

IT時事ネタキーワード「これが気になる！」(第129回)

政府、サイバー攻撃対策で米国基準義務付けへ

2023.08.16



国の行政機関等のサイバーセキュリティ対策の基準を作成する内閣サイバーセキュリティセンター(NISC)は、7月4日、会議「サイバーセキュリティ戦略本部」において「政府機関等のサイバーセキュリティ対策のための統一基準群」を改定した。

統一基準群(ガイドライン、統一基準、統一規範)は、サイバーセキュリティ基本法に基づき、政府機関及び独立行政法人等(以下「政府機関等」)の情報セキュリティ水準を維持・向上させるための統一的な枠組みで、政府機関等の情報セキュリティのベースラインを示す。各機関は統一基準に準拠しつつ、組織や取り扱う情報の特性などを踏まえて各組織の情報セキュリティポリシーを策定する。これにより、政府機関等のどの組織においても一定以上のセキュリティ対策の水準が確保される、という形だ。

政府は業務委託先に米国基準の情報セキュリティ対策を義務付けへ

統一基準群の2005年12月の初版策定から17年、今回の改訂は2年ぶりとなる。サプライチェーンの脆弱な部分を起点としたサイバー攻撃リスクの増大を踏まえた業務委託先に求める対策、ソフトウェアに係る対策の強化、政府機関等でのクラウドサービス利用の拡大、最新のサイバー攻撃に対応した対策強化を盛り込むなど、昨今の状況に即した見直しを行っている。

統一基準群の対象はあくまで「政府機関等」ではあるものの、業務委託やクラウドサービスなどの外部委託に際し、情報保護などのため業務範囲や責任範囲を明確化、双方で情報セキュリティ対策の詳細について合意することに重きを置き、米国基準「NIST SP800-171」を参考とした基準の明確化を図っている。この基準をもとにした対策義務付けが今回の大きな改定の1つだ。6月に政府が業務委託先の企業に対し、2023年度中に対応を義務付ける旨の報道もあり、政府機関等から業務委託される企業に少なからず影響を与えると思われる。

委託先に8項目の確実な実施が契約条件。契約後も運用状況などを報告… 続きを読む