Whitepaper:
Security Transparency for Supply Chain

2023 年 5 月 9 日

日本電信電話株式会社

日本電気株式会社

目次

1. 本書の要旨 3

2. サプライチェーンセキュリティリスク 4

2.1. 顕在化している 2 つのサプライチェーンセキュリティリスク 5
2.2. 一般的なサプライチェーンセキュリティのリスク対策 6

3. セキュリティトランスペアレンシー確保技術 7

3.1. 透明性確保のサイクル 8
3.2. 透明性確保に関する技術要件 9
3.3. セキュリティトランスペアレンシー確保技術を構成する要素技術 11

4. 透明性がもたらす未来（ユースケース） 14

4.1. 公平かつ安全なプライチェーンの実現 15
4.2. 事業者間の協調によって低減するバックドアリスク 17
4.3. 事業者環境のセキュリティの確保 18

5. おわりに 20

付録 A. 関連動向 21

付録 B. 用語定義 24

1. 本書の要旨

インターネットは社会インフラとなり、真の「トラスト」が求められる時代に。
しかし、ネットワークや通信機器の多様化や高機能化に連れて、
それらを支えるサプライチェーンに起因するセキュリティリスクが顕在化。
私たちは、このリスクの抜本的な低減をめざしています。

世界中の企業や組織のネットワークがインターネットに接続し、インターネットはコミュニケーション基盤として仕事や生活を支える必要不可欠な社会インフラになりました。日本政府を含む各国政府も、このインフラのセキュリティ確保を目的としたさまざまな政策を推進しています。近い将来、インターネットは、命を預けることすら可能な「真の信頼（トラスト）」が求められるようになるでしょう。

ネットワークは、その企画・設計段階から構築・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。ネットワーク自体が直接侵害されなくても、サプライチェーンを構成するプレイヤのその事業環境や製品のセキュリティが侵害されると、結果的にそれらが支えるネットワークの侵害につながります。本書ではこれを「サプライチェーンセキュリティリスク」と呼びます。

Society 5.0 では通信機器も多様化・高機能化することから、関係するサプライチェーンも拡大します。結果的にこのようなセキュリティリスクがますます深刻化することでしょう。そして、ネットワーク事業者だけでなくサプライチェーン側事業者にも責任を求められるという意味で、サプライチェーンセキュリティリスクは「社会全体で対応すべき課題」と言えます。

私たちはこのサプライチェーンセキュリティリスクを抜本的に低減し、インターネットを形成するあらゆるネットワークに真の信頼（トラスト）をもたらすことをめざしています。

本書では、「セキュリティの透明性（Security Transparency）」に着目して、これを可能にする技術である「セキュリティトランスペアレンシー確保技術」と当該技術によって可能にするリスク対応の方法（ユースケース）を紹介します。

2. サプライチェーンセキュリティリスク

私たちが利用しているシステムやサービスは、さまざまなハードウェアやソフトウェアによって構成されています。そして、それらはいずれも多様なサプライチェーンによって支えられています。本書では、このサプライチェーンのセキュリティが侵害され、その結果、サプライチェーンによって支えられるサービスやシステムのセキュリティに影響を受けるリスクをサプライチェーンセキュリティリスクと呼びます。

例えばシステムのサプライチェーンについて考えてみましょう。システムの構築には、システムを構成する機器のベンダ、次に機器を組み合わせてシステムを構築するインテグレータ、構築されたシステムを確認・運用する事業者というように、さまざまな事業者が関わります。各事業者間では機器やシステムの授受が行なわれ、その結果、サプライチェーンが形成されます。システムの運用開始後には、ソフトウェアの更新や不具合対応などの保守が必要であるため、そこにもサプライチェーンが存在することに注意が必要です。さらにサプライチェーンの細部に目を向ければ、企画、設計、製造、配送、導入、運用、保守などの多様なプロセスが存在し、各プロセスにはさまざまな人、組織、事業者、それらが利用する事業設備が関わります。

サプライチェーンでは、このようなサプライチェーンをなす要素が増え複雑になるほど、そのセキュリティが損なわれるリスク、すなわちサプライチェーンセキュリティリスクが高まっていくのです。

2.1. 顕在化している 2 つのサプライチェーンセキュリティリスク

サプライチェーンセキュリティには、2 種類のリスクがあります。

(1) サプライチェーンから調達する「製品」が侵害されるリスク
サプライチェーンにおいて授受されるもの（機器、システム、サービス等）が侵害されると、上流の事業者を信頼している下流の事業者は侵害の事実を知らぬまま受け入れて利用してしまうおそれがあります。例えば、機器に搭載するソフトウェアがマルウェアに感染、あるいは機器に不正なソフトウェアが混入する可能性が考えられます。

(2) サプライチェーンにサイバー攻撃を受けるリスク
サプライチェーンに参加する事業者が事業を営む環境に対してサイバー攻撃などで侵害されると（例えば事業者の設備がマルウェアの感染する、あるいは従業員のアカウントが乗っ取られるなど）、サプライチェーン上で行なわれるあらゆるやりとりの信頼が失われます。例えば、取引時の連絡内容（例えば、メール、データ等）は、改ざん、偽造されてしまうかもしれません。

これらの 2 種類のリスクについて、私たちはいずれにも対応しなければなりません。サイバー攻撃を受けた事業者が製造した製品は不正機能が混入するリスクが高まり、一方、サプライチェーンを介して調達した製品が侵害されていれば、その製品を組み込んで構築した事業者の環境は容易に侵害されてしまいます。そのため、私たちはこれらのリスクをどちらか一方ではなく、いずれも合わせて低減していく必要があります。事業環境に対するサイバー攻撃にはセキュリティガイドラインを活用するなどして対処するとともに、製品に対する侵害にも対処する必要があります。

2.2. 一般的なサプライチェーンセキュリティのリスク対策

これらのリスクに対する一般的な対応策は、どのようなものでしょうか。

(1) 信じられる事業者から調達する

これは良好な取引実績がリスク低減につながるという考え方に基づく対応策です。事業者に対する「信頼」を拠り所とするこの対策は、現時点では実施可能な現実的な対策のひとつと言えます。しかし、メーカのサプライチェーンはグローバルに変化しており、今までの信頼性がいつまで続くかは不透明です。また、多くの場合、部材の調達先は非開示であるため、サプライチェーンのさらに下流に位置するエンドユーザにとっての安心感には必ずしもつながりません。

(2) 調達の都度、調達した対象（個体）をよく確認する

これは調達品に対し、受入検査を徹底する対応策です。ペネトレーションテストやファジングなどによって検査を行う方法があります。しかしながら、機能が複雑化した通信機器などの多くの機器においてその内部を隅々まで漏れなく確認するためには、高度な知識や技術力、そして特殊な検査設備が求められる場合があり、完全な確認は容易ではありません。また、直接の取引相手だけでなく、さらに上流の疑わしいサプライヤをターゲットとしてそこから供給され部品を特定して検査することも困難です。

(3) 対策の確実な実施と責任を事前に合意する

これはサプライチェーンにおける取引相手との間で、リスク低減策の実施を契約によって取り決めるものです。契約において、なんらかの損害を被った場合を想定して「責任」を規定しておく方法があります。しかしながら、対策の実施漏れによるセキュリティ事故は多く発生しており、対応策としての有効性はサプライヤの意識に依存します。また、サプライチェーンにおける直接の契約関係にない上流の事業者に起因するリスクには対処し切れないおそれもあります。

上記のいずれもサプライチェーンセキュリティリスクへの抜本的な解決策とはなっていません。それどころか、サプライチェーンセキュリティリスクの顕在化はこれらの効果をいずれも弱体化させ、私たちをより深刻な状況へと追い込みつつあるのです。なお、このような状況に対して各国政府が対策に動き出しています。その動向については本書の「付録 A」を参照してください。

3. セキュリティトランスペアレンシー確保技術

私たちは、サプライチェーンセキュリティリスクの抜本的な低減を図る新たなしくみの鍵は「透明性（Security Transparency）」であると考えています。逆に言えば、サプライチェーンセキュリティリスクは、サプライチェーンにおいて授受されるもの（機器、システム、サービス等）の透明性が確保されていないことに起因すると言えます。

この透明性を確保するために、私たちは、機器ベンダが機器を製造・出荷する際に、機器の「構成」と「リスク」を可視化したデータを生成して、これをサプライチェーンに参加する事業者に共有することを提案しています。以降、本書ではこの可視化データを「ST オブジェクト（Security Transparency Object）」と呼びます。各事業者は、ST オブジェクトが表わす情報から機器が本来含んでいるべきものを知ることができ、これに基づいて機器の中身の正しさを検査できるようになります。もしも、サプライチェーンのどこかで機器に改変や不正要素が混入した場合、製造・出荷時との不整合に気づくことができます。

共有にはもうひとつの意味があります。サプライチェーンにおける以下のようなプロセスを想定してみましょう。

- いくつかの部品を組み合わせて機器を生産する
- いくつかの機器を組み合わせてシステムを構築する
- 機器に部品を追加または変更して機器の機能を追加または変更する

このようなプロセスにおいて、部品や機器に対応する既存の ST オブジェクトを組み合わせる、あるいは追加・変更を行なうことによって、新たな機器やシステムを表わす ST オブジェクトを生成して共有します。このようにして、サプライチェーンを介して生み出されるさまざまな機器やシステムの透明性も確保し続けることができます。

そして、ST オブジェクトは、「構成」に対して特定の評価基準を適用して導出される「リスク」に関する情報も含むこととします。これは、例えば、その時点の脅威情報に基づいて後述するバックドアを含む可能性を評価した結果や脆弱性情報データベースに基づいて残存する脆弱性を判定した結果などです。

3.1. 透明性確保のサイクル

サプライチェーンにおけるセキュリティの透明性確保は、対象となる機器、システム、サービス等に対する ST オブジェクトを生成することで終わりではありません。言い換えると透明性確保が目的ではなく、透明性確保を手段とした真の意味でのサプライチェーンセキュリティリスクの抜本的な低減を実現することが重要です。

最初に対象となる機器、システム、サービス等に対する ST オブジェクト生成による透明性の確認から始まります。続いて、サプライチェーンの事業者などから入手した ST オブジェクトの正しさ確認する透明性の検証を行ったうえで、脆弱性管理や構成管理などセキュリティ運用へと ST オブジェクトを適用する透明性の活用によりサプライチェーンセキュリティリスクの低減につなげていきます。そして、日々の運用や構成変更などに追従した ST オブジェクトの最新化を通じて透明性を更新することによって、透明性確保のサイクルを回し続けることが重要です。

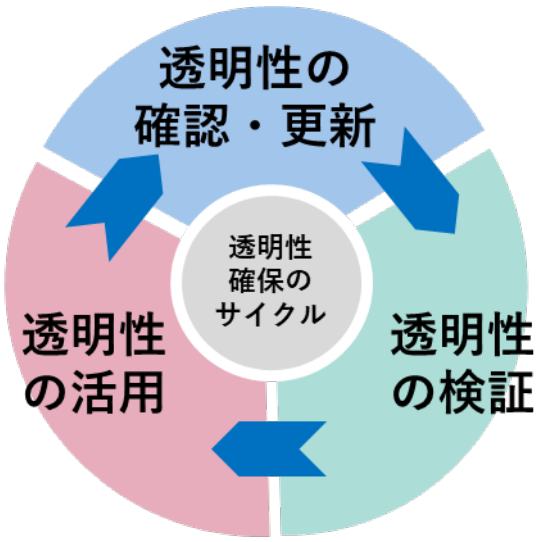

図 3.1-1　透明性確保のサイクル

このような透明性確保のサイクルを回し続け、サプライチェーンにおけるセキュリティの透明性確保を目的として、ST オブジェクトの生成・共有・活用を実現する技術を「セキュリティトランスペアレンシー確保技術：STT（Security Transparency assurance Technology）」と呼びます。

私たちは、第 2.2 節で述べた一般的なサプライチェーンセキュリティリスクへの対応の限界に対して、STT という技術的アプローチによる抜本的な解決策を提案しています。

3.2. 透明性確保に関する技術要件

サプライチェーンセキュリティの透明性確保に資する STT の技術要件は、透明性確保のサイクルの観点から整理することができます。なお、以下に示す技術要件は STT のユースケースの拡大等により継続的にアップデートされるべき要件と考えています。

(1) 「透明性の確認・更新」に関する要件

機器・システムのソフトウェアおよびハードウェアに対する構成を明らかにすることが基本的な要件です。構成を明らかにする際には、可視化データの活用のされ方を意識した詳細度や単位などを表現できることが重要な要件となります。これは第 4.1 節において述べる「透明性レベル」や「機能構成」を考慮した可視化データを作成できることにもつながります。

加えて、構成を明らかにする時点で紛れ込んでいるリスクを事前に検査することによって、リスク確認がされた可視化データ（ST オブジェクト）の作成ができることも要件の一つとなります。一例として、ソフトウェアに関するバックドア検査技術などを用いて、対象機器のバックドアに関する検査を行い、その結果をリスク情報として機器・システムの構成情報とともに可視化データ（ST オブジェクト）に記載します。

(2) 「透明性の検証」に関する要件

サプライチェーン上の他の事業者などから入手した可視化データ（ST オブジェクト）の正しさを明らかにすることが基本的な要件です。正しさを明らかにする際には、そのデータの作成者や作成履歴などに関する確認や記載内容について作成時から意図しない形での変更が加えられていないことを確認できることが重要です。

さらに、可視化データの記載内容が作成者の意図どおりであった場合であっても、機器・システムが備える機能や動作の観点から見た際に、可視化データの記載内容に関する不足や誤りについて確認できることも要件の一つです。例えば、いわゆるバックドアが機器・システムに対して意図的に入れられた場合、同時に生成された可視化データ自身も意図的な隠ぺいや改変が加えられる可能性があり、その信頼性を確認できることも重要な要件です。

(3) 「透明性の活用」に関する要件

構成とリスクの情報である可視化データ（ST オブジェクト）を効果的かつ効率的に共有・活用するためには、セキュリティ運用を行うシステムに機械的に読み込み可能な形であることが要件になります。これについては、機器やシステムを構成するソフトウェア部品を一覧化するための

データ形式である SBOM フォーマットが活用可能です。SBOM フォーマットがもつ柔軟性を活かし、ソフトウェアの「構成」だけでなく、ST オブジェクトが想定する「リスク」に関する情報も表現できます。ただし、SBOM フォーマットで表現されている情報の解釈、取り扱いに関する運用仕様について、事業者間で共通的に定めることも重要となります。

なお、可視化データをセキュリティ運用に活用する際には、想定するセキュリティ運用によりさらに詳細な要件が存在します。例えば、脆弱性管理や改ざん検知、リスク診断など具体的なセキュリティのユースケースごとにさらなる要件の整理が必要です。

3.3. セキュリティトランスペアレンシー確保技術を構成する要素技術

前節においてサプライチェーンセキュリティの透明性確保に必要となる STT の技術要件について述べました。この技術要件を満たす STT の要素技術の例を以下に示します。なお、透明性確保のサイクルを支えるためには、以下に例示する要素技術に留まらない STT を構成する要素技術が必要と考えています。例えば、これまで透明性確保ではない目的のサイバーセキュリティ対策に活用されてきた技術も、STT の技術要件の観点から新たにブラッシュアップすることで、STT の要素技術として活用が可能と考えられます。

(1) バックドア検査技術

バックドア検査技術では、ソフトウェア開発のサプライチェーンで仕込まれる可能性があるバックドアを含む不正機能の混入を検査し、不正機能の有無を可視化します。プログラムのバイナリを静的・動的に解析し、解析結果をリスク情報として ST オブジェクトに出力します。

バイナリを直接検査できることで、サプライチェーンにおいてソフトウェアビルド時に不正機能が混入したとしても、バックドアの混入を検出することが可能です。ソースコードを入手していなくとも検査できるので、ソースコードの ODM（受託開発）等の検査にも適用できます。

今後、重要インフラ等に要求される検査体制、不正機能混入ガイドラインに対応するために、ソフトウェアの安全性検査が求められます。バックドア検査技術により、ソフトウェア安全性検査を効率化することが可能です。また、ST オブジェクトに検査結果を出力して共有することで、サプライチェーンの各開発段階で不正機能の混入リスクが低いことを証明します。

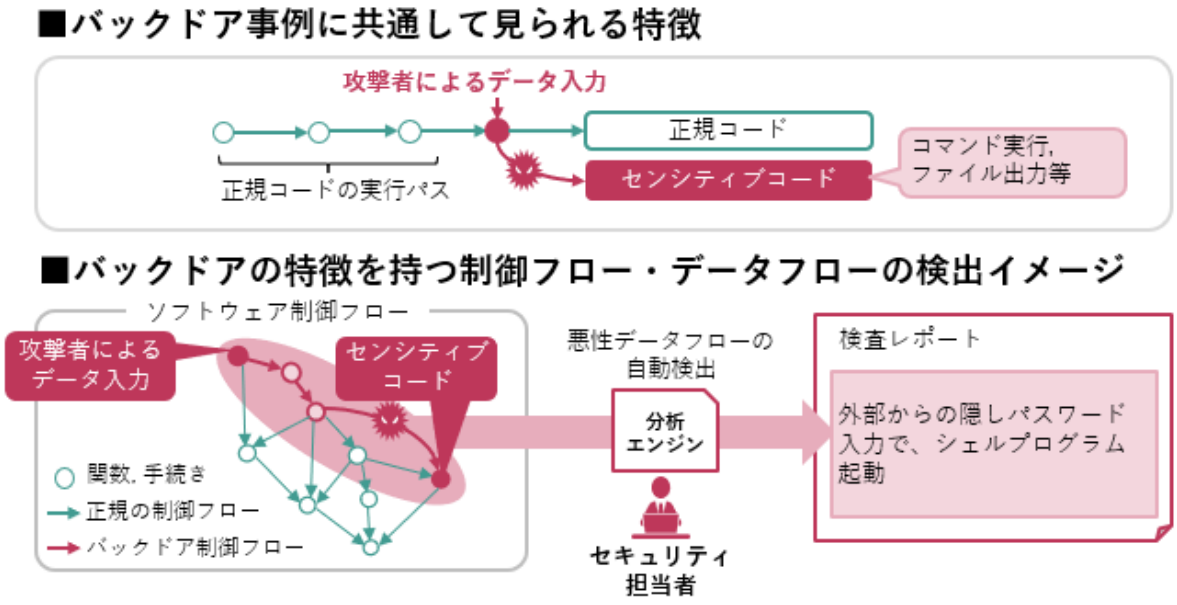

図 3.3-1 バックドア検査の概要

(2) 構成分析技術

構成分析技術は、システムを構成する各機器の構成（ソフトウェアパッケージ、ファイル情報など）を自動的に分析・推定して、SBOM 形式によって ST オブジェクトを生成する技術です。この技術は、機器を直接解析してそのソフトウェア構成を可視化データとして生成する機能に加えて、対象機器から直接得ることが困難な情報を推定・補完する機能も併せ持っています。機器ベンダがそのソフトウェア構成を開示困難な場合に、製品の動作や通信などのような製品の通常利用において外部から観測するなどして知りうる情報（製品の振る舞いに関する情報）などをもとにしてソフトウェア構成を推定し、可視化データを補完することができます。

また、製品が多様かつ多数のソフトウェアによって構成されるようになると、製品を構成するソフトウェア間には製品開発者すら認識し切れない「暗黙的な依存関係」を持つソフトウェアが存在するようになる場合があります。製品を支える基盤ソフト（OS）が備えているパッケージマネージャですら製品内のすべてのソフトウェアを網羅的に管理できているとは限らないのです。このような状況は、例えば他のソフトウェアからソースコードの一部を流用しながらソフトウェアを開発する行為などによって発生することがあります。このようにして生まれるものはコードクローンと呼ばれ、ソフトウェアの保守性を低下させるだけでなく、脆弱性リスクの増大などの重大なセキュリティリスクにつながります。私たちはこのような「暗黙的な依存関係」も含めソフトウェアの構成を網羅的かつ正確に可視化データとして生成可能にすることによって、セキュリティリスクの抜本的な低減を図っていきます[1]。

(3) リスク分析技術

リスク分析技術では、人手で分析することが困難な複雑なシステムのサイバーリスクを網羅的に自動分析し、攻撃がシステムに及ぼす悪影響（深刻さ）や危険度（可能性）を可視化します。システムの構成情報やデータフローからシステムの仮想モデルを生成し、実機を使わずに仮想モデル上で攻撃シミュレーションを行うことで、実機に影響を与えずに膨大な攻撃シナリオが成功するかを試すことができます。分析により、リスクの高い侵入経路とその攻撃手口（システムに存在する脆弱性の悪用可能性）を把握することができるため、リスクの高低に応じた適切なセキュリティ対策を実施していくことができます。リスク分析に投入する情報として、ST オブジェクトとして入力されるバックドア検査の結果や独自ソフトウェアの詳細な構成情報を SBOM から把握することで、より精度の高い診断が可能となります。

最終的に、システムに対してリスク分析した結果を ST オブジェクトとして出力してセキュリティ責任者が確認することで、システムリスクを正確に把握することができます。

[1] “データガバナンスを支える基盤技術特集 セキュリティトランスペアレンシー確保技術によるソフトウェア構成の分析・可視化“ . NTT 技術ジャーナル. 2023/2. https://journal.ntt.co.jp/article/20964, （参照 20230-03-31）

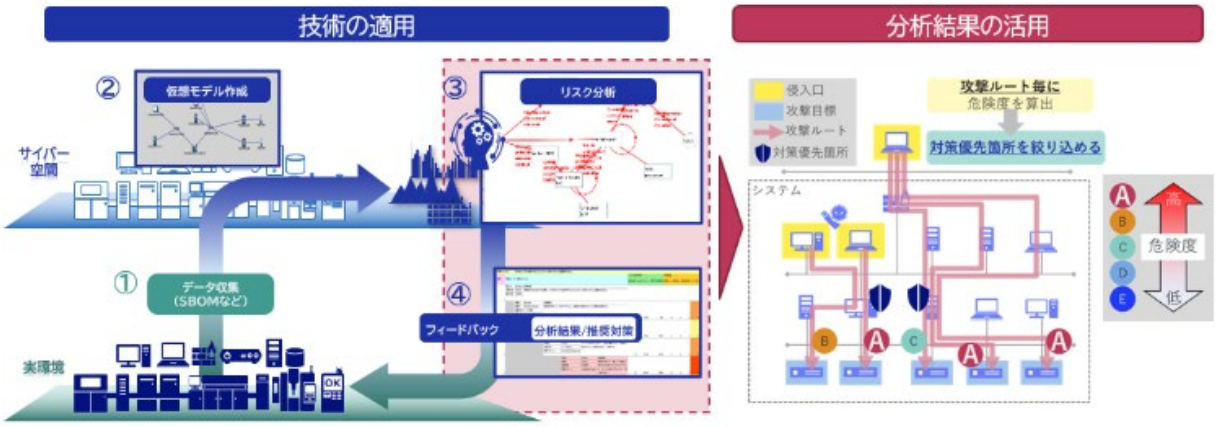

図 3.3-2　リスク分析技術の概要

これら 3 つの要素技術は独立にも活用することができますが、それぞれ組み合わせることで透明性確保のサイクルをより強固に支えることが可能となると考えています。

例えば、(1)のバックドア検査技術を用いて、対象機器のなかにあるソフトウェアについてのバックドアリスクを確認したうえで、(2)の構成分析技術を用いて可視化データ（ST オブジェクト）を生成することにより、より信頼性の高い可視化データを提供することが可能となります。

(2)の構成分析技術を用いてあるシステムを構成する複数機器の可視化データ（ST オブジェクト）を生成し、システムの全体の可視化データとして(3)のリスク診断技術が活用することができます。これにより、従来ヒアリングなどによりヒアリングしいたシステム構成を自動、かつ精緻に取得することができ、リスク診断シミュレーションの精度向上が見込まれます。

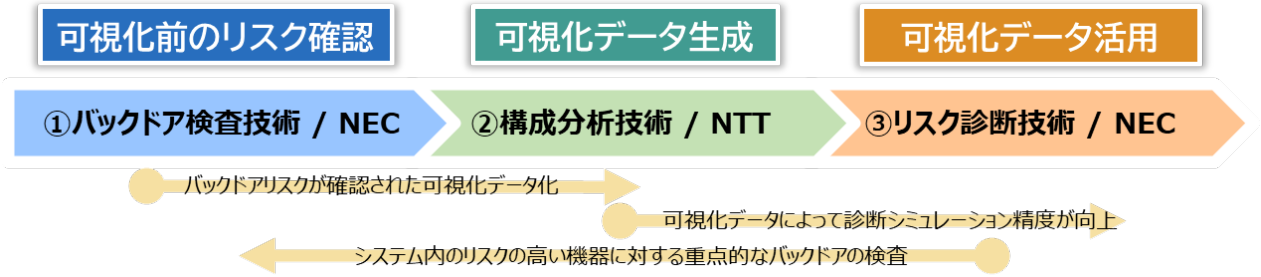

図 3.3-3　各要素技術の組み合わせの例

4. 透明性がもたらす未来（ユースケース）

私たちは、サプライチェーンセキュリティリスクの抜本的な低減を図るキーコンセプトとして「透明性（Security Transparency）」が重要と考えており、機器やシステム等の「構成」や「リスク」を可視化したデータ（ST オブジェクト）の生成・共有・活用によりサプライチェーンにおけるセキュリティ透明性を確保することを提案しています。

この ST オブジェクトが効果を発揮するいくつかのユースケースを見ていきましょう。

4.1. 公平かつ安全なプライチェーンの実現

事業者はサプライチェーンを通じて調達した機器の中身と ST オブジェクトと照合することによって、その構成の正しさを検査でき、機器に不正な改変や不正な要素が混入していることに気づくことができます。これにより、機器の梱包や外観等の目視確認、機器の動作チェック等の従来行なっている検査よりも、深く詳しい検査を行なうことが可能になります。さらに、機器に対するセキュリティ検査結果などのリスクに関する情報が ST オブジェクトに含まれている場合、それを確認することでより機器を安心して利用することができます。

その一方で、ST オブジェクトは新たな懸念も生む可能性があります。それは、機器の ST オブジェクトを生成して共有することは、本来は非公開にしてきた機器の内部仕様を公開につながるのでは、という懸念です。これは機器ベンダにとって受け入れ難いことであり、サプライチェーンを形成する事業者間の公平性が損なわれる可能性があります。

私たちは、このような懸念に対処するいくつかの方法を提案しています。

(1) ST オブジェクトが示す「透明性レベル」

私たちは、ST オブジェクトに含む情報の範囲や詳細度を機器ベンダの裁量に委ね、それに応じて、ST オブジェクトには透明性レベルを設定することを提案しています。

サプライチェーンの下流に位置する事業者は、この透明性レベルを判断材料のひとつとして対象となる機器を受け入れ利用するかどうかを判断します。透明性レベルは、サプライチェーンの事業者間における取引の条件をクリアにして合意形成を図りやすくするとともに、透明性に応じた合理的な取引をサポートします。

(2) 部品構成の代替情報としての「機能構成」

私たちは、ST オブジェクトに、機器の構成要素（ソフトウェア部品やハードウェア部品）を網羅的に組込む代わりに、それらが提供する機能構成（例えば、通信仕様などの機能インタフェース仕様）に相当する情報を組込むことを提案しています。

この方法は、ST オブジェクトによって構成要素を網羅する方法に比べて、機器の中身が十分には分からないことから、ST オブジェクトを活用する一部のユースケースも実践が難しくなるという欠点があります。しかしながら、機器ベンダが機器の情報を明らかにするハードルは下がるため、サプライチェーンの事業者間における ST オブジェクトの共有に関する合意形成には有効な手段になります。

なお、機器を利用する事業者は、この情報を調達仕様に対する適合性を判定することに加えて、運用開始後に正常動作を監視する際に活用するなど、さまざまな応用が可能です。

これらは、私たちが目指すゴールに対して理想的なものではないものの、ゴールに辿り着くまでの過程における現実的な対処法であり、他にもさまざまな工夫を施しながら透明性の価値を社会に浸透させていきます。

4.2. 事業者間の協調によって低減するバックドアリスク

あまり想定したくはないことですが、サプライチェーンに悪意を持つベンダが参加し、機器の製造・出荷時に不正な機能を秘密裏に組込むという事態が広く懸念されています。

このようにして機能を悪用されると、機器利用時に扱われる機密情報を外部から摂取して経済的な利益を得る、あるいは諜報活動に利用するなどが可能になるおそれがあります。一般に、このような機能を「バックドア」と呼びます。なお、バックドアは、開発時にのみ必要な機能を誤って機器に残したまま出荷してしまうような不注意によっても発生することがあります。

このリスクに対して、ST オブジェクトは以下の効果をもたらします。

(1) バックドアリスクに関する機器ベンダの説明力を強化

透明性は、このバックドアリスクにも効果を発揮します。機器の構成要素が漏れなく可視化されると仮定すると、バックドアの存在も構成を可視化した ST オブジェクトとして可視化されます。その結果、機器ベンダは、自社の機器におけるバックドアリスクについて顧客に説明しやすくなります。また、第 3.3 において述べたバックドア検査技術などを用いることによってさらにバックドアリスクに関する正確な説明につながる ST オブジェクトの生成が可能になるでしょう。

(2) 事業者協調によってバックドアリスクを低減

バックドアの存在をなんらかの方法で巧妙に隠したまま ST オブジェクトを生成した場合はどうでしょうか。この場合、サプライチェーンを形成する各事業者が ST オブジェクトに基づいて対象の機器を継続的に監視していれば、ST オブジェクトに記載されたソフトウェア構成や機能から逸脱した動作を高い確率で検知することができるでしょう。

このように ST オブジェクトによって、バックドアを埋め込むことやバックドアを発動させることがしづらい状況を作り出すことができるのです。

4.3. 事業者環境のセキュリティの確保

前章において述べたとおり、サプライチェーンセキュリティリスクを低減するためには、サプライチェーンを形成する事業者の環境が侵害される事態を想定した対策が必要です。ST オブジェクトが事業者環境の透明性とセキュリティの確保に対してもたらす効果を、システムのライフサイクルに基づいて説明します。

(1) 構築：事業者環境の弱点に基づく先回り対応

機器の透明性確保は、機器によって構成されるシステム、ネットワーク、サービスなどの透明性確保も可能にします。ST オブジェクトの集合体は、それらの ST オブジェクトと捉えることができます。このような ST オブジェクトを利用すれば、これまでにない精緻なリスク分析が可能になります。

残存する脆弱性の存在やそれを前提とした時に想定されるサイバー攻撃のルートの特定などを正確に行ない、これに基づいて先回りによる対策をそのリスクに応じて合理的に行なうことを可能にします。

(2) 運用：漏れのない脆弱性管理

サイバー攻撃の主要因のひとつは脆弱性と言われています。脆弱性とはセキュリティに関する欠陥のことです。脆弱性が存在しない機器を開発することや脆弱性がないことを証明することは事実上困難です。したがって、機器を利用する際には、脆弱性が存在することを前提とした上で利用すること、そして、脆弱性が発見された場合には早期かつ漏れなく対処することが求められます。

しかし、実際には脆弱性の対処漏れは頻繁に発生し、結果的にサイバー攻撃は容易に成立しています。これには、さまざまな理由が考えられますが、脆弱性を持つ機器を利用している事実を把握できず未修正のまま放置している、ということも少なくありません。

ST オブジェクトはこのような理由による対処漏れを低減します。ST オブジェクトによって、どこにどのようなソフトウェアが存在するのかは瞬時に把握可能となり、脆弱性の影響を受けるソフトウェアの修正を速やかに判断できます。

(3) 保守：セキュアなアップデート

ST オブジェクトは、機器の更新にも革新をもたらします。更新対象の機器の構成が明らかであるため、漏れのない更新を行なえることは前述の脆弱性管理で述べたとおりです。ST オブジェク

トによって更新に用いるデータのセキュリティも確保することができるため、サイバー攻撃を成立させる要因のひとつである侵害された更新データの持ち込みによる侵害リスクを低減することができます。

外部とネットワークによる接続性を持たない閉域環境は、ネットワークを介してはサイバー攻撃が到達しないという認識からセキュリティ対策が手薄になりがちでした。しかし、実際には担当者が可搬記憶媒体などを利用して持ち込む更新データが侵害されていることが原因で、閉域環境であっても不正ソフトウェアが持ち込まれるインシデントが多発しています。

ST オブジェクトは、侵害された更新データの持ち込みやそれによって不正な状態に更新されてしまった事実を即時に検知することを可能にします。さらに、更新後の構成に基づいて ST オブジェクトを更新するとともに、ST オブジェクトの更新履歴を管理することによって、いつどこが更新されたのかをいつでも正確に確認することが可能になり、インシデント発生時の原因究明や対処にも有効です。

(4) インシデント対応：対応の容易化

「機能構成」や「脆弱性管理」の強化はインシデント発生時の対応が容易化につながります。サプライチェーン事業者の事業設備の透明性も確保することができるようになると、事業設備の脆弱性管理や先回りによるリスク対応が可能になるため、サプライチェーン全体のセキュリティが向上します。サプライチェーンを形成する各事業者の事業設備の侵害やその兆候にもより気付きやすくなれば、サプライチェーンにおいて授受されるもの自体が侵害される以前に対処できるようになるのです。また、インシデントが発生しても、中身がわかっていれば、その影響範囲の特定や強化策を考案することが容易になります。

このようにして、第 2.1 節で述べた「製品の侵害リスク」と「事業設備の侵害リスク」の両者を低減し、サプライチェーンセキュリティリスクの抜本的低減を図ることできるのです。

5. おわりに

セキュリティの「透明性」の確保は、サプライチェーンセキュリティリスクの抜本的な低減のみならず、デジタル化やリモート化における高い信頼（トラスト）の確保にとって不可欠なものです。本構想においてめざすサプライチェーンセキュリティリスク対策は、単一の事業者による活動のみでは実現困難です。サプライチェーンを形成する各事業者が、セキュリティの透明性を確保することに賛同し、協調して活動することが不可欠です。

そこで、私たちは本構想に賛同する事業者が協調して活動する場として、「セキュリティ・トランスペアレンシー・コンソーシアム（Security Transparency Consortium）」を 2023 年度上期に設立することをめざしています。これにより、経済安全保障関連政策の法令等によってサプライチェーンを形成する事業者間における透明性確保が求められる状況を想定して、各事業者にとって望ましい環境の実現に向けた「しくみづくり」や「社会的合意形成」を図っていきます。

付録A. 関連動向

2000 年代以降、米国では例えば以下のようなサプライチェーンに係る深刻なセキュリティ侵害が発生しました。

- 軍の情報システムにおいてルータやスイッチの中国製模造品が混入（2008 年）
- 中国製の偽半導体が混入（2008 年）
- F35 ステルス戦闘機の機密情報が漏洩、部品開発メーカの漏洩であることが判明（2009 年）

上記のようなインシデントの発生やサイバー攻撃の深刻化を受け、欧米及び日本のいずれにおいても法整備や注意喚起等の取り組みが進められています。以下では、そのうち主なものを紹介します。

(1) Cybersecurity Enhancement Act of 2014（2014 年、米国、法律）

サイバーセキュリティ対策に伴う官民連携や研究開発および教育の推進の具体的実施に向けて、本法が制定されました。取り組みが主であり、罰則や義務はありません。
本法では NIST（National Institute of Standards and Technology：米国国立標準技術研究所）に 6 つの役割を与えました。特に、NIST に以下の役割を与え、サイバーセキュリティ撲滅の旗振り役を命じている点が重要と考えられます。

「自主的、業界主導、コンセンサスベース”のサイバーセキュリティのガイドライン、規格の作成と関連する最先端研究の推進。標準の開発には、民間部門と緊密に調整するとともに重要インフラに対するガイドライン、規格を策定する。」

(2) SP800-161: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations（2016 年、米国 NIST、ガイドライン）

動向 1 を受けて NIST が制定したサプライチェーンリスクマネジメントの標準になります。NIST SP800-161 では、情報システムのライフサイクルを通して調達／利用する製品およびサービスのサプライチェーンに対するリスクマネジメントの指針と必要となる管理策をまとめています。

(3) Executive Order 14028: Improving the Nation’s Cybersecurity（2021 年 5 月 12 日、米国、大統領令）

SolarWinds におけるセキュリティ侵害など、国家に影響を及ぼすサプライチェーン攻撃の顕在化

に対抗するために発行された大統領令です。政府機関が調達するソフトウェアに関しては、サプライチェーンの安全性を向上することを目的として、安全な開発環境の確保やソフトウェアの構成要素に関する詳細（SBOM：ソフトウェア部品表）の開示などが求められています。この動きは、本書が重要視する「透明性」の確保に資するものと考えられます。

(4) Threat Landscape for Supply Chain Attacks（2021 年 7 月 29 日、欧州 ENISA、報告書）

2020 年から 2021 年前半にかけて増大したサプライチェーン攻撃に関する ENISA の報告書です。サプライチェーンのセキュリティについて、ENISA は「サプライチェーンを侵害するための手段」と「それによって侵害される資産」の 2 つの分析観点を提案しています。後者には「事業者が利用する設備」と「事業者の生産物」が含まれており、本書ではこのうち「事業者の生産物」に特に焦点を当てています。これは、前述のとおり、事業者の生産物は最終的にサプライチェーンを介して下流の事業者が利用する設備に組込まれることから、より本質的なリスクである「事業者の生産物」を優先して対処する必要があるという考え方によるものです。本報告書は、サプライチェーンセキュリティに関するより精緻な分析が必要な場合に有用です。

(5) Cyber Resilience Act（2022 年 9 月 15 日、欧州委員会、法案）
デバイスやネットワークに直接的/間接的に接続されるものも含むデジタル製品に関する包括的なサイバーセキュリティ要件を規定するものであり、例外を除き、デジタル要素を備えた全ての製品が対象となっています。本法案の付属書において、SBOM 作成や脆弱性に更新プログラムの無償提供などを含む「脆弱性処理要件」を遵守することが、製造者が満たすべき要件として記載されています。本法案は、欧州議会等の審議を経て、2025 年後半の適用をめざしているとされ、上述の Executive Order 14028 とならび、本書が重要視する「透明性」の確保を後押しするものと考えられます。

(6) サイバーセキュリティ戦略（2021 年 9 月 28 日、日本、政策）

2020 年代を迎えた日本を取り巻く時代認識およびサイバー空間をとりまく課題認識から策定された戦略です。サイバー空間を取り巻く課題認識には、サイバーとフィジカルの垣根を超えた各主体の相互連関・連鎖の深化があり、それゆえに攻撃者に狙われる弱点になると述べています。本戦略案の具体的な施策としてサプライチェーン等の信頼性確保に向けた基盤づくりが記されています。

(7) 経済安全保障推進法（2022 年 5 月 11 日、日本、法律）

安全保障の確保に関する経済施策を総合的かつ効果的に推進するための基本方針を策定するとともに、安全保障の確保に関する経済施策として 4 つの制度を創設するものです。同法の構成は以下のとおりです。

「第 1 章 基本方針の策定等」
「第 2 章 重要物資の安定的な供給の確保に関する制度」
「第 3 章 基幹インフラ役務の安定的な提供の確保に関する制度」
「第 4 章 先端的な重要技術の開発支援に関する制度」
「第 5 章 特許出願の非公開に関する制度」

特に、第 3 章では基幹インフラについて重要システムの導入または維持管理等の委託に関する計画書を作成して主務大臣に届け出た上で、導入または維持管理等を行なうことが求められています。この届出では、特に特定妨害行為（導入または維持管理等の委託に関して外部から行なわれる妨害する行為のこと）の手段として重要システムが使用されるおそれが大きいかどうかを審査が行なわれます。このことから、同法においても、システムやそれを構成する機器、及びそれらの維持管理に関する透明性の確保が重要になると考えられます。

(8) 情報セキュリティ 10 大脅威 2023（2023 年 3 月、IPA、報告書）

IPA（独立行政法人情報処理推進機構）が毎年発表している「情報セキュリティ 10 大脅威」の 2023 年版が 3 月 16 日に発表されています。10 大脅威の中に「サプライチェーンの弱点を悪用した攻撃」が 2 位に入りました。昨年の 3 位から順位を上げています。IPA 情報セキュリティ 10 大脅威 2022 では「3 位サプライチェーンの弱点を悪用した攻撃」の脅威と影響について以下のよう述べています。

「直接攻撃が困難な標的に対し、そのサプライチェーンの脆弱な部分を攻撃し、そこを経由して間接的および段階的に標的を狙う。外部に対しては強固なセキュリティ対策を行っている標的でもサプライチェーン上の取引先や導入しているソフトウェア、サービス等を足掛かりとされることで、攻撃者の侵入を許してしまうおそれがある。攻撃を受けた場合、機密情報の漏えいや信用の失墜等、様々な被害が発生する。また、取引先の組織においても、自組織が被害を受けるだけでなく、取引相手にも損害を与えてしまうことで、取引相手を失ったり、場合によっては、損害賠償を求められたりするおそれがある。」

付録B. 用語定義

用語	意味
SBOM（Software Bill of Materials）	コンポーネントやそれらの依存関係の情報も含めた機械処理可能なインベントリー（一覧表）のこと。コンポーネントやその依存関係をすべて表現している場合もある。OSS だけではなくプロプライエタリソフトウェアに活用することもでき、広く一般に公開するほか関係者だけに提示するという使用方法も存在する。
サイバー攻撃（Cyber Attack）	資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試みのこと。[JIS Q 27000:2014]
サイバーセキュリティ（Cybersecurity）	電子データの漏えい・改ざん等や、期待されていた機器、IT システム、制御システム等の機能が果たされないといった不具合が生じないようにすること。[NIST SP800-53　Rev.4]
サプライチェーン（Supply Chain）	複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達にはじまり設計・開発・製造・加工・販売及び購入者への配送に至る一連の流れのこと。[ISO 28001:2007,NIST SP 800-53 Rev.4]
サプライチェーンセキュリティリスク（cybersecurity risks throughout the supply chain）	供給者やその先のサプライチェーン、その製品、またはそのサービスからから生じる危害の可能性のこと。サプライチェーン全体のサイバーセキュリティリスクは、製品およびサプライチェーンを横断するサービスの脆弱性等を悪用した脅威やサプライチェーン自体がもつ脆弱性等により脅威が高まる。[NIST SP 800-161r1]
脆弱性（Vulnerability）	一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点のこと。[JIS Q 27000:2014]
ST オブジェクト（Security Transparency Object）	サプライチェーンにおいて事業者間で授受される機器、システム、サービス等の「構成」と「リスク」を可視化したデータ
セキュリティトランスペアレンシー確保技術（Security Transparency assurance Technology）	ST オブジェクト（Security Transparency Object）の生成・共有・活用に関する要素技術群。