



**JP-RISSA**

情報処理安全確保支援士会



# 情報処理技術者試験 出題予想 令和2年度春期 AP・SC高度「午前」

村山 直紀（むらやま・なおき JP-RISSA理事）  
情報処理安全確保支援士（登録番号第000029号）

# 「セキュリティ」厚めで話します

情報処理技術者試験・情報処理安全確保支援士試験

情報セキュリティマネジメント試験・高度試験・情報処理安全確保支援士試験における人材像・出題範囲・シラバス等の改訂について（新技術への対応、セキュリティ強化など）

2019年11月5日掲載  
2019年11月25日更新

[https://www.jitec.ipa.go.jp/1\\_00topic/topic\\_20191105.html](https://www.jitec.ipa.go.jp/1_00topic/topic_20191105.html)（2019/12/18確認）

- 想定する対象者：下記の受験予定者と、改訂の概要を知りたい方
  - 応用情報技術者（AP）試験
  - 情報処理安全確保支援士（SC）試験
  - 春期実施の高度（AU,DB,ES,PM）試験

+ 知識をアップデートしたい  
登録セキスペ

- 本資料は、担当者（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、当該試験の実施団体（以下「IPA」）の活動とは関係ありません。
- 本資料の内容について万全を期して作成しましたが、IPAが公表する資料と本資料との間で記載内容に相違がある場合は、IPAが公表する資料の記載が優先します。
- 本資料は、本資料の利用者の自己責任での御利用をお願いします。本資料の利用によって利用者が受けた金銭その他の損害の責任を、担当者ならびに情報処理安全確保支援士会（JP-RISSA）は一切負いません。
- 担当者による予想が外れることは割とあります。



# 担当者 村山直紀

- 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～）
- コンサルティング業務，資格試験対策書の執筆・監修（H18～）



- 情報処理安全確保支援士，電気通信主任技術者（伝交・線路）ほか
- 修士（学術）電気通信大学
- IEEE，情報処理学会，社会情報学会 各会員



# 今回の改訂の概要

- 国策に沿い、令和2年度春期からは下記の出題が強化されます。
  - ① 第4次産業革命関連技術（AI、ビッグデータ、IoT）などの新技術への対応
  - ② セキュリティの出題強化

ドキュメント	内容	改訂を実施した試験区分
試験要綱	人材像（対象者像、業務と役割、期待する技術水準）	ST、SA、NW、DB、ES、SC
	午後Ⅰ試験の選択方法・配点割合	ES
	午前の出題範囲（午前Ⅱ試験の出題分野）	ST、SA、PM、DB、ES、SM、AU その他、形式的な変更（*1）： 基本情報技術者試験（FE）、応用情報技術者試験（AP）、高度試験の午前Ⅰ試験
	午後の出題範囲	ST、SA、NW、ES、AU、SC
シラバス		SG、ST、SA、NW、DB、ES、SM、AU、SC（*2）SC追補版（午前Ⅱ）

[https://www.jitec.ipa.go.jp/1\\_00topic/topic\\_20191105.html](https://www.jitec.ipa.go.jp/1_00topic/topic_20191105.html)（2019/12/18確認）

- SC試験 シラバスの改訂版（Ver.2.0）が公開されました。

# まずは“レベル3”の話から

**応用情報技術者（AP）試験  
「午前」対策**

**情報処理安全確保支援士（SC）試験  
春期実施の高度（AU,DB,ES,PM）試験  
「午前Ⅰ」対策**

# AP「午前」・SC高度「午前Ⅰ」①

- 今春以降「中分類11：セキュリティ」の出題数に変化は？  
→ 多分ない — 高度「午前Ⅱ」では増えます（詳しくはp.13以降を）
- じゃあ「○3」から「◎3」に変わったコレ↓とかコレ↓は、なに？

『試験要綱Ver.4.4（変更箇所表示版）』（IPA[2019]p.21）より

	SG 午前	FE 午前	AP 午前	高度 午前Ⅰ	...
11 セキュリティ	◎ 2	<del>○ 2</del> ◎ 2	<del>○ 3</del> ◎ 3	<del>○ 3</del> ◎ 3	

SG（変わらず）

FE 「○2」 → 「◎2」

AP「午前」・SC高度「午前Ⅰ」  
「○3」 → 「◎3」



# AP「午前」・SC高度「午前Ⅰ」②

ドキュメント	内容	改訂を実施した試験区分
試験要綱	人材像（対象者像、業務と役割、期待する技術水準）	ST、SA、NW、DB、ES、SC
	午後Ⅰ試験の選択方法・配点割合	ES
	午前の出題範囲（午前Ⅱ試験の出題分野）	ST、SA、PM、DB、ES、SM、AU その他、形式的な変更（*1）： 基本情報技術者試験（FE）、応用情報技術者試験（AP）、高度試験の午前Ⅰ試験
	午後の出題範囲	ST、SA、NW、ES、AU、SC
シラバス		SG、ST、SA、NW、DB、ES、SM、AU、SC（*2）SC追補版（午前Ⅱ）

（\*1）「試験要綱」内の午前の出題範囲（午前Ⅱ試験の出題分野）において、FE、AP、高度試験の午前Ⅰ試験の非重点分野（○）と重点分野（◎）の示し方を一部変更します。従来、中分類1から23までの全てを一まとめで非重点分野（○）として示していましたが、「中分類11：セキュリティ」を他分野と分けて、重点分野（◎）として示すように変更しました。出題においてセキュリティを重視していることが本ドキュメントからも読み取れるようにするための形式的な変更です。

[https://www.jitec.ipa.go.jp/1\\_00topic/topic\\_20191105.html](https://www.jitec.ipa.go.jp/1_00topic/topic_20191105.html)（2019/12/18確認）

「…従来、中分類1から23までの全てを一まとめで非重点分野（○）として示していましたが、「中分類11：セキュリティ」を他分野と分けて、重点分野（◎）として示すように変更しました。出題においてセキュリティを重視していることが本ドキュメントからも読み取れるようにする

ための**形式的な変更**です。」

## 「セキュリティ」の出題は、すでに強化済みだった！

AP「午前」10問／80問（高度「午前Ⅰ」4問／30問）って、どんな“強さ”？

- ・ 10問／80問 = 「プロジェクトマネジメント」 + 「サービスマネジメント」 + 「システム監査」
- ・ 10問／80問 = 「データベース」 + 「ネットワーク」

この“強い”現状の追認  
が、今回の表記変更（「○3」→「◎3」）です。

## ● 今回の改訂で強化される分野のLv.3出題予想

- ①「AI」（微積・行列【→p.11】，回帰分析，チューリングテスト，主な機械学習アルゴリズムとその特徴（多層パーセプトロン【→p.12】，誤差逆伝播法，敵対的生成ネットワーク（GAN）））
- ②「ビッグデータ」（データレイク，KVS，NoSQL，BASE特性，CAP定理）
- ③「IoT」（MQTT，LPWA，RISC-V，コネクテッドカー，自動運転の5段階のレベル）
- ④「DX」（RPA，アジャイル（特にスクラム） ， DevOps，コンテナとマイクロサービス）
- ⑤ 上記①～④ × 「セキュリティ」（学習結果やアルゴリズムの窃取による模倣，匿名化，IoTと攻撃（サイドチャネル攻撃の種類名，Insecam，Mirai，スマートスピーカやセンサへの虚偽の入力），“つながる社会” のリスク（協力会社等からの攻撃や情報漏えい，サプライチェーンリスク【→p.27「サプライチェーン攻撃」】）

これらの対策：記憶が曖昧ならば軽くググる（概要を覚える），でOK

## ● ナウい話（前ページ以外）のLv.3出題予想

- X-Tech（FinTech, EdTech, LegalTech等）、IPv6、HTTP/2、SD-WAN、5G、Wi-Fi 6、RESTとJSON形式、『JIS X 25010（システム及びソフトウェア製品の品質要求及び評価）』、『PMBOK® 第6版』、『JIS Q 21500:2018（プロジェクトマネジメントの手引）』、会計基準の「収益認識基準」【→p.34】、ITIL® 4、平成30年改訂『システム監査（or システム管理）基準』、スマートコントラクトとブロックチェーン、情報銀行、製造実行システム（MES）、改正民法【→p.34「契約不適合責任」】、技術者倫理

## ● セキュリティのLv.3出題予想

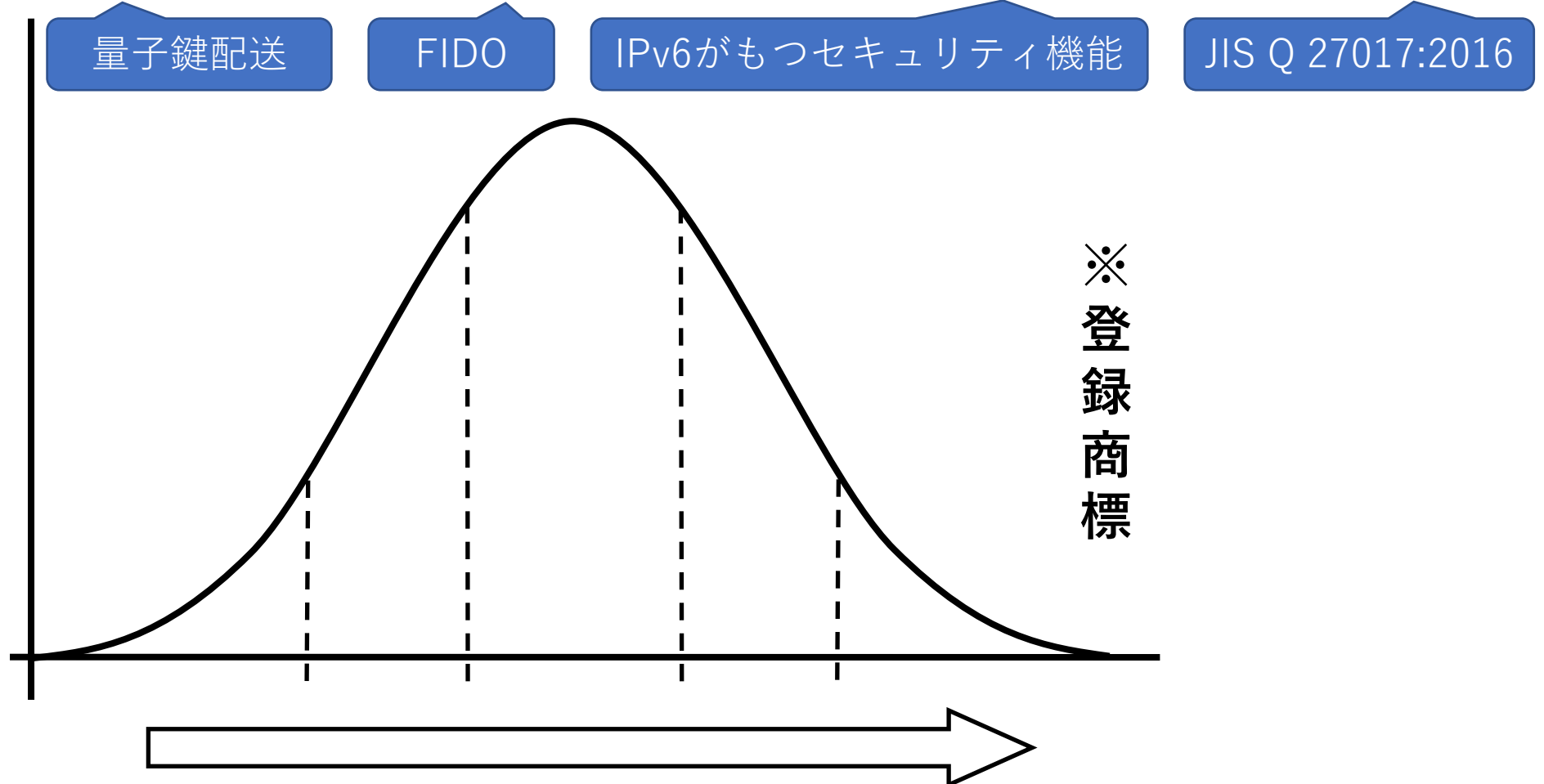
- 量子鍵配送、FIDO、WPA3、キャプティブポータル、DoT/DoH、ゼロトラスト（SC試験（Lv.4）では NIST SP 800-207(Draft) “Zero Trust Architecture”）、OSINT、SIEM、EDR、CASB、クラウドセキュリティ『JIS Q 27017:2016』の概要、クラウド側の完全性・可用性（データ消失への備え）、サイバーキルチェーン

これらの対策：記憶が曖昧ならば軽くググる（概要を覚える）、でOK



# 「出題のライフサイクル<sup>®</sup>」

- 「午前」の出題は、ほぼ下記の順で“お下がり”されてきた
  - 高度午前Ⅱ（バツ） → 高度午前Ⅱ（正解） → AP・高度午前Ⅰ → FE・SG午前



# ところが (R1秋FE午前問4 答ア)

問4  $a$  及び  $b$  を定数とする関数  $f(t) = \frac{a}{t+1}$  及び  $g(t) = \frac{b}{t^2-t}$  に対して、 $\lim_{t \rightarrow \infty} \frac{g(t)}{f(t)}$  はどれか。ここで、 $a \neq 0$ 、 $b \neq 0$ 、 $t > 1$  とする。

ア 0                      イ 1                      ウ  $\frac{b}{a}$                       エ  $\infty$

- 上記は「AI」関連の出題だと分析された
  - 高度試験「午前Ⅱ」を含め、極限の記号を過去15年で見た記憶がない
    - ならばAP「午前」問4（高度「午前Ⅰ」問2）は“行列の積”か“掃出法”ぐらいいは出す…？
    - シラバス上、AP「午前」に出ても文句を言えなくなった（赤字が昨年追記された箇所）

朝イチ組は  
目を通そう！

## (2) 数値計算

連立一次方程式の解法など、数値計算に関する基本的な内容を理解する。

用語例 線形代数、スカラ、ベクトル、固有値、固有ベクトル、行列、逆行列、単位行列、転置行列、等差数列、等比数列、フィボナッチ数列、対数、三角関数、掃出法、近似解法、収束、誤差

『情報処理技術者試験 - 応用情報技術者試験 (レベル3) シラバス (Ver 6.0) -』 (IPA[2019]p.3) より

## ● よっ！ シンギュラリティ！

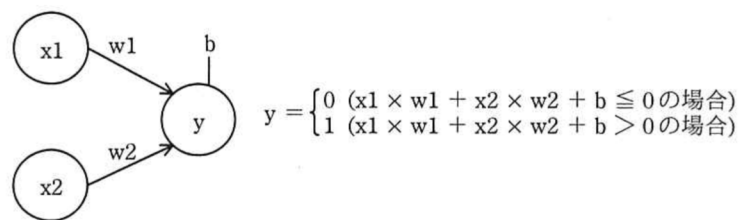


図3 単純パーセプトロンの模式図とノードの演算式

[3層パーセプトロンのプログラム]

3層パーセプトロンの機能を実装するプログラム `three_layer_perceptron` を作成する。表2に示したものに加えて、このプログラムで使用する定数及び配列を表4に、プログラムを図6に示す。`three_layer_perceptron` は、論理演算の入力値の全ての組合せ  $X$  から論理演算の出力値  $Y$  を計算する。

表4 プログラム `three_layer_perceptron` で使用する定数及び配列

名称	種類	説明
NM	定数	中間ノードの数を表す定数。 図5では、中間ノードが $m1$ 及び $m2$ の二つなので、2となる。
M	配列	中間ノードの演算結果を格納する2次元配列。
WM	配列	中間ノードのアーキがもつ重みの値を表す2次元配列。 表3の排他的論理和では、 $[[0.5, 0.5], [-0.5, -0.5]]$ を与える。
BM	配列	中間ノードのバイアスの値( $b$ )を入れる1次元配列。 表3の排他的論理和では、 $[-0.2, 0.7]$ を与える。

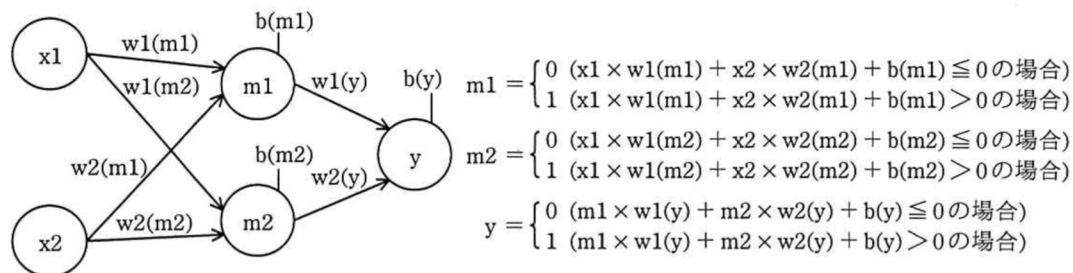


図5 3層パーセプトロンの模式図とノードの演算式



応用情報技術者（AP）試験  
対象外だが「午後」に役立つ

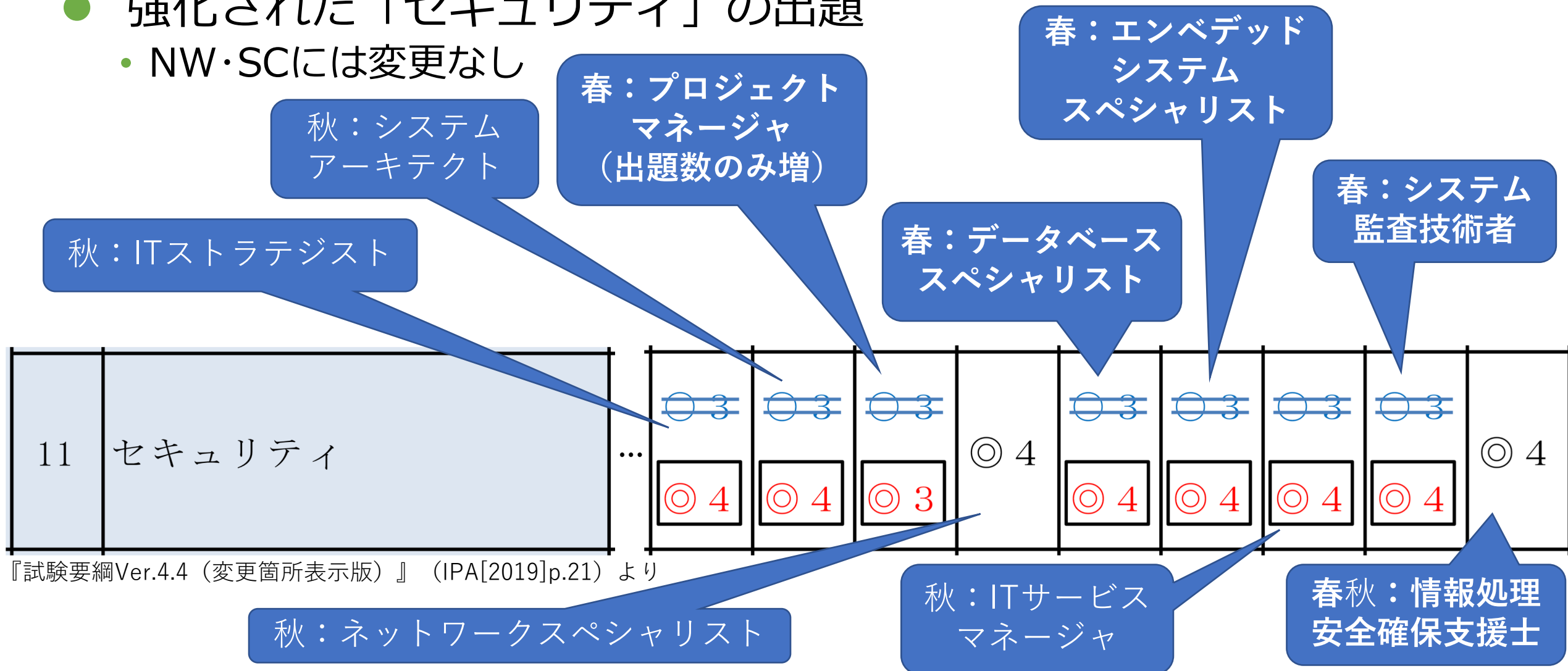
情報処理安全確保支援士（SC）試験  
春期実施の高度（AU,DB,ES,PM）試験  
「午前II」対策

（+「午後I・II」に少し役立つかも？）

# 出題予想 SC高度「午前Ⅱ」①

- 強化された「セキュリティ」の出題

- NW・SCには変更なし







## ● R2春以降の高度「午前Ⅱ」 - 「中分類11：セキュリティ」

### (2) セキュリティの強化

- ▶ SCについて、セキュリティに関する近年の記述（構成・表記）を全面的に更新し
- ▶ 今回の改訂対象である各試験区分につい
- ▶ ST、SA、PM、DB、ES、SM、AUの点分野（○）から重点分野（◎）に変更し、技術レベルを3から4に変更しました

「中分類11：セキュリティ」の知識項目には技術面・管理面の両方が含まれますが、**高度試験の各試験区分では、各人材像にとって関連性の強い知識項目をレベル4として出題**します。

(\*) 「中分類11：セキュリティ」の知識項目には技術面・管理面の両方が含まれますが、高度試験の各試験区分では、各人材像にとって関連性の強い知識項目をレベル4として出題します。

[https://www.jitec.ipa.go.jp/1\\_00topic/topic\\_20191105.html](https://www.jitec.ipa.go.jp/1_00topic/topic_20191105.html) (2019/12/22確認)

# 各人材像と「関連性の強い知識項目」

- …とは、下記のように、人材像と強く結びつく知識項目のこと

## 人材像

※ ABC順

AU

DB

ES

PM

## 知識項目例（IPA公表の項目に限らず）

※ 五十音順

SQLi, GRANT文

故障利用攻撃, Mirai

情報セキュリティガバナンス

DevSecOps

※ 強い結びつきのみを図示

# 以降のスライドでは

- 各試験区分の「午前Ⅱ」 - 「中分類11：セキュリティ」を予想！
  - 話の都合上、まずはSC試験から、以降は略号のABC順に載録
- 情報処理安全確保支援士（SC）試験 p.19
- システム監査技術者（AU）試験 p.20～22
- データベーススペシャリスト（DB）試験 p.23, 24
- エンベデッドシステムスペシャリスト（ES）試験 p.25～29
  - プラス、「中分類21：ビジネスインダストリ」の出題予想
- プロジェクトマネージャ（PM）試験 p.30～34
  - プラス、会計基準と改正民法関連の出題予想

# レベル4の「セキュリティ」SC

- 【予想】 まず，SC試験「午前Ⅱ」では何を出す？

25問中17問  
(予想)

以降の「AU」「DB」「ES」「PM」で述べる「セキュリティ」の予想は 全て SC試験でも出る 覚悟を！

- 改訂後，一発目の試験なので…

- 新作の（＝過去問の暗記では解けない）出題が多数，見込まれる
- IPAは，他の高度試験と全く同じ問題をSC試験でも出せば，「『◎4』にふさわしい難易度だったか？」を検証しやすい（SC受験者は“Lv.4の物差し”）

「将来，過去問題を使い回せるか？」  
の判断材料（だけでもないが）

# レベル4の「セキュリティ」AU①

## ● システム監査技術者試験と近い「◎4」出題例 ①

- JIS Q 27014:2015 (情報セキュリティガバナンス)における、情報セキュリティを統治するために経営陣が実行するガバナンスプロセスのうちの“モニタ”はどれか。
  - イ 戦略的目的の達成を評価することを可能にするガバナンスプロセス (R1秋SC午前II問7)
- 基本評価基準, 現状評価基準, 環境評価基準の三つの基準で情報システムの脆弱性の深刻度を評価するものはどれか。
  - ア CVSS (R1秋SC午前II問9)
- CVSS v3の評価基準には、基本評価基準, 現状評価基準, 環境評価基準の三つがある。基本評価基準の説明はどれか。
  - ア 機密性への影響, どこから攻撃が可能かといった攻撃元区分, 攻撃する際に必要な特権レベルなど, 脆弱性そのものの特性を評価する。(H30春SC午前II問1)
- ブロックチェーンに関する記述のうち, 適切なものはどれか。
  - エ ハッシュ関数が必須の技術であり, 参加者がデータの改ざんを検出するために利用する。(H30秋SC午前II問3)
- デジタルフォレンジックスに該当するものはどれか。
  - エ 犯罪に関する証拠となり得るデータを保全し, その後の訴訟などに備える。(H29秋NW午前II問18)

CVSS v3.1でも三つについては変わらず



## ● システム監査技術者試験と近い「◎4」出題例 ②

- インターネットバンキングサービスを提供するWebサイトを利用する際に、**トランザクション署名の機能をもつハードウェアトークンを利用**する。次の処理を行うとき、**(4)によってできることはどれか**。ここで、ハードウェアトークンは利用者ごとに異なり、本人だけが利用する。
  - 〔処理〕
    - (1) ハードウェアトークンに振込先口座番号と振込金額を入力し、メッセージ認証符号 (MAC) を生成する。
    - (2) Webサイトの振込処理画面に振込先口座番号、振込金額及び (1) で生成されたMACを入力し、Webサイトに送信する。
    - (3) Webサイトでは、本人に発行したハードウェアトークンと同じ処理手順によって振込先口座番号と振込金額からMACを生成する。
    - (4) **Webサイトでは、(2) で入力されたMACと、(3) で生成したMACを比較する。**
  - ウ **振込先口座番号と振込金額が改ざんされていないことを確認できる。** (H31春SC午前II問8)

# レベル4の「セキュリティ」AU③

- 【予想】 AU試験「午前Ⅱ」は何を出す？  
25問中5問  
(予想)
- デジタル・フォレンジック研究会『証拠保全ガイドライン』
- ITガバナンス『JIS Q 38500:2015』等を取り入れた, 平成30年改訂『システム監査基準』『システム管理基準』
- 『サイバーセキュリティ経営ガイドライン Ver 2.0実践のためのプラクティス集』 (IPA[2019]) に基づく監査の, チェックポイント
- 『JIS Q 27014:2015』 (情報セキュリティガバナンス) の概要
- 『情報セキュリティ監査基準』『情報セキュリティ管理基準』
- クラウドセキュリティの『JIS Q 27017:2016』に基づくコントロール, クラウド事業者の可用性や財務状況の確認, 解約時の (データ削除に代わる) 確実な暗号化と暗号化鍵の廃棄の確認
- 行き過ぎたBYODの反省という文脈での, MDMの監査のチェックポイント
- 技術者倫理 (参考: H31春PM午前Ⅱ問23「集団思考」, H31春AP午前問80「公衆の安全」) と絡めた, 人的な面のコントロール

## ● データベーススペシャリスト試験と近い「◎4」出題例

- SQLインジェクション対策について、Webアプリケーションプログラムの実装における対策と、Webアプリケーションプログラムの実装以外の対策として、ともに適切なものはどれか。
  - エ 【Webアプリケーションプログラムの実装における対策】 プレースホルダを利用する。  
【Webアプリケーションプログラムの実装以外の対策】 Webアプリケーションプログラムが利用するデータベースのアカウントがもつデータベースアクセス権限を必要最小限にする。（R1秋SC午前Ⅱ問17）
- HTTP Strict Transport Security (HSTS) の動作はどれか。
  - エ Webサイトにアクセスすると、Webブラウザは、以降の指定された期間、当該サイトには全てHTTPSによって接続する。（H30秋SC午前Ⅱ問12）
- Webアプリケーションの脆弱性を悪用する攻撃手法のうち、Webページ上で入力した文字列がPerlのsystem関数やPHPのexec関数などに渡されることを利用し、不正にシェルスクリプトを実行させるものは、どれに分類されるか。
  - イ OSコマンドインジェクション（H30秋SC午前Ⅱ問13）

# レベル4の「セキュリティ」DB②

25問中4問  
(予想)

- 【予想】 DB試験「午前Ⅱ」は何を出す？
  - 四択から，SQLiを実行可能な文字列を選ばせる
    - 参考：『安全なSQLの呼び出し方』（IPA[2010]）中の記述
  - 四択から，適切なGRANT文を選ばせる
  - 出力時に導出表，特にビュー（view）を用いる意義
  - 『安全なウェブサイトの作り方』（IPA[2015]）中，DB関連の記述
  - ブロックチェーン技術によって実現できること
  - コードサイニング証明書を用いる意義
  - 用語「RPO（目標復旧時点）」「RTO（目標復旧時間）」「MTPD（最大許容停止時間）」の違い

# レベル4の「セキュリティ」ES①

- エンベデッドシステムスペシャリスト試験と近い「◎4」出題例 ①
  - 暗号機能を実装したIoT機器において脅威となるサイドチャネル攻撃に該当するものはどれか。
    - イ 機器が発する電磁波を測定することによって秘密情報の取得を試みる。(R1秋SC午前II問2)
  - サイドチャネル攻撃に該当するものはどれか。
    - ア 暗号化装置における暗号化処理時の消費電力などの測定や統計処理によって、当該装置内部の秘密情報を推定する攻撃 (H31春SC午前II問7)
  - BlueBorneの説明はどれか。
    - ア Bluetoothを悪用してデバイスを不正に操作したり、情報を窃取したりする、複数の脆弱性の呼称 (R1秋SC午前II問10)
  - FIPS PUB 140-2の記述内容はどれか。
    - ア 暗号モジュールのセキュリティ要求事項 (H30秋SC午前II問5)



- エンベデッドシステムスペシャリスト試験と近い「◎4」出題例 ②
  - マルウェアMiraiの動作はどれか。
    - エ ランダムなIPアドレスを生成してtelnetポートにログインを試行し、工場出荷時の弱いパスワードを使っているIoT機器などに感染を広げるとともに、C&Cサーバからの指令に従って標的に対してDDoS攻撃を行う。(H30秋SC午前II問11)
  - 認証デバイスに関する記述のうち、適切なものはどれか。
    - イ 成人の虹彩は、経年変化がなく、虹彩認証では、認証デバイスでのパターン更新がほとんど不要である。(H30春SC午前II問9)
  - テンペスト攻撃を説明したものはどれか。
    - ウ 処理中に機器から放射される電磁波を観測して解析する。(H30春SC午前II問13)

# レベル4の「セキュリティ」ES③

- 【予想】 ES試験「午前Ⅱ」は何を出す？

25問中3問  
(予想)

- サイドチャネル攻撃の詳しい名称 (引用：H28秋SC午前Ⅱ問10 答ア)

問10 サイドチャネル攻撃の手法であるタイミング攻撃の対策として、最も適切なものはどれか。

- ア 演算アルゴリズムに対策を施して、機密情報の違いによって演算の処理時間に差異が出ないようにする。
- イ 故障を検出する機構を設けて、検出したら機密情報を破壊する。
- ウ コンデンサを挿入して、電力消費量が時間的に均一になるようにする。
- エ 保護層を備えて、内部のデータが不正に書き換えられないようにする。

あとの三つは、  
イ：故障利用攻撃  
ウ：電力解析攻撃  
エ：物理プロービング  
への対策。

- 用語「セキュリティ・バイ・デザイン」
- 「ShadowHammer」等のサプライチェーン攻撃
- 音声入力機器への不正な入力（遠方からの超指向性スピーカ，レーザ照射）
- 『IoT開発におけるセキュリティ設計の手引き』（IPA[2019]）
- 『IoT製品・サービス脆弱性対応ガイド』（IPA[2018]）

# ESの「午前Ⅱ」は，これも追加

## ● ES「午前Ⅱ」で追加される「ビジネスインダストリ」とは？

21	ビジネスインダストリ	1	ビジネスシステム	流通情報システム，物流情報システム，公共情報システム，医療情報システム，金融情報システム，電子政府，POSシステム，XBRL，スマートグリッド，Web会議システム，ユビキタスコンピューティング，IoTなど
		2	エンジニアリングシステム	エンジニアリングシステムの意義と目的，生産管理システム，MRP，PDM，CAE など
		3	e-ビジネス	EC (BtoB, BtoC などの電子商取引)，電子決済システム，EDI，ICカード・RFID 応用システム，ソーシャルメディア (SNS, ミニブログほか)，ロングテール など
		4	民生機器	AV 機器，家電機器，個人用情報機器 (携帯電話，スマートフォン，タブレット端末ほか)，教育・娯楽機器，コンピュータ周辺/OA 機器，業務用端末機器，民生用通信端末機器 など
		5	産業機器	通信設備機器，運輸機器/建設機器，工業制御/FA 機器/産業機器，設備機器，医療機器，分析機器・計測機器 など

・ ESでの重点度・レベルは「○3」  
AP「午前」相当が1～2問

・ この出題は，いわば  
“社会で働くコンピュータ”

・ 「○○スペシャリスト試験」  
唯一の「ストラテジ系」！

分野

「ストラテジ系」

大分類

「8：経営戦略」

中分類

「21：ビジネスインダストリ」

『試験要綱Ver.4.4 (変更箇所表示版)』 (IPA[2019]p.31) より

# 「ビジネスインダストリ」出題例

- IoT活用におけるデジタルツインの説明はどれか。
  - エ デジタル空間に現実世界と同等な世界を、様々なセンサで収集したデータを用いて構築し、現実世界では実施できないようなシミュレーションを行うこと（H31春AP午前問71，高度午前Ⅰ問28）
- IoTがもたらす効果を“監視”，“制御”，“最適化”，“自律化”の4段階に分類すると，IoTによって工場の機械の監視や制御などを行っているシステムにおいて，“自律化”の段階に達している例はどれか。
  - ウ クラウドサービスを介して，機械同士が互いの状態を常時監視・分析し，人手を介すことなく目標に合わせた協調動作を自動で行う。（H30秋AP午前問71，高度午前Ⅰ問27）
- 政府は，IoTを始めとする様々なICTが最大限に活用され，サイバー空間とフィジカル空間とが融合された“超スマート社会”の実現を推進している。必要なものやサービスが人々に過不足なく提供され，年齢や性別などの違いにかかわらず，誰もが快適に生活することができるとされる“超スマート社会”実現への取組みは何と呼ばれているか。
  - イ Society 5.0（H30春AP午前問71）
- ドローン，マルチコプタなどの無人航空機に搭載されるセンサのうち，機体を常に水平に保つ姿勢制御のために使われるセンサはどれか。
  - イ ジャイロセンサ（H29秋AP午前問71）
- IoTの技術として注目されている，エッジコンピューティングの説明として，適切なものはどれか。
  - ア 演算処理のリソースを端末の近傍に置くことによって，アプリケーション処理の低遅延化や通信トラフィックの最適化を行う。（H29秋AP午前問72，高度午前Ⅰ問28）

まさに“社会で働くコンピュータ”，現役の学生（非・社会科学系）にはツライ出題

# レベル3の「セキュリティ」PM①

## ● プロジェクトマネージャ試験と近い「◎4」出題例

- ※ Lv.3への“お下がり”が期待できる，出題当時はLv.4だった出題ネタ
  - 総務省及び経済産業省が策定した“電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）”を構成する暗号リストの説明のうち，適切なものはどれか。
    - ウ 電子政府推奨暗号リストとは，CRYPTRECによって安全性及び実装性能が確認された暗号技術のうち，市場における利用実績が十分であるか今後の普及が見込まれると判断され，当該技術の利用を推奨するもののリストである。（R1秋SC午前Ⅱ問8）
  - 経済産業省とIPAが策定した“サイバーセキュリティ経営ガイドライン（Ver2.0）”の説明はどれか。
    - ア 企業がIT活用を推進していく中で，サイバー攻撃から企業を守る観点で経営者が認識すべき3原則と，情報セキュリティ対策を実施する上での責任者となる担当幹部に，経営者が指示すべき事項をまとめたもの（H30秋SC午前Ⅱ問6）

SC試験で過去に出題されたPM寄りの問題は，とても少なかった

# レベル3の「セキュリティ」PM②

## ● プロジェクトマネージャ試験と近い「○3」出題例 ①

### ● ※ 過去のAP「午前」より抜粋

- JIS Q 27000:2019（情報セキュリティマネジメントシステム－用語）では、情報セキュリティは主に三つの特性を維持することとされている。それらのうちの二つは機密性と完全性である。残りの一つはどれか。
  - ア 可用性（R1秋AP午前問40）
- ファジングに該当するものはどれか。
  - ウ ソフトウェアに、問題を引き起こしそうな多様なデータを入力し、挙動を監視して、脆弱性を見つけ出す。（R1秋AP午前問44，高度午前Ⅰ問14）
- 脆弱性検査手法の一つであるファジングはどれか。
  - イ ソフトウェアのデータの入出力に注目し、問題を引き起こしそうなデータを大量に多様なパターンで入力して挙動を観察し、脆弱性を見つける。（H30秋AP午前問43，高度午前Ⅰ問15）



# レベル3の「セキュリティ」PM③

## ● プロジェクトマネージャ試験と近い「○3」出題例 ②

### ● ※ 過去のAP「午前」より抜粋

- 情報セキュリティにおけるエクスプロイトコードの説明はどれか。
  - エ ソフトウェアやハードウェアの脆弱性を検査するために作成されたプログラム (H31春AP午前問36)
- 情報セキュリティにおけるサンドボックスの説明はどれか。
  - エ 不正な動作をする可能性があるプログラムを特別な領域で動作させることによって、他の領域に悪影響が及ぶのを防ぐ。(H31春AP午前問43, 高度午前I問14)
- サイバーレスキュー隊 (J-CRAT)は、どの脅威による被害の低減と拡大防止を活動目的としているか。
  - ウ 標的型サイバー攻撃 (H30春AP午前問40)

# レベル3の「セキュリティ」PM④

- 【予想】PM試験「午前Ⅱ」は何を出す？
  - 用語「DevSecOps」「OWASP ZAP」「OSINT」
  - 『制御システムのセキュリティリスク分析ガイド 第2版』（IPA[2018]）
  - 『ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン』（経済産業省[2019]）

25問中4問  
(予想)

# PMとAUの「午前Ⅱ」は、これも追加

- 会計基準の「工事進行基準」は「収益認識基準」に
- 改正民法関連の出題
  - 請負契約の「瑕疵担保責任」は「契約不適合責任」に
    - 権利を主張できる期間は、引渡しから最長10年（契約不適合を知ってから1年）
  - 準委任契約の細分化（「成果完成型」と、旧来同様の「履行割合型」）
  - 新しい『情報システム・モデル取引・契約書』（IPA[2019]）
    - 下記の2分冊，改正民法+DX という文脈で出題？
      - 「受託開発（一部企画を含む）、保守運用」
      - 「パッケージ、SaaS/ASP活用、保守・運用」

改正民法に対応した「情報システム・モデル取引・契約書」を公開  
～ユーザ企業・ITベンダ間の共通理解と対話を促す～

2019年12月24日公開  
独立行政法人情報処理推進機構  
社会基盤センター

<https://www.ipa.go.jp/ikc/reports/20191224.html> (2019/12/25確認)

Copyright © 2020 JP-RISSA All Rights Reserved.

# 今後のスケジュール

## ● TBD (タイトルは仮)

- ~~2019年12月~~ ~~来春の「午前 I・II」新出題を予想~~
  - ~~(YouTube配信を予定)~~ → 本資料です (2020年1月公開)

本資料

- ~~2020年1月~~ ~~今春のSC試験「午後」新出題を予想~~
  - ~~(YouTube配信を予定)~~

2月8日の  
「対策セミナー」に  
統合します

- 2020年2月8日 午後 「情報処理安全確保支援士試験 対策セミナー」
  - (都区内での実施を計画中, 配信は未定)
- 2020年3月or4月 直前SC試験対策会
  - (希望者が多数なら実施, 配信は未定)



HomePage : <https://www.jp-rissa.org/>

お問い合わせ : [contact@jp-rissa.org](mailto:contact@jp-rissa.org)

Twitter : @jp\_rissa



**JP-RISSA**

情報処理安全確保支援士会