

2013年1月8日

独立行政法人情報処理推進機構(IPA)

サプライチェーン・インテグリティ ～ICT サプライチェーンにおけるリスク、課題および改善に向けて～

本概要は、欧州ネットワーク情報セキュリティ庁(ENISA:European Network Information Security Agency)が発行する、“Supply Chain Integrity – An overview of the ICT supply chain risks and challenges, and vision for the way forward”のエグゼクティブ・サマリーの抄訳となります。

内容の詳細につきましては、原文をご参照ください。(※本文中のリンク先は全て英文となります)

URL: <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/sci>

エグゼクティブ・サマリー

情報通信技術(ICT)産業におけるサプライチェーン・インテグリティ(SCI)は、サプライチェーン・コントロールの幅広い見直しの一環として、官・民(例:ベンダ、重要インフラ所有者・運用管理者など)両方から注目を集めている問題である。サプライチェーンへの理解は事業の成功、つまりは国家の経済に不可欠な要因のひとつであり、その中でもインテグリティはサプライチェーンの管理のための重要な要素として、EU加盟国にガイダンスを提供するべく本報告書で取り上げている。本報告書の目的のひとつは、ICT産業におけるSCIとは何かを明らかにし、また、SCIを確保するための方法を提案することである。ICT産業は非常に包括的で、1冊の報告書で全てをカバーするのは困難なため、本報告書ではICT産業のモデルとして、主に通信産業について記すものとする。

サプライチェーンはグローバル化が進み、地理的にも広く、介在する業者の数的にも多くなってきている。これは、市場のより幅広いグローバル化の動きとも、ある主要産業とその関連サプライヤーが地理的に集約している状況からの脱却の動きとも一致している。通信事業者と通信機器ベンダにおける、グローバルに調達しているシステム構成部品への依存度も益々高くなっている。ニッチな市場では、ただ1社のサプライヤーが産業全体の需要を賄い、流通経路が依存性の高い市場を支えている(例:マイクロソフト社はPC市場の83%にOSを供給している)。ICT市場の大部分にあてはまる特徴の1つは、ソフトウェアやファームウェア、チップの設計などを電子データ(soft formats)で流通させることができる点であり、これが原材料、ロジスティクス・ネットワーク、作業員といった形態の他のサプライチェーンとは異なる観点をもたらしている。

本報告書の根底を為すのは、政府、企業、組織、消費者など、我々のICT製品およびサービス、引いてはICTサプライチェーンへの依存度が益々高まっているという認識である。結果として、開発・流通・運用の中での意図的な改ざんや、流通前または流通経路での偽物(複製品または余剰品)とのすり替えといった脅威、サプライチェーンを通じた社会経済への攻撃など、サプライチェーンへの依存性という脅威に注目が集まるようになった。

本報告書ではこうした脅威の性質を特定し、対策を講じるに役立つ戦略を検討する。サプライチェーンの関係者は、ICT サプライチェーンのリスクを評価・管理するのに、共通の基準となる業界のベストプラクティスに沿って必要な対策を実施するよう勧告する。また、政府は民間と協力し、国際的な評価フレームワークを確立しなければならない。

フレームワークは、以下の特徴を備えているべきである。

- リスクベースで、適切な脅威モデルに基づいていること
- 透明性があること
- 一貫性があること (consistent)
- 柔軟性があること
- 標準ベースであること
- 国際通商取引に通用する相互認証制度であること

本報告書は、欧州委員会 (EC)、EU が資金援助している調査研究プログラム、加盟国の関係者、標準化団体など、様々な組織やコミュニティに推奨施策を提示している。

これらの組織やコミュニティでは、以下を考慮に入れて SCI に取り組むべきである。

1. 改良された、革新的なトラスト・モデル
2. 評価およびインテグリティの検証技術の改善
3. 現行様々な分野や政府調達で利用されているグッドプラクティスの吟味
4. 模造品や余剰品を検知・防止する技術的ソリューション
5. セキュリティを確保するための新しいアプローチ
6. 棚卸および設定の管理・維持運用に対するより良いアプローチ
7. グローバル規模でのポリシーの必要性を検討するためのアプローチの調査
8. 共通仕様に基づく認証の国際的な相互認証制度の確立
9. SCI 関連の用語や定義を公式に纏めた SCI フレームワークの確立

以上