を読んで，設問1～3に答えよ。

J社は，ビッグデータ解析を専門とする，従業員数150名の調査会社である。従業員は，情報収集のための Web アクセス，並びに営業活動及び情報交換のための社外との電子メール送受信にインターネットを利用している。J社では，情報セキュリティポリシを整備して運用している。

J社では，20XX年3月に標的型攻撃を受け，PCがマルウェアに感染して業務サーバ上の秘密情報を外部に送信してしまった。情報システム部（以下，情シ部という）が感染状況を調査し，感染が確実な PC だけでなく，疑わしい PC も合わせて 40 台の PC を初期化した。調査を始めてから初期化を完了するまでに 48 時間掛かり，その間，業務は停止せざるを得なかった。

〔標的型攻撃対策〕

J社は，事態が一段落したところで，情報セキュリティコンサルティング会社の K 社に，標的型攻撃への対策についてのアドバイスを求めた。K社の担当コンサルタントである情報処理安全確保支援士（登録セキスペ）の N 氏は，標的型攻撃への対応事例を示した上で，感染予防だけでなく，感染拡大防止や情報漏えい防止の対策も取り入れるべきであり，具体的には，マルウェアが，外部の C&C（Command and Control）サーバと通信を開始しようとする段階や，ほかの機器に感染を拡大しようとする段階で検知し対処できれば，情報漏えいの被害を軽減できるとアドバイスした。そこでJ社は，IT サービス会社の P 社が提供する監視サービス（以下，P サービスという）及びマルウェア対策ソフトベンダ R 社が提供するマルウェア対策製品（以下，R システムという）の導入，並びにインシデント対応手順など関係する規則類の改定を決めた。作業は，情シ部の E 部長の指示によって，G さんら 3 名が担当した。

P サービス及び R システムの導入を終えた 20XX 年 9 月時点の，J社情報システムの概要を図1に，J社情報システムの構成要素を表1に示す。また，改定後のインシデント対応手順を図2に示す。

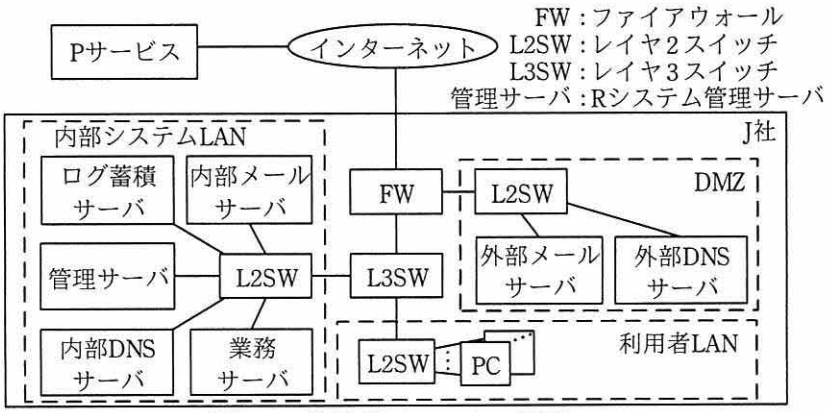



図1　J社情報システムの概要

表1　J社情報システムの構成要素（抜粋）

| 構成要素 | 概要 |
|---|---|
| FW | ・ステートフルパケットインスペクション型である。<br>・フィルタリングルールをもち，送信元 IP アドレス，宛先 IP アドレス，ポートによって不要な通信を拒否する。<br>・日時，FW の動作，送信元 IP アドレス，宛先 IP アドレス，ポート，データサイズを，FW のログとして取得し，P サービス及びログ蓄積サーバに syslog で送信する。<br>・J社と P サービスの間を，インターネット VPN で接続する。 |
| 業務サーバ及び PC | V 社製のマルウェア対策ソフトを導入しており，次のように設定している。<br>・マルウェア定義ファイルを，起動時及び起動後 1 時間ごとに V 社の Web サーバからダウンロードし，更新する。<br>・ファイルの読み書き時にリアルタイムスキャンを行う。<br>・毎週，月曜日の昼の 12 時にフルスキャンを開始する。<br>・マルウェア定義ファイルのダウンロード及び更新，並びにフルスキャンは，いつでも手動で実行できる。 |
| R システム | ・管理サーバ及びエージェントプログラムによって構成される。<br>・エージェントプログラムは，PC 及び業務サーバに導入している。全てのプロセスの生成から終了までの動作，実行したプログラムのハッシュ値並びに通信の宛先の IP アドレス及びポートを，ログ（以下，R システムで取得するログを R ログという）として取得し，ログ蓄積サーバに syslog で送信する。<br>・J 社が社内外からマルウェアのハッシュ値を入手し，管理サーバに登録すると，エージェントプログラムは，そのマルウェアの実行を禁止する。<br>・管理サーバには，ログ蓄積サーバに保存された R ログを検索する機能があり，情シ部員は，R ログをマルウェアのハッシュ値で検索することによって，そのマルウェアが実行された痕跡があるかどうか調査することができる。 |

表1　J社情報システムの構成要素（抜粋）（続き）

| 構成要素 | 概要 |
|---|---|
| ログ蓄積サーバ | ・syslogで送信された，FWのログ及びRログを蓄積して保存する。 |
| Pサービス | ・Pサービスでは，受信したJ社のFWのログを分析する。ただし，FWのログは蓄積しない。過去に遡っての分析は行わない。<br>・ログの分析によって C&C サーバへの通信を検知すると，情シ部員に電子メール及び電話で通知する。<br>・通知する内容は，C&C サーバへの接続日時，送信元の IP アドレス，宛先の C&C サーバの IP アドレス，ポート及びデータサイズの5項目である。 |

情シ部員が実施する手順
(1) P サービスからの通知を基に，C&C サーバと通信した PC（以下，不審 PC という）を特定する。
(2) 不審 PC の電源が入っていれば，電源を入れたままにしておく。
(3) 不審 PC に接続している LAN ケーブルを抜き，利用者 LAN から切り離す。
(4) P サービスから通知を受けた通信の宛先の C&C サーバの IP アドレスについては，その IP アドレスへの通信を拒否するフィルタリングルールを FW に登録する。
(5) P サービスから通知を受けたデータサイズを基に，情報漏えいのおそれがあるかどうかを判断する。
(6) ログ蓄積サーバにある R ログを調査し，マルウェアを特定する。
(7) マルウェアが特定できた場合は，そのハッシュ値を管理サーバに登録し，そのマルウェアの実行を禁止する。
(8) 不審 PC からの情報漏えいの可能性が高いと判断した場合は，外部の専門業者に不審 PC のメモリやストレージの調査及び分析を依頼する。
(9) (1)～(8)が終了したら，不審 PC を必ず初期化する。その後，必要なアプリケーションソフトウェアをインストールして従業員に再配付する。

図2　改定後のインシデント対応手順（抜粋）

〔セキュリティインシデントの検知と対応〕

P サービスと R システムを導入して数週間が経過した 20XX 年 10 月 8 日，C&C サーバへの通信を検知したという通知を P サービスから受け，G さんは図 2 の手順に従って対応した。G さんによるインシデント対応の記録を表 2 に示す。

表2　Gさんによるインシデント対応の記録（抜粋）

| 時刻 | 対応内容 |
|---|---|
| 13:27 | Pサービスから，J社内のIPアドレスからC&Cサーバへの通信を検知したという通知を受けた。通知内容は次のとおりであった。<br>C&Cサーバへの接続日時　20XX年10月8日 13:17:15<br>送信元のIPアドレス　192.168.1.20<br>宛先のC&CサーバのIPアドレス　w1.x1.y1.z1 [1)]<br>ポート　80/tcp<br>データサイズ　200バイト |
| 13:43 | IPアドレス管理台帳で192.168.1.20を調べると，営業部の従業員Lさんの PC（以下，L-PCという）であった。 |
| 13:49 | Lさんに電話を掛け，L-PCの電源を入れたまま，L-PCからLANケーブルを抜くように指示した。 |
| 14:03 | 宛先がw1.x1.y1.z1の通信を拒否するフィルタリングルールをFWに登録した。 |
| 14:28 | FWのログを確認したところ，Pサービスからの通知のとおり，C&Cサーバに送信しているデータサイズは200バイトであった。 |
| 14:42 | 13:17:15前後のRログを確認して，C&Cサーバに接続したプログラムをマルウェアMとして特定した。同時にL-PC上で，表3のコマンドがマルウェアMによって，実行されていたことが判明した。 |
| 14:58 | マルウェアMのハッシュ値を管理サーバに登録した。 |

注 [1)]　w1.x1.y1.z1はグローバルIPアドレスである。

表3　L-PC上で実行されていたコマンド（抜粋）

| コマンド | 想定される攻撃フェーズ | 想定される攻撃者の目的 |
|---|---|---|
| ipconfig /all | 初期調査 | a |
| systeminfo | | b |
| tasklist | | c |
| dir /a | 探索活動 | 秘密情報を含むファイルやフォルダを発見するために一覧を取得する。 |
| net view | | d |

Gさんは，ここまでの対応を報告書にまとめて，E部長に提出した。

〔インシデント対応手順の改善〕

報告書を読んだ E 部長は，他社での標的型攻撃への対応事例と比較すると，対応が不十分であると考えた。次は，E 部長と G さんの会話である。

E 部長：ほかにもマルウェア M に感染した PC 又はサーバがある場合を想定する必要があるのではないか。

G さん：13:27 以降，P サービスから新たな通知は来ていません。感染したのは，L-PC だけと考えてよいのではないでしょうか。

E 部長：13:17:15 より前の，ログ蓄積サーバ中の FW のログに［　e　］が含まれているかどうかを確認する必要がある。

G さん：分かりました。早速確認します。

E 部長：ただし，①PC 又はサーバの状態によっては，FW のログを使った確認ではマルウェア M に感染していることを検知できないことがあるので，②R ログを使った確認もする必要がある。

G さん：分かりました。

G さんは，ログを確認し，感染した PC 又はサーバは，ほかに発見されなかったという結果を E 部長に報告した。E 部長は，マルウェアに感染した PC 又はサーバを特定するためのログの調査手順を，インシデント対応手順に追加するよう G さんに指示した。これによって，J 社ではインシデント対応手順を更に改善することができた。

設問1　〔標的型攻撃対策〕について，(1)，(2)に答えよ。

(1)　図2中の(2)のようにする目的を，25字以内で述べよ。

(2)　図2中の(3)について，不審PCを利用者LANから切り離さない場合，マルウェアがどのような活動をすると想定されるか。想定される活動のうち，J社にとって望ましくないものを二つ挙げ，それぞれ20字以内で述べよ。

設問2　表3中の［　a　］～［　d　］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。

解答群

ア　L-PCからその時点で接続可能な端末の一覧を取得する。

イ　L-PC内で悪用できる脆弱(ぜい)性を確認するために，OSのバージョンや脆弱性修正プログラムの適用状況を確認する。

ウ　L-PCのIPアドレス，MACアドレスなどネットワークアダプタの詳細な情報を取得する。

エ　L-PCの秘密情報を含んだファイルを暗号化する。

オ　実行中のプロセス一覧を取得し，マルウェアの解析環境でないか確認する。

カ　パスワードを含む，L-PCにログインするための情報を取得する。

設問3　〔インシデント対応手順の改善〕について，(1)～(3)に答えよ。

(1)　本文中の［　e　］に入れる適切な内容を25字以内で具体的に述べよ。

(2)　本文中の下線①について，検知できないのはPC又はサーバがどういう状態にある場合か。40字以内で述べよ。

(3)　本文中の下線②について，マルウェアMに感染しているPC又はサーバをRログを使って検知する方法を，30字以内で具体的に述べよ。

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 | 13:10 ～ 13:50 |
|---|---|

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。
13. 午後Ⅱの試験開始は **14:30** ですので，**14:10** までに着席してください。