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、ソフトウエ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

今回の改正で、政府機関等が業務委託を行うに当たり、委託先の情報セキュリティ対策は通常、直接管理できないため、政府機関等で実施・確認すべき事項と委託先に求める事項を区分して明確化する。また、政府情報の適切な取り扱いのため、業務委託先に求める情報セキュリティ対策の事項を定めるという。さらに、委託先に求める情報セキュリティ対策の事項は、米国国立標準技術研究所（NIST）が公表しているサプライチェーンにおける情報セキュリティ対策のガイドライン「NIST SP800-171」を参考に8項目を規定する。今後、各府省の調達において、委託先に求める要件としてこれらを契約に含めることとなった。

8項目の基本対策事項とは、①インシデント等への対処能力の確立・維持、②アクセスする主体の識別とアクセス制御、③ログの取得・監視、④機器等の物理的保護、⑤要員への周知と統制、⑥資産管理・リスク評価、⑦システム及び情報の完全性の保護、⑧セキュリティ対策の検証・評価・見直し、となる。「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の改定のポイント」の図表（23～24ページ）が参考になる。

なお、委託業務でクラウドサービスを利用する場合、原則ISMAP（政府情報システムのためのセキュリティ評価制度）などのクラウドサービスリストから選定すること、ソフトウエアをはじめとする機器などの調達に関しても「IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」に基づいた選定や管理を行うこと、なども明確化している。

契約の際は、ガイドラインの順守と適正な情報セキュリティ対策の実施が要件となるが、契約中は情報セキュリティ対策の履行状況の定期的な報告、委託された業務でのインシデントの発生や情報の目的外利用を認知した場合の措置などを報告する義務がある。これらが順守されない場合は、委託業務の中止や契約解除の可能性もあるので注意が必要だ。

防衛省では既に各種の取り組みを進める

防衛省では2022年3月、防衛産業におけるサイバーセキュリティ体制の強化のための施策を促進するため、先行する米国の取り組みを参考に「NIST SP800-171」と同水準の管理策を盛り込んだ新たな情報セキュリティ基準である「防衛産業サイバーセキュリティ基準」を整備している。防衛産業に携わる企業を対象に2023年度から施行し、国が民間に供給網のセキュリティを義務付けるのは、国内初の試みという。

背景には、防衛産業の国際化の大幅な進展およびサイバー攻撃などのリスクにより旧基準では情報の適切な保護が難しくなったこと、同盟国・パートナー国との間で秘密情報を適切に保護するため「実質的同等」な産業保全制度が不可欠になったこと、2022年12月の国家防衛戦略において、国際水準を踏まえた防衛産業保全の強化を行う方針を決定したこと、などが挙げられる。

旧情報セキュリティ基準はISOベース（ISO2700、情報セキュリティマネジメントの国際標準規格、2006年）で、サイバー攻撃を未然に防止することに重きを置き、攻撃を受けた場合の対応や復旧のための対策に欠けていた。新基準は攻撃を受けた後の対策として、従来の「特定」「防御」に「検知」「対応」「復旧」の3項目が加わり、サイバー攻撃に対し、早期発見・対処のための措置を充実させている。

なお、米国では2017年から、国防調達において保全が必要な情報を取り扱うすべての企業に「NIST SP800-171」の要求事項を満たすことを義務化している。取引先を侵入口とするサイバー攻撃を想定、迅速に復旧するための備えを強めているのだという。

話を戻して、今回の統一基準群の外部委託に対する改訂は、委託先が運用するファイル共有ツールへの不正アクセスにより事業者に委託していた政府機関等の情報が流出する事案が発生したこともあり、サプライチェーンの複雑化に伴い、委託先などの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によるリスクの増大を想定、防衛省における情報セキュリティ対策基準の見直しを他省庁にも広げた、と考えられるだろう。

今後の動向は？

今回のメインテーマとして扱った統一基準群の内容は多岐にわたり、実施すべきことは多数にのぼる。政府機関等の委託先にとって、今後の契約に先述の情報セキュリティ対策が要件となること、および今のサイバー情勢を考えると、整備は急務といえる。必要に応じて専門家知見を活用する、関連ソリューションの導入を検討する、なども有効だ。

統一基準群、特に8項目の基本対策事項は、事業者すべてにおいて、今後のセキュリティ対策の基準となっていくと思われる。政府機関との取引がなくても企業の存続にとって情報セキュリティ対策は重要な事項だ。ぜひ目を通し、今後の動きに注目しよう。

※掲載している情報は、記事執筆時点のものです