JP-RISSA
情報処理安全確保支援士会

情報処理安全確保支援士試験対策セミナー

一般公開用スライド

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

2020年2月8日　於 電気通信大学 創立80周年記念会館3F

免責事項

JP-RISSA
情報処理安全確保支援士会

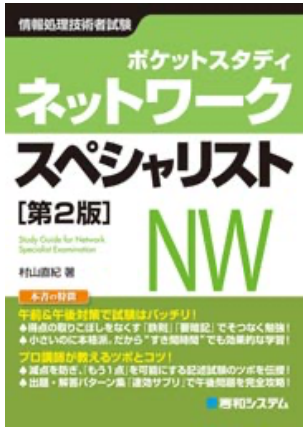
- 本資料は，担当者（村山）が独自に調査した結果や考察を公表したものであり，当該試験の実施団体（以下「IPA」）の活動とは関係ありません。
- 本資料の内容について万全を期して作成しましたが，IPAが公表する資料と本資料との間で記載内容に相違がある場合は，IPAが公表する資料の記載が優先します。
- 本資料は，本資料の利用者の自己責任での御利用をお願いします。本資料の利用によって利用者が受けた金銭その他の損害の責任を，担当者ならびに情報処理安全確保支援士会（JP-RISSA）は一切負いません。
- 担当者による予想が外れることは割とあります。

TLP：WHITE

~~本日の~~担当 村山直紀

JP-RISSA
情報処理安全確保支援士会

- 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

TLP：WHITE

SC「午前Ⅰ・Ⅱ」の予想は，こちらを

https://www.jp-rissa.org/post/1214/

TLP：WHITE

ナウなヤングを狙い撃ち！

JP-RISSA 情報処理安全確保支援士会

- 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

ナウい①

ナウい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）

ナウい③

ナウい④

https://www.jitec.ipa.go.jp/1_00topic/topic_20191105.html（2019/12/18確認）

- SC試験シラバス（主に「午後」）の改訂版（Ver.2.0）が公開

TLP：WHITE

SC「午後」の出題範囲 削除・追加箇所

JP-RISSA 情報処理安全確保支援士会

旧（～R01秋）

総入れ替え！

~~1　情報セキュリティシステムの企画・要件定義・開発・運用・保守に関すること~~

~~情報システムの企画・要件定義・開発，物理的セキュリティ対策，アプリケーション（Webアプリケーションを含む）のセキュリティ対策，セキュアプログラミング，データベースセキュリティ対策，ネットワークセキュリティ対策，システムセキュリティ対策など~~

~~2　情報セキュリティの運用に関すること~~

~~情報セキュリティポリシ，リスク分析，業務継続計画，情報セキュリティ運用・管理，脆弱性分析，誤使用分析，不正アクセス対策，インシデント対応，ユーザセキュリティ管理，障害復旧計画，情報セキュリティ教育，システム監査（のセキュリティ側面），内部統制など~~

~~3　情報セキュリティ技術に関すること~~

~~アクセス管理技術，暗号技術，認証技術，マルウェア（コンピュータウイルス，ボット，スパイウェアなど）対策技術，攻撃手法（ソーシャルエンジニアリング，サイバー攻撃など），セキュリティ応用システム（署名認証，侵入検知システム，ファイアウォール，セキュアな通信技術（VPNほか），鍵管理技術，PKIなど。また，周辺機器も対象とする），監査証跡のためのログ管理技術など~~

~~4　開発の管理に関すること~~

~~開発ライフサイクル管理，システム文書構成管理，ソフトウェアの配布と操作，人的管理手法（チーム内の不正を起こさせないような仕組み），開発環境の情報セキュリティ管理，脆弱性情報収集管理など~~

~~5　情報セキュリティ関連の法的要求事項などに関すること~~

~~情報セキュリティ関連法規，国内・国際標準，ガイドライン，著作権法，個人情報保護，情報倫理など~~

引用：『情報処理技術者試験 情報処理安全確保支援士試験 試験要綱Ver.4.4 変更箇所表示版』（IPA[2019]p.40）

TLP：WHITE

SC「午後」の出題範囲 削除・追加箇所

JP-RISSA 情報処理安全確保支援士会

新（R02春～）

「マネジメント」

総入れ替え！

1　情報セキュリティマネジメントの推進又は支援に関すること

情報セキュリティ方針の策定，情報セキュリティリスクアセスメント（リスクの特定・分析・評価ほか），情報セキュリティリスク対応（リスク対応計画の策定ほか），情報セキュリティ諸規程（事業継続計画に関する規程を含む組織内諸規程）の策定，情報セキュリティ監査，情報セキュリティに関する動向・事例の収集と分析，関係者とのコミュニケーションなど

2　情報システムの企画・設計・開発・運用におけるセキュリティ確保の推進又は支援に関すること

企画・要件定義（セキュリティの観点），製品・サービスのセキュアな導入，アーキテクチャの設計（セキュリティの観点），セキュリティ機能の設計・実装，セキュアプログラミング，セキュリティテスト（ファジング，脆弱性診断，ペネトレーションテストほか），運用・保守（セキュリティの観点），開発環境のセキュリティ確保など

「セキュリティテスト」

3　情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること

暗号利用及び鍵管理，マルウェア対策，バックアップ，セキュリティ監視並びにログの取得及び分析，ネットワーク及び機器（モバイル機器ほか）のセキュリティ管理，脆弱性への対応，物理的及び環境的セキュリティ管理（入退管理ほか），アカウント管理及びアクセス管理，人的管理（情報セキュリティの教育・訓練，内部不正の防止ほか），サプライチェーンの情報セキュリティの推進，コンプライアンス管理（個人情報保護法，不正競争防止法などの法令，契約ほかの遵守）など

「コンプライアンス管理」

「サプライチェーン」

4　情報セキュリティインシデント管理の推進又は支援に関すること

情報セキュリティインシデントの管理体制の構築，情報セキュリティ事象の評価（検知・連絡受付，初動対応，事象をインシデントとするかの判断，対応の優先順位の判断ほか），情報セキュリティインシデントへの対応（原因の特定，復旧，報告・情報発信，再発の防止ほか），証拠の収集及び分析（ディジタルフォレンジックスほか）など

「証拠の収集及び分析」

引用：『情報処理技術者試験 情報処理安全確保支援士試験 試験要綱Ver.4.4 変更箇所表示版』（IPA[2019]p.40-41）

TLP：WHITE

「業務と役割」削除・追加箇所

JP-RISSA 情報処理安全確保支援士会

旧（～R01秋）	新（R02春～）
~~セキュリティ機能~~の企画・~~要件定義~~・開発・運用~~・保守を推進又は支援する~~業務，~~若しくはセキュアな情報システム基盤を整備する業務~~に従事し，次の役割を主導的に果たすとともに，下位者を指導する。	情報セキュリティマネジメントに関する業務，情報システムの企画・設計・開発・運用におけるセキュリティ確保に関する業務，情報及び情報システムの利用におけるセキュリティ対策の適用に関する業務，情報セキュリティインシデント管理に関する業務に従事し，次の役割を主導的に果たすとともに，下位者を指導する。
~~① 情報システムの脅威・脆弱性を分析，評価し，これらを適切に回避，防止するセキュリティ機能の企画・要件定義・開発を推進又は支援する。~~	① 情報セキュリティ方針及び情報セキュリティ諸規程（事業継続計画に関する規程を含む組織内諸規程）の策定，情報セキュリティリスクアセスメント及びリスク対応などを推進又は支援する。
② ~~情報~~システム~~又はセキュリティ機能の開発プロジェクトにおいて，情報システムへの脅威を分析し，プロジェクト管理を適切に~~支援する。	② システム調達（製品・サービスのセキュアな導入を含む），システム開発（セキュリティ機能の実装を含む）を，セキュリティの観点から推進又は支援する。
③ ~~セキュリティ侵犯への対処やセキュリティパッチの適用作業~~など情報システム~~運用プロセス~~におけるセキュリティ~~管理作業~~を~~技術的な側面から~~支援する。	③ 暗号利用，マルウェア対策，脆弱性への対応など，情報及び情報システムの利用におけるセキュリティ対策の適用を推進又は支援する。
~~④ 情報セキュリティポリシの作成，利用者教育などに関して，情報セキュリティ管理部門を支援する。~~	④ 情報セキュリティインシデントの管理体制の構築，情報セキュリティインシデントへの対応などを推進又は支援する。

マネジメント寄りの役割増

「ポリシの作成」は古い

「支援」→「推進又は支援」

「支援」→「推進又は支援」

「支援」→「推進又は支援」

引用・参考：『情報処理技術者試験 情報処理安全確保支援士試験 試験要綱Ver.4.4 変更箇所表示版』（IPA[2019]p.10-11）

TLP：WHITE

「期待する技術水準」削除・追加箇所①

JP-RISSA 情報処理安全確保支援士会

旧（～R01秋）	新（R02春～）
~~情報セキュリティ技術の専門家として，他の専門家と協力しながら情報セキュリティ技術を適用して，セキュアな情報システムを企画・要件定義・開発・運用・保守~~するため，次の知識・実践能力が要求される。	情報処理安全確保支援士の業務と役割を円滑に遂行するため，次の知識・実践能力が要求される。
① 情報システム~~又は~~情報システム基盤の~~リスク~~分析~~を行い，情報セキュリティポリシに準拠して具体的な情報~~セキュリティ要件を抽出できる。	① 情報システム及び情報システム基盤の脅威分析に関する知識をもち，セキュリティ要件を抽出できる。
② ~~情報~~セキュリティ対策~~のうち，技術的な対策について基本的な技術と複数の特定の領域における応用技術~~をもち，~~これらの技術~~を対象システムに適用するとともに，その効果を評価できる。	② 情報セキュリティの動向・事例，及びセキュリティ対策に関する知識をもち，セキュリティ対策を対象システムに適用するとともに，その効果を評価できる。
③ ~~情報セキュリティ対策のうち，物理的・管理的な対策について基本的な知識と適用場面に関する技術をもつとともに，~~情報セキュリティマネジメント~~の基本的な考え方を理解し，これを適用するケースについて具体的な~~知識をもち，~~評価~~できる。	③ 情報セキュリティマネジメントシステム，情報セキュリティリスクアセスメント及びリスク対応に関する知識をもち，情報セキュリティマネジメントについて指導・助言できる。

「他の専門家と協力しながら」が

より自立した立場に

「評価」は

「指導・助言」へと表現を変更

引用・参考：『情報処理技術者試験 情報処理安全確保支援士試験 試験要綱Ver.4.4 変更箇所表示版』（IPA[2019]p.11）

TLP：WHITE

「期待する技術水準」削除・追加箇所②

JP-RISSA 情報処理安全確保支援士会

旧（～R01秋）	新（R02春～）
④ ~~情報技術のうち，~~ネットワーク，データベース~~，システム開発環境について基本的な~~知識をもち，~~情報システムの機密性，責任追跡性などを確保するために必要な~~暗号，認証，フィルタリング，ロギングなどの要素技術を~~選択~~できる。	④ ネットワーク，データベースに関する知識をもち，暗号，認証，フィルタリング，ロギングなどの要素技術を適用できる。
⑤ ~~情報~~システム開発~~における工程管理~~，品質管理~~について基本的な~~知識~~と具体的な適用事例の知識，経験をもつ。~~	⑤ システム開発，品質管理などに関する知識をもち，それらの業務について，セキュリティの観点から指導・助言できる。
⑥ 情報セキュリティ~~ポリシ~~に関する~~基本的な~~知識をもち，~~ポリシ策定，利用者~~教育などに~~関して，情報セキュリティ管理部門を支援~~できる。	⑥ 情報セキュリティ方針及び情報セキュリティ諸規程の策定，内部不正の防止に関する知識をもち，情報セキュリティに関する従業員の教育・訓練などについて指導・助言できる。
⑦ 情報セキュリティ関連の法的要求事項~~など~~に関する~~基本的な~~知識をもち，~~これらを適用~~できる。	⑦ 情報セキュリティ関連の法的要求事項，情報セキュリティインシデント発生時の証拠の収集及び分析，情報セキュリティ監査に関する知識をもち，それらに関連する業務を他の専門家と協力しながら遂行できる。

「システム開発環境」を削除

「内部不正の防止」を明記

「情報セキュリティ監査」を明記

「証拠の収集及び分析」を明記

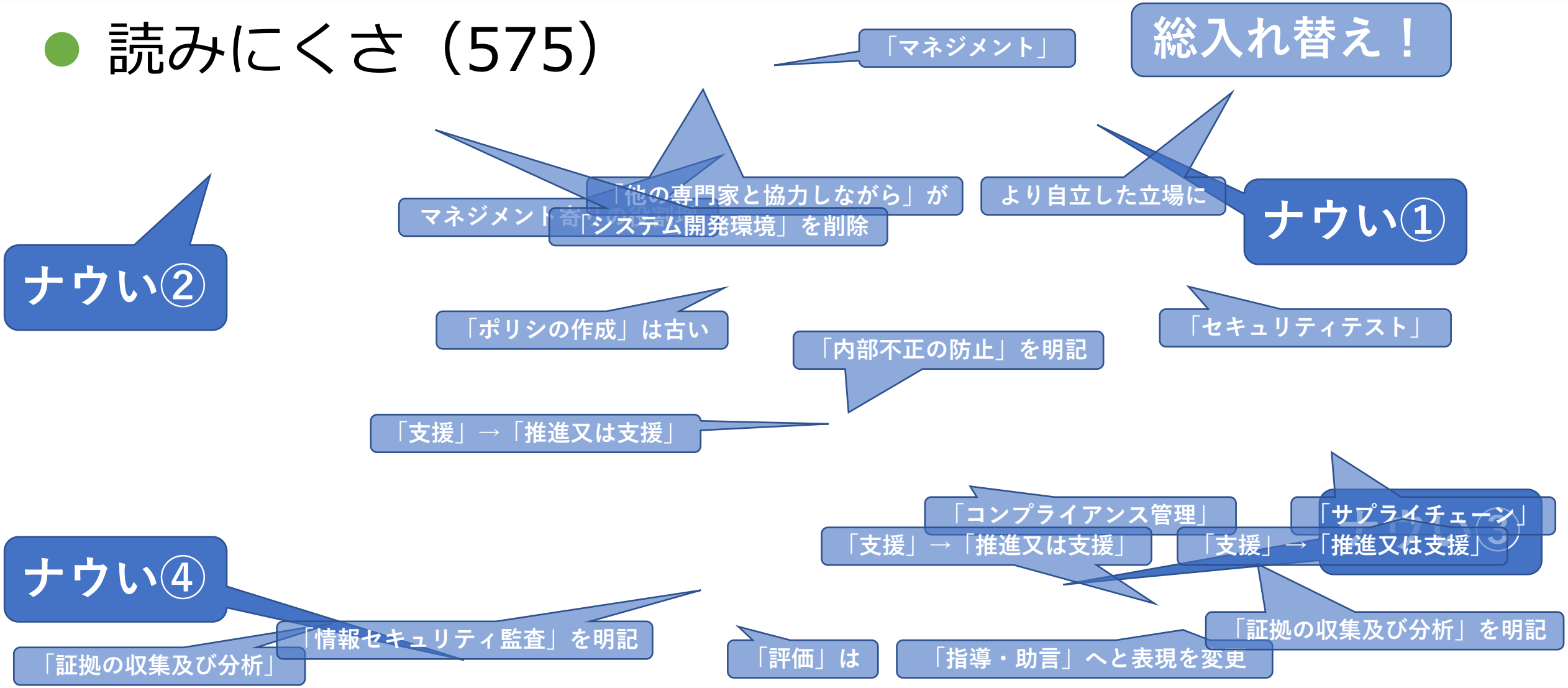
引用・参考：『情報処理技術者試験 情報処理安全確保支援士試験 試験要綱Ver.4.4 変更箇所表示版』（IPA[2019]p.11）

TLP：WHITE

フキダシを集めて分かる

JP-RISSA
情報処理安全確保支援士会

- 読みにくさ（575）

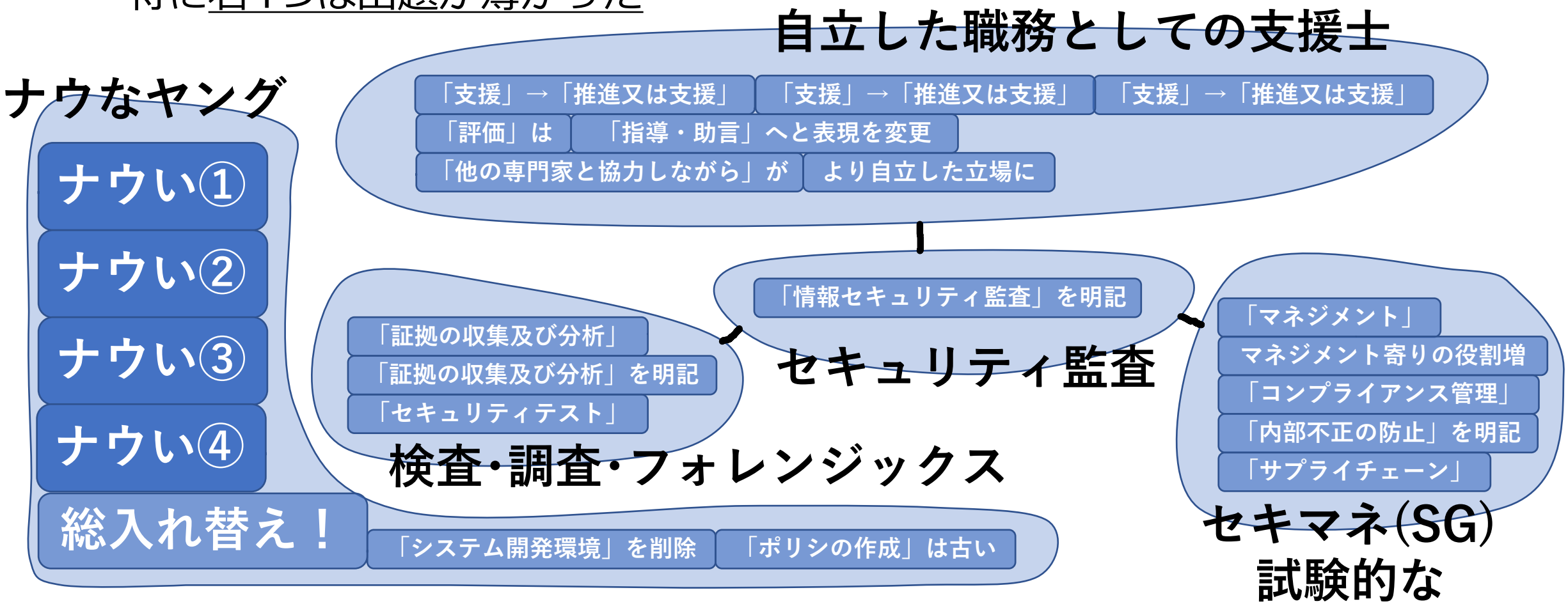


TLP：WHITE

はいプロKJ法のために生まれた男

JP-RISSA
情報処理安全確保支援士会

- これらの比重が今春から高まる
  - 特に右4つは出題が薄かった



TLP：WHITE

そこで~~本日の~~進行ですが

- これらの5点を軸に，SC試験「午後Ⅰ・Ⅱ」を勝手に予想します
  - ①「自立した職務としての支援士」　p.17
  - ②「セキュリティ監査」　p.18，19
  - ③「セキマネ（SG）試験的な」　p.20～23
  - ④「検査･調査･フォレンジックス」　p.24～28
  - ⑤「ナウなヤング」　p.29～42
    - AI，ビッグデータ，IoT，DX，その他のヤマ張り
  - ~~もしも時間が余ったら…昨秋試験から抽出した「速効サプリ®」を初公開~~
    - ~~「村山に『こう回答したら点がつくかな？』を判別させる会」あると嬉しいですか？~~

TLP：WHITE

忘れない内に，この話から（1/3）

JP-RISSA 情報処理安全確保支援士会

- 改訂されたSC試験シラバス（主に「午後」向け）
  - 『情報処理安全確保支援士試験（レベル4）シラバス（Ver.2.0）』
- 村山が“新しい”と気になった「要求される知識」を，以下に抜粋

大項目	要求される知識（抜粋）
1 情報セキュリティマネジメントの推進又は支援に関すること	・脅威分析（STRIDE分析，アタックツリー分析（ATA）など）に関する知識 ・サイバー保険に関する知識 ・ITの動向（クラウドコンピューティング，仮想化，モバイル，組込みシステム，Web技術，AI，ビッグデータ，IoTなど）及びその情報セキュリティへの影響に関する知識 ・サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）に関する知識 ・攻撃の分析モデル（サイバーキルチェーン，ATT&CKなど）に関する知識 ・脅威インテリジェンス（OSINTなど）に関する知識 ・サイバー情報共有イニシアティブ（J-CSIP），サイバーレスキュー隊（J-CRAT）に関する知識 ・情報セキュリティ早期警戒パートナーシップに関する知識

引用：『情報処理安全確保支援士試験（レベル4）シラバス（Ver.2.0）』（IPA[2019]p.1-2）

TLP：WHITE

続き（2/3）

大項目	要求される知識（抜粋）
2 情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること	・セキュリティバイデザイン，プライバシーバイデザインに関する知識 ・システム及びソフトウェア製品の品質要求及び評価（SQuaRE）に関する知識 ・要塞化（ハードニング）に関する知識 ・仮想化，コンテナ技術に関する知識 ・ITセキュリティ関連の規格（CC/CEM，FIPS 140など）に関する知識 ・ITセキュリティ関連の認証制度（JISEC，JCMVPなど）に関する知識 ・耐タンパ性，サイドチャネル攻撃に関する知識 ・サービスマネジメント，ITSMS，SLAに関する知識

引用：『情報処理安全確保支援士試験（レベル4）シラバス（Ver.2.0）』（IPA[2019]p.3-4）

大項目	要求される知識（抜粋）
4 情報セキュリティインシデント管理の推進又は支援に関すること	・PSIRTに関する知識 ・監督官庁などへの報告，報道機関などへの公表に関する知識 ・証拠保全の手順及びツールに関する知識 ・Chain of Custody（証拠保全の一貫性）に関する知識

引用：『情報処理安全確保支援士試験（レベル4）シラバス（Ver.2.0）』（IPA[2019]p.8-9）

TLP：WHITE

続き（3/3）

大項目	要求される知識（抜粋）
3 情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること	・ハードウェアセキュリティモジュール（HSM），TPMに関する知識 ・マルウェアによる攻撃（C&C通信，ファイル暗号化など）に対する多層防御に関する知識 ・脅威インテリジェンスの共有のための標準（STIX/TAXIIなど）に関する知識 ・SIEMに関する知識 ・脆弱性情報（JVN，CVE，CVSS，CWEなど）に関する知識 ・セキュリティ設定共通化手順（SCAP）に関する知識 ・脆弱性ハンドリングに関する知識 ・バグバウンティプログラムに関する知識 ・need-to-know，need-to-use，最小権限の原則に関する知識 ・職務規程，雇用契約，守秘義務協定に関する知識 ・セキュリティクリアランスに関する知識 ・製品・サービスのサプライチェーンのリスクに関する知識 ・契約，倫理，公益通報者保護制度に関する知識

引用：『情報処理安全確保支援士試験（レベル4）シラバス（Ver.2.0）』（IPA[2019]p.5-7）

TLP：WHITE

じゃあ「午後Ⅰ・Ⅱ」を予想するよ

JP-RISSA
情報処理安全確保支援士会

- 予想①「自立した職務としての支援士」　p.17
- 予想②「セキュリティ監査」　p.18，19
- 予想③「セキマネ（SG）試験的な」　p.20～23
- 予想④「検査･調査･フォレンジックス」　p.24～28
- 予想⑤「ナウなヤング」　p.29～42
  - AI，ビッグデータ，IoT，DX，その他のヤマ張り

※ 喋っててあんまり面白くない話から好きな話へ，の順。

TLP：WHITE

①「自立した職務としての支援士」

JP-RISSA
情報処理安全確保支援士会

- どう出題するのだ，この分類。話の流れ的には失敗だわ。。
  - 私の…心の中のKJが…「こう分類しろ」と囁いたの…
  - 近年のSC試験「午後Ⅰ・Ⅱ」に出てくる，「情報処理安全確保支援士（登録セキスペ）のM氏は」といった登場人物の振舞いを見れば，イメトレできる？
  - 今どき「セキュリティポリシの（新規）作成」なんて出題されない。出すとしたら，本文中の伏線を読み解かせた上で「管理規程に追加すべき項目を述べよ。」
  - ~~あとは「交流と質問会」で，現役のRISSに訊いてみて下さい~~
- 次，いきましょう

TLP：WHITE

②「セキュリティ監査」（1/2）

JP-RISSA
情報処理安全確保支援士会

- ペネトレーションテスト等，技術と絡めた出題が見込まれる
  - IoT機器の検索サイト（Shodan，Censys，Insecam等）は，自組織のIoT機器が “外から丸見え” かを確認するためのツールとしても使える
  - TLPT（Threat-Led Penetration Test(ing) ）
    - 脅威ベースペネトレーションテスト。各チームの役割は下記
    - レッドチーム　　：攻撃を行う
    - ブルーチーム　　：検知・ブロックを行う
    - ホワイトチーム　　：全体の管理（計画，両者から結果を入手，課題のまとめや評価）

- 例えば，攻撃者が暗号資産（仮想通貨）を掘りたい場合
  - 攻撃者にとって，侵入先が『重要なデータを扱っているか』は不問
    - DBサーバ上の機密情報よりも，GPU等の計算機リソースの強さが大切。このため，情報漏えいへの警戒とは異なる観点の「猜疑心」も必要
    - 古い考えで「守るべきサーバとは，こうだ」に固執した受験者は，足もとをすくわれる
      - 参考：R01秋SC午後 II 問1設問3（2）

TLP：WHITE

②「セキュリティ監査」（2/2）

JP-RISSA
情報処理安全確保支援士会

- 契約によって「サプライチェーンリスク」を緩和しているか
  - 2020年4月施行の改正民法では「『瑕疵担保責任』が、契約内容に適合しない場合に修補・追完を請求できる『契約不適合責任』に変更された。これにより、契約時における契約内容の明確化がより一層求められるようになりITサプライチェーンにも大きく影響するものと考えられる。例えば、納品後のソフトウェアプログラムに脆弱性が発見され、委託先に修補を求めようとする場合、あらかじめ、そのような脆弱性のないプログラムの納品を契約内容としておく必要がある。（中略）仕様書を作成する委託元が、より要件を明示しなければならなくなる。」引用：『情報セキュリティ白書2019』（IPA[2019]p.187）

- システム監査技術者（AU）試験での『システム監査基準』『システム管理基準』の出題は，ITガバナンス『JIS Q 38500』等を取り入れた平成30年4月改訂版へと移行済み
- 事業継続マネジメントシステム『JIS Q 22301』『JIS Q 22313』

TLP：WHITE

③「セキマネ(SG)試験的な」（1/4）

JP-RISSA 情報処理安全確保支援士会

- 昨秋のSC試験は，ネットワーク技術に寄った出題が多かった
  - 秋期にはNW試験も実施されるためか，出題者たちの色がにじみ出る
  - その理屈で言えば，今春試験はシステム監査やプロマネ寄り？

- ガイドライン各種
  - IPAのガイドライン
    - 『サイバーセキュリティ経営ガイドライン』Ver 2.0
      - 本文中に「セキュリティは投資（コストではない），経営者が推進していく」といった表現が入れば，これ。
      - 『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』もあり
    - 『制御システムのセキュリティリスク分析ガイド 第2版』
  - 経済産業省のガイドライン
    - 『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』

TLP：WHITE

「標的型攻撃」の分析技法

JP-RISSA
情報処理安全確保支援士会

- 「サイバーキルチェーン」
  - サイバー攻撃の7フェーズに沿った分析のスキルは，SC試験では必須
    - この分析を扱った出題：H31春SG午後問1，R01秋SC午後Ⅱ問2
    - 7段階とは：偵察，武器化，配送，攻撃実行，インストール，遠隔制御，目的の実行
- 「MITRE ATT&CK」フレームワーク
  - ATT&CK：Adversarial Tactics, Techniques, and Common Knowledge
  - スライドp.15（新シラバス）では「サイバーキルチェーン」と同列の扱い
    - そろそろ出題される順番…？
- 攻撃前の調査としてのOSINT，攻撃対策としてのSIEM
  - OSINT　：Open Source Intelligence
  - SIEM　　：Security Information and Event Management

TLP：WHITE

「サプライチェーンリスク」出題予想

JP-RISSA 情報処理安全確保支援士会

- 「サプライチェーン攻撃」での，マルウェア混入のタイミングは？
  - 製造時（ICチップ内，回路，ファームウェアを疑う）
    - ハードウェアのレベルでバックドアが仕込まれると，納品（検収）時での検証は困難
  - 流通時（出荷・物流・小売・納品・設置の各業者を疑う）
    - 機器が，マルウェアに感染済みで納品されてくる
  - 運用中（定期メンテ時の出入りの業者，時には “本家” を疑う）
    - “本家” がヤラレて，ソフトウェア更新時に感染を広げた例（ShadowHammer）
- 川上側が不正に混入させるリスクと絡めて，ついに『ISO/IEC 15408（CC：コモンクライテリア）』を出題する時が来た？
- 答として書かせるなら…（技術的な策，管理策）
  - ソフトウェアへのディジタル署名（コードサイニング証明書）の採用と検証
  - CCへの準拠性の確認，契約の明文化（→スライドp.21「改正民法」）
  - 「午前」の試験なら「DevSecOps」「セキュリティ・バイ・デザイン」

TLP：WHITE

③「セキマネ(SG)試験的な」（4/4）

JP-RISSA 情報処理安全確保支援士会

- その他，出題ネタとして考えられること
  - クラウド側の可用性を考慮させる出題
  - ビル等，規模の大きい（PCよりも融通の利きにくい）設備
    - 更新までのサイクルが10～20年，システムの更新は年1回の法定点検のタイミング
  - CSIRTやSOCの運営，ISACとの連携
    - 参考：R01秋SC午後Ⅰ問2設問1（4）
  - Stripe等のオンライン決済プラットフォームを利用する利点，とくれば
    - カード番号を自社のサーバを一度も通さず，トークン化させることができる
    - カード情報を自社のDBにもたせたり各種の通貨に対応させたり，というのはしんどい
    - そこでSC試験では，（本文中に伏線を張った上で）「PCI DSSに絡む手間を省ける」を答えさせる出題が考えられる
      - 本文中の伏線（例）
        - 「Y社では今回，初めてクレジットカードによる決済を始める。」→ 素人だよ
        - 「サービス開始までの期間は限られている。」→ 余計な手間をかけられないよ
        - 「コンプライアンスも重視」→ セキマネ的な視点の出番だよ

TLP：WHITE

④「検査・調査・フォレンジックス」(1/5)

JP-RISSA 情報処理安全確保支援士会

- サイバーセキュリティを目的とするリバースエンジニアリングは，「当該著作物に表現された思想又は感情を自ら享受し又は他人に享受させることを目的としない場合」にあたり，著作権法上は問題ない

  - （著作物に表現された思想又は感情の享受を目的としない利用）
  - 第三十条の四
    - 一　著作物の録音、録画その他の利用に係る技術の開発又は実用化のための試験の用に供する場合
    - 二　情報解析（多数の著作物その他の大量の情報から、当該情報を構成する言語、音、影像その他の要素に係る情報を抽出し、比較、分類その他の解析を行うことをいう。第四十七条の五第一項第二号において同じ。）の用に供する場合
    - 三　前二号に掲げる場合のほか、著作物の表現についての人の知覚による認識を伴うことなく当該著作物を電子計算機による情報処理の過程における利用その他の利用（プログラムの著作物にあつては、当該著作物の電子計算機における実行を除く。）に供する場合

TLP：WHITE

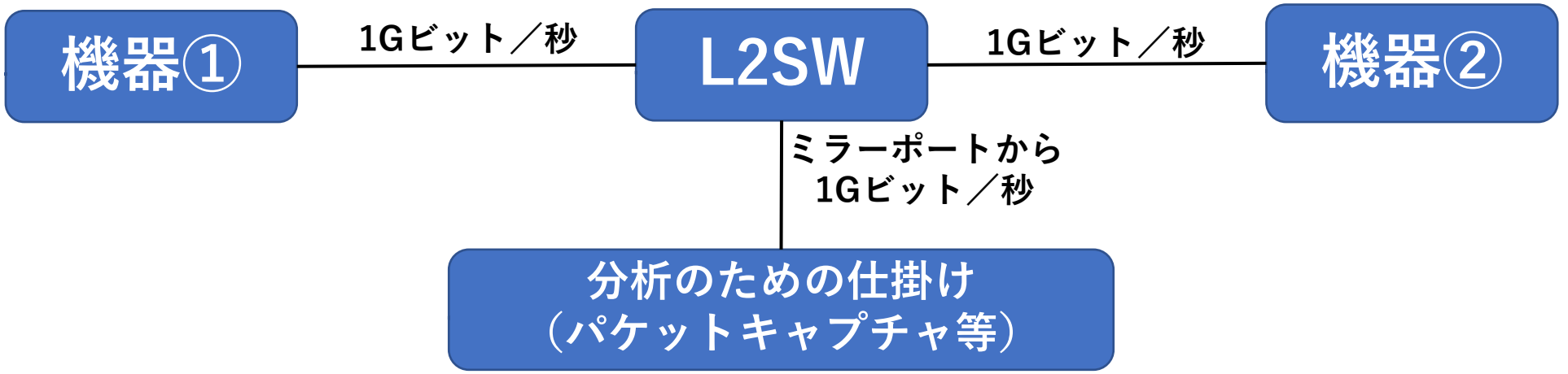
実務的な出題の予想①

- ディジタルフォレンジックス
  - 『証拠保全ガイドライン』 デジタル・フォレンジック研究会
- アンチフォレンジックス
  - 『データ消去技術 ガイドブック』 ADEC（データ適正消去実行証明協議会）

- ペネトレーションテスト
  - 双方で検査範囲を確認する。なぜ？
    - それを逸脱すると最悪の場合，被検査側の業務が止まる
    - 悪影響を防ぐか最小限に留めるには，事前の調整・説明が必要
  - 検査・操作の全記録を，機密性を確保した上で一定期間保存する。なぜ？
    - 後でトラブルになった時に検証するため
    - たまたま同時刻に本物の攻撃を受けていた場合，被検査側のログとの差分をとることで検証できるようにするため

TLP：WHITE

実務的な出題の予想②



- すべて1Gビット／秒のLAN（全二重）とした場合
- 「機器①」－「機器②」間の帯域は，上下で実質2Gビット／秒
- だが，分岐させた部分も1Gビット／秒である
- とくれば，書かせる点は二つ
  - 問題点は「ピーク時にとりこぼす可能性」
  - 解決策（例）は「2Gビット／秒以上の帯域（例：10GのLAN）を用意する」

TLP：WHITE

④「検査・調査・フォレンジックス」(4/5)

JP-RISSA 情報処理安全確保支援士会

- Webアプリケーションの脆弱性診断ツール「OWASP ZAP」が，R01秋SC午後Ⅱ問1設問3（1）に，選択肢の一つとして出た
  - ということは今後，ツール類を固有名詞で問うてくる…のでは？
    - 「Ghidra」　米NSAが公開するソフトウェアのリバースエンジニアリングツール
    - 「Kali Linux」　ペネトレーションテストに特化したLinuxディストリビューション
    - 「Metasproit」　ペネトレーションテストのフレームワーク
    - 「Mimikatz」　Windows用，Kerberos認証のゴールデンチケットの作成に使える
    - 「Nmap」　ペネトレーションテストにも使うポートスキャナ
    - 「sqlmap」　SQLインジェクションの脆弱性診断ツール
    - 「XVWA」　攻撃の学習用途として，脆弱性を含ませたWebアプリケーション
  - Webサイトだと，例えば下記
    - 「CrackStation」　パスワードハッシュの解析サイト（ソルト付きハッシュは非対応）
    - 「MailTester」　“生きた”メールアドレスの確認サイト
    - 「VirusTotal」　各社のマルウェアスキャンを試せるサイト
      - 「VirusTotal」にアップロードされたファイルは有償サービスだと入手可能なので利用に注意

④「検査・調査・フォレンジックス」(5/5)

JP-RISSA 情報処理安全確保支援士会

- OSのコマンドの内，ワクワクするやつを集めました

コマンド	（SC試験的に）嬉しいこと	コマンド	（SC試験的に）嬉しいこと
arp	ARPテーブルの確認や操作	netstat	現在のTCPコネクションの確認
curl	URLやプロトコルを指定してのファイルのダウンロード	nft	パケットフィルタリング（iptables等の機能を統合・高機能化）
dig，host	ドメイン名やIPアドレスの調査	nslookup，whois	DNSのレコードの調査
ifconfig	MACアドレスの偽装	passwd	パスワードの変更，パスワードの有効期限の設定
iptables	パケットフィルタリング	ping	あるIPアドレスが実運用されているかの確認
lshw	ハードウェアの情報を表示	pvscan	物理ボリュームのスキャン・一覧表示
lslogins，lastlog	ユーザの最終ログイン情報の表示	ssh	「telnetの代替」の正解候補
lsof	あるポートを使っているプロセスの調査	top	実行中のプロセスの確認
lsusb	接続されるUSBデバイスの情報を表示	vgscan	ボリュームグループのスキャン・一覧表示
lvscan	論理ボリュームのスキャン・一覧表示	wget	URLを指定してのファイルのダウンロード

TLP：WHITE

予想⑤「ナウなヤング」（1/14）

JP-RISSA
情報処理安全確保支援士会

AI，ビッグデータ，IoT，DX，その他のヤマ張り

TLP：WHITE

予想⑤-1 「AI」出題予想

JP-RISSA
情報処理安全確保支援士会

- 「AIとセキュリティ」の出題（予想）は，大きく三つに分けられる
  - ① AIへの攻撃
    - 機械学習の教師データの改ざん
    - 偏った（不正な）教師データを与え，誤った学習をさせることによる品質の劣化
    - 訓練結果だけの窃取や漏えい
    - 攻撃手法を学習データとして使う場合，どのようなデータかを攻撃者に知られてしまうと回避策を探られてしまう（学習済みだった攻撃パターンを回避して攻撃される）
  - ② AIによる攻撃
    - ディープフェイク
    - 画像を用いたCAPTCHA等の認証を突破（コンサートチケットの大量購入）
    - 「敵対的生成ネットワーク」を利用し，認証突破が可能なよう自動学習
    - OSINTからの自動的な学習
  - ③ AIによる防御
    - マルウェア検知
      - ベイジアンフィルタ，ヒューリスティックスキャン

TLP：WHITE

予想⑤-2 「ビッグデータ」出題予想

JP-RISSA
情報処理安全確保支援士会

- CAP定理，BASE特性と絡めた出題
- ブロックチェーンと絡めた出題
  - 51%アタック，スマートコントラクト
- 高速な通信インフラが，高速な拡散を招く
  - 400Gイーサ，Wi-Fi 6，5G
- 正直，そう思いつかない…次いきましょう

TLP：WHITE

予想⑤-3 「IoT」出題予想（1/5）

JP-RISSA 情報処理安全確保支援士会

- ヤマ張り
  - IoT機器を踏み台とした，内部ネットワークへの攻撃
    - 多数のIoT機器をボットネット化した，DDoS攻撃
    - 通信経路の暗号化や，マルウェア感染の拡大を防ぐ等の，ネットワーク技術面からの制限がなされていないケースも多い（一旦侵入に成功されると感染が広がりやすい）
  - IoT機器に接続する通信回線への攻撃により，データ収集等が滞るリスク
  - 特に健康に関する機器で，その盗聴や漏えいのリスクに留意すべき理由は？
    - とくれば，答の軸は「センシティブなデータを扱うため」
  - 温度調節等の機能をもつ機器への不正アクセスだと，設定値が変更される
  - Webカメラの場合
    - カメラからの画像を受信・表示する管理用画面ではユーザ認証が行われていても，カメラからの映像は暗号化も認証もなされていないケース
    - 本文中に伏線を張った上で，「管理用画面を表示させるサーバにもたせる証明書が，オレオレであっても有効期限が長くても，そう問題ないという理由は？」
      - とくれば答の候補は「カメラとの間の暗号化が主目的であり，認証は考えなくてもよいから」

TLP：WHITE

予想⑤-3 「IoT」出題予想（2/5）

JP-RISSA 情報処理安全確保支援士会

- ITと比べた，OT（Operational Technology）機器の，情報セキュリティ面の留意点
  - システムのライフサイクルの長さゆえの問題
    - 古い機器の場合，インターネットとの接続を考慮していない機器がある
    - アップデートの体制や方法が確立されていない頃の設計のままで運用
    - サポート切れの機器やソフトウェアを使い続けるリスク
  - 攻撃の目的として，機密情報の窃取に加えて，可用性を下げる（システムの停止を狙う）攻撃が多い
  - 「安定運用」志向が裏目に出る
    - 特に，プラント等の連続操業される環境では，可用性を低める攻撃は致命傷
    - パッチ適用による可用性の低下を嫌う（適用失敗へのおそれや，適用のための作業時間そのものを嫌う）
    - 緊急性の高いパッチでも，GW，夏休，年末年始といった休止タイミングまで待たされる

予想⑤-3 「IoT」出題予想（3/5）

JP-RISSA 情報処理安全確保支援士会

- 「IoT」への攻撃
  - 多く普及するデバイス（Raspberry Pi等）を踏み台として用いた攻撃
  - 多数のIoT機器を乗っ取ることでの，DDoS攻撃のプラットフォームの構築
    - 例：2018年の「mirai」
  - 同じ攻撃するなら，多く普及する機器を用いた攻撃の方が（攻撃者にとって）有利な理由，とは？
    - とくれば「攻撃者側も同じ環境を入手・構築しやすい」「ボットネット構築に好都合」
  - 最近の攻撃手法例
    - ShadowHammer
      - 更新ファームウェアに乗じたマルウェアの配付
      - メーカの正規のディジタル証明書付きで配付されてしまった
    - レーザ光線を用いたマイクの遠隔操作

TLP：WHITE

予想⑤-3 「IoT」出題予想（4/5）

JP-RISSA 情報処理安全確保支援士会

- 通信ネットワークと絡めた着眼点
  - IoT機器がRESTの通信に耐えられるか
  - IoT機器に向く通信プロトコル等
    - MQTT（Message Queuing Telemetry Transport），ZigBee，Bluetooth，IPv6
  - IoT機器の認証（Wi-Fi，技適，VCCI等）
  - 遠隔地の機器との回線
    - 自前のLPWAか，業者によるサービス（「SORACOM Air」等）の利用か
  - 通信速度が非対称の回線（ADSL等）で，大量のIoT機器を管理したい場合，アップロード側の帯域が不足する
  - メインの処理を，本体で行うかクラウド（サーバ）側に投げるかの判断も必要
  - ということは，セキュリティに関わる重い処理も，本体でさせるかクラウド（サーバ）側に投げるかの判断が必要

TLP：WHITE

予想⑤-3 「IoT」出題予想（5/5）

JP-RISSA 情報処理安全確保支援士会

- その他，IoTならではの着眼点
  - 売った後のサポートが手薄になりがち
  - ライセンス違反（例：ハード・ソフトのライセンスが多岐にわたる，例えば画面にニュース等を映すとしたら情報提供業者の契約との照合も必要）
  - 情報提供業者やプラットフォームが，IoT機器のライフサイクルに耐えられる事業継続性をもつか（長期のサポートを受けられるか）
  - 現地に出向かないとファームウェアの更新ができない仕様だった
  - そもそも管理対象の機器が多かった
  - 開発時にテストの工数が増える（例：画面が映らない理由として，少なくともハードかソフトかの切分けが必要）
  - 某国で組み立てる，といったオフショアゆえのサプライチェーンリスク
  - 考慮すべきソフトの数や種類が増える
    - OSだけでも，組込みOS・操作端末としてのスマホのOS・Windows・macOS，さらに各OSでライセンスやAPIが異なる

予想⑤-4 「DX」出題予想

JP-RISSA
情報処理安全確保支援士会

- どう出すというのだろう。
- DXと好相性の通信プロトコル
  - WebSocket，IFTTT，QUIC，HTTP/2，IPv6
- “つながる社会”で組織外（協力会社等）からの攻撃や情報漏えい
- 正直，そう思いつかない…次いきましょう

TLP：WHITE

予想⑤-5 「その他」出題予想（1/5）

JP-RISSA 情報処理安全確保支援士会

- 量子コンピュータ
  - 実用化が早かったのは「量子鍵配送」
  - では，「耐量子計算機暗号」の出題は？
    - 本命は「格子暗号」だが，その規格が定まるのは3～4年後の見込み
      - 『CRYPTREC暗号リスト』に載るとしても，その後
  - 本文中に伏線として「署名・暗号化するデータの保存期間が数十年間」「量子コンピュータ（特に量子ゲート型）の技術向上が見込まれる」と書かれ，「なぜ早期に技術動向を調査すべきと判断したのか」とくれば，答の候補は
    - 「データの保存期間が長いから」
    - 「採用する暗号化アルゴリズムが，量子コンピュータによる解析技術に左右されるから」
- 「FIDO2」の特徴
  - CHAPと同様の技術を用いることで，ネットワーク上には平文パスワードや生体認証の情報を流さない
    - R01秋SC午前Ⅱ問1に「FIDO 1.1」が出たから，次は…

TLP：WHITE

予想⑤-5 「その他」出題予想（2/5）

JP-RISSA 情報処理安全確保支援士会

- ゼロトラストネットワーク
  - 信頼なんてできないから，検証の連続。本文中に伏線として「常に検証しながらとなると，検証のための手間が格段に増える」を読み取らせた場合…
    - 答の候補は「自動化させる」
  - 関連文書
    - O'Reilly本，NIST SP800-207（draft），BeyondCorp（Google）
  - FWでは守り切れない，FWよりも内側での攻撃例
    - サイドチャネル攻撃
    - 仕込まれたマルウェア，ランサムウェアによる攻撃
    - 不満を持った従業員による犯行
    - 物理的な破壊や侵入
- DNS関連
  - DoT/DoH（DNS over TLS，DNS over HTTPS）
  - RPZ：Response Policy Zones

予想⑤-5「その他」出題予想（3/5）

JP-RISSA 情報処理安全確保支援士会

- 「IPv6」関連（その①）
  - ICMPv4とICMPv6は，かなり異なる。では，どう出す？
    - 本文中に「ICMPを禁止する」とだけ書かれていて，受験者に「実害なんてせいぜいpingが通らない程度かな」と思わせつつ，実は「ICMPv6のタイプ1～3が使えない」「近隣探索（含・ルータ広告）が使えない」からIPv6環境が破綻する，と見破らせる出題
  - 不正な機器がRA（ルータ広告）を発し，LAN上の通信を吸い込む攻撃
    - 回避策の例
      - サーバやネットワーク機器の，ラックへの収納と施錠
      - 正当なRAへは，ルータ優先度をhighに設定しておく（他の追随を許さない作戦）
      - 経由するL2SWでの「RA Guard（RFC 6105）」
  - 一つのインタフェースが複数のIPv6アドレスをもつ
    - 「リンクローカル」「ユニークローカル」「グローバルユニキャスト」アドレス，等
    - 「グローバルユニキャストアドレス」は複数の値を設定できる。では，どう出す？
      - 複数もたせたIPv6アドレスの個々に対し，アクセス制御を行える（きめ細かいvs管理が面倒）
      - あるIPv6アドレス値をキーにログを検索する場合，同一ホスト宛てのパケットであっても，他のIPv6アドレス値を使った通信は検索に引っ掛からない

TLP：WHITE

予想⑤-5 「その他」出題予想（4/5）

JP-RISSA 情報処理安全確保支援士会

- 「IPv6」関連（その②）
  - IPv6環境では，IPアドレスの自動生成も可能。では，どう出す？
  - （注：現在では非推奨）「各端末はルータからのRA（ルータ広告）でプレフィックス（/64）を受信＋MACアドレスを基に算出したModified EUI-64を下位64ビットに用い，各端末自身のIPv6アドレスとする」方式の問題点は？
    - 公開サーバならともかく，「各端末のIPv6アドレスが固定値となり，しかもグローバルユニキャストアドレスなので，世界から “狙い撃たれる” 可能性」
    - 「各端末がもつMACアドレス値を推測できる」
  - では，その解決策は？
    - 「Privacy Extensions for SLAAC（RFC 4941）で，乱数値のハッシュ値を用い，一定時間で更新」 （SLAAC : Stateless Address Auto Configuration）
  - では，上記の解決策だとマズい点は？
    - 「サーバ用途には適さない」

予想⑤-5 「その他」出題予想（5/5）

JP-RISSA 情報処理安全確保支援士会

- 「IPv6」関連（その③）
  - IPv6のアドレス幅は128ビット。では，どう出す？
    - 逆引きを書くのが面倒（PTRレコードでは，連続するゼロを “::” で省略できない）
      - 本文中に「（手間が掛かるから，等で）逆引きは設定していない」と書かれていた
        - 答の候補は，「逆引きできないが故のトラブル」
    - IPv4との併用環境で，ログ中のIPアドレスのフォーマットが崩れる可能性
      - IPv6アドレス値の推奨される表記方法が，RFC 5952で規定されている。これはなぜ？
        - 答の候補は，「ログの検索時に，狙ったアドレス値をヒットさせやすくするため」
    - UDP53（一般的な512バイトまでのDNS応答）では足りない，長大な応答があり得る
      - 「EDNS0（RFC 6891）」や「TCP53」の設定も行う
    - 「多数のIoTデバイスに割り当てるには，IPv6アドレスを使うしかない」と答えさせる

- 以上，出題予想でした。
  - 当会からの最新情報は，次のスライドを。

TLP：WHITE

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

お問い合わせ : contact@jp-rissa.org

Twitter : @jp_rissa

JP-RISSA

情報処理安全確保支援士会