

開催報告

デジタル庁「ISMAP-LIU に対する意見公募手続きの開始」に伴う説明会

令和4年6月28日(火)、社会の革新委員会 デジタル社会推進部会(加藤健(株)オーイーシー 代表取締役社長)による標記説明会がオンラインで開催され、84名が参加した。

本説明会は、デジタル庁 戦略・組織グループ セキュリティ・危機管理 主査 三宅宗俊氏から「ISMAP-LIU について」説明があった。その後、参加者との質疑応答・意見交換が行われた。

現在、政府は政府情報システムのためのセキュリティ評価制度(ISMAP)の枠組みにおいて、民間企業・団体等から広く意見を募集している。今回の説明会では、意見公募をするに当たり、JISA 会員向けに「ISMAP-LIU 策定の背景」や「基本構成」、「対象業務一覧の取扱いについて」等について説明があった。本仕組みについては、ISMAP が対象とするクラウドサービスのうち、セキュリティ上のリスクの小さな業務・情報の処理に用いる SaaS サービスに対する仕組みであり、情報システムの調達においては、業務・情報の影響度に応じたセキュリティを確保すべきとの考え方から、影響度が低いと評価される業務、情報に用いられる SaaS を対象とする制度となる。

ISMAP セキュリティ確保の仕組み

- 本制度は、クラウドサービスの情報セキュリティに関するJIS Q(ISO/IEC) 27017等を基礎としてクラウドサービスに係る**統一的なセキュリティ基準(管理基準)**を策定・公表。基準の策定の際には、システム監査にかかる知見者を集めたWGにおいて議論。
- 本制度が選定する**監査主体**による**監査プロセス**を経て、**クラウドサービス事業者(CSP)**において、**管理基準**が適切に実施されているかを確認。毎年、登録簿更新審査を行い、継続的な確認を実施。
- 管理基準では、情報セキュリティマネジメントに加えて、クラウドサービスのパフォーマンス、信頼性、データ、ネットワーク、ソフトウェア等に係る**セキュリティ対策の実装**を要求しており、**監査**においてもこれらの実装状況まで確認を行うこととしている。

CSP登録の流れ

① 規制的事務
内閣府(ISC、ITP)・経済産業省(ISC、ITP、JISA)

② 登録
登録簿

③ 監査
監査主体
クラウドサービス事業者(サービス事業者)

④ 登録簿更新審査(毎年)

管理基準の構成

クラウドサービス事業者(CSP)

① バランス基準
② マネジメント基準
③ 管理基準
④ 個別のセキュリティ対策

① バランス基準
目的: 経営者は、情報セキュリティの義務及び方針を承認する。
内容: 経営者、管理者、情報セキュリティの義務及び方針を策定・実施させる。
目的: 目的は、監査時に、情報セキュリティの目的を事業目的に合わせた確認させる。

② マネジメント基準
目的: 情報セキュリティマネジメントの確立
内容: 情報セキュリティマネジメントの運用
目的: 情報セキュリティマネジメントの維持及び改善

③ 管理基準
目的: クラウド事業者に対する要求事項
内容: パフォーマンス(運用)のモニタリング
目的: 信頼性の確保
内容: サービスの信頼性
目的: 脆弱性による脆弱性の
内容: サービス脆弱性
目的: マルウェア/ランサムウェア
内容: ネットワークセキュリティ
目的: 高度化の促進
内容: ネットワークセキュリティ
目的: 冗長性
内容: ソフトウェア管理

(デジタル庁主査三宅氏資料より抜粋)

参加者からは、政府におけるクラウドセキュリティの考え方や監査方法等について意見交換・質問があった。

(小泉)