

## 日立ソリューションズ Forum 2021

---

# 「透明」なソフトウェアがめざす世界 ～SBOMから始めるリスク対策～

2021/10/28

株式会社 日立ソリューションズ  
ITプラットフォーム事業部 デジタルシフト開発支援本部  
OSS管理ソリューショングループ

渡邊歩

## ■ Software Component Transparency, 「透明な」ソフトウェア



ソフトウェアの透明性は  
なぜ重要なのか

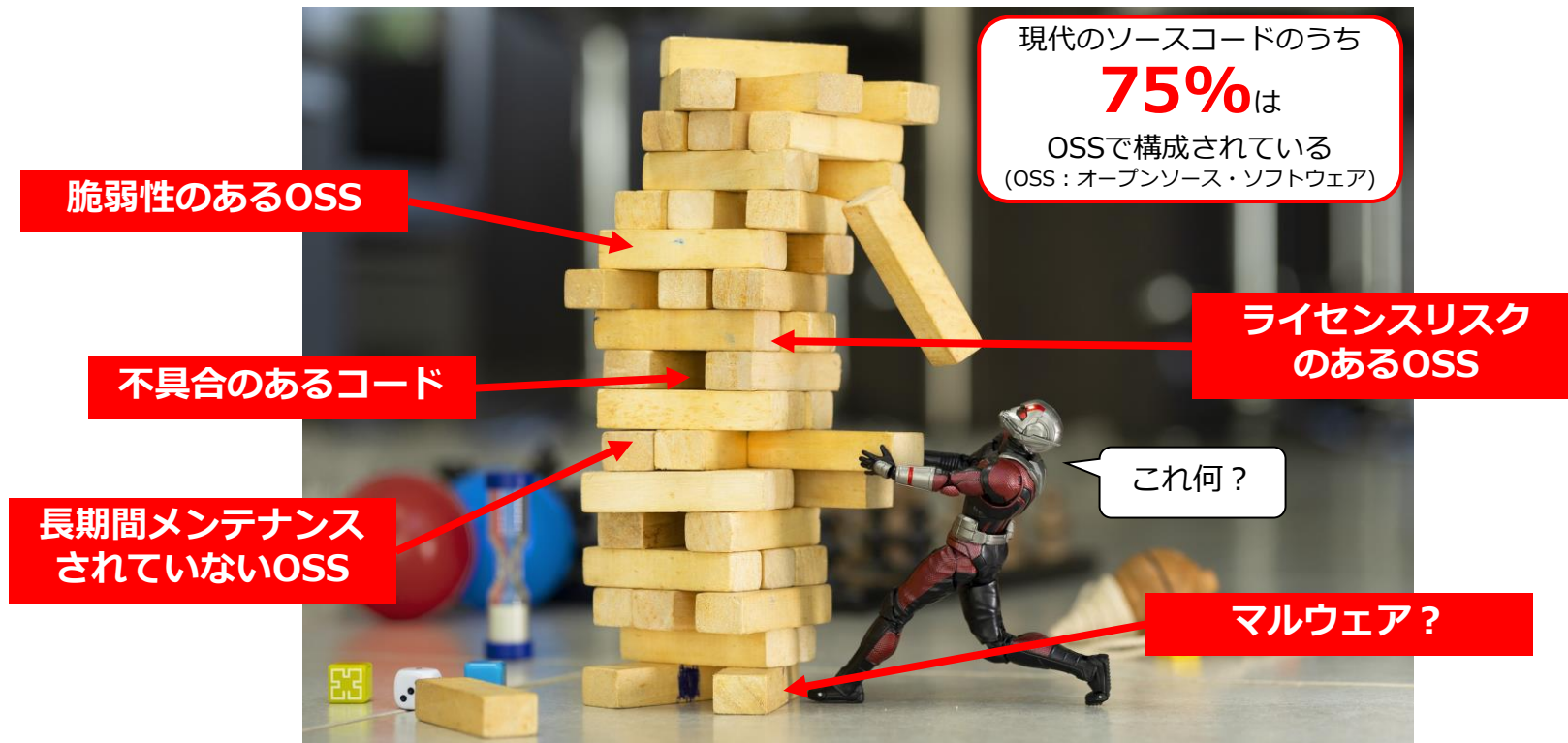
透明性を実現する手段  
SBOM

SBOMによる脆弱性リスク、  
コンプライアンスリスクの対応

国際的な標準化の動向


オープンソース管理ソリューション  
のご紹介

## ■ 現代のソフトウェアは脆い第三者の成果物に依存している



### ■ 透明性を実現する手段、Software Bill of Materials(SBOM)

**Software Bill of Materials**  
**Transparency in the**  
**Software Supply Chain**



Information Session  
for the Energy Community  
January 26, 2021

**Summing up**

- Software Bill of Materials is a technical and operational model of tracking software dependencies
- SBOMs enable better software security and supply chain risk management
  - Vulnerability Management
  - Procurement
  - Dealing with emerging risks
- While we need cross-sector solutions, each community will need to understand its own unique implementation.
- Need continued industry leadership to guide investment, standards, and policy around the world.
- More information
  - Published documents: [ntia.gov/SBOM](https://www.ntia.gov/SBOM)
  - About the SBOM process: [ntia.gov/SoftwareTransparency](https://www.ntia.gov/SoftwareTransparency)
  - Reach out to get involved: [afriedman@ntia.gov](mailto:afriedman@ntia.gov)

SBOMの具体例

Component Name	Version	URL	License
OpenSSL	1.0.2h	<a href="https://www.openssl.org/">https://www.openssl.org/</a>	OpenSSL and SSLeay License
glibc	2.23	<a href="http://www.gnu.org/software/libc/">http://www.gnu.org/software/libc/</a>	ISC License and others
zlib	1.2.8	<a href="http://www.zlib.net/">http://www.zlib.net/</a>	zlib License
GnuPG	1.0.5	<a href="http://www.gnupg.org/">http://www.gnupg.org/</a>	GNU General Public License v2.0 or later
libpng	1.2.44	<a href="http://www.libpng.org/pub/png/libpng.html">http://www.libpng.org/pub/png/libpng.html</a>	libpng License

脆弱性


ライセンス  
リスク

SBOMによって、  
より良いソフトウェアセキュリティおよび  
サプライチェーンリスクマネジメントが実現できる

- 脆弱性の管理
- 調達
- 発生し得るリスクへの対応

#### ■ 2021年の米国大統領令でもSBOMの重要性について言及

THE WHITE HOUSE



MENU

BRIEFING ROOM

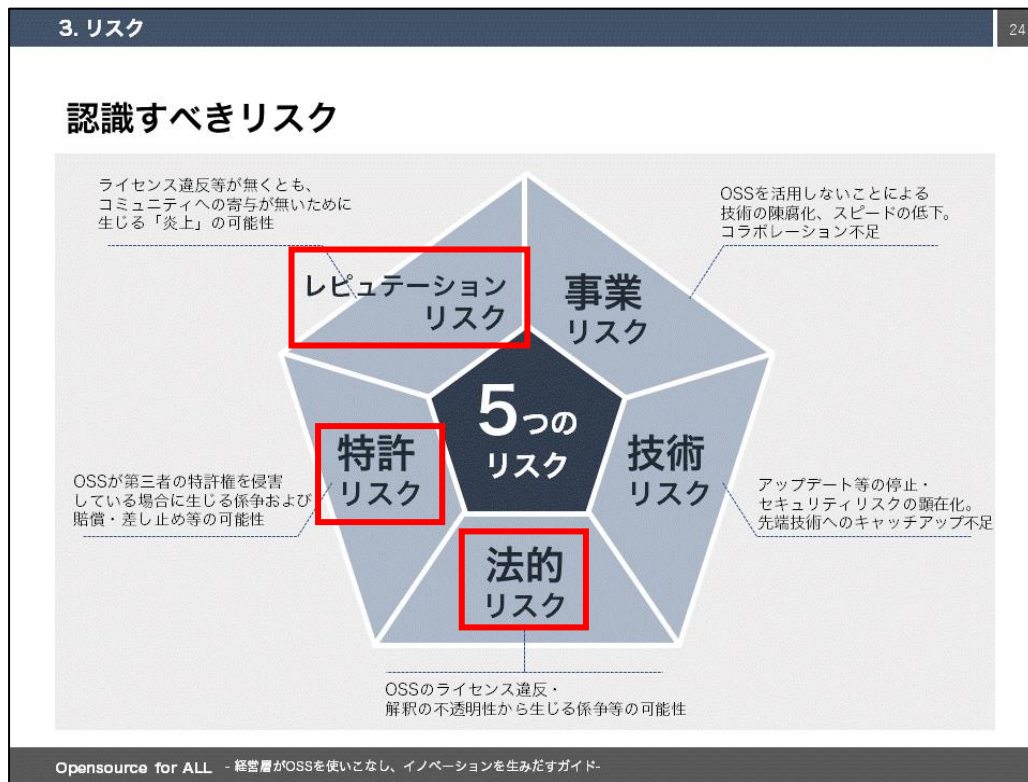
## Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

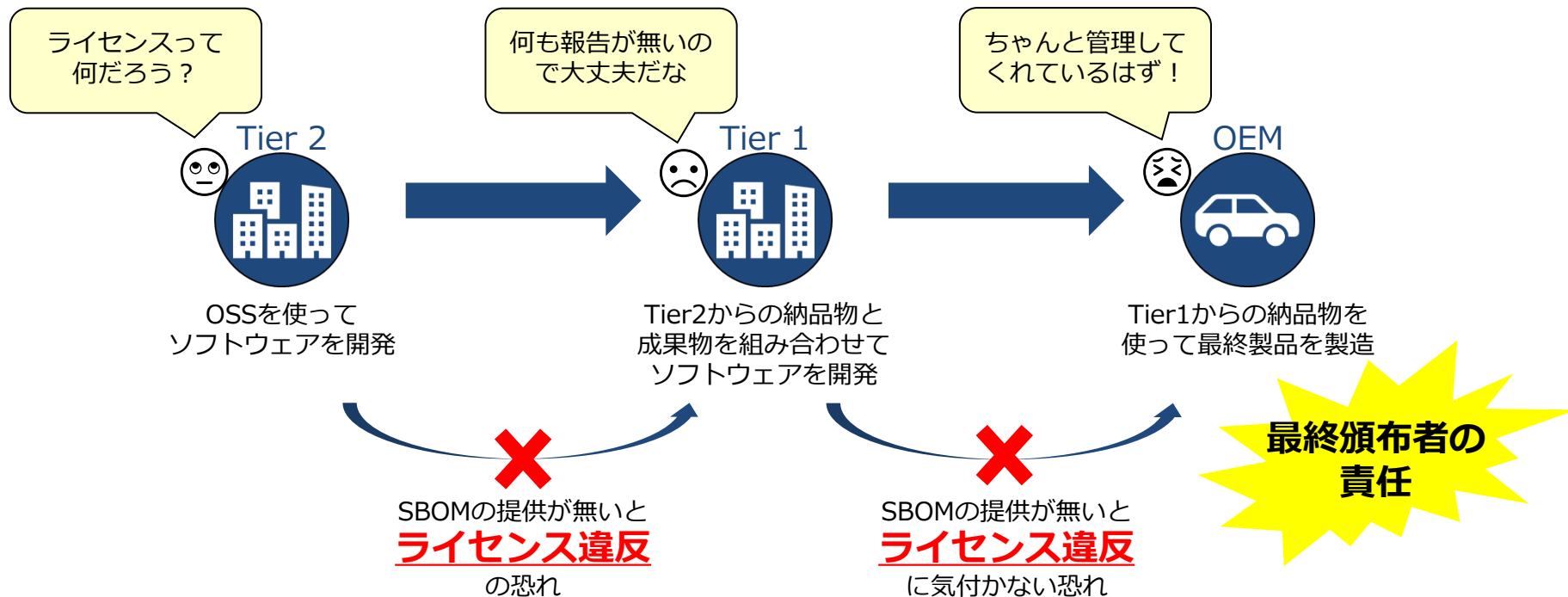
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and

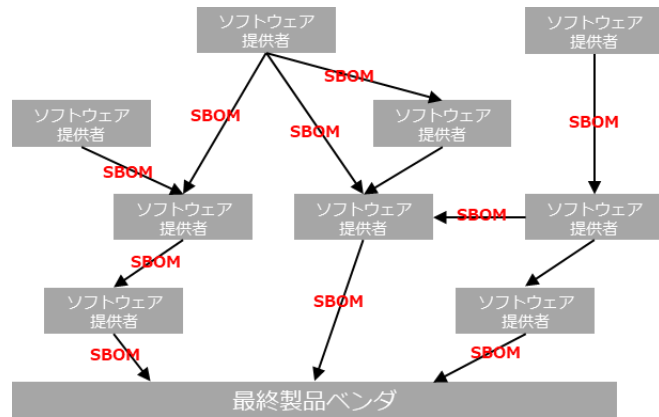
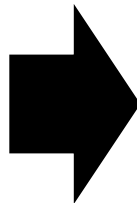
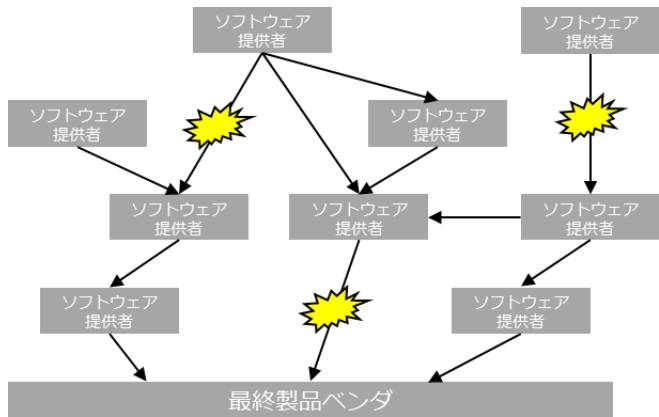
## ■ 内閣府も提言、コンプライアンスリスクは企業の経営課題である



## ■ コンプライアンスリスクは企業間のミスコミュニケーションに起因する



### ■ ソフトウェアとSBOMが一体となって流通する世界をめざして

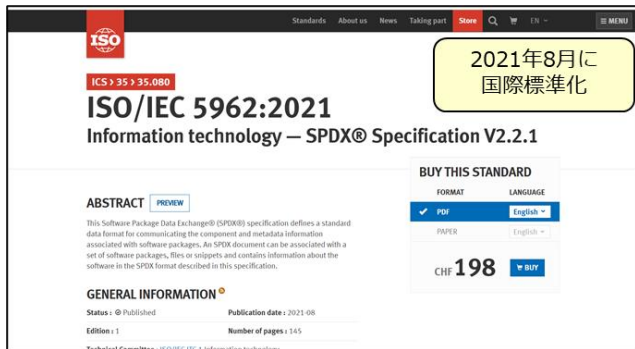
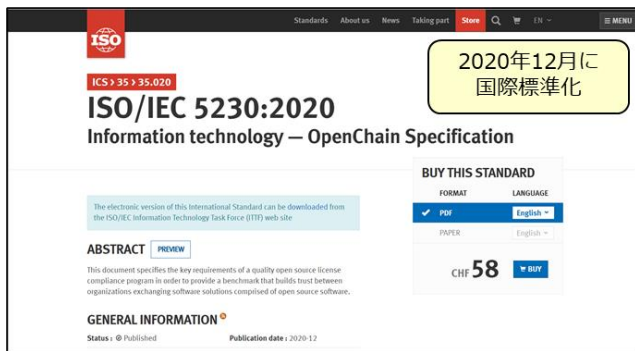


- 企業間の信頼関係が構築できず、受入検査や提供された情報の確認の負荷が高くなる

- 企業間の信頼関係が構築でき、受入検査や提供された情報の確認の重複がなくなる



## ■ プロセスやフォーマットの標準化に日本企業も取り組む必要がある



トヨタ自動車は2020年12月に  
日本企業で初となるISO/IEC 5230の準拠を発表

### ■ ここまでの内容のまとめ

- サードパーティー製のソフトウェア(特にOSS)の割合が増えている
- **ソフトウェアの透明性**は企業にとって重要な課題
- **SBOMによる可視化**が必要不可欠に
  - ✓ セキュリティ…脆弱性の早期発見と対策によりリスク低減
  - ✓ コンプライアンス…適切な管理によりライセンス違反リスクを低減
- ソフトウェアとSBOMが一体となって流通する世界をめざす
- **国際的な標準化**の流れに早めの備えが必要

機械的に抜け漏れなくSBOMを作る方法は？  
プロセス整備とは具体的にどういうこと？



## ■ 豊富な経験をもとにお客様の課題に最適なソリューションを提供

### 企業におけるOSSマネジメントの課題を解決します

オープンソースの利用において、以下のようなお悩みはありませんか？

#### リスクの管理

- ✓ 自社の製品・サービスがOSSライセンスに違反していないが確認したい。
- ✓ 自社で利用しているOSSのセキュリティ脆弱性を把握したい。
- ✓ 他社を含めたサプライチェーンに潜むOSSとそのリスクを管理したい。



#### ツール導入・効率向上

- ✓ スキャンツールでOSS混入をチェック・解析したい
- ✓ OSSリスト (SBOM) の作成と管理を効率的に行いたい
- ✓ ツールを導入したいがどれが良いが分からない



#### 体制構築・プロセス改善

- ✓ OSSの取り扱いに関するルールを整備し、ポリシーやガイドラインを作りたい。
- ✓ 社員向けにコンプライアンス教育を行いたい。教育コンテンツが欲しい。
- ✓ OSPOを立ち上げ、ISO/IEC 5230 (OpenChain) 認証を取りたい。



### オープンソース管理ツール

OSS管理の効率化に不可欠な、先進的なツールを複数ラインナップしています。

Black Duck



WhiteSource

FOSSA

「Black Duck」はOSSのライセンスや脆弱性を管理するためのOSS管理ツールです。

「WhiteSource」はOSSのライセンスや脆弱性を管理するためのOSS管理ツールです。

「FOSSA」はOSSのライセンスや脆弱性を管理するためのOSS管理ツールです。

### オープンソース管理コンサルティング

独自ツ

経験豊富なコンサルタントがお客様のお悩みに応じてさまざまなサービスを提供します。



「Insignary Clarity」は独自IPの解析に特化したOSS管理ツールです。

正式ラインソリューションとして提供しております。



OSS管理プロセス構築支援

企業におけるOSSの利用ポリシー策定やガイドライン作成の支援などを行うサービスです。



OSS教育

社員向けのOSS教育を実施するサービスです。



OSSチェック

ソフトウェアに含まれるOSSをお客様に代わって調査するサービスです。



ISO/IEC 5230

ISO/IEC 5230

認証取得コンサルティング  
ISO/IEC 5230 (OpenChain) の認証取得の支援を行うサービスです。



OSSよろず相談

OSSの管理に関する悩みや課題を何でも相談できるサービスです。



その他メニュー

その他のメニューです。

**END**

---

「透明」なソフトウェアがめざす世界  
～SBOMから始めるリスク対策～

2021/10/28

株式会社 日立ソリューションズ  
ITプラットフォーム事業部 デジタルシフト開発支援本部  
OSS管理ソリューショングループ

渡邊歩

※本資料に記載の会社名、商品名、ロゴ等は各社の商標または登録商標です。