資料３－２

「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」について

「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」について

平成25年度～26年度の取組

「政府機関の情報セキュリティ対策のための統一基準（平成26年度版）」の改定
（平成26年５月19日情報セキュリテイ政策会議決定）

機器等を調達する場合、府省庁外の者に情報システムの構築やアプリケーション開発等を外部委託する場合等における情報セキュリティ上のサプライチェーン・リスク対策として、機器等の製造過程や外部委託先において政府機関の意図せざる変更が加えられない管理がなされていることを、委託先や機器等の選定条件とすることについて、統一基準に追加規定。

さらなる対策強化、対策の実効性向上を目的に

平成26年度～27年度の取組

「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」の策定

サプライチェーン・リスク対応の目的や具体的な対策例等を解説し、統一基準の規定内容に関する理解を深めることで、府省庁における情報セキュリティ上のサプライチェーン・リスクに対応するための調達仕様書の円滑な作成に資することを目的に策定。

「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」について

- 政府機関の情報システムの構築、運用等の外部委託や機器等の調達のうち、WTOによる政府調達協定の“第三条安全保障のための例外及び一般的例外”を除いたものが、本手引書の主な対象。
- IT調達における調達側と供給側の管理の手法に係る国際規格のうち、情報通信技術に係るサプライチェーンに関するセキュリティのガイドラインであるISO/IEC27036パート3の規定事項※を踏まえるなど、国際規格を参考に規定。

※ ISO/IEC27036パート3の規定内容
『国境をまたいで増大するサプライチェーン・リスクに対応するために、WTOによる政府調達協定を尊重しつつ、供給側との関係を構築し、モニタリングして、調達案件における情報セキュリティを確保することが必要である』と謳われている。

- サプライチェーン・リスクに係る脅威や脆弱性、それらによって生じるリスクを例示し、リスク軽減の考え方を解説。

リスク軽減の考え方の一例

脅威		脆弱性		リスク
委託先、再委託先等の従業員によって不正なプログラムが情報システムに埋め込まれる	＋	委託先、再委託先等の従業員や納入する機器やソフトウェアのセキュリティ管理が不十分	＝	情報システム稼働後に、不正プログラムが起動され、情報システムで取り扱われる機密性の高い情報が窃取される

脅威に対する対策（例えば不正なプログラムが埋め込まれていないことを確認すること）は困難な場合があるため、委託先等に対してセキュリティに係る厳格な管理体制を求めることで脆弱性を解消しリスク軽減を図る。

- 委託先、再委託先等におけるセキュリティ管理体制の確認等を目的とした仕様書記載例を提示。

  - 府省庁の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、具体的な管理手順や品質保証体制を証明する書類等を提出すること。
  - 情報システムに意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、府省庁と連携して原因を調査し、排除するための手順及び体制を整備していること。それらが妥当であることを証明するため書類を提出すること。
  - 再委託する場合は、受託者は、契約上受託先に求められる水準と同等のセキュリティ水準が再委託先においても確保すること。
  - 委託事業の運用に係る要員を限定すること。また、全ての要員の所属、専門性（資格等）、実績及び国籍について提示することこと。