第 58 回日米財界人会議デジタル分科会共同声明付属文書

「ICT サプライヤーの信頼」を構築するための推奨される諸原則

製造、流通、販売又は供給を行う企業（以下「サプライヤー」という）を、重要な情報通信技術（ICT）ネットワークの構築と運用を可能とする技術の信頼できる供給源として取り扱うべきかどうかを評価するには、多様な要素が関係する。以下を満たす場合、サプライヤーは「信頼できる」ものとする。

1. サプライヤーの製品又はサービスに関連する技術リスクが合理的に理解され、適正に管理されていること。

   a. 技術の設計、開発、導入が、当該製品又はサービスの予想されるライフサイクルを通じてリスクを特定、評価、管理するための、透明性が高く、検証可能で、開かれた、合意に基づく標準ベースで、且つプロセス指向のフレームワークに従って行われている。これには以下を含む。

      i. 製造システムへの不正侵入等に対する開発・構築環境の保護
      ii. 国際的な産業標準（例：ISO27001）に準じた「統制フレームワーク」の適用。これには、粒度の細かい、役割ベースでのアクセスコントロールの展開を含む
      iii. 既知の脆弱性に対するコードのスキャンニング
      iv. 予見される脅威とリスクのモデル化、及び
      v. ソフトウエアとファームウエアのアップデートメカニズム及び経路の安全性の維持

   b. オープンソースを含むコードの出典、系統及び整合性が、結果として生じる製品の安全性及び知的財産権の順守を保証するために合理的に実証可能であること。

   c.リスクを管理するために実装された統制の標準ベースでの適合性の検証が技術によって可能であること。また検証されたコードが、運用環境下で実装・使用される完成品のコードに対して検証可能であるように生成プロセスの再現性を保証することが可能であること。

   d. 承認されたユーザーやデバイスの代理として行動する、承認されたユーザーやプロセスへのアクセスを効果的に制限するアクセスコントロールの適用を確実にするため、検証可能な技術的施策が実施されていること。

   e. 脆弱性への対処、修復と開示に関して、国際的なベストプラクティスと整合した方針が採用され、透明性の高い方法で伝達され、定期的に活用されており、また法令順守を確実にするためにその方針の評価が可能であること。

f. 個人データの保護と個人の権利の尊重のための情報セキュリティとプライバシー保護が適用され、透明性の高い方法で伝達され、また法令順守を確実にするための評価がなされること。

g. サプライヤーにより採用される統制、緩和策、方針、及び手順が以下の業者にも明示され適用されるべきであること。
   i. 製品内に含まれるコンポーネントとソースコードのサプライヤー
   ii. 機密データ、専有データ及び又は個人データのプロセッサ/サブプロセッサ
   iii. 市場においてサプライヤーの技術を受領、据え付け、インテグレート、販売、及び又は保守する販売業者、パートナー、再販業者

h. 製品とサービスの供給安定性が確保され、事業継続計画が策定されていること。

2. 以下を含め、サプライヤーは一般的に認識されている企業行動規範を遵守していることを実証すること。

a. サプライヤーの中核的価値観、原則及び慣行を概説した正式な「企業行動規範」。

b.調達、投資及び契約に関する意思決定が、所有権、パートナーシップ、ガバナンス構造及び資金調達先における透明性を通じた商業的判断に従っていることを担保するために、持分の取引が公開されていること、もしくは同等の仕組み。

c. 市場で一般的に採用されている監査及び会計基準(例:GAAP(一般に認められた会計原則)又はIFRS(国際財務報告基準))に準拠していることについての対外的な説明。当該監査及び会計基準は、隠された、又は不透明な、又は異なる状況下では経済合理性のない資金調達源、融資元、又は補助金支給源が存在しないことを担保するよう設計されていること。

d. 内部統制の仕組みで、明確に表現・実行され、外部の審査に服するもので、以下の保護に対するコミットメントを示すもの。

   i. ユーザーと顧客の安全とプライバシーの、サイバーを利用した攻撃や他の不当侵入からの保護
   ii. プライバシーと個人の権利の、透明性、公平性及び説明責任が確保された方法による保護
   iii. 窃盗、改ざん、不正アクセスに対する製品、サービス及びデータの完全性の保護
   iv. 知的財産の窃盗、侵害又は横領からの保護
   v. 公平で開かれた競争の保護
   vi. 環境資源の有害又は持続不可能な慣行からの保護
   vii. 人権の強制的又は不公正な労働慣行からの保護
   viii. 正当なガバナンス、公衆衛生及び幸福の保護

3. サプライヤーは、国際的な商業規範とともに各国及び国際間の法令・標準の双方に従って事業活動を行う。サプライヤーの意思決定は商業的動機に基づき、市場の動きに応じて行われるものであり、内部統制や経営に対する不適切で直接的な政府による支配や影響によるものではない。このことは以下によって実証できる。

a. 企業データ、設備、各種経営資源又は業務運用への恣意的なアクセスが無く、政府の指示に協力する義務が存在しないこと— これらは政府からのかかる要求に対する異議申し立てが独立した司

法または中立的な仲裁者により扱われることを可能にする透明性と適法手続き（デュープロセス）のメカニズムへの合理的なアクセスにより実証される。

b. 政府職員を企業組織の中又は意思決定プロセスの中に含めなければならないという要件により、サプライヤーが市場主導の原則下で経営を行う独立した企業体として行動する能力を制限するようなことがないこと—これらは組織／ガバナンス構造、所有権の権益の透明性及び公開性により実証される。

4. サプライヤーが本拠を置き、設立され、事業を行う国の法令には以下のような規定がなければならない。

a. 法の支配への尊重を明示することによるネットワークと接続サービスの統制。これは当該国政府の権力の行使に対する明確な法的又は司法上の制限により示される。

b. 適切な権力分立を伴う法の支配に従った統治。これは、独立した司法または適法手続き（デュープロセス）と保護された権利に関する他の中立的な仲裁者によって守られる。

c. 国連の持続可能な開発目標のような、グローバルな人間開発に重要となる、国際的に合意された規範、標準、条約の支持。これは、ICT の調達と取得における、環境資源の適切な管理、公正な労働慣行の実行、知的財産権の保護、公衆衛生と幸福の保護、及びプライバシーと人権の尊重を含む。