

平成 30 年度 秋期 情報処理安全確保支援士

<午後Ⅱ 解答・解説>

<問 1> クラウド環境におけるセキュリティ対策

■設問 1

[試験センターによる解答例]

GDPR

2018 年 5 月 25 日に適用が開始された欧州連合（EU）の個人情報保護に関する法規制は、GDPR（General Data Protection Regulation：EU 一般データ保護規則）である。GDPR は、EU における個人データの処理や移転、権利保護等について定めている。

■設問 2

[試験センターによる解答例]

(1) R&D 情報は、物理的な入退室管理が行われているプロジェクトルーム内に配置されたプロジェクト専用サーバに保管する。(56 字)

(2) 満たせなくなる基本要件の具体的内容：

- ・生産関連サーバは、X 社の工場及びデータセンタに配置する。(28 字)
- ・生産関連サーバのバックアップを他の工場又はデータセンタに配置する。(33 字)
- ・同じ重要インフラ設備を製造する工場及び生産関連サーバは同一の国又は地域内の 2 か所以上に配置する。(48 字)

IaaS C のサービス仕様の内容：

日本国内のデータセンタが被災した場合はシンガポールのデータセンタでサービスが継続される。(44 字)

(3) X 社のシステムの機器に割り当てている IP アドレスが、IaaS C で予約されているプライベートアドレスと重複する可能性があるという問題 (66 字)

- (1) 問題文にある基本要件の具体的内容を見ると、一番目の要件として「R&D 情報は、物理的な入退室管理が行われているプロジェクトルーム内に配置されたプロジェクト専用サーバに保管する。」とある。したがって、プロジェクト専用サーバをクラウド環境に移行した場合には、この要件を満たせなくなる。
- (2) 生産関連サーバに関する基本要件と IaaS C のサービスについて確認する。
まず、三番目の要件に「生産関連サーバは、X 社の工場及びデータセンタに配置する。」とあるが、生産関連サーバをクラウド環境に移行すれば、この要件を満たせなくなる。
続いて、四番目の要件に「生産関連サーバは、(中略) バックアップを他の工場又はデータセンタに配置する。」とあるが、生産関連サーバをクラウド環境に移行すると、この要件も満たすことができなくなる。
続いて、五番目の要件に「各国及び各地域の輸出管理規制への準拠のために、同じ重要インフラ設備を製造する工場及び生産関連サーバは同一の国又は地域内の 2 か所以上に配置する。日本国内では、システムを東日本地区のシステムと西日本地区のシステムに分け (以下略)」とある。一方、IaaS C のサービス仕様では、日本国内のデータセンタは 1 か所であり、当該データセンタが被災した場合はシンガポールのデータセンタでサービスが継続されることになっている。この仕様により、五番目の要件も満たすことができない。
- (3) IaaS C のサービス仕様には、IP アドレスに関して「あらかじめ予約されているプライベート IP アドレスがあり、利用者はそれらを使うことができない。」とある。そのため、X 社の機器に割り当てている IP アドレスをそのまま使用した場合、IaaS C であらかじめ予約されているプライベートアドレスと重複し、使用できなくなる可能性がある。この問題を回避するために、FW の NAT 機能を用いて一部のアドレスを変換することにしたと考えられる。

■設問 3

【試験センターによる解答例】

- (1) 一度のログインで全システムにアクセスできるという利便性 (27 字)
- (2) 業務サーバ： ㊶、㊷
構成要素： ㊸、㊹、㊺、㊻

(1) SAML (Security Assertion Markup Language) は、ユーザ ID やパスワードなどの認証情報を安全に交換するための XML 仕様であり、同一ドメイン内や特定のベンダ製品にとどまらない大規模なサイトなどにおいて、相互運用性の高いシングルサインオン (SSO) の仕組みや、セキュアな認証情報管理を実現する技術である。SPNGO (Simple and Protected GSS-API Negotiation) は、HTTP を用いてクライアントと Web サーバ間で資格情報を交換するためのプロトコルである。これらの技術を用いることにより、SSO が実現できるため、X 社の従業員は、一度のログインで全システムにアクセスできるようになる。

(2) 問題文の冒頭に、「従業員が Web ブラウザを用いて Linux 及び商用 UNIX の業務サーバにログインする際は、認証サーバ B1 による利用者認証が行われる。」とある。したがって、案 2 を選択し、認証サーバ B1 を IaaS C に移行した場合、負荷が高くなるのは、社内 PC から、図 2 の業務サーバ (Linux) (㊦) と、業務サーバ (商用 UNIX) (㊧) への通信である。

また、負荷が高くなる構成要素は、X 社の社内 PC から IaaS C の認証サーバ B1 との通信経路上にある機器や回線である。これに該当するのは、東日本データセンタの IPS (㊤)、FW1 (㊦)、FW1 とインターネットを接続する回線 (㊤)、IaaS C の FW2 (㊧) である。

■設問 4

【試験センターによる解答例】

- (1) ティア 1 : イ
ティア 2 : ウ
ティア 3 : ア
- (2) 標準ソフトウェア以外のソフトウェアは、脆弱性管理がされないという不都合 (35 字)
- (3) ・ 正確である。(6 字)
・ 作業が速くできる。(9 字)

(1) ティア 4 が最も高い段階であるから、解答群を低い順に並べればよい。これらの中で、最も低いティア 1 に該当するのはイの「部分的である (Partial)」であることは明白である。アの「繰り返し適用可能である (Repeatable)」は、PDCA サイクルが確立され

た状態と考えることができるため、比較的高いレベルであり。したがって、ティア 2 に該当するのがウの「リスク情報を活用している (Risk Informed)」であり、ティア 3 に該当するのがアの「繰り返し適用可能である (Repeatable)」である。

なお、NIST (National Institute of Standards and Technology : 米国国立標準技術研究所) の「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」では、ティア 1~4 を次のように定義している。

ティア 1 : 部分的である (Partial)

リスクマネジメントプロセス - 組織のサイバーセキュリティリスクマネジメントプラクティスが定められておらず、リスクは場当たり的に、場合によっては事後に対処される。サイバーセキュリティ対策の優先順位付けが、組織のリスク目標、脅威環境、またはビジネス・ミッションの要求事項に基づいていない。(以下略)

ティア 2 : リスク情報を活用している (Risk Informed)

リスクマネジメントプロセス - リスクマネジメントプラクティスは経営層によって承認されているが、組織全体にわたるポリシーとして定められていない場合がある。サイバーセキュリティ対策と保護ニーズの優先順位付けは、組織のリスク目標、脅威環境、またはビジネス・ミッション上の要求事項に基づいて直接伝えている。(以下略)

ティア 3 : 繰り返し適用可能である (Repeatable)

リスクマネジメントプロセス - 自組織のリスクマネジメントプラクティスは正式に承認され、ポリシーとして述べられている。組織のサイバーセキュリティプラクティスは、ビジネス・ミッション上の要求事項の変化と、脅威及びテクノロジー状況の変化へのリスクマネジメントプロセスの適用に基づいて、定期的に更新されている。(以下略)

ティア 4 : 適応している (Adaptive)

リスクマネジメントプロセス - 自組織は過去と現在のサイバーセキュリティプラクティス(そこから学んだ教訓と、それらの対策から得た兆候を含む)を基に、サイバーセキュリティ対策を調整する。自組織は最新のサイバーセキュリティ技術及びプラクティスを組み入れた継続的な改善のためのプロセスを介して、変化するサイバーセキュリティの技術と実践に進んで順応し、進化・高度化する脅威にタイムリーかつ効果的に対応している。(以下略)

出典 : セキュリティ関連 NIST 文書 (IPA) 「Cybersecurity Framework Version 1.1 (頁対訳)」

<https://www.ipa.go.jp/files/000071204.pdf>

- (2) 運用サービス 1 及び 2 が提供されると、標準ソフトウェアを対象として、情報セキュリティ標準の改定 3「脆弱性管理の実施」の内容を行うことが可能になる。しかし、標準ソフトウェア以外のソフトウェアはこのサービスの対象外となるため、脆弱性管理がされないという不都合が生じることになる。
- (3) 製品 D における、セキュリティ設定パラメタの設定値のチェックに関する仕様は次のようになっている。

- ・エージェントソフトウェアが、サーバ又は PC におけるパッチの適用状況及びセキュリティ設定パラメタの設定値を収集し、サーバソフトウェアに送信する。
- ・管理画面において、必要なパッチ、並びに必要なパッチが適用されていないサーバ及び PC の一覧や、セキュリティ設定パラメタの設定値が指定した値と異なるサーバ及び PC の一覧を表示することができる。

これを情報セキュリティ標準を基に手作業及び目視でセキュリティ設定パラメタの設定値をチェックする方法と比べてみると、作業が正確で、効率的（速くできる）ことが利点として挙げられる。

■設問 5

【試験センターによる解答例】

(1) 案 A :

	クライアント	業務サーバ
①	Ⓗ	Ⓓ
②	Ⓘ	Ⓓ

案 B :

	クライアント	業務サーバ
①	Ⓖ	Ⓑ
②	Ⓗ	Ⓑ
③	Ⓘ	Ⓑ

- (2) a : カ
b : ウ
c : イ
d : ア

e : オ
f : ク
g : キ
h : エ

- (1) 前述のように、問題文の冒頭に「従業員が Web ブラウザを用いて Linux 及び商用 UNIX の業務サーバにログインする際は、認証サーバ B1 による利用者認証が行われる。」とある。図 3 において、クライアントに該当するのは㉔の社内 PC、㉕のスマートフォン、㉖である。案 C では、スマートフォン及びタブレットから、IaaS C にある㉗の業務サーバ (Linux) にアクセスする場合、IaaS C にある認証サーバ B2 で利用者認証が行われる。一方、案 A では、スマートフォン及びタブレットは、インターネットを経由して東日本データセンタの認証サーバ B1 で利用者認証を行った上で、IaaS C にある㉗の業務サーバ (Linux) にアクセスする必要がある。そのため、通信経路上の構成要素の負荷が高くなると考えられる。なお、社内 PC から IaaS C にある㉗の業務サーバ (Linux) にアクセスする場合には、案 A、案 C ともに通信経路に大きな違いはないため、構成要素の負荷には影響しないと考えられる。

続いて案 B では、認証サーバ B1 が IaaS C に移行するため、クライアントが東日本データセンタにある㉗の業務サーバ (Linux) にアクセス場合の通信経路が案 C とは異なる。まず㉔の社内 PC の場合、案 C では東日本データセンタの認証サーバ B1 で利用者認証を行った上で同センタの業務サーバ (Linux) にアクセスする。一方、案 B では、社内 PC はインターネットを経由して IaaS C の認証サーバ B1 で利用者認証を行った上で、東日本データセンタの業務サーバ (Linux) にアクセスすることになるため、案 C に比べ、通信経路上の構成要素の負荷が高くなることが考えられる。スマートフォン及びタブレットについては、案 C ではインターネットを経由し、東日本データセンタの認証サーバ B1 で利用者認証を行った上で同センタの業務サーバ (Linux) にアクセスする。一方、案 B では、スマートフォン及びタブレットは、インターネットを経由して IaaS C の認証サーバ B1 で利用者認証を行った上で、東日本データセンタの業務サーバ (Linux) にアクセスすることになる。そのため、案 C に比べ、通信経路上の構成要素の負荷が高くなることが考えられる。

- (2) 「モバイル環境の検討」の対策 2 にあるように、従業員がモバイル端末からインターネット経由でクラウド環境にアクセスする際、VPN サーバでクライアント証明書を用いた端末認証が行われた後、認証サーバ B1 による利用者認証が行われ、トークンが発行される。

これを踏まえ、図 4 の通信シーケンスを考察する。

図 4 で、スマートフォンがトークンなしで SaaS Q にアクセス要求を行った場合は、SaaS Q から認証サーバ B1 が発行したトークン要求が返ることになるため、a にはカが入る。

図 4 の 3 つ目の通信シーケンスでスマートフォンで認証サーバ B1 へのアクセスに必要な VPN クライアントを起動しているため、次に続くのは、スマートフォンと VPN サーバ間での端末認証である。したがって、b にはウの接続要求、c にはイのクライアント証明書の要求、d にはアのクライアント証明書が入る。VPN サーバへの接続が完了した後の通信シーケンスは、スマートフォンと認証サーバ B1 間での利用者認証及びトークンの発行である。

まず、スマートフォンから認証サーバ B1 に対してトークンの発行要求が行われると、同サーバから利用者 ID 及びパスワードの入力要求が返るので、スマートフォンは利用者 ID 及びパスワードを同サーバに送る。したがって、e にはオ、f にはク、g にはキが入る。

図 4 のように、その後は認証サーバ B1 と認証サーバ A1 間で利用者 ID 及びパスワードの検証が行われた後、スマートフォンのパッチ適用状況及びセキュリティ設定の確認が行われ、問題なければ認証サーバ B1 からスマートフォンにトークンが発行される。したがって h にはエが入る。

＜問 2＞ セキュリティインシデントへの対応

■設問 1

【試験センターによる解答例】

- (1) a : エ
b : イ
※a, b は順不同
- (2) c : ケ
d : ウ
e : コ

- (1) NIST の文書 SP 800-61 「コンピュータセキュリティインシデント対応ガイド」では、インシデント対応チームが提供するサービスの例として、侵入検知、脆弱性や脅威に

ついでのアドバイザリの配信、教育と意識向上、及び社内外での情報共有の推進を挙げている。したがって , には、イ、エが入る。(順不同)

- (2) NIST SP 800-61 の内容を知らなくても、インシデント対応ポリシーに記載する項目の例であるから、空欄の前後の内容から正解が導き出せると思われる。 は、インシデント対応ポリシーで責任表明するのであるから、ケの「マネジメント層」が入る。 は、インシデント対応ポリシーで定義する対象であり、深刻度評価を行う対象となるものであるから、ウの「インシデント」が入る。 は、インシデントについて、深刻度評価と並んで行うものであるから、コの「優先順位付け」が入る。

■設問 2

【試験センターによる解答例】

- (1) f : ログを取得する機器 (9 字)
g : 取得するログの種類 (9 字)
h : 保存期間 (4 字)
※f, g は順不同
- (2) i : タイムゾーン (6 字)
j : 統一 (2 字)
- (3) ネットワークトラフィック量と比較して異常を検知する。(26 字)

- (1) 図 3 の(6)d に「開発部はログ取得を定めた規程をもたず、開発部が管理する機器のうちログを取得していたものは少数だった。また、取得していたログの種類や保存期間にはばらつきがあった。」とある。このような課題を解決するために定める要件であるから、要件 1 の取得するログについての要件における , には、「ログを取得する機器」と「取得するログの種類」が入る。(順不同)
また、要件 2 の取得したログについての要件における には、「保存期間」が入る。
- (2) 各機器が出力するログに記録する時刻情報について行うべき設定であるから、該当するのは が「タイムゾーン」、 が「統一」である。タイムゾーン(時間帯)とは、同じ標準時を使う地域のことであり、UTC (Coordinated Universal Time :

協定世界時) を基準として、その差分で表される。

- (3) 通常時のネットワークトラフィック量や日、週、月、年の中でのその推移などの情報を把握しておくことで、サイバー攻撃により、ネットワークトラフィック量が通常時よりも大幅に増加した等の異常を検知することが可能となる。

■設問 3

【試験センターによる解答例】

- (1) プロキシサーバのログからアクセス先がサイト M のエントリを抽出し、このエントリから PC-A の IP アドレスを得た。(55 字)
- (2) HTTP リクエストによる活動 : C&C サーバへのコマンド要求又は応答 (18 字)
HTTP レスポンスによる活動 : C&C サーバからのコマンド受信 (15 字)
- (3) 問題 : PC のネットワークインタフェースや通信の状態についての情報が失われること (36 字)
措置 : メモリダンプを取得する。(12 字)
- (4) k : プロキシサーバのログから、IPn のサイトにアクセスした機器がほかにはないか (36 字)
- (5) 7 回
- (6) l : ハッシュ値 (5 字)
- (7) 行番号 : 28 行目
役立つ情報 : プロキシサーバがインターネットに送信したデータのサイズ (27 字)

- (1) 問題文の「サイト M のログに残っていたアクセス元の IP アドレスは A 社のプロキシサーバのものだった」という記述からもわかるように、サイト M にはプロキシサーバを経由して接続しているため、プロキシサーバのログからサイト M にアクセスした PC を特定することが可能である。具体的には、プロキシサーバのログからアクセス先がサイト M のエントリを抽出し、当該エントリの送信元 IP アドレスを確認する。続いて、

当該送信元 IP アドレスが割り当てられた PC を確認すればよい。

- (2) マルウェアに感染した PC-A が特定のサイトにアクセスし、その後頻繁に同じサイトにアクセスを繰り返したということは、特定のサイトが C&C サーバ (Command and Control sever : 指令サーバ) であり、そこから指令コマンドを受け取った可能性が高い。このアクセスにおいて、HTTP リクエストと HTTP レスポンスによってマルウェアが行っていた活動としては、HTTP リクエストでは C&C サーバに対するコマンドの要求や応答、HTTP レスポンスでは C&C サーバからのコマンドの受信、と考えられる。
- (3) インシデント調査の観点からすると、マルウェアが活動している状態をそのまま維持しておくことが望ましい。特に、活動している不正なプロセスに関する情報、ネットワークインタフェースや通信の状態、メモリの内容などはマルウェアの特性や活動内容を調査する上で重要な情報となるが、感染 PC をネットワークから切断すると、これらの情報が失われる可能性がある。この問題を軽減するためには、感染 PC をネットワークから切断する前に、メモリの内容を記録しておくため、メモリダンプを取得しておくことよい。そのためには、マルウェア感染等のインシデントに備え、あらかじめ各 PC にメモリダンプ取得用のツールをインストールし、手順書等を作成しておくことが望ましい。
- (4) 図 6 からわかるように、マルウェア K に感染した PC-A が頻繁にアクセスを繰り返していたサイトの IP アドレスは IPn である。したがって、プロキシサーバのログから IPn のサイトにアクセスした機器がほかにはないかを調査することで、マルウェア K がほかの機器にも感染している可能性を簡易に確認することが可能である。
- (5) 図 8、図 9 で、9 月 5 日 10 時 35 分から 45 分までの時間帯における PC-B 上での last コマンド、lastb コマンドの実行結果を見ると、攻撃者は 9 月 5 日 10 時 35 分から 10:40 までに 7 回ログインに失敗した後、10:41 にログインに成功していることがわかる。
- (6) ファイル名が異なっていた場合であっても、目的とするファイルと同じ内容であることを確認するには、各ファイルのハッシュ値を照合するとよい。ハッシュ値はファイルの名称は影響されず、内容によって出力結果が変わる。同じ手法でハッシュ値を出力した場合、ファイルの内容が同一であれば出力されるハッシュ値も常に同じだが、比較対象となるファイルの内容がわずか 1 バイトでも異なれば、出力されるハッシュ値は大きく異なる。
- (7) 表 1 にあるように、“new3.exe”は、指定されたファイルを HTTP の POST メソッドを用

いて IPn のサイトに送信する機能をもっている。図 6 で、9 月 8 日 3 時 35 分以降のログを見ると、行番号 27～30 の 4 行が該当するが、この中で、行番号 28 だけが POST メソッドであり、レスポンスメッセージのサイズも“35618”と大きな値となっている。したがって、行番号 28 がファイルを社外に送信した可能性を示す記録である。また、プロキシサーバ又は FW が取得できる情報のうち、図 6 中に示された情報以外で、合わせて見ることによってファイル送信の有無を判断するのに役立つ情報としては、プロキシサーバがインターネットに送信したデータのサイズが挙げられる。マルウェアの挙動によってはファイルを小さなサイズに分割し、何度かに分けて外部のサイトに送信するケースも多いが、その場合であっても、感染が疑われる PC が特定のサイトに対して送信したデータのサイズを確認することで、情報流出の有無を判断する手掛かりとなる。

■設問 4

【試験センターによる解答例】

- (1) ア : 9/4 14:31
イ : 9/4 14:37
ウ : 9/5 10:41

- (2) m : タ
n : コ
o : ソ
p : ケ
q : シ
r : 力
s : オ

- (1) ア : 図 7 の D さんへのヒアリング内容によると、D さんは 9 月 4 日午後に ZIP 形式の“samplebun.zip”をダウンロードしている。図 6 のプロキシサーバのログを見ると、4 行目に HTTP で“samplebun.zip”にアクセスした記録が残っていることがわかる。このログが出力された日時は“9/4 14:31”である。

イ : 図 6 のプロキシサーバのログより、マルウェア K による IPn のサイトとの頻繁な通信が開始されたのは 8 行目であり、その日時は“9/4 14:37”である。

ウ：設問 3 の(5)の解説にあるように、攻撃者が PC-B へのログインに成功したのは“9/5 10:41”である。

(2) m：表 1 にあるように、ファイル W はダウンロードの機能をもつマルウェア L である。したがって にはタが入る。

n：マルウェア L がアクセスし、“new3.exe”をダウンロードするサイトはサイト M である。したがって にはコが入る。

o, p：表 1 にあるように、“new3.exe”は遠隔操作の機能をもつマルウェア K であり、実行されると IPn のサイトにアクセスし、そのレスポンスに従って動作する。したがって にはソ、 にはケが入る。

q：図 7 にあるように、攻撃者は PC-B へのログインに成功した後、9 月 7 日 4:15 までに、漏えいが疑われるファイルのコピーとファイル A を、PC-B のローカルディスクに作成している。したがって にはシ、 にはカが入る。

s：問題文にあるように、C さんがフォレンジックツールを用いてファイル A のファイルサイズとハッシュ値をキーにしてファイルを検索した結果、PC-A において、9 月 8 日 3:35 にファイル A と同じ内容のファイルが作成されていたことがわかった。したがって にはオが入る。

■設問 5

[試験センターによる解答例]

課題：b

措置：インシデント対応の作業手順書を作成する。(20 字)

図 3 中の(6)に示された課題 a～d は概ね次の通りである。

- a. インシデント対応についての各部の責任や役割が曖昧
- b. インシデント対応についての作業手順が不明確
- c. インシデント対応の経験をもつ者又はスキルをもつ者がいない

- d. ログ取得を定めた規程がなく、取得するログの種類や保存期間にばらつきがある

これらのうち、a の課題についてはインシデント対応ポリシーを策定し、A-CSIRT 及び各部の役割、責任及び権限レベルを規定することで改善を図っている。

c の課題については、各部で A-CSIRT の構成メンバを見直すとともに、システム部所属のメンバを増やしている。加えて定期的に勉強会を開催し、外部の研修に参加する方針を立てる等して改善を図っている。

d の課題については、ログを取得する機器、取得するログの種類、ログの保存期間等の要件を定めたログ管理ポリシーを作成し、情報セキュリティ委員会から各部に同ポリシーに従った運用を指示することで改善を図っている。

残る b の課題については特に措置が講じられておらず、未対応となっている。b の課題を解決するには、インシデント対応の作業手順書を作成する必要がある。