

高度午前Ⅱ試験 (DB, ES, AU) セキュリティレベル4 補足資料

2019,12,20 (株) アイテック IT 人材教育研究部

はじめに

令和2年度春期試験から、プロジェクトマネージャを除く高度情報処理技術者の午前Ⅱ試験で、セキュリティ分野の問題を最も高いレベル4で出題し、かつ、重点分野として出題数を増やすことが発表されました(プロジェクトマネージャの午前Ⅱ試験は、現在のレベル3のままです)。出題数は、各試験で従来よりも1~2問増えると予想しています。

なお、各試験でセキュリティ関連問題が全てレベル4で出題されるわけではなく、従来も出題されている応用情報技術者試験のレベル3問題に加えて、各試験区分の人材像にとって関連性の強い知識項目がレベル4として出題されます。

・参考 URL

https://www.jitec.ipa.go.jp/1_00topic/topic_20191105.html

この補足資料では、令和2年度春期のデータベーススペシャリスト試験(DB)、エンベデッドシステムスペシャリスト試験(ES)、システム監査技術者試験(AU)を受験される方が、試験区分に関係なく理解しておくべき、暗号化や認証、サイバー攻撃などのセキュリティ(レベル4)の知識と、各試験区分ごとに理解しておくべきセキュリティ(レベル4)の知識を、シラバスの内容を基に説明しています。

試験種別に関係なく共通して理解しておくべきレベル4の知識 下記が新しい内容です。

マルウェア・不正プログラム、脆弱性、攻撃者の種類・動機、攻撃手法、暗号技術、認証技術、公開鍵基盤、情報セキュリティ組織・機関、セキュリティ関連制度・規格

[各試験ごとに理解しておくべきレベル4の知識]

- ・DB……データベースセキュリティ、アプリケーションセキュリティ
- ・ES……制御システムのセキュリティ評価、IoTシステムの設計・開発におけるセキュリティ
- ・AU……前記のDB、ES向け知識、セキュリティ評価基準、脆弱性評価の指標、セキュリティ情報共有技術、マルウェア解析

関連問題が既に出題されている場合は、問題と解説も収録しています。この資料の内容を理解して、来春の午前Ⅱ試験を余裕をもって突破していただきたいと思います。

・参考資料の URL

「情報処理安全確保支援士試験(レベル4)」シラバス 追補版(午前Ⅱ) Ver.3.0

https://www.jitec.ipa.go.jp/1_13download/syllabus_sc_am2_tsuiho3_0.pdf

レベル4の知識を理解するには、応用情報技術者試験レベルのセキュリティの知識が必須になるので、まずはじめに「基本情報レベル」→「応用情報レベル」のセキュリティ知識を十分に理解し、その上でこの資料の内容を学習していただくことをお勧めします。

0. 各試験共通のセキュリティ（レベル4）

ここで説明した内容は、高度系試験で出題が予想されるレベル4のセキュリティの知識で、試験種別に関係なく理解しておく必要があると思われるものです。これまでの情報処理技術者試験（レベル3）で出題されている内容も含まれていますが、概要を理解しておきましょう。基礎知識に不安のある方は、基本情報、応用情報レベルの知識から復習してください。

(1) 情報セキュリティ

① マルウェア・不正プログラム

・ボットネット、C&Cサーバ

ボットは、コンピュータの中に潜み、ネットワークを経由して受け取った命令を実行する攻撃プログラム（マルウェア）で、感染するとコンピュータが遠隔操作されてしまう。ボットネットは、ボットに感染したコンピュータ群とこれらを遠隔操作するC&Cサーバ（Command and Control server）で構成されるネットワークである。

C&Cサーバは、標的型攻撃において、ボットに感染したPCなどを攻撃者が遠隔操作するためのサーバで、ボットはPCからインターネット上のC&Cサーバにアクセスするバックドア通信（コネクトバック通信）を行い、PCへの不正な指令や新たなマルウェアを受け取らせるために使用される。

なお、ボットネットを統制して、悪意のある行為を指揮する者をボットハーダ（bot herder）という。

・ステルス技術（ポリモーフィック型、メタモーフィック型ほか）

ステルス技術とは、攻撃相手がマルウェアに感染していることに気づかないように隠ぺいする技術である。

ポリモーフィック型マルウェアは、感染ごとにマルウェアのコードを異なる鍵で暗号化することによって、パターンマッチング方式のマルウェア対策ソフトでは検知されないようにしたもの。復号するプログラム部分は変わらないので、この部分が検知されるとマルウェアとして認識されてしまう。

メタモーフィック型マルウェアは、自分自身のマルウェアのコードを書き換えることによって検知されないようにしたもの。それぞれが違うコードになるためパターンマッチングによる検知が困難になる。

・ファイルレスマルウェア

従来のマルウェアと異なり、攻撃用のプログラム（プログラムファイル）を対象となる機器に保存せずに攻撃を行うマルウェア。WindowsなどのOSに初めから組み込まれているソフトウェアやツールのコードを悪用して攻撃を実行する。通常利用するツール・プログラムが悪用されるため、マルウェア対策ソフトや専門家によつての検出が困難である。

- ・ エクスプロイトキット (Exploit Kit)

OS やアプリケーションソフトウェアの脆弱性を悪用した攻撃ができる複数のプログラムや管理機能を統合したツールが、エクスプロイトキット (Exploit Kit) である。脆弱性に関する専門的な知識がなくても、エクスプロイトキットを利用することによって、不正な活動が簡単にできてしまう。脆弱性を悪用するプログラムはエクスプロイトコードと呼ばれ、端末においてエクスプロイトコードを実行させれば、ダウンロードされたマルウェアに感染させるといったことなどが容易にできる。

② 脆弱性

- ・ バッファエラー

メモリバッファ上で処理を行うソフトウェアにおいて、確保したバッファの境界外への読み書きが可能なときに発生する脆弱性のこと。

特定の言語ではメモリアドレスの直接指定が許可されているため、他のプログラムの変数や関連するメモリの位置への読み書きが可能である。このため、攻撃者は任意のコード実行、意図する制御フローへの改ざん、機密情報の読取りやシステム破壊が可能になる。

- ・ パスワードのハードコード (hard code)

プログラムに本来記述すべきでないパスワードを直接記述することをハードコードという。暗号化されたソースプログラムの解読や、実行形式プログラムの逆アセンブルによって情報を取られてしまう。なお、パスワードの他に IP アドレス、暗号化鍵、実行環境などの情報も書き込むべきではないとされている。

- ・ レースコンディション (race condition)

排他制御の不具合などによって変数やファイルの競合が発生し、データの整合性が保証されなくなる脆弱性のこと。並列動作する複数のプログラム (プロセスやスレッド) が同じリソースに対して、ほぼ同時にアクセスしたとき、予定外の処理結果が生じる問題である。

- ・ BlueBorne (ブルーボーン)

BlueBorne は、2017 年 9 月に公開された Bluetooth (近距離無線通信の規格の一つ) の実装における複数の脆弱性情報の呼称である。Android, iOS, Windows, Linux などの複数の OS に存在し、これらの脆弱性が悪用された場合、Bluetooth の電波が届く範囲内から攻撃者によって任意のコードが実行され、デバイスを不正に操作されたり、情報を窃取されたりする可能性がある。

問題 (H30 春-AP 問 39)

ポリモーフィック型マルウェアの説明として、適切なものはどれか。

- ア インターネットを介して、攻撃者が PC を遠隔操作する。
- イ 感染ごとにマルウェアのコードを異なる鍵で暗号化することによって、同一のパターンでは検知されないようにする。
- ウ 複数の OS 上で利用できるプログラム言語でマルウェアを作成することによって、複数の OS 上でマルウェアが動作する。
- エ ルートキットを利用して、マルウェアに感染していないように見せかけることによって、マルウェアを隠蔽する。

解説

ポリモーフィック (polymorphic) は、多様あるいは多態という意味である。ポリモーフィック型マルウェアの特徴は、感染ごとにマルウェアのコードを異なる鍵で暗号化することによって、同一のパターンでは検出されないようにすることである。したがって、(イ) が適切である。なお、ポリモーフィック型マルウェアは、ミューテーション型マルウェアとも呼ばれ、ミューテーション (mutation) は、突然変異という意味である。

ア：RAT (Remote Administration Tool) 型マルウェアの説明である。

ウ：クロスプラットフォーム対応のマルウェア。マルチプラットフォーム対応のマルウェアとも呼ばれる。

エ：ステルス型マルウェアの説明である。

正解 イ

(2) 攻撃者の種類・動機, 攻撃手法

① 攻撃者の種類・動機

・ダークウェブ (Dark Web)

社会的に問題になっている違法性のある Web サービスを指す用語で、違法ドラッグや盗まれた個人情報が売買される闇マーケット、児童ポルノの共有フォーラムなどが存在する。主なダークウェブは、Tor (The Onion Router, トーア) 秘匿サービスと呼ばれる匿名化されたネットワーク上に存在するが、検索エンジンはなく、実態の解明が難しい。

・ハクティビズム (hacktivism)

ハッカーとアクティビズム (積極行動主義) を合わせた造語で、社会的・攻撃的な主義主張を目的としたハッキング活動のこと。ネットワークに侵入して、著作権の侵害、サーバの乗っ取り、ホームページの改ざんなど様々な攻撃を行う。政府機関などの Web サイトを標的にしてサイト情報を改ざんすることもある。

- ・サイバーキルチェーン (cyber kill chain)

標的型攻撃における攻撃者の動きを七つの段階に分類したもの。負の連鎖を断ち切ることを意味する軍事用語のキルチェーン (kill chain) の考え方を、サイバー攻撃に適用した。

攻撃者の動きを示す七つの段階は、偵察、武器化、デリバリー (通信方法の確立)、エクスプロイト (システム内移動)、侵入 (高権限の PC に移動)、潜伏活動、目的の実行 (情報の窃取と痕跡消し) である。

② 攻撃手法

- ・クロスサイトスクリプティング (反射型, 格納型, DOM ベース)

クロスサイトスクリプティング (XSS) は、Web アプリケーションに含まれる脆弱性を悪用した攻撃で、攻撃者が用意した悪意のあるスクリプトを、ユーザが Web ブラウザ上で実行してしまうことによって、ウイルス感染や情報の搾取などの被害が生じる。

反射型クロスサイトスクリプティングは、XSS の攻撃方法の一つで、悪意のあるスクリプトを URL に埋め込んでおき、ユーザがこの URL をクリックすることによって実行されてしまうものである。

格納型クロスサイトスクリプティングは、攻撃用のスクリプトを、Web サイトのコンテンツに事前に紛れ込ませておき、ユーザがこのコンテンツを表示するときに実行されてしまうものである。

DOM ベースのクロスサイトスクリプティングの DOM (Document Object Model) は、JavaScript などのプログラムから HTML 文書や XML 文書を利用するための API である。DOM ベースの XSS は、JavaScript による Web ページ操作に不正なデータを送り込むなどの問題がある指定をしたときに起きる XSS である。

- ・セッション ID の固定化攻撃 (Session Fixation)

セッション ID の固定化攻撃は、セッションハイジャック攻撃の一種である。悪意のある者が正規の Web サイトから取得したセッション ID を利用者の Web ブラウザへ送り込み、利用者がそのセッション ID でログインして、セッションがログイン状態に変わった後、利用者になりすますことが特徴である。

セッション ID の固定化攻撃に対する脆弱性は、Web サイト側が、ログイン前とログイン後に同じセッション ID を使い続ける点である。そのため、対策としては、利用者のログイン時に新たなセッション ID を発行することが有効となる。

- ・マルチベクトル型 DDoS 攻撃

複数の異なる DDoS 攻撃 (Distributed Denial of Service ; 分散型サービス妨害) 手法を組み合わせた攻撃が、マルチベクトル型 DDoS 攻撃である。例えば、ある Web サイトに対して、TCP 接続要求の SYN パケットを大量に送りつける TCP SYN Flood 攻撃と、HTTP GET リクエストを繰り返し送りつける HTTP GET Flood 攻撃を同時に行い、サーバに過度の負荷を掛ける攻撃がこれに該当する。

- ・ ICMP Flood 攻撃

TCP/IP 環境において、ping によってホストなどの接続性を確認するときには、ICMP (Internet Control Message Protocol) で定義されているエコー要求/応答メッセージを利用する。

この要求/メッセージである ICMP エコーパケットを攻撃対象のサーバに大量に発信することによって、サーバのリソースを枯渇させたり、サーバに至るまでの回線を過負荷にしてアクセスを妨害したりする DoS 攻撃 (サービス妨害攻撃) が、ICMP Flood 攻撃である。Ping Flood 攻撃とも呼ばれる。

- ・ Smurf 攻撃

攻撃対象が接続されているネットワークに対して、詐称した攻撃対象の IP アドレスを送信元 IP アドレスに設定した上で、ICMP エコー要求パケットをブロードキャストで送信し、大量の ICMP 応答パケットを受信させることを利用して過負荷な状態にする DoS 攻撃の一つである。

- ・ リフレクション攻撃

リフレクション (reflection) とは反射という意味で、要求に対する応答を利用した攻撃のこと。

DNS リフレクション攻撃は、DNS サーバへ問い合わせる際に、送信元 IP アドレスを攻撃対象の IP アドレスに偽装する攻撃である。送信元を偽装して、DNS サーバへ大量の問い合わせをすることによって、大量の応答パケットを攻撃対象に送りつけ、攻撃対象の負荷を増大させる。

NTP リフレクション攻撃は、時刻同期を行うために使用されるプロトコルの NTP (Network Time Protocol) を悪用した攻撃である。ボットウイルスに感染させた攻撃元の PC が、送信元 IP アドレスを攻撃対象のものに偽った NTP のリクエストを送信すると、問い合わせを受けた NTP サーバは踏み台として悪用され、攻撃対象のホストにレスポンスを返してしまう。その際、NTP サーバにおいて、monlist と呼ばれる状態確認機能が有効になっていると、レスポンスデータのサイズが大きくなるので、増幅型のリフレクション攻撃になる。

- ・ DNS 水責め攻撃 (ランダムサブドメイン攻撃)

DNS の名前解決の仕組みを使った攻撃であり、存在しないランダムなサブドメインを大量に生成し、DNS サーバに問い合わせをすることで DNS キャッシュサーバ、又は当該ドメインの権威 DNS サーバをサービス不能状態にする攻撃である。

- ・ バージョンロールバック攻撃

SSL (Secure Sockets Layer) 通信において、通信経路に介在する攻撃者が脆弱性のある通信方式を強制することによって、暗号化通信の内容を解読して情報を得る攻撃のこと。

通信経路に攻撃者が介在すると、クライアントが SSL3.0 (TLS1.0) で暗号化して通信しようとしても、攻撃者がそれを脆弱性がある SSL2.0 に改ざんすれば、クライアントとサーバは SSL2.0 で通信するようになり、解読されてしまうリスクがある。

なお、TLS1.0 の規格では SSL2.0 へのバージョンロールバックは禁止されることになっているが、サーバでクライアントの不具合を回避するオプションを使っていると、SSL2.0 へのバージョンロールバックが許可されてしまうので注意が必要である。

③ サービス及びソフトウェアの機能の悪用 (RLO (Right-to-Left Override), オープンリゾルバ, オープンリダイレクトの悪用ほか)

・ RLO

Unicode の制御文字の一つで、文字の表示順を右から左へ読むように変換するものである。例えば、ファイル名が `sample_fdp.exe` という実行形式の不正なプログラムがあるとす。OS の機能を利用してファイル名のアンダバーの後ろに制御文字の RLO を挿入すれば、アンダバー以降の文字の表示順が逆になり、ファイル名が `sample_exe.pdf` と表示される。このため、ファイルの利用者には拡張子が `pdf` に見えるが、実体は実行形式の `sample_fdp.exe` であるので、それをクリックすると不正なプログラムが実行されてしまう。このような RLO を利用する拡張子の偽装攻撃への対策としては、OS の機能によって制御文字の RLO を含むファイルは実行しない設定にしておくことが有効である。

・ オープンリゾルバ

内部のクライアントだけではなく、外部のクライアントからの再帰的な DNS クエリを受け付けて、その結果を応答する DNS サーバのこと。外部のクライアントからインターネット上のドメイン名についての名前解決を行う DNS クエリを受け付けてしまうと、DNS リフレクション攻撃や DNS キャッシュポイズニング攻撃などに悪用されるおそれがある。

・ オープンリダイレクトの悪用

HTTP リクエストを外部のドメインの URL へリダイレクト (自動的に移動) してしまう問題である。この機能を悪用すると、不正なサイトに気付かぬうちに移動させることができってしまう。対策として、システムで使用している URL 以外へのリダイレクトを制限することが行われる。

問題 (H30 秋・SC 午前Ⅱ問 4)

マルチベクトル型 DDoS 攻撃に該当するものはどれか。

- ア 攻撃対象の Web サーバ 1 台に対して、多数の PC から一斉にリクエストを送ってサーバのリソースを枯渇させる攻撃と、大量の DNS 通信によってネットワークの帯域を消費させる攻撃を同時に行う。
- イ 攻撃対象の Web サイトのログインパスワードを解読するために、ブルートフォースによるログイン試行を、多数のスマートフォンや IoT 機器などの踏み台から成るボットネットから一斉に行う。
- ウ 攻撃対象のサーバに大量のレスポンスが同時に送り付けられるようにするために、多数のオープンリゾルバに対して、送信元 IP アドレスを攻撃対象のサーバの IP アドレスに偽装した名前解決のリクエストを一斉に送信する。
- エ 攻撃対象の組織内の多数の端末をマルウェアに感染させ、当該マルウェアを遠隔操作することによってデータの改ざんやファイルの消去を一斉に行う。

解説

マルチベクトル型 DDoS (Distributed Denial of Service ; 分散型サービス妨害) 攻撃とは、複数の DDoS 攻撃手法を組み合わせた攻撃である。例えば、攻撃対象の Web サーバ 1 台に対して、多数の PC から一斉にリクエストを送ってサーバのリソースを枯渇させる攻撃と、大量の DNS 通信によってネットワークの帯域を消費させる攻撃を同時に行うことは、複数の DDoS 攻撃を行う手法を組み合わせたものなので、マルチベクトル型 DDoS 攻撃に該当する。したがって、(ア) が正しい。

イ：ボットネットから一斉に行うログイン試行は、DoS 攻撃に結びつき得るが、複数の攻撃手法を組み合わせていないので、マルチベクトル型 DDoS 攻撃とはいえない。

ウ：攻撃対象のサーバに、多数のオープンリゾルバから大量のレスポンスが同時に送り付けられるようにする攻撃は、DDoS 攻撃に該当するが、複数の攻撃手法を組み合わせていない。

エ：マルウェアに感染させた PC を遠隔操作することは、DoS 攻撃に結びつき得るが、複数の攻撃手法を組み合わせていない。

正解 ア

(3) 情報セキュリティに関する技術

① 暗号技術

・SHA-3

メッセージから、改ざんチェック用のメッセージ認証符号を生成するためのハッシュ関数には、MD5 (Message Digest Algorithm 5), SHA-1 (Secure Hash Algorithm 1), SHA-2 などがあるが、MD5, SHA-1 は攻撃方法 (解読方法) が明らかになっている。

後継の SHA-2 に対し、SHA-3 は従来のものと仕組みが大きく異なる最新のハッシュ関数で、データと状態の初期ビットの排他的論理和を取ってからブロック置換を行うスポンジ構造を採用している。

・Camellia

NTT と三菱電機が共同で、2000 年に開発した共通鍵暗号方式である。ソフトウェアで高速の実装ができ、ハードウェア実装ではコンパクトで低消費電力の実装が可能である。日本国産暗号として、初めてインターネット標準暗号 (IETF Standard Track RFC) として承認された。

・KCipher-2

株式会社 KDDI 総合研究所が開発した共通鍵暗号方式のアルゴリズムで、データをビットやバイト単位で暗号化するストリーム暗号の一つである。同じ共通鍵暗号方式の AES などと比べて、7~10 倍の速度で暗号化/復号処理が可能で、マルチメディアコンテンツサービスやブロードバンド通信サービスなどの安全性を向上させることができる。2012 年に国際標準規格 (ISO/IEC 18033-4) に採用されている。

・擬似乱数生成器 (PRNG ; Pseudo Random Number Generator)

擬似乱数はソフトウェアによって生成する乱数のことで、これを生成する機器が擬似乱数生成器である。最近のセキュアプロトコルで利用される暗号技術は、共通鍵暗号・公開鍵暗号の各技術を組み合わせるだけでなく、ハッシュ関数や擬似乱数生成技術も組み合わせられて利用されており、暗号強度を高めている。

② 認証技術

・ブラインド署名, グループ署名, トランザクション署名

ブラインド署名は、メッセージ内容を見ることなく署名することで、電子マネーや電子投票で匿名性の確保が求められるときの署名技術として応用される。

グループ署名は、グループ員の誰かが署名する行為で、誰が署名したかは分からないようになっている。グループに所属しているが匿名性も生かしたいときに利用される。

トランザクション署名は、インターネットバンキングなどで、利用者が Web ブラウザで入力した情報と、金融機関が受信した情報が同じであることを検証することで、マルウェアが通信に介入する MITB (Man-in-the-Browser) 攻撃の対策として有効である。

- ・ HMAC, フィンガプリント

HMAC (Hash-based Message Authentication Code) は, 秘密鍵, ハッシュ関数, メッセージ, シークレットデータから計算されるハッシュコードのことで, メッセージの改ざん検知に用いられるメッセージ認証符号である。

フィンガプリント (fingerprint; 指紋, 拇印) は, 公開鍵証明書が改ざんされていないことを証明するデータのことである。

- ・ パスワードレス認証 (FIDO; Fast IDentity Online, ファイド)

パスワードを入力せずに本人認証をすること。スマートフォンや PC に含まれる認証デバイスに生体情報を登録しておき, 守秘性の高い生体情報をネットワーク上でやり取りせずに認証することができる。従来から問題になっていたパスワードの漏えいや不正利用, パスワード管理の煩雑さから解放されるメリットがある。

③ 公開鍵基盤

- ・ VA (Validation Authority; 検証局)

VA は, PKI (Public Key Infrastructure; 公開鍵基盤) を構成する要素の一つで, デジタル証明書の CRL (Certificate Revocation List; 証明書失効リスト) を管理して, 失効状態についての問合せに応答するという役割を担っている。失効状態の確認には, CRL ファイルをダウンロードする方法, あるいは OCSP (Online Certificate Status Protocol) を用いて指定したデジタル証明書の失効状態を問い合わせる方法の二つがある。

- ・ ITU-T X.509

ITU-T X.509 は, 証明書の標準として, ITU-T (国際電気通信連合 電気通信標準化部門) が策定したもので, ISO/IEC の国際標準として規定されている。X.509 証明書は用途によって次の種類があり, 一般に「証明書」という場合は「公開鍵証明書」のことを指す。

[参考資料; IPA PKI 関連技術情報 3.3 電子証明書]

<https://www.ipa.go.jp/security/pki/033.html>

公開鍵証明書 (Public Key Certificate) ……公開鍵とその所有者を証明する。

属性証明書 (Attribute Certificate) ……公開鍵証明書で証明された人に対して, その人が所有する権限や役割を証明する。公開鍵証明書と組み合わせて使用する。

特定証明書 (Qualified Certificate) ……人 (自然人) に対して発行することを目的とした証明書で, 電子署名に用いられる。

この中の公開鍵証明書は, 発行する対象によって次のように分類できる。

CA 証明書 ……CA に対して発行する証明書。CA 自身の秘密鍵で署名した自己署名証明書と, 他の CA に発行された証明書がある。

エンドエンティティ証明書 ……PKI ユーザに対して発行する証明書。Web クライアントや Web サーバ, VPN ルータなどに利用される。

問題 (R01 秋-SC 午前II問1)

認証処理のうち、FIDO (Fast IDentity Online) UAF (Universal Authentication Framework) 1.1 に基づいたものはどれか。

- ア SaaS 接続時の認証において、PIN コードとトークンが表示したワンタイムパスワードとを PC から認証サーバに送信した。
- イ SaaS 接続時の認証において、スマートフォンで顔認証を行った後、スマートフォン内の秘密鍵でデジタル署名を生成して、そのデジタル署名を認証サーバに送信した。
- ウ インターネットバンキング接続時の認証において、PC に接続されたカードリーダーを使って、利用者のキャッシュカードからクライアント証明書を読み取って、そのクライアント証明書を認証サーバに送信した。
- エ インターネットバンキング接続時の認証において、スマートフォンを使い指紋情報を読み取って、その指紋情報を認証サーバに送信した。

解説

FIDO (ファイド) は、パスワードに依存しない、あるいはパスワードへの依存を少なくすることを目的とする認証方式の規格である。現在、FIDO には FIDO UAF (Universal Authentication Framework) 1.1, FIDO U2F (Universal Second Factor) 1.2, FIDO2 の三つの規格がある。これらのうち、FIDO UAF 1.1 と FIDO2 は、パスワードを使わないパスワードレス認証方式である。

FIDO UAF 1.1 は、主にスマートフォンの利用を想定した規格で、SaaS 接続時の認証において、スマートフォンで顔認証を行った後、スマートフォン内の秘密鍵でデジタル署名を生成し、そのデジタル署名を認証サーバに送信するので (イ) が正しい。

ア：UAF 1.1 の特徴は、認証器を用いて利用者認証をローカルで行うことであり、PIN コードのような利用者の認証情報は認証サーバに送信されない。

ウ：UAF 1.1 で認証器を事前に登録する際、認証器と対応する公開鍵証明書を認証サーバに登録するが、利用者に対応するクライアント証明書は認証サーバに送信されない。

エ：(ア) と同様に、生体認証は認証器を用いてローカルで実行され、利用者の指紋情報は認証サーバに送信されない。

正解 イ

問題 (H30 春・SC 午前Ⅱ問 8)

X.509 における CRL (Certificate Revocation List) に関する記述のうち、適切なものはどれか。

ア PKI の利用者は、認証局の公開鍵が Web ブラウザに組み込まれていれば、CRL を参照しなくてもよい。

イ 認証局は、発行した全てのデジタル証明書の有効期限を CRL に登録する。

ウ 認証局は、発行したデジタル証明書のうち、失効したものは、シリアル番号を失効後 1 年間 CRL に登録するよう義務付けられている。

エ 認証局は、有効期限内のデジタル証明書のシリアル番号を CRL に登録することがある。

解説

CRL (Certificate Revocation List ; 証明書失効リスト) は、デジタル証明書の有効期限内に秘密鍵が漏えいした場合などに、そのデジタル証明書を認証局 (CA) が失効させるために発行するものである。したがって、認証局は、有効期限内のデジタル証明書のシリアル番号を CRL に登録することがあると記述された (エ) が正しい。

ア：CRL を参照するのは、デジタル証明書が失効しているかどうかを確認するためであり、認証局の公開鍵が Web ブラウザに組み込まれているかどうかとは、関係しない。

イ：有効期限はデジタル証明書に記載される内容であり、CRL に登録されるものではない。

ウ：CRL に登録する期限は、デジタル証明書に記載された有効期限によって決まる。つまり、有効期限内にあるものは CRL に登録される必要があるが、有効期限が切れるとその時点で破棄されるので、失効後 1 年間という義務があるわけではない。

正解 エ

(4) 情報セキュリティ組織・機関

① 情報セキュリティ組織

- ・ CSIRT (Computer Security Incident Response Team ; シーサート)

行政機関や企業内においてコンピュータやネットワークで発生する問題の監視・原因解析・影響調査などを実施する組織の総称。日本でも 1996 年に JPCERT/CC が発足しており、国内外で発生している問題に関する情報の配信などを行っている。

- ・ 組織への設置が推奨されている窓口

企業・団体など組織が設置すべきメールボックスについて、公開された技術仕様である RFC2142 で、組織内の担当部門とインターネットの電子メールで連絡する場合に利用するメールアドレス (メールボックス名@ドメイン名) について説明されている。

ネットワーク運用に関連するメールボックス名に関しては、「運用に関するアドレスは、その組織のインターネットサービスに対する難点を経験した顧客やプロバイダなどが連絡を取り合うことを想定している」として、次の三つ (abuse@ドメイン名, noc@ドメイン名, security@ドメイン名) が挙げられている。

メールボックス	分野	取扱い
ABUSE	顧客関連	公共における不適当なふるまい
NOC	ネットワーク管理	ネットワーク・インフラストラクチャ
SECURITY	ネットワークセキュリティ	セキュリティに関する報告又は問合せ

- ・ 脆弱性報奨金制度 (Bug Bounty ; バグバウンティ)

公開したプログラムやシステムのバグを発見したら報奨金を支払う制度のこと。現在ではこの制度を実施する企業が増えており、健全な目的でプログラムやシステムのバグ・脆弱性を調べるホワイトハッカーの活躍が大きい。

② 情報セキュリティ機関

- ・ 内閣サイバーセキュリティセンター (NISC ; National center of Incident readiness and Strategy for Cybersecurity)

NISC は、2014 年に制定されたサイバーセキュリティ基本法に基づき内閣官房に設置された組織であり、サイバーセキュリティ政策に関する総合調整を行いつつ、“世界を率先する” “きょうじん強靱” で “活力ある” サイバー空間の構築に向けた活動を行っている。

- ・ CRYPTREC (Cryptography Research and Evaluation Committees)

CRYPTREC は、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法や運用法を調査・検討するプロジェクトである。活動は、総務省及び経済産業省、IPA、NICT (独立行政法人 情報通信研究機構) などによって行われている。また、公募された暗号技術や業界で広く利用されている暗号技術を評価・検討し、安全性及び実装性能ともに優れ

たものを選択して、電子政府における調達のための推奨すべき暗号のリスト（電子政府推奨暗号リスト）を決定し公表している。

- ・米国国立標準技術研究所（NIST；National Institute of Standards and Technology）
科学技術分野における計測と標準に関する研究を行う米国商務省に属する政府機関である。共通鍵暗号方式として広く利用されている AES は NIST が標準化した。
- ・JPCERT/CC（Japan Computer Emergency Response Team Coordination Center；
一般社団法人 JPCERT コーディネーションセンタ）
JPCERT/CC は、コンピュータセキュリティインシデントについて、日本国内に関する報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言、などを技術的な立場から行っている機関である。
- ・サイバー情報共有イニシアティブ（J-CSIP；Initiative for Cyber Security Information sharing Partnership of Japan）
サイバー情報共有イニシアティブは、経済産業省がサイバー攻撃による被害拡大の防止を図る目的から、重要インフラで利用される機器の製造業者を中心に、参加組織間の情報共有と早期対応の場として発足させた体制である。

③ セキュリティ関連制度・規格

コンピュータ不正アクセス届出制度、コンピュータウイルス届出制度、ソフトウェア等の脆弱性関連情報に関する届出制度のほか、ソフトウェアの脆弱性の取扱いに関する国際標準として、次の規格が制定されている。日本の企業が海外展開を図り、顧客から脆弱性対応に関する取組みについて説明を要求された場合に、国際標準に対応した体制・取組みを行っていることを説明することで、円滑な理解が得られることが期待できる。

- ・ソフトウェア製品開発者の脆弱性開示（ISO/IEC 29147:2018）
ソフトウェア製品に関わる事業者（製品開発者、オンラインサービス事業者、中間ベンダなどを指す）の脆弱性に関する社外とのやり取り（外部からの脆弱性に関する情報の受領、ユーザに対する脆弱性対策のアドバイザリ配布など）を規定している。
- ・脆弱性情報取扱手順（ISO/IEC 30111:2019）
ベンダの社内での脆弱性取扱いのプロセス（脆弱性の検証、脆弱性対策の開発等）の指針を提供している。

問題 (H30 春-SC 午前II問 10)

サイバー情報共有イニシアティブ (J-CSIP) の説明として、適切なものはどれか。

- ア サイバー攻撃対策に関する情報セキュリティ監査を参加組織間で相互に実施して、監査結果を共有する取組み
- イ 参加組織がもつデータを相互にバックアップして、サイバー攻撃から保護する取組み
- ウ セキュリティ製品のサイバー攻撃に対する有効性に関する情報を参加組織が取りまとめ、その情報を活用できるように公開する取組み
- エ 標的型サイバー攻撃などに関する情報を参加組織間で共有し、高度なサイバー攻撃対策につなげる取組み

解説

サイバー情報共有イニシアティブ (J-CSIP) は、経済産業省がサイバー攻撃による被害拡大の防止を図る目的から、重要インフラで利用される機器の製造業者を中心に、情報共有と早期対応の場として発足させた体制である。このため、J-CSIP の説明としては、標的型サイバー攻撃などに関する情報を参加組織間で共有し、高度なサイバー攻撃対策につなげる取組みが該当し、(エ) が正しい。なお、情報を集約するハブ機能は、IPA (独立行政法人 情報処理推進機構) が担っている。

ア：J-CSIP は、高度なサイバー攻撃対策につなげる取組みであり、監査結果を共有する取組みではない。

イ：サイバー攻撃から保護する取組みでもない。

ウ：サイバー攻撃に対する有効性に関する情報を活用できるように公開する取組みでもない。

正解 エ

(5) 技術的セキュリティ対策

① マルウェア検出手法

・パターンマッチング法

既知のマルウェア (ウイルス) を検出する最も一般的な方法である。対策用の検索エンジン (ソフトウェア) が、検査対象のソフトウェアとマルウェア定義ファイル (パターンファイル) を照合し、検知する。

・ビヘイビア法

パターンマッチング法が新種のマルウェアに対しては無力であるため、その対応方法として考えられたのがビヘイビア法 (振り舞い監視法) である。これは、検査対象となるソフトウェアを実際に動作させ、そのときに生じる現象からウイルスであるかどうかを判断するものである。このため、ウイルス感染や発病によって生じるデータの読み込みと書き込み動作・通信などの変化を監視して、感染を検出することができる。

- ・ヒューリスティック法

ビヘイビア法と同様に挙動（動作）によってウイルスを検出する方法である。ウイルスの挙動としてよく見られる動作を動作パターンとして登録しておき、その動作パターンに一致する挙動を検出する。

② 秘密分散（電子割符）

- ・秘密分散

秘密分散は、機密情報を複数のシェアという単位に分割し、全てのシェアが揃った場合に機密情報を参照することができるようにする考え方である。個々のシェアの内容は意味をもたないため、仮に漏えいしても機密情報の内容を解読することはできない。

- ・電子割符

秘密分散の考え方に基づく暗号技術の一つで、この方法で分割された情報のことを電子割符（でんしわっぷ）といい、分割された情報を集めて元の情報を復元する。複数人の協力があって初めて得られる秘密情報の隠ぺいに用いられる。

③ 電子メール・Web のセキュリティ

- ・スパム対策（ベイジアンフィルタリング、送信元ドメイン認証機能ほか）

ベイジアンフィルタリングは、ベイズ理論に基づいて迷惑メールを検出するフィルタリング手法の一つで、まず、利用者が振り分けた迷惑メールから特徴を学習し、特徴的な単語の出現確率などを基に、迷惑メールかどうかを統計的に解析し判定する。そして、迷惑メールと判定した際には、自己学習して単語の出現確率を更新していく。ベイズ理論は、現実の世界から集められたデータに基づいて推測を行い、データの数が多ければ多いほど、より確実な推測を引き出せるという考え方である。

送信元ドメイン認証機能は、この機能がないと送信元メールアドレスを偽装したスパムメールを受信してしまう可能性がある。送信元メールアドレスのドメイン名から DNS に問合せを行い、SPF レコードから正規の IP アドレスを調べる SPF 認証や、送信側のメールサーバが電子メールに付与したデジタル署名を、受信したメールサーバが検証して、送信元を認証する DKIM (Domainkeys Identified Mail) がある。

- ・メール無害化

標的型メール攻撃などの手口が巧妙化し、不審に思わないうちにマルウェアに感染する被害が増えてきている。この対策として行われているのがメール無害化で、具体的には、HTML メールテキスト化、URL リンクの削除、添付ファイルのウイルス・マクロの除去、添付ファイルの画像変換、メールサーバでのチェックなどを行う。

④ ハードウェアのセキュリティ

・TPM (Trusted Platform Module ; セキュリティチップ)

TPM は、PC などの機器に搭載され、公開鍵ペアや共通鍵の元になる乱数の生成やハッシュ演算及び暗号化処理を行うセキュリティチップである。TPM 内の鍵などの秘密情報を外部から読み出せない耐タンパ性をもっている。

・SED (Self Encrypting Drive ; 自己暗号化ドライブ)

暗号化機能をもつハードディスクやソリッドステートドライブのことを自己暗号化ドライブという。ハードウェア的に全てのドライブ内容を暗号化し、取り出すときに復号される。特長としては、暗号化をハードウェアで行うため速度低下がない、自動的に暗号化／復号するので利用者が意識する必要がない、といったことが挙げられる。

問題 (H29 春-SC 午前II問 4)

PC などに内蔵されるセキュリティチップ (TPM : Trusted Platform Module) がもつ機能はどれか。

- ア TPM 間での共通鍵の交換 イ 鍵ペアの生成
ウ デジタル証明書の発行 エ ネットワーク経由の乱数送信

解説

TPM (Trusted Platform Module) は、PC のマザーボードなどに搭載されるセキュリティチップのことで、一般に公開鍵暗号の鍵ペアを生成したり、乱数を発生させたり、OS が生成した共通鍵を暗号化して保存したりするほか、耐タンパ性を有するという特徴をもつ。したがって、(イ) が正しい。

その他の記述には、次のような誤りがある。

ア：TPM 内では、データの暗号化に使用する共通鍵は生成しない。共通鍵は、TPM が生成した乱数を基にして、OS が生成する。

ウ：デジタル証明書の発行は、認証局 (CA) の役割であり、TPM が発行するものではない。

エ：TPM には、コンピュータの外部と通信する機能はない (ネットワーク経由で乱数を送信する機能はない)。

正解 イ

2. エンベデッドシステムスペシャリスト

エンベデッドシステムスペシャリストを受験される方は、セキュリティ技術評価の「制御システムのセキュリティ評価」と、セキュリティ実装技術「IoTシステムの設計・開発におけるセキュリティ」の内容を理解しておく必要があります。

まず、「制御システムのセキュリティ評価」の内容としては、組織の産業用オートメーション及び制御システム（IACS；Industrial Automation and Control System）を対象として、制御システム及び重要インフラのセキュリティの仕組みを理解する必要がありますが、ここではポイントとなる事項として、CSMS 適合性評価制度、CSMS 認証基準（IEC 62443-2-1）、EDSA 認証について説明します。

また、「IoTシステムの設計・開発におけるセキュリティ」の内容としては、IoTシステム、IoT機器の設計・開発について策定された各種の指針・ガイドラインを理解する必要がありますが、ここでは、シラバスの用語例で挙げられている、つながる世界の開発指針、IoT開発におけるセキュリティ設計の手引き、IoTセキュリティガイドラインについて説明します。

(1) 制御システムのセキュリティ評価

① CSMS 適合性評価制度

CSMS（Cyber Security Management System）適合性評価制度は、産業用オートメーション及び制御システム（IACS；Industrial Automation and Control System）を対象としたサーバーセキュリティマネジメントシステムに対する第三者認証制度である。組織が構築・運用するCSMSが、CSMS認証基準に適合しているかどうかを認証審査し登録する認証機関、審査員の資格を付与する要員認証機関、及びこれらの各機関がその業務を行う能力を備えているかを見る認定機関からなる総合的な運用の仕組みである。

IACSは、従来、外部とは隔離された専用システムで構築されており、セキュリティ上の脅威は一部の人的・物理的脅威以外はほとんど意識されてこなかった。しかし、近年、業務システムとの連携、外部情報の活用、工場機器のIoT化などの進展によって、IACSがサイバー攻撃の対象となり得る状況になり対策が必要となった。サイバー攻撃を受けた場合、社会インフラやビジネスに深刻な影響を及ぼすことになる。

② CSMS 認証基準（IEC 62443-2-1）

制御システムにおけるCSMSを確立、実施、維持及び改善するための一般要求事項を定めた認証基準である。規格のIEC 62443-2-1：2010は、「Industrial communication networks - Network and system security - Part2-1: Establishing an industrial automation and control system security program」である。

③ EDSA 認証

EDSA（Embedded Device Security Assurance；組込みデバイスセキュリティ保証）認証とは、ISCI（ISA Security Compliance Institute）^{注1}が提供している認証プログラムで、制御シ

システムを構成する制御機器やシステム全体が、ISA-SP99 注2に基づいた制御システムのセキュリティ標準に準拠しているかを認証するプログラムである。

注1 ISCI は、システムに関わる規格の標準化及び普及啓発活動を実施する国際計測学会（ISA；International Society of Automation）のメンバを中心として評価認証を担う組織である。

注2 ISCI がまとめたセキュリティ規格である。

問題 (H30 秋-SC 午前II問 8)		
EDSA 認証における評価対象と評価項目について、適切な組みはどれか。		
	評価対象	評価項目
ア	組込み機器である制御機器	組込み機器ロバストネス試験
イ	組込み機器である制御機器が運用されている施設	入退室管理の評価
ウ	複数の制御機器から構成される制御システム	^{ぜい} 脆弱性試験
エ	複数の制御機器から構成される制御システムを管理する組織	セキュリティポリシーの評価

解説

EDSA (Embedded Device Security Assurance) 認証は、制御機器のセキュリティ保証に関する認証制度で、制御システムの組込み機器である制御機器を評価対象とする。そして、EDSA 2.0.0 では、セキュリティ開発ライフサイクルプロセス評価、組込み機器機能セキュリティ評価、組込み機器ロバストネス (堅牢性) 試験という三つを評価項目として挙げている。したがって、評価対象と評価項目の組みとしては、(ア) が適切な組みとなる。

組込み機器とは、組込みソフトウェアを実行する特殊目的のデバイスであり、産業プロセスを直接監視し、制御し、又は作動させるように設計されたものと説明されている。例えば、PLC (Programmable Logic Controller)、フィールドセンサデバイス、SIS (Safety Instrument System) などがある。また、組込み機器ロバストネス試験では、例えば、正常データと同時に様々な異常データを送信するファジングテストを実施して脆弱性の有無を評価する。EDSA 認証制度のスキームは、ISA (The International Society of Automation；国際計測制御学会) によって開発されている。

イ：(エ) の CSMS 認証に含まれる組み
 ウ：制御システムを対象とする SSA (System Security Assurance) 認証における組み
 エ：制御システムを運用する組織を対象とする CSMS (Cyber Security Management System) 認証における組み

正解 ア

(2) IoT システムの設計・開発におけるセキュリティ

① つながる世界の開発指針

IoT 製品の利用者や製品の安全性・セキュリティを脅かすリスクの発生に対して、開発者が考慮すべきリスクや対策に関する検討結果を取りまとめ指針として明確化したものである。指針の内容は、IPA の Web サイト上に公開されている（以下、参考 URL は 2019 年 12 月 12 日現在のもの）

- ・「つながる世界の開発指針」

<https://www.ipa.go.jp/sec/reports/20160324.html>

- ・「つながる世界の開発指針（第 2 版）」

<https://www.ipa.go.jp/sec/reports/20170630.html>

② IoT 開発におけるセキュリティ設計の手引き

IoT の構成要素を「サービス提供サーバ・クラウド」「中継機器」「システム」「デバイス」「直接相互通信するデバイス」の五つに分類して定義し、IoT の全体像をモデル化し、各構成要素におけるセキュリティ上の課題の抽出・整理を行ったものである。IPA の Web サイト上に公開されている。

- ・「IoT 開発におけるセキュリティ設計の手引き」

<https://www.ipa.go.jp/security/iot/iotguide.html>

③ IoT セキュリティガイドライン

IoT セキュリティガイドラインは、経済産業省及び総務省主催の「IoT 推進コンソーシアム IoT セキュリティワーキンググループ」が策定したガイドラインで、対象者を、供給側の経営者、機器の生産者、サービス提供者、利用側の企業利用者、一般利用者として、IoT セキュリティの考え方や留意事項、実現方法など、セキュリティ確保の観点から必要な取組みを示したものである。

経済産業省と総務省の Web サイトに個別に公開されている。

- ・「IoT セキュリティガイドライン」（経済産業省）

<https://www.meti.go.jp/press/2016/07/20160705002/20160705002.html>

- ・「IoT セキュリティガイドライン」（総務省）

http://www.soumu.go.jp/main_content/000428393.pdf

問題 (ITEC 作成 予想問題 802897)

IoT システムや IoT 機器について策定された“IoT セキュリティガイドライン”に関する記述として、適切なものはどれか。

- ア IoT 関連システムや機器によるセキュリティ被害を削減するための具体的なセキュリティ対策をまとめたものである。
- イ IoT 関連システムや機器の開発に携わる人材を想定したガイドラインであり、一般利用者は対象としていない。
- ウ IoT 関連システムや機器の開発を促進するために、セキュリティ確保の観点から必要な取組みを示している。
- エ IoT 関連システムや機器へのサイバー攻撃を想定して、様々な事例における法的責任の所在を明確に示している。

解説

IoT セキュリティガイドラインは、IoT 機器やシステム、サービスの供給者や利用者が自己の役割を認識しつつ、分野ごとの性質に応じたセキュリティ確保の取組みが促進されることを期待して、総務省と経済産業省によって策定されたものである。

策定目的の一つとして、「IoT 機器やシステム、サービスについて、関係者がセキュリティ確保の観点から求められる基本的な取組みを明確化することによって、産業界による積極的な開発等の取組みを促す」という主旨のことが述べられており、(ウ) が正解である。

ア：具体的な対策をまとめたものではなく、役割に応じたセキュリティ対策の指針や要点を示したものである。そして、その内容を基に、それぞれの対象者において、守るべきものやリスクの大きさなどを踏まえ、役割・立場に応じて適切なセキュリティ対策の検討が行われることを期待している。

イ：IoT セキュリティガイドラインには、一般利用者向けのルールも記載されている。

エ：被害発生時の法的責任を明らかにするのではなく、取り組むべき IoT のセキュリティ対策の認識を促し、関係者相互の情報共有を促すための材料を提供することを目的としている。

正解 ウ