HITACHI
Inspire the Next

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

はじめに

HITACHI
Inspire the Next

■ 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

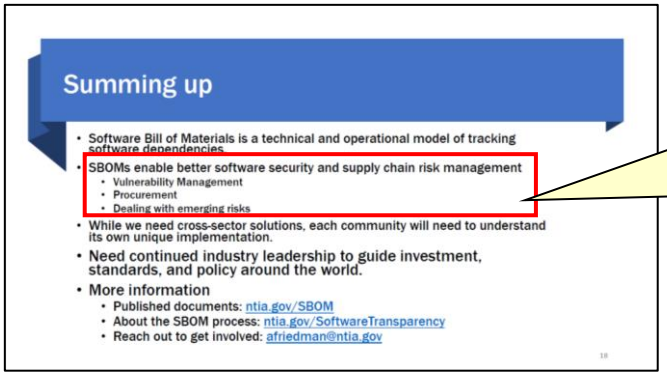
オープンソース管理ソリューション
のご紹介

HITACHI
Inspire the Next

■ 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

HITACHI
Inspire the Next

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



SBOMの具体例

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

脆弱性

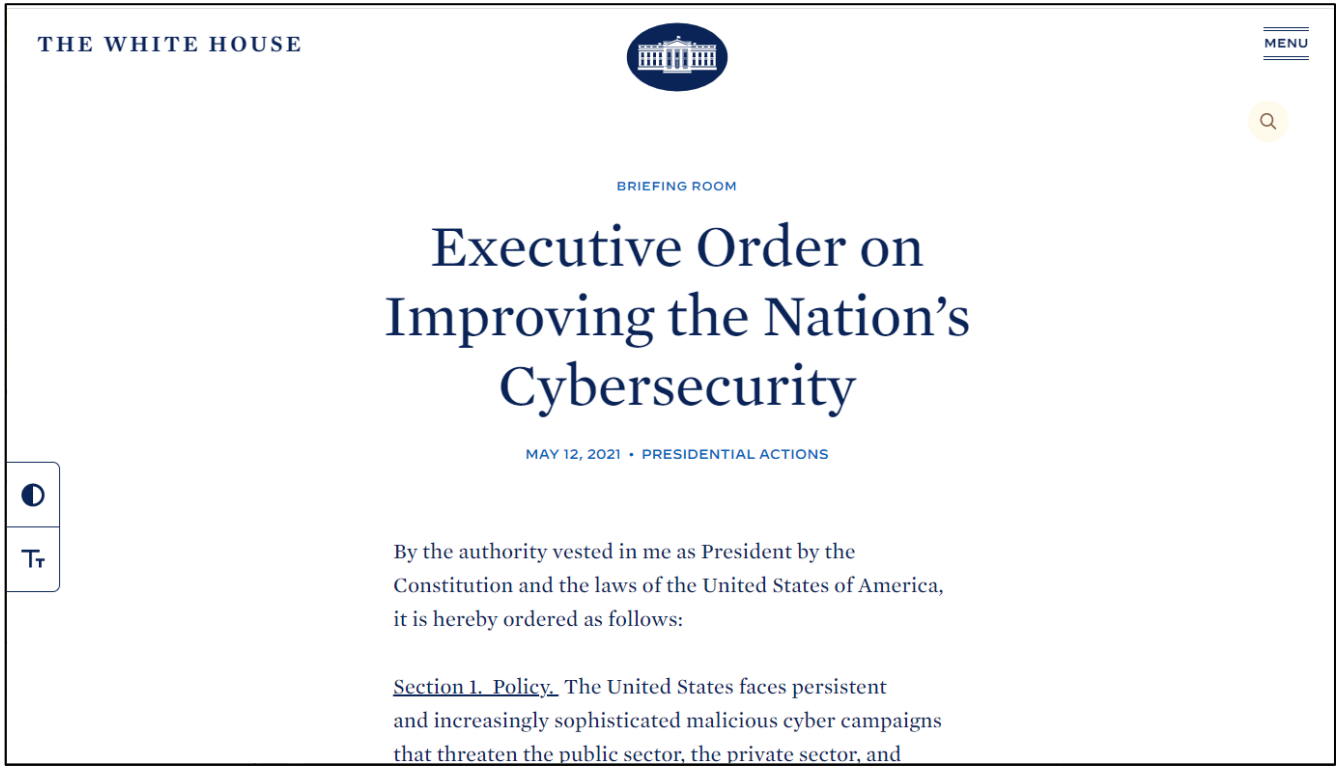
ライセンス
リスク

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

(https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_energy_jan2021overview_0.pdf)

3 セキュリティリスクに対する効果

■ 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:

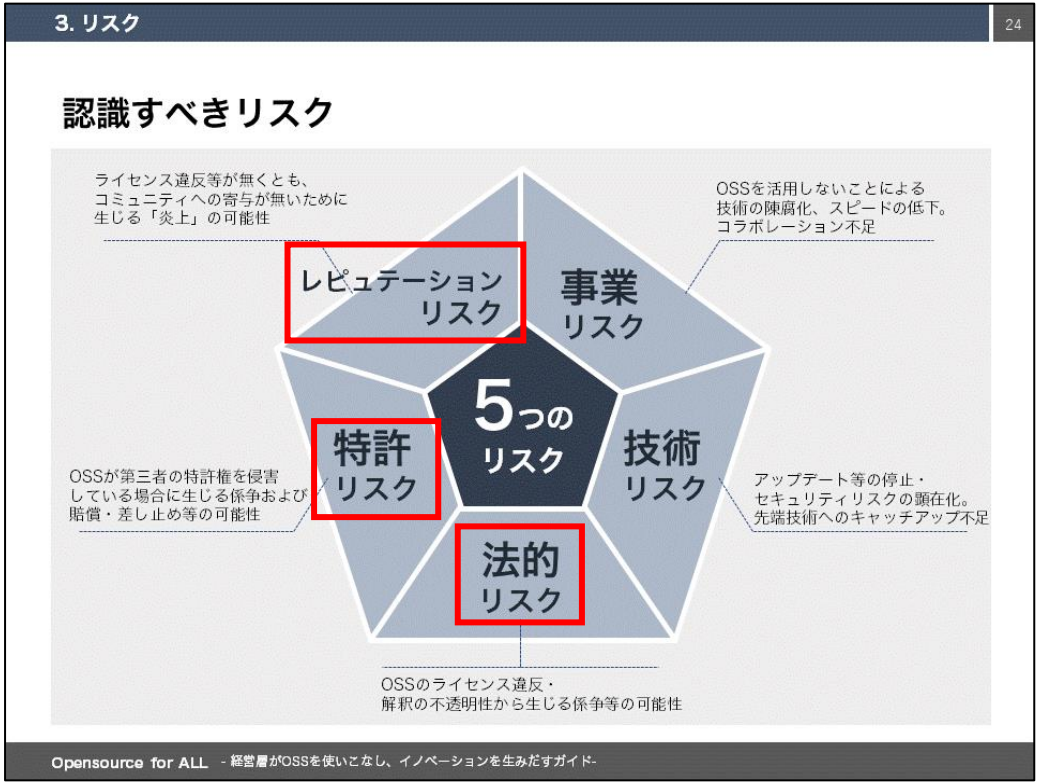
Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and

(https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)

4 OSSの活用に伴うコンプライアンスリスク

HITACHI
Inspire the Next

■ 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

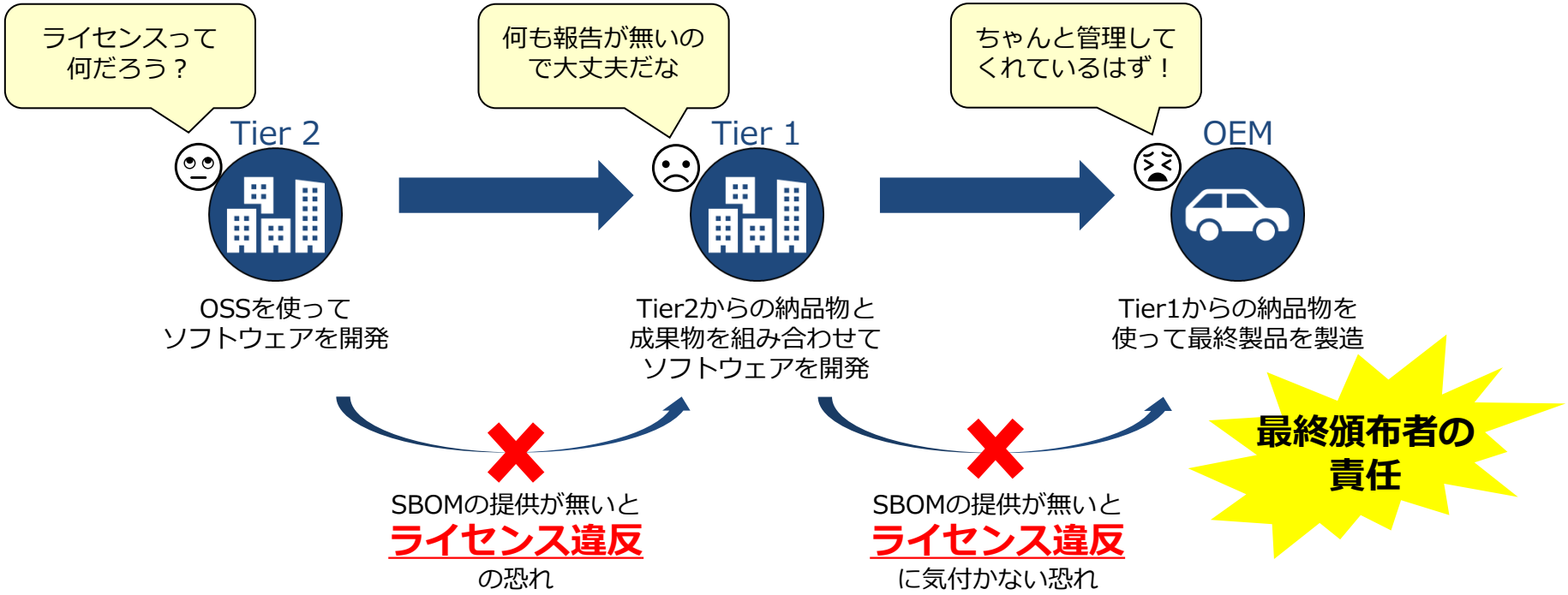


(https://www.jpo.go.jp/resources/report/takoku/document/zaisanken_kouhyou/2019_06_1.pdf)

5 コンプライアンスリスクに対する効果

HITACHI
Inspire the Next

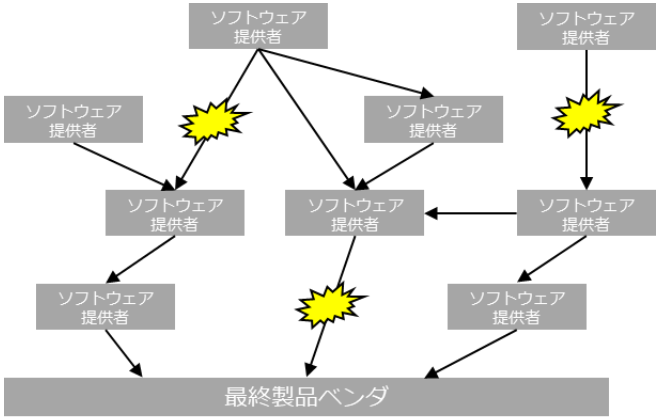
■ コンプライアンスリスクは企業間のミスコミュニケーションに起因する

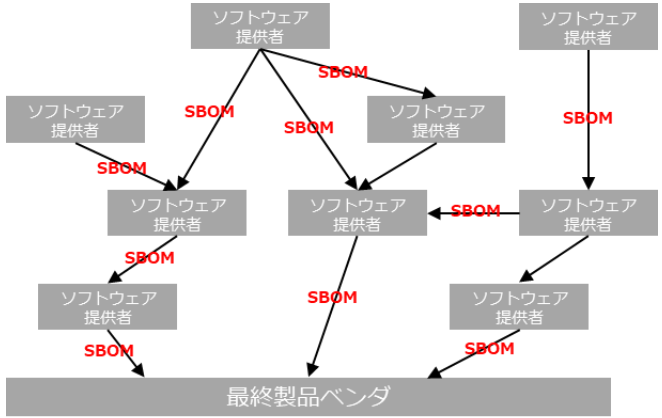


6 複雑化するサプライチェーン

HITACHI
Inspire the Next

■ 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



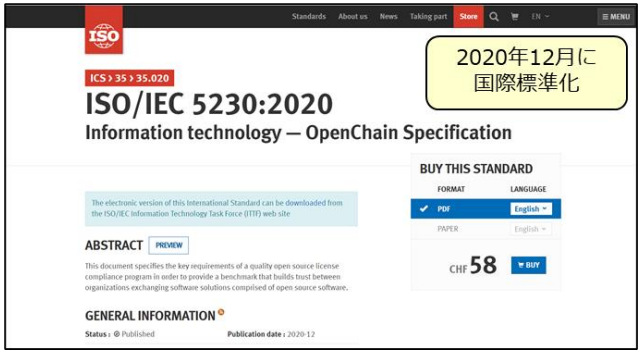


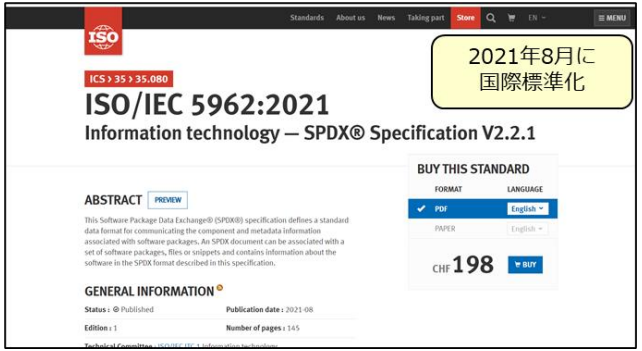
- 企業間の信頼関係が構築できず、受入検査や提供された情報の確認の負荷が高くなる

- 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

7 国際的な標準化の動向

■ 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

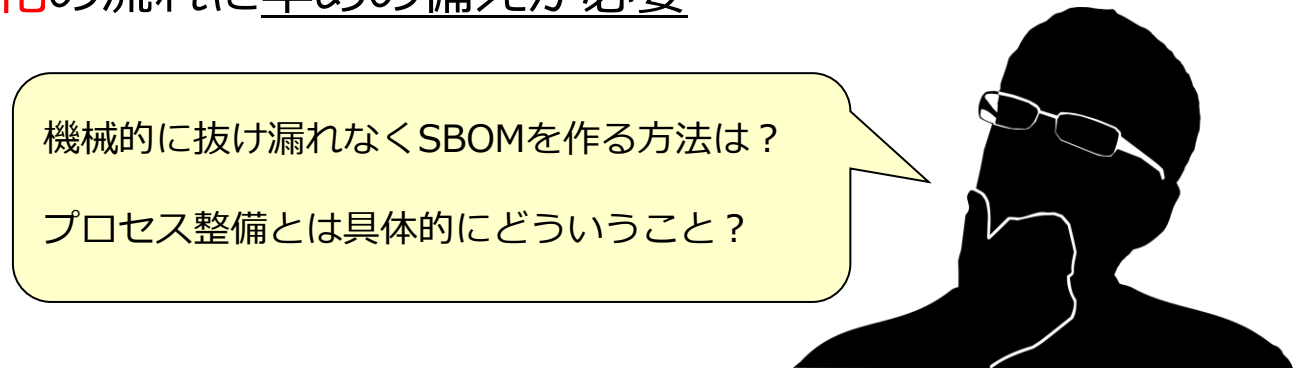
(https://digitaltrend.hitachi-solutions.co.jp/contents/000209.php)

8 まとめ

HITACHI
Inspire the Next

■ 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



HITACHI
Inspire the Next

■ 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

(https://www.hitachi-solutions.co.jp/oms/sp/)

HITACHI
Inspire the Next

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