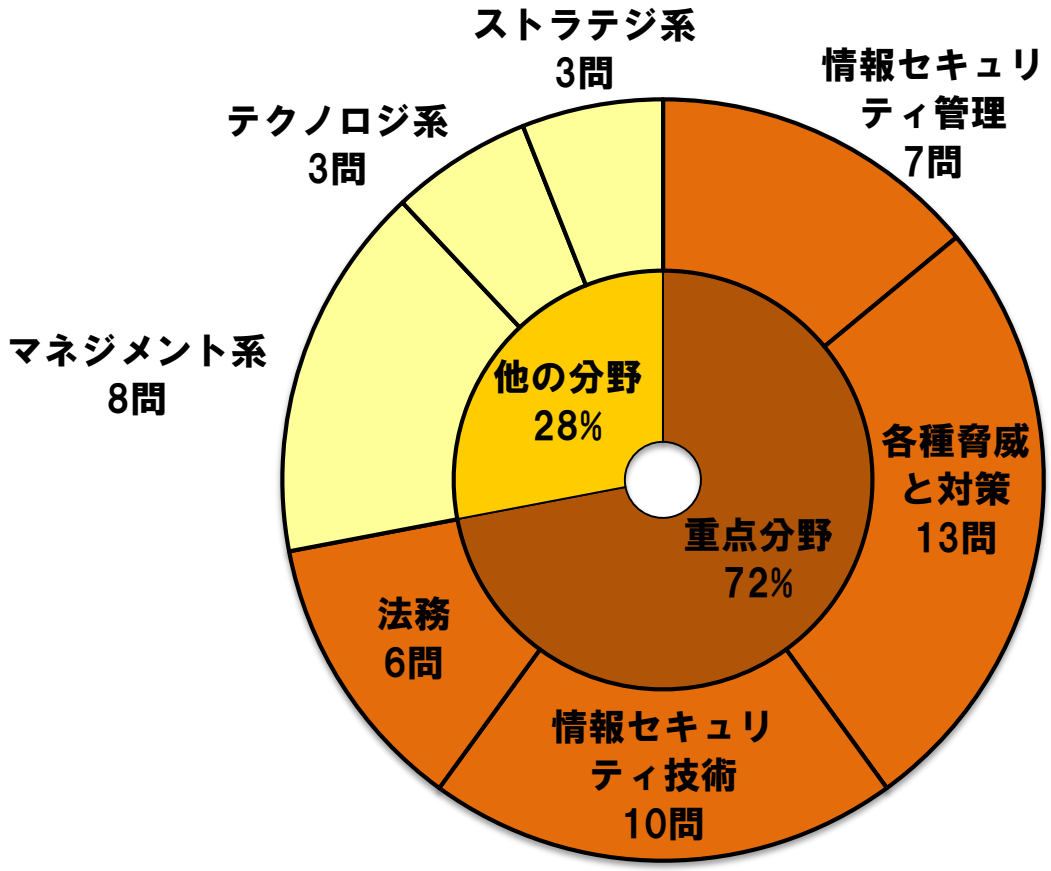
令和元年度　秋期試験
情報セキュリティマネジメント（SG）
出題傾向・分析

TAC株式会社

2019年11月

午前　出題比率



午前　出題テーマ

問1～30の3分野は，ややランダムに配置されている

- **情報セキュリティ管理**
  - 各種ガイドライン・リスクマネジメント
    （JIS Q 27000シリーズが多い）
- **各種脅威と対策**
  - 各種攻撃の特徴や，それらに対する対策
  - ネットワークセキュリティの問題が目立った印象
- **情報セキュリティ技術**
  - 暗号化技術，PKI（公開鍵基盤）
  - 今回は問題数が増加した

午前　出題テーマ

・法務　（問31～36）

情報セキュリティ関連の出題が少なく，
派遣や就労規則などの労働関連の出題が多め

・その他の分野　（問37～50）

［マネジメント系］

監査が4問，サービスマネジメントが2問，
プロジェクトマネジメントが2問

［テクノロジ系・ストラテジ系］

各分野から1問ずつ

午前　新規出題テーマ

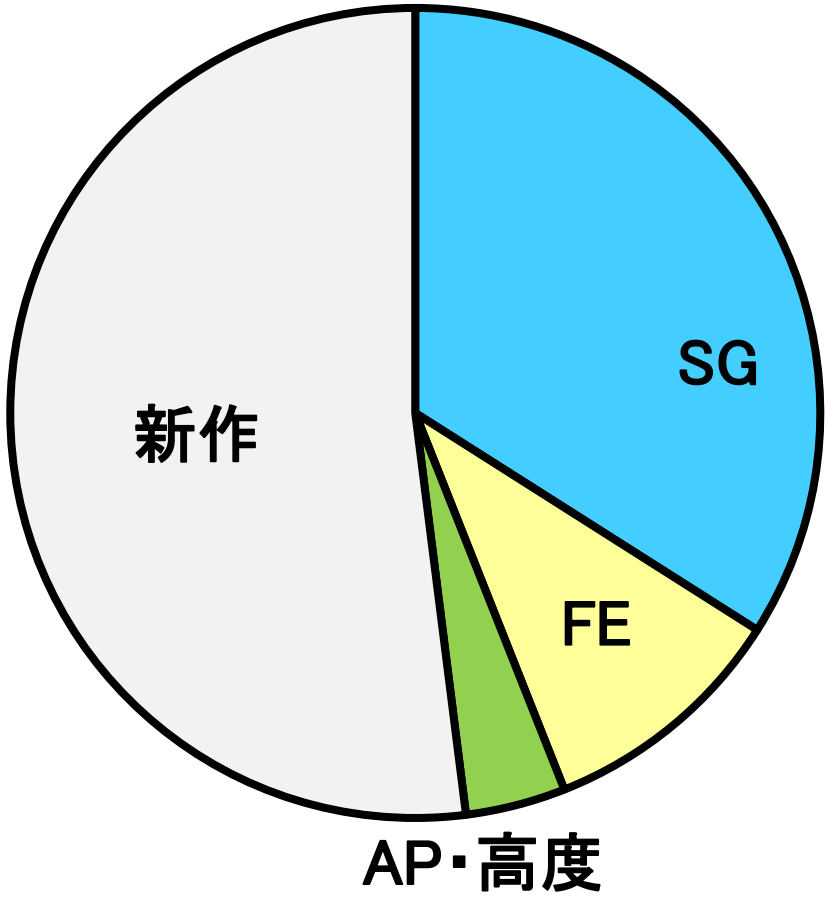
重点分野

- JIS Q 27017
- BEC
- リバースブルートフォース
- トランザクション署名
- フォールスポジティブ
- ランダムサブドメイン攻撃
- SMTP-AUTH など

その他の分野

- エラープルーフ
- RPA
- テキストマイニング など

午前　過去問題の流用



- 同区分(SG)からの流用が増加
- 今回は新作問題が多め

午前　難易度：やや高め

- 「問われる内容が深化した問題が多い」という傾向が続いている
- 各分野で初出用語などの問題が出題される

⇒ 難易度はやや高め

ただし，

SGからの過去問流用が増えてきた！

午後 問1：出題テーマ

ECサイトのセキュリティ改善

- **パスワードクラック手法**がメインテーマ

攻撃	調査結果
攻撃 1	J サイトの 2018 年 10 月からのログインログを確認したところ，2018 年 11 月 5 日の 3:00～4:00 に海外のある IP アドレスから，不正ログインの試みと思われる攻撃が 980 件の顧客用アカウントに対して 1 件ずつあり，その全てが J サイトに実在する顧客用アカウントに対するものであった。980 件の不正ログインの試みのうち，90 件が成功していた。
攻撃 2	J サイトのアクセスログの中からアカウント新規登録画面へのアクセスのログを確認したところ，攻撃 1 と同一の IP アドレスから合計 100,000 件のアカウントの登録が 2018 年 10 月から試みられており，攻撃 1 の不正ログインで利用された 980 件が登録済みアカウントとしてエラーとなっていた。
攻撃 3	2018 年 11 月 1 日に，J サイトのログインログに，国内の複数の IP アドレスからそれぞれ一つの顧客用アカウントへのログイン試行が，IP アドレスごとに平均 1,000 件程度記録され，全てログイン失敗になっていた。
攻撃 4	2018 年 11 月 6 日に，誘導メッセージが書かれた問合せを J サイトに 50,000 件投稿するという攻撃があった。カスタマサポート部は問合せの中から誘導メッセージ以外のメッセージを抽出するのに多くの工数を取られ，顧客の問合せ対応が遅延した。問合せ内容に書かれた電話番号数件に電話で確認したところ，投稿はしていないとのことであった。 誘導メッセージは，攻撃 1，攻撃 2 とは別の海外のある IP アドレスから投稿された。1 件目と 2 件目は問合せフォームを閲覧してから問合せが投稿されていたが，3 件目以降は閲覧せずに問合せが投稿されていた。

「パスワード管理」の知識で対応可能

（令和元年度秋期　情報セキュリティマネジメント試験　午後試験問1より）

午後 問2：出題テーマ

アカウント乗っ取りのインシデント対応

・システムやサービスの仕様に関する情報が多く，これらを読み解くのにやや時間がかかる

1 基本機能
1.1 利用者は PC の Web ブラウザ，又はスマホの Web ブラウザ若しくは V サービス専用アプリケーションソフトウェア（以下，V アプリという）を利用してアクセスする。
1.2 同一利用者が PC とスマホの両方から同時にログインできる。
2 ワークスペース（以下，WS という）
2.1 利用者は，WS を作成することができる。WS を作成した利用者は，作成した WS の管理者権限をもつ。
2.2 WS の管理者権限をもつ利用者（以下，WS 管理者という）は，他の利用者を WS に参加させること，WS に参加している利用者（以下，WS 参加者という）に管理者権限を付与すること，及び WS を削除することができる。
3 グループチャット（以下，GC という）
3.1 WS 管理者は，WS 内に GC を作成し，WS 参加者を GC に参加させることができる。
3.2 利用者は，V サービスにログイン後，自身が参加している WS 及び GC にアクセスできる。
3.3 利用者は，GC 内で文字列のメッセージ（以下，GC メッセージという）及びファイルを送信できる。GC メッセージ及びファイルは GC 内に保存され，GC に
下，GC 参加者という）だけが閲覧できる。
3.4 GC メッセージ及びファイルには，送信した利用者のアカウント名
送信情報という）が記録される。
3.5 送信された GC メッセージは GC ごとに直近の 1,000 件分が，ファ
100 件分が保存され，それより前のものは自動的に削除される。削除
びファイルについての GC 送信情報も同時に削除される。
3.6 WS 管理者は，WS 内の GC メッセージ，ファイル，及び GC 送信情

4 セキュリティ機能
4.1 V サービスへの接続には，HTTP over TLS を使用する。
4.2 各利用者のアカウントは，メールアドレスを利用者 ID として登録し，ログイン時の利用者認証のためのパスワードを設定する。パスワードは英大文字，英小文字，数字，記号の文字種の全てを組み合わせ，8 文字以上でなければならない。
4.3 Web ブラウザを閉じた場合は，一定時間後に自動的に V サービスからログアウトされる。V アプリを閉じた場合は，その時点で自動的に V サービスからログアウトされる。
4.4 利用者が自身のパスワードを変更した場合，利用中の全てのセッションで V サービスからログアウトされ，再度ログインを求められる。
4.5 利用者は追加の利用者認証機能（以下，V 認証機能という）を有効にすることができる。
・V 認証機能を有効にした場合は，V サービスへのログイン時に，利用者 ID とパスワードによる利用者認証に加え，あらかじめ登録しておいた電話番号に SMS で送信される 6 桁の数
ールアドレスに送信される 6 桁の数字を入力するこ
号，又は V サービスへのログイン時に発行される
スを利用する端末かどうかを判断する。
までの 2 度目以降の V サービスへのログイン時の追加
（以下，V 省略機能という）を有効にすることができ

選択肢の取捨選択に迷う設問が多め

（令和元年度秋期　情報セキュリティマネジメント試験　午後試験問2より）

午後 問3：出題テーマ

業務委託におけるセキュリティ

・職位ごとのアカウント設定や入退室管理，PCごとのアクセス管理などが論点

項番	要求事項	評価結果	評価根拠
5	X 業務で N サービスへのアクセスが可能な業務エリアは Y-CS 部の業務エリアだけに限定すること	NG	・現状のままでは，Y 社で N サービスにアクセスできるようになったら，［ c ］が，3 階以外から N サービスにアクセスできてしまう。 ・（省略）
8	X 業務を実施する業務エリアへの入室は，入室権限が与えられている従業員だけに制限すること	NG	入室権限に，次の 2 点の不備がある。 ・［ d ］ ・［ e ］
12	（省略）	NG	・②複合機が初期設定のままになっている。
13	X 業務には，Y 社貸与の PC を使用すること	OK	（省略）
14	X 業務で使用する PC では，外部記憶媒体へのアクセスを禁止すること	NG	・Y-PC で実装している技術的な制限では，外部記憶媒体のデータの読込みが可能となっている。
18	インターネット上の Web サイトへの X 情報の持出しをけん制する対策があること	NG	（省略）

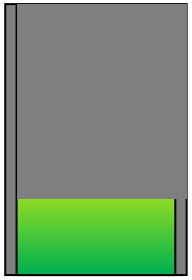
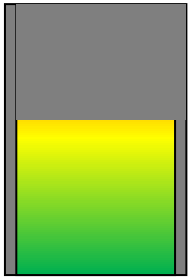
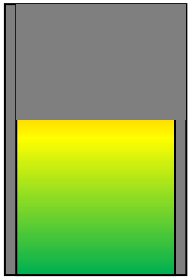
複数の要件確認の必要があり，時間がかかる。

（令和元年度秋期　情報セキュリティマネジメント試験　午後試験問3より）

午後　難易度

・問題文のボリュームは，13，14ページ
ただし，問1が平易な問題

⇒ 午後試験全体としては，
時間的に余裕をもって解答が可能

問1	問2	問3
		
易しめ	標準	標準

午前試験対策

【テキスト学習】

- 各種ガイドラインに目を通す

  JIS Q 27000シリーズ

  組織における内部不正防止ガイドライン

  サイバーセキュリティ経営ガイドライン

  中小企業の情報セキュリティ対策ガイドライン

- 各種攻撃と対策の基礎知識 → 午後対策

午前試験対策

【テキスト学習】

- 技術は「暗号化」と「認証」を中心に
- システム監査とサービスマネジメント
- シラバス Ver3.0の新用語

【演習】

- 同区分(SG)からの流用率が増加

⇒ **過去問演習が重要**

午後試験対策

- 「インシデント対応・対策」,「アクセス制御」,「リスク分析」 の重要テーマを中心に
- 可能ならば，全ての過去問題の演習を！

午後試験対策

- 時間内で長文読解する練習を!!
  - 「問題文を読む」,「設問を解く」などの時間配分を意識する
  - 下線を引いたり，丸で囲んだり，手を動かしながら解く
  - 選択肢もヒントにし，消去法も駆使して，正解候補を絞り込む

ご清聴ありがとうございました