情報セキュリティマネジメント　独自問題

分野ごと練習問題

[サイバー攻撃手法編]

１．マルウェアであるウイルス、ワーム、トロイの木馬の内、自己増殖しない（増えない）のは[　a　]である。
２．マルウェアであるボットに感染した PC を[　b　]PC と呼ぶ。この PC が大量に集まった集合体を[　c　]ネットと呼び、攻撃者の[　d　]サーバから指令を受け DDoS 攻撃などを行う。攻撃者の C&C サーバから送られる指令を受け取る攻撃者が仕組んだプログラムを[　e　]ドアと呼ぶ。
（補足）ボットは重要な情報を盗むプログラムや、攻撃者からの遠隔操作を可能にするバックドアを含む
３．ウイルス対策ソフトが検知できる状態になる前にマルウェアを組織に送り込む攻撃を[　f　]デイ攻撃と呼ぶ。
４．SNS などから流出した ID とパスワードが他のサイト（銀行とか）で使いまわしされていることを期待して、その ID、パスワードを使って不正ログインを試みる攻撃を[　g　]攻撃という。サイトからの流出だけでなくネットワーク機器の脆弱性を悪用した情報の窃取も多発しており、近年の不正アクセス攻撃の主流となっているようだ。
５．サイバー攻撃の流れを示すサイバーキルチェーンは偵察、[　h　]、[　i　]、攻撃実行、インストール、遠隔制御、[　j　]の 7 段階から成る。
６．攻撃者が誘導用に作った Web ページの上に正規の Web ページを透明にして配置し、正規のページにある「なんらかのボタン」を押させる攻撃を[　k　]と呼ぶ。
７．長年時間をかけて複数の攻撃手法を使うなど念入りに行う高度な攻撃を[　l　]攻撃と呼ぶ。この攻撃は、標的とする組織に合わせてカスタマイズしたマルウェアを用いたり、ゼロデイ攻撃やサプライチェーン攻撃を行う。
８．人間をだますテクニックは[　m　]エンジニアリングと呼ばれます。
９．ブルートフォース攻撃で不正ログインを試みる場合は 1 つのユーザ ID に対してパスワードを順次変えながらログインを試すが、現在では試行回数の制限などで効果が低くなっている。そこで 1 つのパスワードに対してユーザ ID を順次変えながらログインを試す[　n　]攻撃が多くなってきた。
10. 攻撃者がサイバー攻撃の前に行うターゲットの情報収集、下調べは[　o　]と呼ばれる。この中の 1 つにターゲットのサーバ上でどんなプログラム（メールサーバプログラム、Web サーバプログラム、ファイルサーバプログラムなど）が動いているかを下調べする[　p　]スキャンがある。
11. ユーザの ID やパスワードが暗号化して流れているデータを取得し、復号はできないが、

そのまま暗号化されたID、パスワードを再利用して不正ログインを試みる攻撃を[　q　]攻撃と呼ぶ。

12. 通信を行う二者の間に割り込んで、両者が交換する情報を盗んだり書き換える（改ざん）攻撃は英字4文字で[　r　]と呼ぶ。日本語では「中間者攻撃」と呼ばれる。似た攻撃にMITB攻撃がある。こちらはブラウザと正規のWebサーバとの間の通信をマルウェアが盗聴、改ざんする手法だ。こちらも日本語では「中間者攻撃」と呼ばれる。ネットバンキングなどでの被害が報告されている。

[暗号・認証、セキュリティ管理編]

１．総務省と経済産業省が安全性を認めた暗号技術のリストを[　s　]暗号リストという。
２．公開鍵で暗号化した場合、復号できる鍵は[　t　]鍵のみである。また、その逆も成り立つ。
３．ハイブリッド暗号は処理速度の速い共通鍵暗号方式でメールや通信内容を暗号化するため事前に共通鍵を[　u　]鍵で暗号化して相手に送る。共通鍵を復号できるのは[　v　]鍵を持っている相手のみである。以後は共通鍵で暗号、復号しながら通信を行う。
４．電子証明書は有効期限内にもかかわらず失効させなければならない場合がある。秘密鍵を盗まれた場合などである。失効した電子証明書の一覧は[　w　]というリストに記録される。また、リストで確認するのではなく電子証明書の有効性をオンラインで問い合わせてリアルタイムで確認する[　x　]という通信の仕組み（プロトコル）もある。
５．いつから文書（ファイル）が存在し、その日以降改ざんされていないことを証明するために[　y　]が利用される。TSA（時刻認証業務認定事業者）が発行する。
６．サーバ側がアクセスしてきたユーザの環境（位置、OS、ブラウザなど）がいつもと違う場合、念のため追加の認証（生年月日やメールアドレスへのワンタイムパスワード送付）を行うことを[　z　]認証と呼ぶ。
７．暗号化の処理速度は公開鍵方式、共通鍵方式、どちらが速いか。[　A　]方式
８．大きなデータと小さなデータを同じハッシュ関数でハッシュ値（メッセージダイジェスト、フィンガープリント、指紋）を求めた。出力された２つのハッシュ値の長さは[　B　]。（「同じ」、「違う」のいずれかで答えよ）
９．Web サーバから送られてくる Web ページが改ざんされていないかどうかは Web ページとともに送られてくる[　C　]認証コード（MAC）で分かる。なお、MAC の作成にハッシュ関数を利用した場合は HMAC と呼び、AES 暗号化処理を利用したものを CMAC と呼ぶ。
10．生体認証で誤って本人を拒否する確率を FRR と呼び、誤って他人を受け入れる確率を[　D　]と呼ぶ。

[セキュリティ管理、対策、関連法規編]

１．JIS Q 27001 の要求事項を満たすと[　E　]認証が取得できる。
２．情報セキュリティ方針（ポリシ）は基本方針、対策基準、[　F　]から成る。
３．リスクアセスメントが終わりリスク対応を行うが、リスク対応にはリスク回避、リスク低減、[　G　]、リスク保有がある。
４．インシデント（セキュリティ上の事件）が起こった時、また、ソフトウェア、ハードウェアにセキュリティ上の脆弱性（欠陥）が見つかった時、最初に発表される情報には先頭に CVE が付けられ MITRE（マイター）社から発信される。その脆弱性の深刻度（危険度）は世界共通の基準で定量的に評価する[　H　]という手法で数値化される。また、脆弱性の種類は国が違っても理解できるように共通脆弱性タイプ一覧[　I　]（英字３文字）で表される。
５．現在、マルウェア（ウイルスなど）を会社の内部ネットワークに入れないように対策する入口対策では不十分であり、仮に内部にマルウェアが侵入しても情報を外部に出さない[　J　]対策が併せて必要である。
６．送信者個人が電子証明書を購入し、送信メールに電子署名、暗号化の処置を施すことで、受信側でメールの送信者の確認、暗号化による盗聴防止、メールの改ざん防止が実現できる方法として[　K　]がある。
７．ランサムウェアでデータを暗号化されて業務が停止したなどの被害を受けた場合、攻撃者を特定するため、また、特定した後の裁判のため「攻撃された証拠」を集める必要がある。このことを[　L　]フォレンジックスと呼ぶ。
８．自分の著作物を公表する時に、著作者名を表示するかしないか、表示するとすれば実名とするか変名（ペンネームとか）とするかを決定する権利は著作者[　M　]権の１つである。
９．Web ページや掲示板上でプライバシー侵害や著作権侵害があった場合、プロバイダ、サーバの管理者・運営者、掲示板管理者などの損害賠償責任の制限（何でもかんでもその人たちの責任にするのを防ぐ）および発信者情報の開示を請求する権利を定めた法律は[　N　]責任制限法である。

［テクノロジ、マネジメント編］

１．ファイアーウォールはパケット（通信データ）の[　O　]部を見る。例えば IP アドレスやポート番号を見て通過を許可（accept)、拒否（reject：拒否したというエラーを送信元に返す)、廃棄（drop：送られてきたパケットを廃棄し、エラーは返さない。攻撃には有効。）する。これに対し、Web サーバ専用の WAF はパケットの[　P　]部を見てパケットの通過を許可、拒否（エラーページ 403 forbidden をブラウザに返す）する。例えば、データベース検索条件入力フォームに SQL コマンドの一部を入れる SQL インジェクションやフォームに<script>・・・</script>のプログラムを入れた場合、WAF が検知し拒否する。（ヒント：いずれもヘッダ、データのどちらか)

２．IDS は不正アクセスなどの異常を検知し、管理者にメールなどで通報する。その機能に加え、さらにファイアーウォールのルールを自動で更新する機能を持たせたシステムは[　Q　]と呼ばれる。

３．サーバ、ネットワーク機器、アプリケーション、セキュリティ機器のログを集めて分析し異常があれば管理者に通報する仕組みは[　R　]（S で始まる英字 4 文字）と呼ばれる。SOC（セキュリティ・オペレーションセンター）などで利用される。

４．遠隔地から盗まれたスマホやノートパソコンをロックして使用不能にしたり、データを消去したりできる機能は[　S　]（英字 3 文字）と呼ばれる。

５．サーバが不要でコンピュータ同士が対等な関係で通信し合う方式は[　T　](3 文字で）と呼ばれる。メッセンジャー、仮想通貨のブロックチェーン作成もこの方式を使っている。

６．会社の拠点間をつないだり、出先のノートパソコンを会社のネットワークにつなぐとき安上がりな方法としてインターネット VPN がある。インターネット上に仮想的なプライベートなネットワーク VPN を作る。具体的にはログイン ID とパスワードだけでなくクライアント証明書を使ってノートパソコンなどの端末を認証（間違いないか確認）した後に会社に接続する。暗号化方式はノートパソコンを会社に接続するときは SSL/TLS を使い、拠点間を接続するときは IP[　U　]（英字 3 文字）を使うのが基本だ。

７．クラウド事業者などはサービスレベルを表す数値として何%稼働し続けるかを利用する。例えばあるクラウド業者は 99.95%以上と表記している。これは[　V　]（英字 3 文字）と呼ばれる。この数値を下回った場合、クラウド業者には利用料の値下げなどのペナルティが課されることが多い。

[ストラテジ編]

1. クラウドサービスのうち、例えば顧客管理ステムなどのアプリケーションまで含めてクラウド事業者から借りるタイプのサービスは[　W　]（英字 4 文字）と呼ばれる。ハードウェアのみ借りるサービスは[　X　]（英字 4 文字）と呼ばれる。
2. 例えばある企業が事業拡大のためネットショッピングサイトを開始することを決めたとします。ネットショッピングサイト構築をどこかの企業に依頼するのですが、まずは情報集めです。例えば候補となる 5 社ほどに構築できるシステムについての情報提供を依頼します。これは RFI と呼ばれます。その情報からさらに企業を絞り込んで今度は具体的なシステムの機能、構築スケジュール、価格などを載せた提案書の提出を依頼します。これを[　Y　]（英字 3 文字）と言います。
3. サイバー攻撃だけでなく、災害が起こった時も事業を継続するための計画を事業継続計画と呼びます。一般的には英字 3 文字で[　Z　]と呼びます。

総合問題

１．各文が正しい場合○、誤っている場合×を解答欄に記入せよ。
（１）感染が疑われる端末は外部のＣ&Ｃサーバと通信していないかを確認するため、しばらくはネットワークに接続したままにしておく必要がある。　　解答欄[　a　]
（２）証券会社のサイトで「ログインパスワード」と別に株を買うときには「取引パスワード」が必要である。ともに記憶する形式のパスワードである。これは２要素認証（多要素認証）に当たる。　解答欄[　b　]
（３）記憶するタイプのパスワードは英大文字、英小文字、数字、記号を含む 10 桁にしておけばかなり強力になるので SNS やネットショップサイトで使いまわしをしても大丈夫である。　解答欄[　c　]
（４）ISMS の PDCA サイクルの Plan で策定する情報セキュリティ基本方針は基本方針、対策基準、実施手順の 3 層になっている（中小企業は下 2 つを 1 つにする 2 層も認められている)。この 3 層のうち、最上位の基本方針は外部に公開することになっている。
解答欄[　d　]
（５）画像、音楽、映像データに著作権者の情報を埋め込む技術はステガノグラフィと呼ばれる。　解答欄[　e　]
（６）欧州連合（EU）の個人情報保護法である GDPR（一般データ保護規則）は外国の法律であるから日本のどの企業にも関係ない。　解答欄[　f　]
（７）IMAP4 は Web ページをやり取りするプロトコル（通信規則）である。
　　解答欄[　g　]
（８）派遣契約では労働者は派遣先企業から業務の指揮命令を受ける。解答欄[　h　]

２．括弧をうめよ。
（１）労働基準法では労働時間（１日８時間以内、かつ、週４０時間以内）を超えた時間外労働を労働者にさせる場合、労使間で[　i　]協定を締結しなければならないことが定められている。
（２）「[　j　]に関する法律」は特定商取引（通信販売、訪問販売）における、事業者と消費者との間のトラブルを防ぐための法律である。業者や商取引についての情報開示・勧誘方法の規制・クーリングオフ制度による解決手続きなどについて定められている。。
（３）取引先になりすまして偽りのメールを送り付け、金銭をだまし取る詐欺（ビジネスメール詐欺）は英字 3 文字で[　k　]と呼ばれる。
（４）デジタル署名（電子署名）は送信するデータ（メール、文書など）をハッシュ関数を用いてハッシュ値（メッセージダイジェスト、フィンガープリント）を求め、それを[　l　]鍵で暗号化したものである。受信側は送られてきた文書に付いた電子署名を[　m　]鍵を使

って確認（検証）し、改ざんやなりすましを発見できる。
（５）OS やアプリケーションなどすべてのプログラムには作成者が気づいていない欠陥（脆弱性）が潜んでいる。その脆弱性を突いて多くの攻撃は行われる。よってその脆弱性を自ら発見することも重要である。その方法の１つとしてプログラムを作るときには予想されていないほどの大きなデータを送ったり細工を施したデータ（通常現れない、ランダムな文字列など）を送ったりして、そのプログラムの誤動作を発見する手法がある。これは[　n　]と呼ばれる。
（６）不正のトライアングルは[　o　]、動機、正当化の３つの要因のことで、すべてが揃った場合に内部不正などの犯罪が起こると言われている。
（７）[　p　]は不正な挙動の検知と、マルウェア感染後の速やかなインシデント対応を目的に組織内の情報端末を監視する製品である。マルウェア感染を完全に防ぐことは困難なため、感染後の対応を効率的に行うことに主眼を置いている。
（８）「インシデント（セキュリティ上の事件）の根本原因を突き止め、解決策や再発防止策を実施する」というサービスマネジメントプロセスは[　q　]管理と呼ぶ。また、「可能な限り迅速にサービスを正常な状態（標準の運用）に復旧させる」は[　r　]管理と呼ぶ。
（９）企業の施設・設備を維持保全するための取り組みは[　s　]マネジメントと呼ばれる。盗難防止のためのセキュリティワイヤや無停電電源装置などがこれに当たる。
（１０）適用宣言書は JISQ27001 の附属書 A から自社の ISMS にとって、必要な情報セキュリティ管理策を選択し、それらを記載することで作成します。追加もできます。選択しない場合はその[　t　]を書く必要があります。
（１１）多要素認証では頭で覚えるパスワードは知識認証と呼び、トークンなど所有していないと認証できない場合は[　u　]物認証と呼ぶ。
（１２）プロキシサーバはネットワーク構成図の[　v　]に設置する。
（ヒント：外部ネットワーク、内部ネットワーク、DMZ のいずれかである）