第 70 回：「どこより早い令和 6 年春期セキスペの分析」
～午前 2 試験から読み解く情報セキュリティの最新トレンド～

掲載日：2024 年 5 月 9 日
執筆者：株式会社スクウェイブ
カウンセラー
和田　柊平

先日、情報処理安全確保支援士試験（以下セキスペ）の令和 6 年春期試験を受験した。さっそく午前試験について自己採点を行ったところ、午前 1 試験は 30 問中 26 問（合格ラインは 18 問）、午前 2 試験は 25 問中 19 問（合格ラインは 15 問）正解していた。午後試験については自信がないものの、次回は午前 1 試験の受験が免除されることも踏まえれば、最低限の結果は残すことができたのではないかと感じている。

ところで、古くから「鉄は熱いうちに打て」という。そこで、令和 6 年春期試験の午前 2 試験の問題を参照し、今回問われた新論点を抽出することにより、情報セキュリティに関する最新トレンドについて（おそらくどこより早く！）分析したい。本記事が企業のセキュリティ担当者だけでなく、将来のセキスペ受験者にとって有益なものとなることを願ってやまない。

まず、午前 2 試験の第 7 問では、「ISMAP-LIU」が問われた。「政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program：ISMAP）」とは、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録し、政府機関が情報システムを構築する際には原則的には ISMAP に登録されているものから選択することで、クラウドサービスの円滑な導入に資することを目的とする制度である。この ISMAP 自体は 2020 年から運用が開始されていたが、ISMAP の枠組みのうち機密性の観点から重要度の低い情報のみを扱うサービスに用いる SaaS のみを対象としたものが「ISMAP-LIU」であり、2022 年 9 月に運用が開始された。

また、第 8 問では、「SIM3」が問われた。近年では CSIRT を設置する企業が増加しており、これ自体は情報セキュリティの観点からは望ましい傾向であるといえる。しかし、CSIRT が形骸化しているケースも多々あり、これではいくらわざわざ組織を設置したとしても意味がない。そうした背景から、組織・人材・ツール・プロセスの 4 つの観点から CSIRT の成熟度を評価するモデルである「SIM3（Security Incident Management Maturity

Model)」に注目が集まっている。その内容にはたとえば、プロセスの観点の中には、社内のメール管理者や Web サーバー管理者との連携を評価する、P-10「E-mail や Web 上のベストプラクティス」という項目などが含まれている。なお、2022 年には欧州ネットワーク情報セキュリティ機関（ENISA：The European Union Agency for Cybersecurity）が SIM3 をベースに CSIRT の成熟度を測るフレームワークを改訂している。

さらに、第 17 問では、「SBOM」が問われた。この「SBOM」とは Software Bill of Materials の略であり、パッケージソフトウェアやデジタル機器向けの組み込みソフトウェアを構成するコンポーネント及び、コンポーネント間の関係性を一覧化したソフトウェア管理手法のことである。この SBOM の導入の背景には、2020 年頃から米国企業や米国政府がソフトウェアに仕掛けられたバックドアによって相次いでサイバー攻撃被害を受けたことから、ソフトウェアサプライチェーンの管理が重視されるようになったことが挙げられる。この SBOM は、脆弱性管理やライセンス管理を効率化できる手段としても注目を集めており、日経コンピュータ 2024 年 4 月 18 日号では特集を組まれている。

最後に、第 25 問では内部統制について出題されたが、ここでも問題文には「“財務報告にかかる内部統制の評価及び監査に関する実施基準（令和 5 年）”」と記載されていた。午前 1 試験の第 21 問でも、「システム監査基準（令和 5 年）」との記載がある。気付きにくいかもしれないが、昨年の改訂が問題文中に反映されていたのである。

わずか 25 問の午前 2 試験において「ISMAP-LIU」、「SIM3」、「SBOM」、「“財務報告にかかる内部統制の評価及び監査に関する実施基準（令和 5 年）”」と 4 つの新論点が出題されたことは注目に値する。それだけ、近年の IT や情報セキュリティを取り巻く環境の変化が激しいということを示唆しているようにも思える。ちなみに、同日行われた応用情報技術者試験の午後問題では、「ゼロトラスト」が出題されていたことが X（旧 Twitter）で話題になっていた。投稿を見る限り、この問題の正答率は高くなかったようである。それだけに、最新の IT 動向やセキュリティ動向に注視し続けることが必要なのである。

なお、当社では昨年改訂され新しくなったシステム監査基準や統一基準群について熟知した監査人によるシステム監査を実施している。また、当社のコアコンピタンスが IT に関連するベンチマークであることもあり、CSIRT の成熟度や情報セキュリティインシデント対応についても評価し改善に向けた提言を提供できる。さらに、当社ではクロスワードパズルを用いた教育ツール「Cyber Cross」を展開しているが、サンプルとして、例えば「セキュリティ用語」や「IT パスポート対策 ストラテジ系」編などを提供している。いずれのツールやソリューションについても、関心のある方は官民問わず、お気軽にお声がけいただきたい。