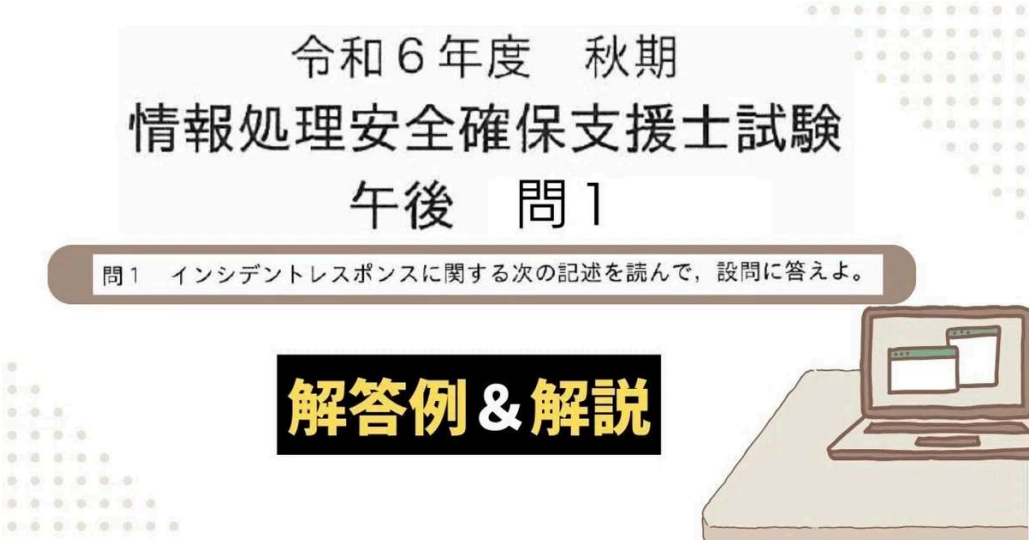


【解答例＆解説】令和6年度 秋期 情報処理安全確保支援士試験 午後 問１

まさ@情報処理技術者試験研究家
2024年10月23日 18:08

情報処理安全確保支援士試験の、解答例とオリジナル解説を公開します。
あくまでも解答例ですので、正解はIPAのサイト（2024年12月24日正午公開）で確認してくださいね。
この記事の最終更新日は、2024年10月23日です。
皆さまの解答例、ご意見も参考にしたいので、コメントお待ちしております。

目次

設問１（８）①

すべて表示

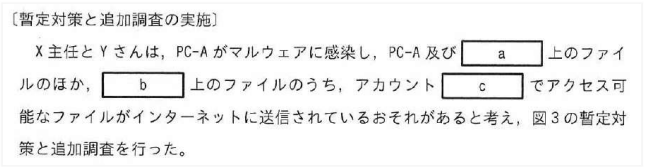
■解答例

設問１（１）a　PC-C
設問１（２）b　filesv
設問１（３）c　ad01¥user019
設問１（４）d　アカウント停止措置
設問１（５）全てのドメインユーザについて、URLフィルタリング機能の管理者拒否リストに、https://△△△.com/を設定する。
設問１（６）プロキシサービスの通信ログで、全てのL社内ホストを対象として、https://△△△.com/、https://〇〇〇.com/、https://□□□.com/への通信記録の有無を確認する。
設問１（７）全てのL社内ホストを対象に、タスク名installのタスクが登録されていないか確認する
設問１（８）①L社内ホスト全てを対象に、installタスクが登録された時に情シス部へアラートが通知される仕組み
設問１（８）②L社内ホスト全てを対象に、マルウェア対策ソフトが停止した時に情シス部へアラートが通知される仕組み
設問２　e　仮想環境の設定にて、仮想PCのRDP接続を禁止する。
設問２　f　FWの設定を行い、RDR形式ファイルのアップロードを禁止する。

■解説

設問１（１）a

解答：PC-C
解説：問題文から抜粋問題


〔暫定対策と追加調査の実施〕
X主任とYさんは，PC-Aがマルウェアに感染し，PC-A及び［ a ］上のファイルのほか，［ b ］上のファイルのうち，アカウント［ c ］でアクセス可能なファイルがインターネットに送信されているおそれがあると考え，図３の暫定対策と追加調査を行った。

［ａ］上のファイルと［ｂ］上のファイルがインターネット上に送信されている。したがって、PC-Aと同様にマルウェアに感染されたと考えられる［ａ］と［ｂ］を表３から表５で探します。
［ａ］については、表３でPC-AからのRDP接続が許可されているPC-Cだとわかります。PC-C以外はRDP接続が失敗しています。

12/04 23:32:35	PC-A から PC-C に，ad01¥user019 で，RDP 接続が失敗した。	auth.csv
12/04 23:32:51	PC-A から PC-C に，.¥administrator で，RDP 接続が許可された。	auth.csv
12/04 23:35:01	PC-A から PC-D に，ad01¥user019 で，RDP 接続が失敗した。	auth.csv

表３

設問１（２）b

解答：filesv
解説：問題文から抜粋問題
次に、マルウェアに感染されたと考えられる［ｂ］を表３から表５で探します。PC-Aからファイルを参照されている filesv を見つけることができます。

12/04 22:38:12	D ドライブのファイルが参照された。	file.csv
（省略）[2]		
12/04 22:42:06	¥¥filesv のファイルが参照された。	file.csv
（省略）[3]		
12/04 22:59:07	s.rar が作成された。	file.csv

表３

設問１（３）c

〔暫定対策と追加調査の実施〕
X 主任と Y さんは，PC-A がマルウェアに感染し，PC-A 及び［ a ］上のファイルのほか，［ b ］上のファイルのうち，アカウント［ c ］でアクセス可能なファイルがインターネットに送信されているおそれがあると考え，図３の暫定対策と追加調査を行った。

［ｃ］には、ファイルにアクセスしたアカウントが入ります。表３から表５でアカウント情報があるのは、表３と表５です。
表５より、「ad01￥user019」が解答になります。

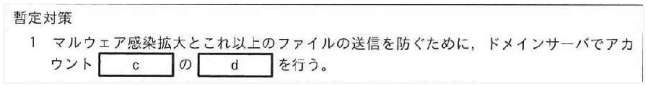
表５　プロキシサービスの通信ログのうち送信元が PC-A であるもの（抜粋）

日時	利用者 ID	宛先	宛先ポート番号	フィルタアクション	送受信量（M バイト）
12/04 22:12:28	ad01¥user019	https://○○search.com/	443	許可	1.0
12/04 22:20:34	ad01¥user019	https://△△△.com/i.ps1	443	許可	2.0
12/04 22:33:25	ad01¥user019	https://△△△.com/v/q.ps1	443	許可	4.0

表５

設問１（４）d

解答：アカウント停止措置
解説：問題文のヒントから考える問題

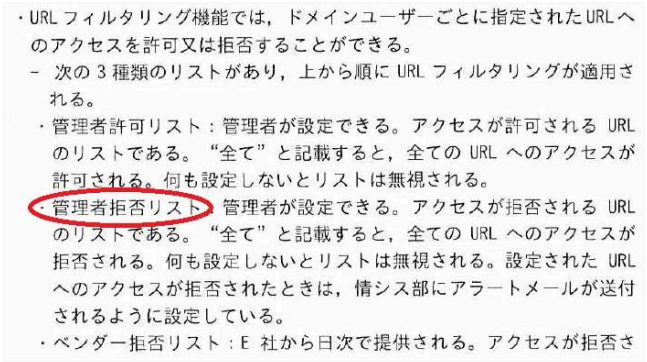

暫定対策
1 マルウェア感染拡大とこれ以上のファイルの送信を防ぐために，ドメインサーバでアカウント [c] の [d] を行う。

暫定対策としてすべきことは、アカウント「ad01￥user019」を使えなくすることですね。「アカウント停止措置」などが解答になります。

設問１（５）

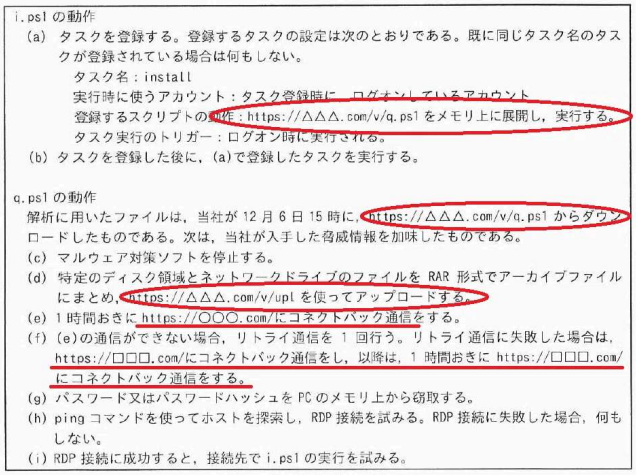
解答：全てのドメインユーザについて、URLフィルタリング
機能の管理者拒否リストに、https://△△△.com/
を設定する。
解説：問題文のヒントから考える問題

下線①について、ファイルの送信を防ぐためのプロキシサーバで行う設定内容が問われています。
この場合は、まずプロキシサーバの機能を確認します。表1ですね。表１のプロキシサーバの仕様説明のファイル送信を防ぐ機能としては、URLフィルタリング機能の管理者拒否リストがあります。


・URL フィルタリング機能では，ドメインユーザーごとに指定された URL へのアクセスを許可又は拒否することができる。
－ 次の 3 種類のリストがあり，上から順に URL フィルタリングが適用される。
・管理者許可リスト：管理者が設定できる。アクセスが許可される URL のリストである。“全て”と記載すると，全ての URL へのアクセスが許可される。何も設定しないとリストは無視される。
・管理者拒否リスト：管理者が設定できる。アクセスが拒否される URL のリストである。“全て”と記載すると，全ての URL へのアクセスが拒否される。何も設定しないとリストは無視される。設定された URL へのアクセスが拒否されたときは，情シス部にアラートメールが送付されるように設定している。
・ベンダー拒否リスト：E 社から日次で提供される。アクセスが拒否さ

では次にどのURLへの送信を拒否するかを表５で確認します。
表５の通信ログの宛先は、次の４つがあります。
・https://〇〇search.com/
・https://△△△.com/
・https://〇〇〇.com/
・https://□□□.com/

次にマルウェアのファイル送信動作を知る必要があります。そのために、図４のマルウェア解析結果を確認します。



i.ps1 の動作
(a) タスクを登録する。登録するタスクの設定は次のとおりである。既に同じタスク名のタスクが登録されている場合は何もしない。
タスク名：install
実行時に使うアカウント：タスク登録時に，ログオンしているアカウント
登録するスクリプトの動作：https://△△△.com/v/q.ps1 をメモリ上に展開し，実行する。
タスク実行のトリガー：ログオン時に実行される。
(b) タスクを登録した後に，(a)で登録したタスクを実行する。

q.ps1 の動作
解析に用いたファイルは，当社が 12 月 6 日 15 時に，https://△△△.com/v/q.ps1 からダウンロードしたものである。次は，当社が入手した脅威情報を加味したものである。
(c) マルウェア対策ソフトを停止する。
(d) 特定のディスク領域とネットワークドライブのファイルを RAR 形式でアーカイブファイルにまとめ，https://△△△.com/v/upl を使ってアップロードする。
(e) 1 時間おきに https://○○○.com/にコネクトバック通信をする。
(f) (e)の通信ができない場合，リトライ通信を 1 回行う。リトライ通信に失敗した場合は，https://□□□.com/にコネクトバック通信をし，以降は，1 時間おきに https://□□□.com/にコネクトバック通信をする。
(g) パスワード又はパスワードハッシュを PC のメモリ上から窃取する。
(h) ping コマンドを使ってホストを探索し，RDP 接続を試みる。RDP 接続に失敗した場合，何もしない。
(i) RDP 接続に成功すると，接続先で i.ps1 の実行を試みる。

図４　C 社の解析結果（概要）

図４より△△△.comと通信を行いファイルアップロードの準備をしていることがわかります。また、ファイルのアップロードタイミングは、（ｄ）のタイミングであることがわかります。

これらの情報を確認した上で、下記のURLについて、管理者拒否リストへの登録対象とするか確認します。
・https://○○search.com/
・https://△△△.com/
・https://○○○.com/
・https://□□□.com/

・https://○○search.com/
表３より、https://○○search.com/へのアクセスは、https://△△△.com/へのアクセスやウイルススキャンソフトの停止前（図４の(c)参照）よりも前に接続を試みているため、ファイル送信のための通信ではないと判断できます。管理者拒否リストへの登録対象外です。

表３　PC-A の time.csv（抜粋）

日時	事象	ファイル名
12/04 22:12:28	https://○○search.com/に接続を試みた。	net1.csv
12/04 22:20:34	https://△△△.com/に接続を試みた。	net1.csv
12/04 22:32:48	i.ps1 が作成された。	file.csv
12/04 22:33:12	i.ps1 が PowerShell で実行された。	file.csv
12/04 22:33:21	“タスク名：install” が登録された。	srv.csv
12/04 22:33:22	“タスク名：install” が実行された。	srv.csv
12/04 22:33:25	https://△△△.com/に接続を試みた。	net1.csv
12/04 22:34:28	VSCAN SVC [1] が停止された。	srv.csv
12/04 22:38:12	D ドライブのファイルが参照された。	file.csv
（省略）[2]		
12/04 22:42:06	¥¥filesv のファイルが参照された。	file.csv
（省略）[3]		

表３

・https://△△△.com/
　https://△△△.com/へ通信を行いファイル送信準備を行っているため、管理者拒否リストへの登録対象です。

・https://○○○.com/
　図４より、コネクトバック通信を行っているだけのため、管理者拒否リストへの登録対象外です。また、ベンダー拒否リストにも登録されています。

〔インシデント発生時のFツール活用〕
12月6日，情シス部のYさんは，プロキシサービスからアラートメールを受信した。Yさんが，アラートメールを確認したところ，PC-Aが，https://〇〇〇.com/にアクセスしようとしてアクセスが拒否されたこと及びそのURLがベンダー拒否リストのマルウェア感染のカテゴリに一致したことが分かり，上司のX主任に報告した。

・https://□□□.com/
図４より、コネクトバック通信を行っているだけのため、管理者拒否リストへの登録対象外です。したがって、解答は次のようになります。「全てのドメインユーザについて、URLフィルタリング機能の管理者拒否リストに、https://△△△.com/を設定する。」

<参考>

コネクトバック-つうしん【コネクトバック通信】 の解説
マルウエアに感染した端末が、インターネットを通じて攻撃者のサーバーと接続する際に用いられる通信。攻撃者は、端末側からの通信に応答する形でファイアウォールをすり抜けることができる。バックドア通信。
出典：デジタル大辞泉（小学館）
goo 辞書

設問１（６）

解答：プロキシサービスの通信ログで、全てのL社内ホストを対象
として、https://△△△.com/、https://〇〇〇.com/、
https://□□□.com/への通信記録の有無を確認する。
解説：知識問題

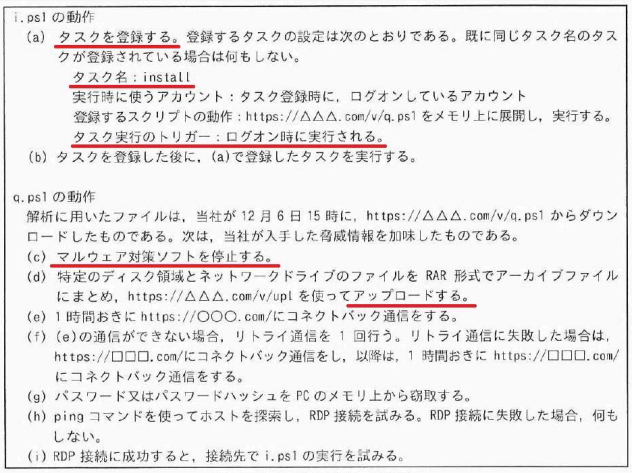
下線②について、PC-A,PC-C以外のL社内ホストがマルウェア感染していないかの確認方法が問われています。これは知識問題ですね。表５で確認した通信記録を全てのホストを対象に確認する必要があります。
「プロキシサービスの通信ログで、全てのL社内ホストを対象として、https://△△△.com/、https://〇〇〇.com/、https://□□□.com/への通信記録の有無を確認する。」などが解答になります。

設問１（７）

解答：全てのL社内ホストを対象に、タスク名installのタスクが
登録されていないか確認する
解説：問題文のヒントから考える問題

Yさんは図４の解析結果から，図３の追加調査の１及び２では，図４で解析したマルウェアが，今後，活動する可能性があるL社内ホストを見逃したおそれがあると考えた。Yさんは③追加調査の３として，L社内ホストの全てに対して新たな調査を行う必要があるのではないかとX主任に相談した。X主任は同意し，調査には時間が掛かるので，調査と並行して，④図４のマルウェアの活動を自動的に検出する新たな仕組みを作るように指示した。

まず最初に、Yさんの考えた「マルウェアが今後活動する可能性があるL社内ホスト」とは、どのような状態のことを指しているのか確認します。
感染しているけれど、まだ活動していない状態とは？



i.ps1 の動作
(a) タスクを登録する。登録するタスクの設定は次のとおりである。既に同じタスク名のタスクが登録されている場合は何もしない。
タスク名：install
実行時に使うアカウント：タスク登録時に，ログオンしているアカウント
登録するスクリプトの動作：https://△△△.com/v/q.ps1 をメモリ上に展開し，実行する。
タスク実行のトリガー：ログオン時に実行される。
(b) タスクを登録した後に，(a)で登録したタスクを実行する。

q.ps1 の動作
解析に用いたファイルは，当社が 12 月 6 日 15 時に，https://△△△.com/v/q.ps1 からダウンロードしたものである。次は，当社が入手した脅威情報を加味したものである。
(c) マルウェア対策ソフトを停止する。
(d) 特定のディスク領域とネットワークドライブのファイルを RAR 形式でアーカイブファイルにまとめ，https://△△△.com/v/upl を使ってアップロードする。
(e) 1 時間おきに https://○○○.com/にコネクトバック通信をする。
(f) (e)の通信ができない場合，リトライ通信を 1 回行う。リトライ通信に失敗した場合は，https://□□□.com/にコネクトバック通信をし，以降は，1 時間おきに https://□□□.com/にコネクトバック通信をする。
(g) パスワード又はパスワードハッシュを PC のメモリ上から窃取する。
(h) ping コマンドを使ってホストを探索し，RDP 接続を試みる。RDP 接続に失敗した場合，何もしない。
(i) RDP 接続に成功すると，接続先で i.ps1 の実行を試みる。

図４　C 社の解析結果（概要）

Yさんの考えた「マルウェアが今後活動する可能性があるL社内ホスト」とは、図４より、i.ps1でinstallタスクが登録されているけれどまだ実行されていない（対象PCがログオンされていない）状態だとだと考えられます。この状態を確認するためには、「全てのL社内ホストを対象に、タスク名installのタスクが登録されていないか確認する」必要があります。

設問１（８）①

設問１（８）②

解答①：L社内ホスト全てを対象に、installタスクが登録された時
　　に情シス部へアラートが通知される仕組み
解答②：L社内ホスト全てを対象に、マルウェア対策ソフトが
　　停止した時に情シス部へアラートが通知される仕組み
解説：問題文のヒントから考える問題
図４のマルウェアの活動を自動的に検出する仕組みが問われています。図４のマルウェアの活動としては下記の動作があります。
・installタスクの登録
・installタスクの実行
・マルウェア対策ソフトを停止する
・ファイルをアップロードする
これらのことより、「installタスク登録の検出」と「マルウェア対策ソフト停止の検出」が解答として考えられます。
以下のような解答となります。
「L社内ホスト全てを対象に、installタスクが登録された時に情シス部へアラートが通知される仕組み」「L社内ホスト全てを対象に、マルウェア対策ソフトが停止した時に情シス部へアラートが通知される仕組み」

設問２　e

解答：仮想環境の設定にて、仮想PCのRDP接続を禁止する。
解説：問題文のヒントから考える問題

表６　攻撃者による目的実行までの活動を阻止するための技術的対策

今回の攻撃者による活動	技術的対策
i.ps1 と q.ps1 を PC-A で実行させた。	PowerShell の実行ポリシーを設定し，署名のないスクリプトの実行を禁止する。
PC-A からマルウェア感染を広げた。	e 。
q.ps1 がファイルを不正に持ち出した。	f 。

表６

「PC-Aからマルウェア感染を広げた」ことを防ぐ技術的対策が問われています。表３より、マルウェア感染はRDP接続で行われていることがわかります。そのため、RDP接続を禁止することが技術的対策となります。

12/04 23:10:05	s.rar が削除された。	file.csv
12/04 23:31:15	PC-A からドメインサーバに，ad01¥user019 で RDP 接続が失敗した。	auth.csv
12/04 23:32:05	PC-A から PC-B に，ad01¥user019 で，RDP 接続が失敗した。	auth.csv
12/04 23:32:16	PC-A から PC-B に，.¥administrator で，RDP 接続が失敗した。	auth.csv

表３

解答を書くために、L社のPC環境を表１で確認します。

表１　図１の各構成要素の仕様，機能及び利用方法（抜粋）（続き）

構成要素	仕様，機能及び利用方法
仮想 PC	・L 社の従業員には，一人 1 台割り当てられている。 ・従業員がシンクライアント PC から RDP で接続して利用する。 ・従業員が利用するアカウントは，ドメインユーザーであり，仮想 PC 上のローカルアドミニストレーター権限をもっている。 ・各ドメインユーザーは，割り当てられた仮想 PC にだけログオンできる。 ・ホスト名は PC-x [2]である。 ・マルウェア感染が確認された場合，情シス部が仮想環境の仮想スイッチから切り離し，感染拡大を防ぐ。

これらのことより「仮想環境の設定にて、仮想PCのRDP接続を禁止する。」などが解答となります。

設問２　f

解答：FWの設定を行い、RDR形式ファイルのアップロードを禁止する。
解説：

表６　攻撃者による目的実行までの活動を阻止するための技術的対策

今回の攻撃者による活動	技術的対策
i.ps1 と q.ps1 を PC-A で実行させた。	PowerShell の実行ポリシーを設定し，署名のないスクリプトの実行を禁止する。
PC-A からマルウェア感染を広げた。	e 。
q.ps1 がファイルを不正に持ち出した。	f 。

「q.ps1がファイルを不正に持ち出した」ことを防ぐ技術的対策が問われています。表６にタイトルを見ると「目的実行までの活動を阻止するための技術的対策」ですので、データの暗号化などは含まれないと考えられます。
送信を阻止する方法？

送信を阻止する方法といえば、ファイアウォール（FW）ですが、この問題にFWの機能説明はありません。？
プロキシサービスでの制御が考えられるが、プロキシサービスでファイルの送信防止は設問１(5)の暫定対策に登場している。？

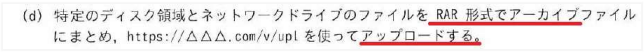

(d) 特定のディスク領域とネットワークドライブのファイルを RAR 形式でアーカイブファイルにまとめ，https://△△△.com/v/upl を使ってアップロードする。

図４

図４のファイルアップロード部分のキーワードを使用して解答を作成します。
〇〇の設定を行い、RDR形式ファイルのアップロードを禁止する。
〇〇部分が問題文から見つからないため、FWの設定で解答することにします。したがって「FWの設定を行い、RDR形式ファイルのアップロードを禁止する。」などが解答になります。

最後までお読みいただきありがとうございました。
ご意見、ご質問、間違いの指摘などあれば、遠慮なくコメントお願いします。皆さんのコメントをお待ちしております。
少しでも皆さんの勉強の参考になれば幸いです。
～ 仲間がいれば、勉強は楽しい！～

■更新履歴

2024/10/13(日)　試験日
2024/10/23(水)　作成・公開