2015 年 12 月 25 日
独立行政法人情報処理推進機構（IPA）

ENISA Supply Chain Integrity 概要

本概要は、欧州ネットワーク情報セキュリティ機関（ENISA）発行の“*Supply Cain Integrity – An overview of the ICT supply chain risks and challenges, and vision for the way forward Version 1.1*”の概訳となります。内容の詳細につきましては、原文をご確認ください。
URL：
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/sci-2015

サプライチェーン・インテグリティ（SCI）は、近年大きな注目を集めている。サプライチェーンもグローバル化が進み、サプライヤーが世界中に散在していたり、パーツや工程の多さから多数のサプライヤーが存在するなど、“チェーン”が地理的にも長さ的にも拡張している。本ガイドの目的の 1 つは、情報通信技術（ICT）分野における SCI とは何かを明らかにし、SCI を確保するための方策を提示することにある。

本ガイドは、意志決定者向けとなっており、机上調査および様々な業界の関係者へのインタビューを基に以下をまとめている。

- ICT 機器およびサービスの SCI に対する脅威とリスク
  → 特に、信頼できないサプライヤーによる偽造品の混入や改変等の可能性
- 解決策の提案
  → 特に、サプライチェーンにおける悪意ある行為を検知・防止し、リスクを低減するための対策
- 信頼できないサプライヤーの製品やサービスの取り扱いに関するアドバイス

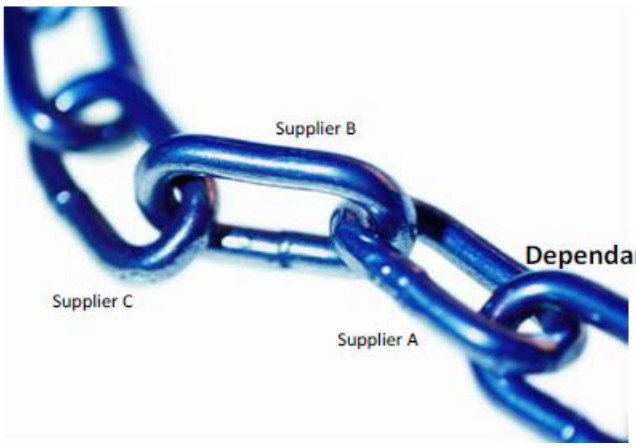
なお、ICT 分野は非常に幅広いため、本ガイドでは電気通信業界をモデルとして記している。

◆ サプライチェーン・インテグリティとは

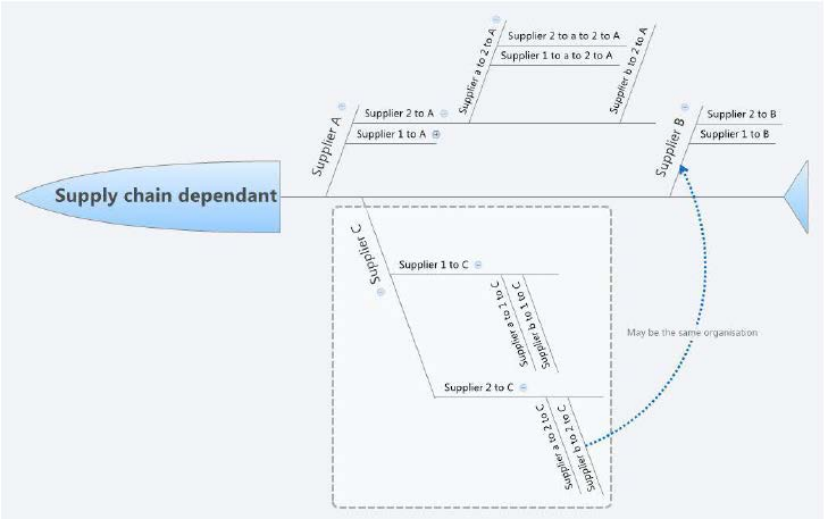
「インテグリティ」という言葉の意味は、文脈によって変わる。例えば、情報セキュリティではデータの完全性（データが不正に改変されていないこと）を示し、ソフトウェア開発では開発プロセスが管理され、適切な品質を有することを示し、一般的な ICT では、セキュリティと信頼性の保証に関する複雑な概念を示す。

ICT 分野における SCI は、前述の定義の組合せであり、その目的は ICT 製品等が適切なグッドプラクティスや規格に準拠し、決められた仕様を満たしていることを保証することにある。これには、納品された製品等が意図した通りに機能し、故意または不注意によって意図しない動作や結果を引き起こさないことを含む。

実際のサプライチェーンは、サプライヤーが数珠つなぎになった「鎖状」ではなく、各サプライヤーの下にそれぞれ別のサプライチェーンが存在する「魚の骨状」に近い。



原文中の図 1:シンプルなサプライチェーンの概念(「鎖状」



原文中の図 2:一般的なサプライチェーンの概念(「魚の骨状」)

通常、サプライチェーンの一貫性およびインテグリティを確保するため、チェーンの各構成要素の真正性や完全性を確認するための技術的対策や運用的対策が要求される。一般的に、リスクマネジメントやライフサイクルマネジメントにおける様々なプロセス(開発、品質保証、運用、監査、トラブル対応、マネジメントなど)の確立、サプライヤーおよび製品(ソフトウェア、ハードウェア、ドキュメント)の真正性の確認等を通じてサプライチェーンの信頼性の構築に取り組むものの、信頼性を測るのは困難であり、SCI を評価するためのより具体的な手法が求められている。

◆ 課題

- サプライチェーンの複雑化、グローバル化
- SCI の実現および評価のための共通的なガイドラインの欠如(異なる業界で異なるガイドライン等が作成されている例はあるが、整合性がない)
- エンドユーザーが製品を検証する手法や技術の不十分さ
- 偽造品や不正な改変等を検知するのに幅広く使えるツールや手法、プロセスの欠如 など

そのほか、電気通信業界のサプライヤー（機器ベンダ）、通信事業者、規制当局、政府関係者などへのインタビューから、以下のような問題点も見られた。

- SCI に対する取組みの多くはサプライチェーンにフォーカスしたものでなく、従来のセキュリティや調達の枠組みの中で行われている。
- SCI のメトリクスとして使われているのは従来のもの（サービスであれば Service Level Agreement（SLA））で、SCI に特化したメトリクスは使われていない。
- 一般的に SCI は一部のベンダを除き殆ど取り組まれておらず、重要性も理解されていない。

◆ 環大西洋貿易投資連携協定（TTIP）に伴うサプライチェーン・インテグリティの展望

TTIP の目的は、EU と米国の間の貿易・投資を増やすことにあり、障害となっている事柄（例えば、互換性のない規制や標準など）の改善などが盛り込まれている。SCI に関する事柄が明記されている訳ではないが、TTIP の目指すところの 1 つが EU－米国間の公的調達を容易にすることである以上、互換性とセキュリティの観点から、SCI は TTIP の関心の範疇であると考えられる。

◆ 推奨施策の提言

※＜＞内は、ENISA が想定する推奨施策の実行者

【研究・開発分野】

- トラスト・モデルの改善・革新　＜EU の研究開発プログラム（FP7）＞
  現状、多くの商用システムは最終的な提供者に対する暗黙の信頼の上に運用されているが、ICT システムのエンド・ツー・エンドでの検証を可能にするようなモデルの検討が望まれる。
- インテグリティの評価・確認手法の改善　＜EU 研究開発プログラム（FP7）＞
- 各業界で使われているサプライチェーン・マネジメント、および政府調達で使われているベストプラクティスの詳細調査を通じた、SCI の強化・促進のための知見の取得　＜EU 機関（加盟国による要支援）＞
- 偽造品や過剰生産を検知・防止する技術の改善　＜EU の研究開発プログラム（FP7）＞
- セキュリティを保証する新たなアプローチ　＜EU の研究開発プログラム（FP7）＞
  監査可能で、透明性が高く、統一的な SCI を実現する対策やツールの開発が求められる。 など

【認証制度】

- CC 国際承認アレンジメント（CCRA）や Senior Officials Group Information Systems, Mutual Recognition Agreement（SOGIS MRA）のような、共通の基準に基づくグローバルな SCI 認証の開発　＜EU 機関、加盟国の政策立案者＞

【サプライチェーン・インテグリティ・フレームワーク】

- 必要であれば規制を含む、SCI フレームワークの策定　＜国際標準化機構（ISO）＞

【法規制】

- SCI に関する継続的な調査を促す法案の立案　＜EU 機関＞

以上