外部委託先まで考慮

認識不足 浮き彫りに

独立行政法人情報処理推進機構（IPA）が先頃公開した「ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」によると、情報通信業以外の委託元は過半数が、実施すべき情報セキュリティー対策を仕様書などで委託先に明示しておらず、特に、製造業では71・1％、卸売・小売業で74・2％と顕著であった。また、委託契約における情報セキュリティー上の責任範囲（責任分界点）が分からないと回答する割合が、委託元、委託先とも最多という結果であった。委託元のサプライチェーンに対するセキュリティー意識の不足が浮き彫りとなった。

しかし、サプライチェーン上のインシデントの影響は、直接の被害組織だけでなく、複数の関係者に影響を及ぼす可能性があり、看過できない課題となっている。

今後、サプライチェーン上で要求されるセキュリティー要件をクリアしないとサプライチェーンに加わることができない、あるいは、サプライチェーンから排除されてしまう可能性も出てくることが想像される。委託元とも委託先ともなり得るであろう中小企業は、いずれの立場においてもセキュリティー対策に取り組んでいく必要がある。

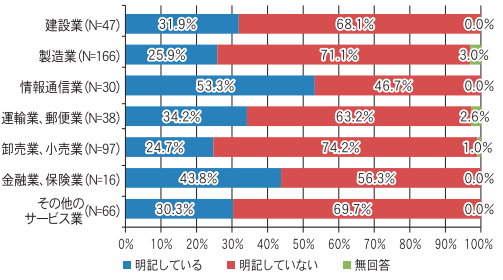
責任範囲を契約書に明記

IPAが2016年に公開した「中小企業の情報セキュリティ対策ガイドライン（以下、ガイドライン）」には、経営者が認識すべき3原則が示されており、うち一つに「委託先の情報セキュリティ対策まで考慮する」ことを挙げている。また、ガイドラインでは取り組みの具体例も挙げているので紹介したい。

業務の一部を外部に委託する場合は、委託先でも少なくとも自社と同等の対策が行われるようにしなければならない。そのためには契約書に情報セキュリティーに関する委託先の責任範囲や実施すべき対策、再委託の取り扱いなどを明記し、合意する必要がある。また、必要に応じて委託先を訪問し、対策の実施状況を確認する。

ITシステム（電子メール、ウェブサーバー、ファイルサーバー、業務アプリケーションなど）に関する技術に詳しい人材がいない場合には、外部サービスを利用した方が、コストと情報セキュリティー対策との両面から有利なときがある。ただし、無償の外部サービスなど情報セキュリティー対策を求めることが難しい場合や、有償であっても個別契約などでサービス提供者の責任や対策を規定することが難しい場合もあるので、利用規約やサービスに付随する情報セキュリティー対策などを確認した上で選定するよう経営者は担当者に指示する必要があるだろう。

なお、ガイドラインでは「委託契約書機密保持条項サンプル」を提供している。サプライチェーンに対するセキュリティー対策を検討する上で参考としてほしい。詳しくはIPAのウェブサイト（https://www.ipa.go.jp/security/keihatsu/sme/guideline/）で確認してほしい。

（独立行政法人情報処理推進機構・江島将和）

委託先が実施すべき具体的な情報セキュリティー対策の仕様書などでの明記の有無（委託元の回答）