URL　https://journal.ntt.co.jp/article/29272
DOI　https://doi.org/10.60249/24095101

透明性によるサプライチェーンセキュリティリスクへの挑戦

NTTは，「透明性」をキーコンセプトとしてサプライチェーンセキュリティリスクの低減を図る技術の研究開発を推進するとともに，サプライチェーンを形成する多様な事業者と協調して当該リスクの低減等に取り組む場となる「セキュリティ・トランスペアレンシー・コンソーシアム」を運営しています．本稿では，サプライチェーンセキュリティリスクに関する国内外の動向や関連技術，および本コンソーシアムの概要について紹介します．

キーワード：#サプライチェーンセキュリティ，#可視化データ，#SBOM

後藤　厚宏（ごとう　あつひろ）[†1]
中嶋　良彰（なかじま　よしあき）[†2]

情報セキュリティ大学院大学[†1]
NTT社会情報研究所　所長[†2]

従来にない深刻なリスクの出現

経済活動や日常生活を支え，健康や生命にとっても重要な社会基盤となったインターネットにおいて，今やサイバー攻撃は人類共通の重大な脅威となりました．そして，このサイバー攻撃に関する新たなリスクとして「サプライチェーンセキュリティリスク」が世界的に注目されています．

人々が利用するサービス・システム・製品は，その設計開発段階から導入・運用段階までを含め，多様なサプライチェーンによって支えられています．このサプライチェーンを形成するいずれかの事業者が侵害されると，その影響がサプライチェーンの下流全体に伝搬します．サービス・システム・製品の高度化によってその複雑性が増すほど，サプライチェーンは深く広くなり，影響の伝搬範囲も急拡大します．また，影響が伝搬するサプライチェーンの下流側では，サプライチェーンを把握することはおろか，その存在を認識できていないことも珍しくなく，影響を回避・低減することは容易ではありません．このような性質に起因して生じるリスクがサプライチェーンセキュリティリスクであり，その大きさに注目が集まるとともに，すでに実害も発生しています．

このような中，NTT社会情報研究所では，サプライチェーンセキュリティリスクの要因は，サプライチェーンとその対象物（サービス・システム・製品等）が「不可視」であることと考え，対象物に含まれるソフトウェアコンポーネントなどの構成を利用者側からも確認できる「透明性」をキーコンセプトとして，抜本的にリスク低減を図る研究開発に取り組んでいます．また，このリスク低減のためには，サプライチェーンを形成する多様な事業者の協調が不可欠であることから，その活動の場となる「セキュリティ・トランスペアレンシー・コンソーシアム」を2023年9月に発足し，本稿の筆者でもある情報セキュリティ大学院大学の後藤厚宏学長が会長に就任しました[(1)]．

次に，サプライチェーンセキュリティリスクについて解説するとともに，当該リスクの低減に向けた上記のコンソーシアムを中心とした取り組みについて紹介します．

リスクの分類とインシデント事例

サイバー空間とフィジカル空間の高度な融合が進んでいる現在の社会では，サプライチェーンも多様化と拡大が進んでいます．サプライチェーン全体を正確に把握してリスクに備えることは事実上困難であることから，サプライチェーンの性質を利用したサイバー攻撃はたいへん強力です．このリスクは，例えば**図1**のように分類することができます．リスク①は，サプライチェー

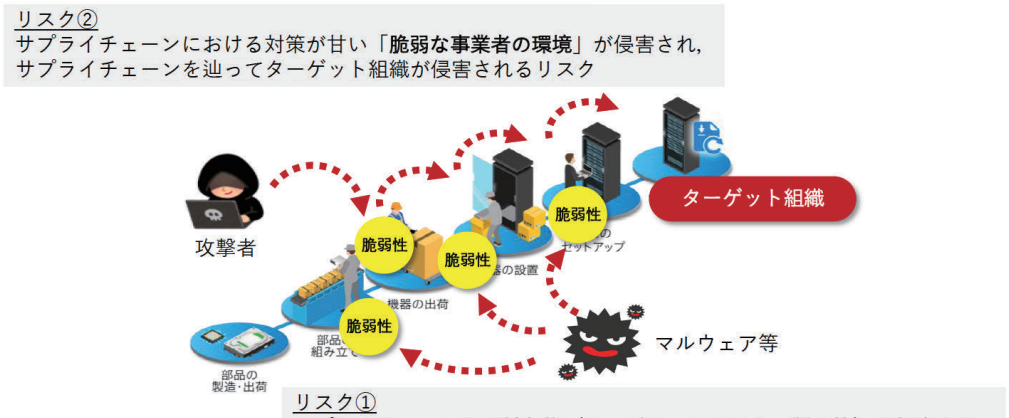


図1　サプライチェーンセキュリティリスクの分類

ンにおいて授受されるもの（サービス・システム・製品等）が侵害され，上流の事業者を信頼している下流の事業者が侵害の事実を知らぬまま利用してしまい，その結果として自身も侵害を受けるリスクです．例えば，製品に搭載されているソフトウェアにマルウェア等の不正なソフトウェアが混入しているケースが考えられます．また，製品導入時点だけでなく，運用中のソフトウェアのアップデートの際に脆弱性や不正なソフトウェアが混入するというケースも考えられます．

リスク②は，サプライチェーンを形成する事業者のIT環境がサイバー攻撃（例えば事業者設備のマルウェア感染，従業員アカウントの乗っ取り等）によって侵害され，取引先とのさまざまなやり取り（事業者間のシステム連携・メール連絡等）が，改ざん，偽造，マルウェア感染等の脅威に晒されるものです．

国内外において，このようなサプライチェーンセキュリティリスクの顕在化を実感させられるインシデントが相次いで発生しています．**表**は，上記の分類ごとに象徴的なインシデント事例をまとめたものです．

リスク対応に向けた各国および業界の動向

前述のインシデント発生等も契機となり，日本政府を含む各国政府はサプライチェーンセキュリティリスクの重要性や対応の困難性を踏まえ，セキュリティ向上に向けたさまざまなルール整備等の政策を推進しています．また，関連する標準化等の活動が各業界団体によって進められており，これらを土台として各事業者のセキュリティ業務およびセキュリティビジネスの改善や発展が期待されています．**図2**は，これらの全体像をまとめたものです．

■ 米国

米国では2021年5月に発令された大統領令（Executive Order 14028：Improving the Nation's Cybersecurity）を起点として，ソフトウェアサプライチェーンのセキュリティ強化，ソフトウェアの信頼性向上，サイバーインシデント報告義務の強化などが進められています．この大統領令に基づき対策を実践するためのベストプラクティスおよびガイドライン等を，米国のNIST（国立標準技術研究所），NTIA（国家電気通信情報局），CISA（サイバーセキュリティ・インフラストラクチャ庁）等が公表しています[(2)]．

上記の取り組みにおける重要な要素としてSBOM（Software Bill of Materials）と呼ばれるソフトウェア部品表が挙げられます．SBOMとはソフトウェア製品に含まれるコンポーネントとその情報（ソフトウェアバージョン情報，ソフトウェア間の依存関係等）をリスト化したものです．この情報によって，サプライチェーン全体を通じて，サービス・システム・製品等を構成するソフトウェアの存在を適切に認識できるようになり，脆弱性の特定やリスク確認，必要な対処を迅速かつ効果的に行えるようになることが期待されています．

SBOMの普及に向けた米国の取り組みは加速しており，SBOMの標準化やSBOMの運用に関するベストプラクティス公表に加えて，米国政府と取引する企業や重要インフラ事業者等に対してSBOMの作成や提供を求める取り組みも進められています．

■ EU

EUでもサプライチェーンセキュリティリスク対応のための政策が進められています．特に，2022年9月に欧州委員会が公表したサイバーレジリエンス法（CRA：Cyber

表　サプライチェーンセキュリティリスクに関するインシデント事例

発生時期	概要	分類
2020年12月	SolarWinds社が提供するシステムのアップデートプログラムが侵害を受け，サプライチェーンを通じて顧客（約1.8万件）に影響	リスク①
2021年7月	Kaseya社が提供するIT管理システムのアップデートプログラムが侵害を受け，サプライチェーンを通じて顧客（約3.6万件）に影響	リスク①
2022年10月	国内医療機関において取引先の給食事業者が侵害を受け，両者のシステム連携を通じてランサムウェアが伝搬し，院内の多数のサーバおよび端末機器（約1300台）に感染が拡大	リスク②
2022年12月	ログ出力ライブラリのデファクトスタンダードである「Apache Log4j」に発覚した深刻な脆弱性によって多くのシステムに攻撃リスクが発生（サプライチェーンにおいて該当バージョンのLog4jが搭載されているソフトウェアの特定が困難であり問題が深刻化）	リスク①

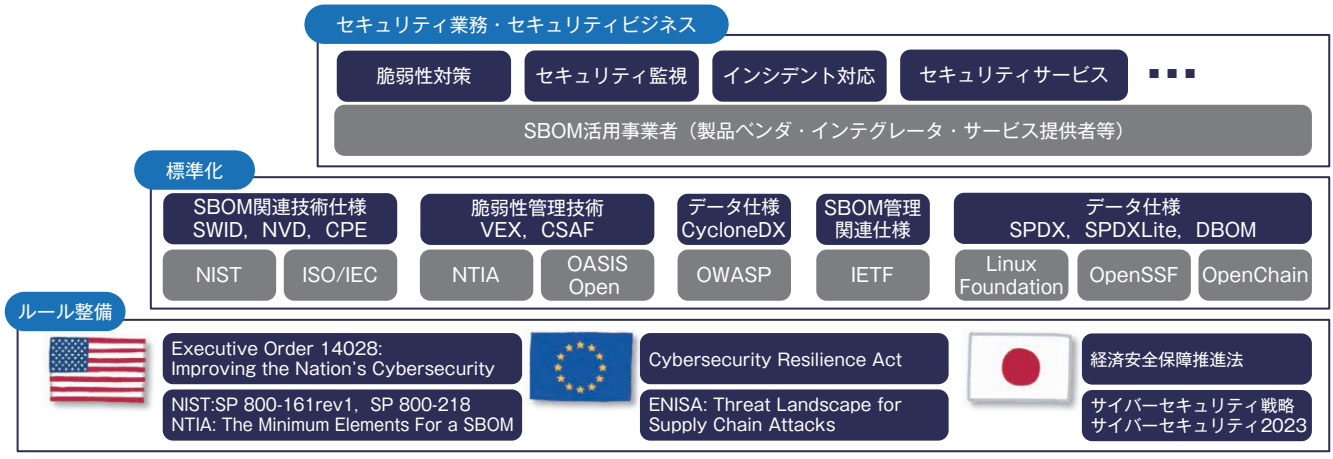


図2　サプライチェーンセキュリティリスクに関する各動向の全体像

Resilience Act)[3]では，デジタル要素を備えた製品を対象としてサプライチェーンセキュリティリスクを含むさまざまなサイバーセキュリティ関連規則が規定されており，2024年にいよいよ施行の予定です．

CRAによってサプライチェーンを形成する上流（事業者）の責任と下流（ユーザ）の権利を明確化するとともに，サプライチェーン全体でリスクに対応するための環境整備が進むことが期待されています．このCRAでは，サイバーセキュリティリスク対応に必要な情報提供が各事業者に義務付けられています．そして，そのための重要な手段の1つとしてSBOMが位置付けられていることから，米国と同様にEUにおいてもSBOM作成は広く求められていく見込みです．

■ 日本

日本政府は，2021年に閣議決定したサイバーセキュリティ戦略においてサプライチェーンの信頼性確保に向けた基盤づくりを重要施策に位置付けるとともに，年次計画である「サイバーセキュリティ2023」においてSBOMを含むサプライチェーンセキュリティリスク対策強化の取り組みを進めることとしています．

上記の政策の一環として，経済産業省，総務省，厚生労働省ではSBOM導入やSBOMによる脆弱性管理に関する手引書を公表するなど，SBOM普及に向けたさまざまな取り組みを進めています．また，大規模なサプライチェーンを特徴とする自動車業界では，SBOMの運用面（運用コスト等）を考慮して独自の工夫を行ったフォーマットを策定・採用する動きもみられます．

リスク対応のために真に求められること

製品・システム・サービス等がサプライチェーンを通じてセキュリティ侵害を受けるサプライチェーンセキュリティリスクは，各構成要素の供給元などを含めた全世界に広がるサプライチェーン全体を通じて対応が求められます．各国政府が整備や検討を進めているSBOMは，保護すべき対象の中身の把握とそこに潜む脆弱性などのリスク確認を容易にする情報（可視化データ）をサプライチェーンに提供し，システム構成の透明性を高めセキュリティリスクを低減する効果をもたらすことが期待できます．サプライチェーンの上流から下流までの全体を通じて可視化データを共有し，セキュリティ対策に活用することができれば，サプライチェーン全体のリスクを効果的に低減することができます．

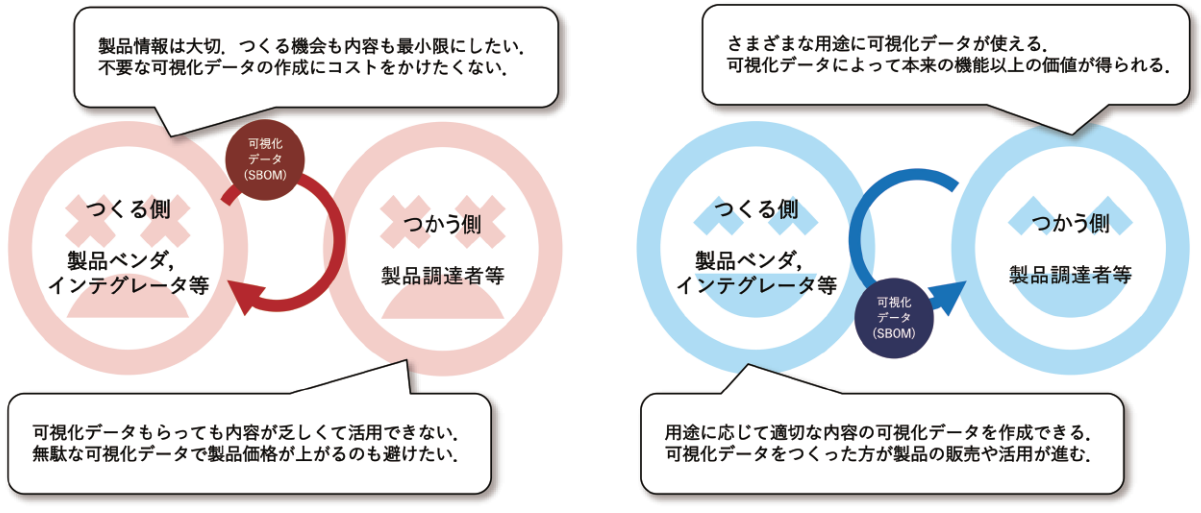
一方で，SBOM作成義務化に向けた動きを背景として，SBOMによる可視化データを「つくる側」の視点に取り組みがよりフォーカスしていくと，例えば可視化データの生成コストのような「つくる側」の問題への対処に関心や取り組みが偏重してしまう可能性があります．その結果，**図3**(a)のように，可視化データを現実的な範囲でつくることが目的化してしまい，可視化データが本来もたらすはずであった利点を損なうおそれがあります．

そのため，私たちは「つかう側」の視点に立った検討も行い，上記のような偏重に陥らずバランス良く「つかう側」と「つくる側」の両視点から取り組むことが不可欠であると考えています．例えば，「つかう側」の視点から，可視化データを効果的につかうためのデータ条件を見出すことは，「つくる側」において無駄な可視化データの生成を回避できるメリットをもたらすでしょう．さらに，「つくる側」にとって可視化データの作成が製品の販売促進に寄与するのであれば，より多くの資源が投入され，可視化データの活用が一層進むことも期待できます．

このようにサプライチェーンセキュリティリスクを真に解決するためには，サプライチェーンにおける「つくる側」と「つかう側」にあたる多様な事業者が協調して両者の視点を取り入れた問題対処に取り組むことが不可欠なのです．

コンソーシアムがめざすリスク対応の好循環

可視化データの作成および提供は製品等のサプライヤ事業者におけるコスト負担を伴うことから，当該コストに見合うレベルの効果的な可視化データの活用が不可欠で



(a) つくる側とつかう側のギャップによる「悪循環」　(b) つかう側を起点としたつくる側との「好循環」

図3　可視化データに関する「悪循環」と「好循環」

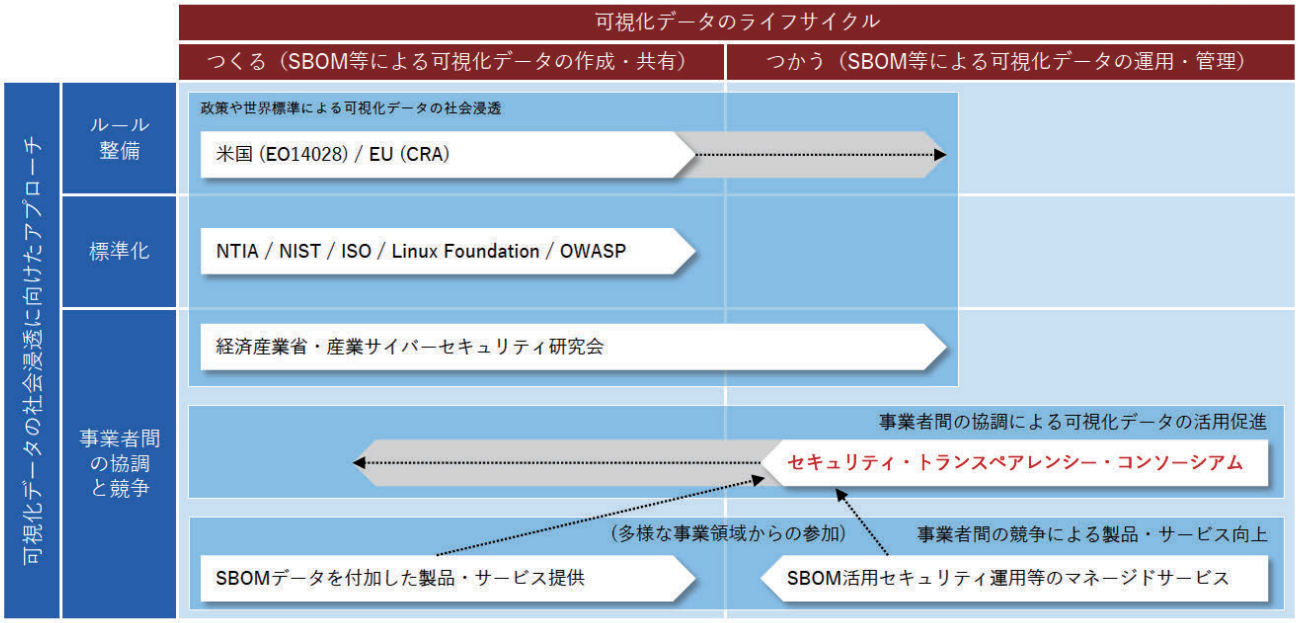


図 4　コンソーシアム運営に関する基本的な立ち位置

あり，効果的な活用は可視化データの作成および提供を促し，活用シーンのさらなる拡大を生む（図 3 (b)）好循環につながります．

私たちは，サプライチェーンを形成する多様な事業者（製品ベンダ，システムインテグレータ，セキュリティベンダ，サービス・システム・製品を利用・運用する事業者等）と協調し，可視化データの活用促進に資する「知見の共創」に取り組むため，「セキュリティ・トランスペアレンシー・コンソーシアム」を立ち上げました．

可視化データの作成および提供を促進するとともに，各会員が持つ知見やノウハウを共有することによって，活用シーンの具現化と拡大をめざしています．このコンソーシアムにおける取り組みの柱は以下の 3 つです．

- 可視化データの活用シーンおよび活用手法について広く具現化に取り組みます．具体的には，ソフトウェア構成等の可視化データによって高まる透明性の活用について，セキュリティ運用等を対象として課題分析，解決策の検討，および実証等を行います．
- 特定の業種や分野に限定しない多様な事業者の参加によって，可視化データの「提供側」および「利用側」の両者を含む広い視点から検討を行います．
- 検討成果の公表を通じて，サプライチェーンセキュリティリスク対応等の社会課題解決への貢献をめざし，それらの取り組みに資するコミュニティ活動や政府関係機関などとの連携も推進します．

上記の取り組みにあたって，サプライチェーンを形成する多様な事業者の知見を取り入れるためには「参加のしやすさ」が特に重要になります．そこで，私たちは「協調領域」と「競争領域」に関する考え方を明確にしてコンソーシアムを運営しています．

コンソーシアムでは，会員共通の問題・課題認識（活動ビジョン）を定義・公表し[4]，これらに対処するための知見（SBOMをはじめとする可視化データの効果的な活用を促進する知見等）を「協調領域」として議論・共創しています．また，このプロセスにおいて，各会員は独自の機密情報を持ち込まず（公開情報のみを使って）活動することとしています．そのうえで，各会員がコンソーシアム活動を通じて獲得した知見を自らの事業（ビジネスや技術開発等）にフィードバックし，「競争領域」において切磋琢磨することによって，社会全体としてリスク対応力を強化していきます．以上のようなコンソーシアム運営の基本的な立ち位置をまとめたものを**図 4** に示します．

私たちは，このようなコンソーシアムの場や活動を通じて「セキュリティの透明性」のさらなる社会浸透に取り組み，これをキーコンセプトとしてさまざまな社会課題の解決にチャレンジしていきます．

■参考文献

(1) https://group.ntt/jp/newsrelease/2023/10/11/231011a.html
(2) https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity
(3) https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
(4) https://group.ntt/jp/newsrelease/2024/02/16/240216b.html

（左から）　後藤　厚宏 / 中嶋　良彰

サプライチェーンセキュリティリスクは，システムやサービスを提供する事業者だけでなく，サプライチェーンを支える事業者にもそのリスク対応を求められるという意味で「社会全体で対応すべき課題」といえます．

◆問い合わせ先

NTT 社会情報研究所
企画担当
E-mail　solab @ ntt.com