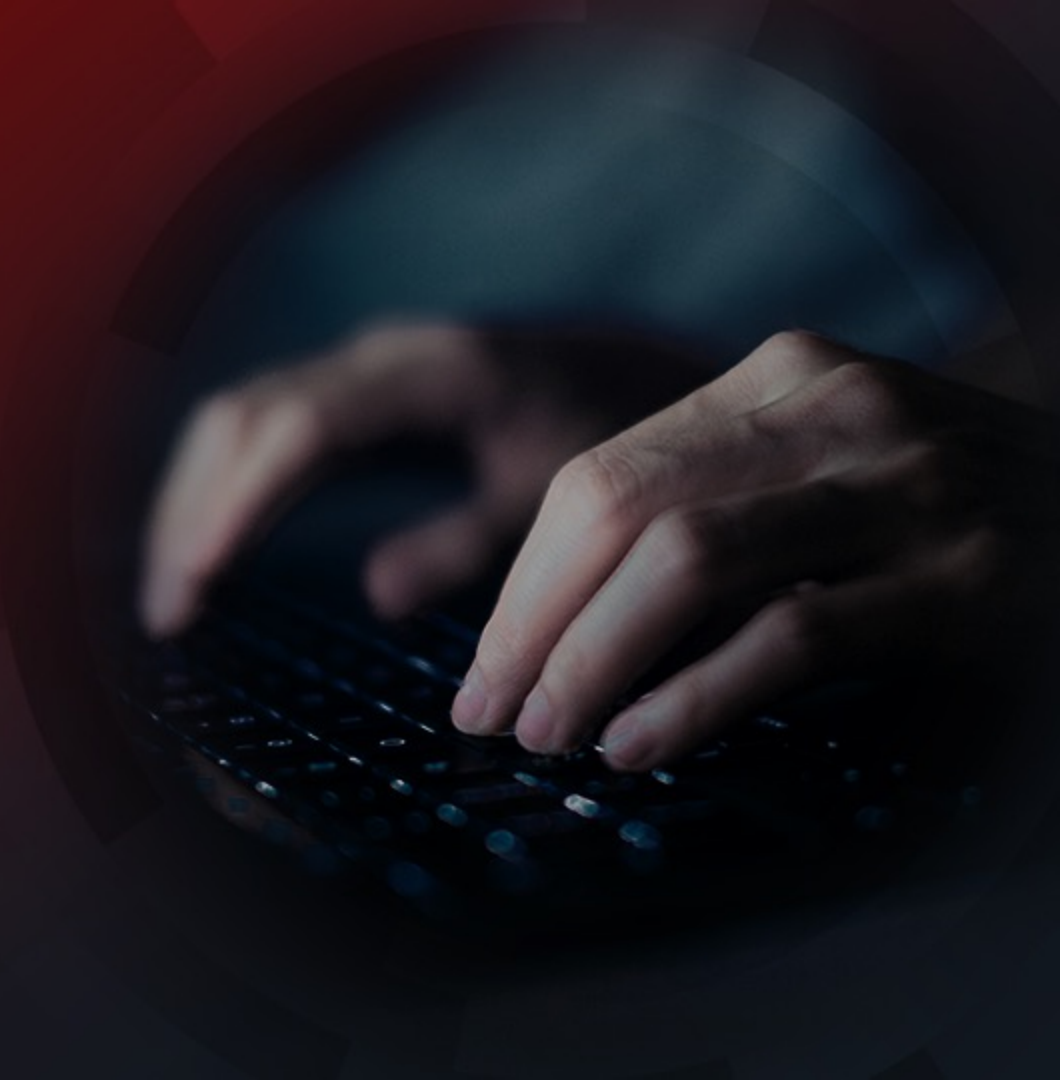
第二部
国内におけるSBOM(ソフトウェア部品表)に関する実態調査結果について

2023年4月25日

タニウム合同会社

TANIUM

本調査実施の背景



タニウムの企業概要

Tanium Inc.

設立：2007年 (2012年製品提供開始)
代表：Dan Streetman (CEO)
従業員数：2,200+名
本社：ワシントン州 カークランド
評価額：90億ドル

タニウム合同会社

設立：2015年
代表：古市 力 (アジア太平洋日本地域プレジデント 兼 日本法人代表執行役社長)
従業員数：約100名
本社：東京都千代田区
営業拠点：東京、大阪、名古屋

70%
Fortune 100 企業における採用率

8
米国トップ 10 金融機関における採用数

7
世界トップ 10 流通業における採用数

5
米国軍組織における採用数

3,000 万
グローバルで管理しているエンドポイント数

国内のお客さま（公開可能企業のみ。五十音順）

- 伊藤忠テクノソリューションズ株式会社
- 株式会社エイチ・アイ・エス
- 株式会社 荏原製作所
- 株式会社エヌ・ティ・ティ・データ
- 九州旅客鉄道株式会社
- 京セラ株式会社
- 鴻池運輸株式会社
- 株式会社 資生堂
- セガサミーホールディングス株式会社
- 積水化学工業株式会社
- 積水ハウス株式会社
- 株式会社 セゾン情報システムズ
- 全日本空輸株式会社
- 株式会社ダイセル
- 東急不動産ホールディングス株式会社
- 東芝デジタルソリューションズ 株式会社
- 西日本電信電話株式会社
- 日本電気株式会社
- 福井県
- 古野電気株式会社
- 株式会社ベネッセホールディングス
- 株式会社みずほフィナンシャルグループ
- ローム株式会社

© 2023 Tanium. All rights reserved.

タニウム国内ビジネスアップデート（2022年2月～2023年1月）

50+%

国内売上成長率

99+%

更新率

7倍

＊エマージング
エンタープライズ領域
昨対成長率

＊エマージングエンタープライズ：従業員1,000～10,000名までの企業群を意味する

© 2023 Tanium. All rights reserved.

お客様の DX 施策を強力に保護する XEM

DX の浸透に伴って拡大するアタックサーフェス

多様化するエンドポイント

日々拡張するサプライチェーンネットワーク

コンバージド・エンドポイント管理（XEM）

- あらゆる変化に適応可能なワンストップ型エンドポイント管理ソリューション -

IT 運用管理

- IT 資産管理
- アプリ配信
- データ可視化
- 性能監視
- パッチ管理
- モバイル管理

セキュリティ

- 脆弱性管理
- シャドー IT 管理
- 脅威ハンティング
- リスク分析
- EDR

© 2023 Tanium. All rights reserved.

いま何故SBOM（ソフトウェア部品表）が注目されるのか？

SBOM: Software Bill of Materials

- **BOM (Bill of Materials)とは、モノづくりの現場で古くから使われてきた「部品表」のこと：**
  - 完成品を構成する各種部品を階層化・一覧化したリスト
  - 設計部門・生産部門・購買部門などにまたがってPLM（Product Lifecycle Management: 製品ライフサイクル管理）を実現するために不可欠な情報
  - BOM管理が徹底されることで部品不具合によるリコール対応などが迅速に行えるメリット

- **自動車業界などでは部品共通化やモジュラー化の進展によるメガリコールが課題、BOMの重要性が向上**

- **SBOMとは、BOMの考え方をソフトウェア領域に適用させること**
  - 米国商務省 電気通信情報局 (National Telecommunications and Information Administration: NTIA)が下記の様に定義しています。※
    - SBOMとはソフトウェア構築において使用される多種多様なコンポーネントの詳細や、そのサプライチェーン関係を表した公式な記録のこと。これらのコンポーネントにはライブラリやモジュールが含まれ、オープンソースかプロプライエタリか、商用か否か、データが一般公開されているかそうでないか、を問わない。

- **ソフトウェア産業においてもサプライチェーンが複雑化することで部品表管理がより重要に**
  - オープンソースソフトウェアや共有ライブラリの活用が進展
  - 近年話題となったLog4Jを起因とした脆弱性の問題ですが、これはJavaにおける１ロギングライブラリで**しかない**ソフトウェア部品が引き起こした世界的な課題の一例

※ SBOM FAQ (https://ntia.gov/sites/default/files/publications/sbom_faq_-_20201116_0.pdf)

© 2023 Tanium. All rights reserved.

ソーラーウィンズ事件を覚えていますか？

過去最大級のソフトウェアサプライチェーン攻撃

Q: ソーラーウィンズ事件とは？
A: 2020年12月に発覚した、米国のソフトウェア会社ソーラーウィンズが提供するネットワーク管理ソフトウェアがサイバー攻撃をうけた事件です。この事件は民間企業のみならず複数の政府機関などが長期間攻撃を受けました。この攻撃により、ソーラーウィンズの顧客が使用するソフトウェアに悪意のあるバックドアが組み込まれました。この攻撃は、SBOMの重要性を浮き彫りにし、ソフトウェアサプライチェーンのセキュリティに対する取り組みがますます重要になっていることを示しました。

商用ソフトウェアに悪意のあるプログラムが混入

SBOMレベルでの脆弱性管理の必要性

大統領令へのきっかけ

© 2023 Tanium. All rights reserved.

SBOMの具体的なイメージ

- ソフトウェア提供者が正しい製品であることを利用者に示すための仕組み
- 食品表示ラベルのソフトウェア版と考えるとわかりやすい

食品表示ラベル

名称	チョコレート
原材料名	カカオマス、砂糖、ココアバター、脱脂ココアパウダー／乳化剤、香料（一部に乳成分・大豆を含む）
内容量	300g
賞味期限	2024.04.01
保存方法	直射日光、高温多湿を避けて保存してください
製造者	株式会社XXXXXXX 東京都港区XXXXXXX

SBOM（ソフトウェア部品表）の最小要素の定義※

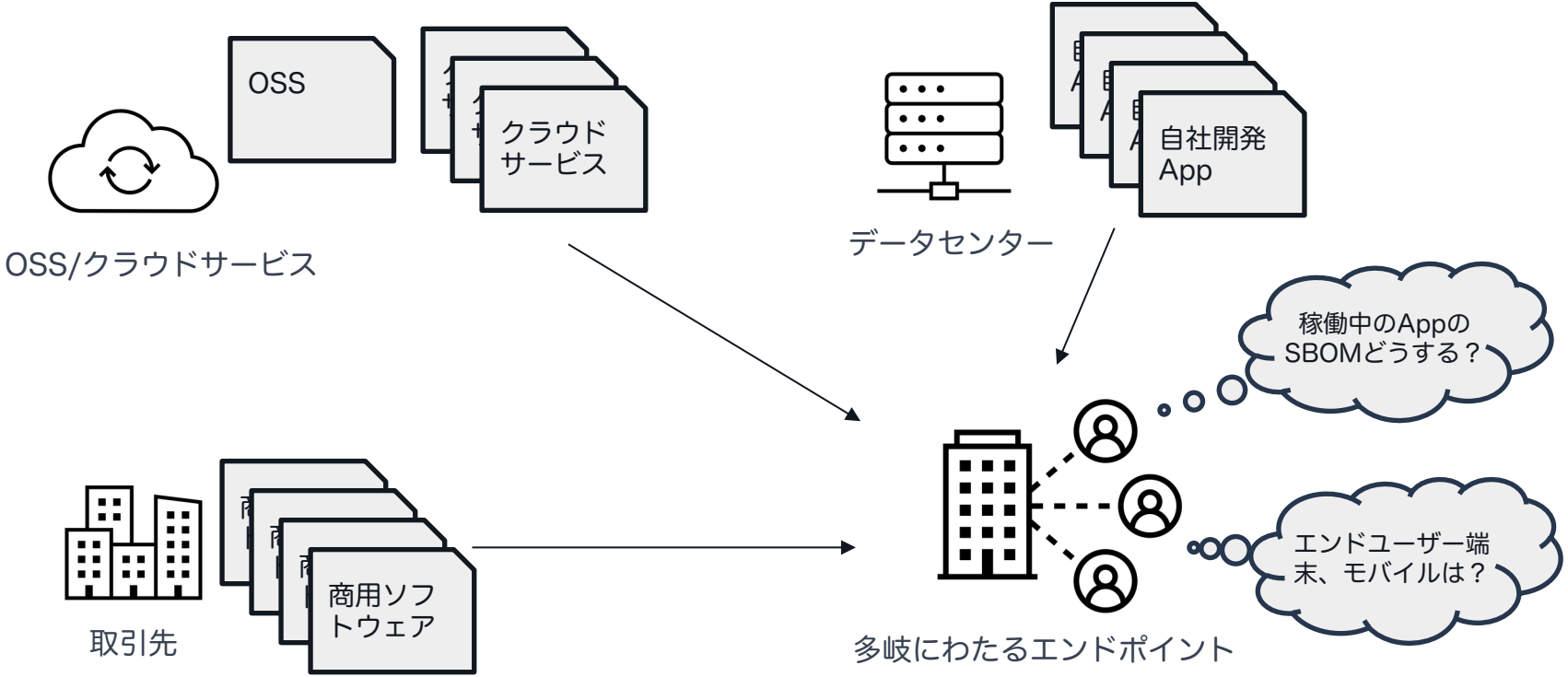
サプライヤー名	コンポーネントを開発、定義及び識別するエンティティの名称
コンポーネント名	サプライヤーによって定義された、ソフトウェアのある単位に対する名称
コンポーネントのバージョン	コンポーネントを識別するために使用されるバージョンに関する識別子
その他の一意な識別子	コンポーネントを識別するために使用される又は関連するデータベースの検索キーとして機能するその他の識別子
依存関係	コンポーネントがあるソフトウェアに含まれているという関係性の特徴づけの情報
SBOM作成者	コンポーネントのSBOM を作成するエンティティの名称
タイムスタンプ	SBOM データを作成した日付と時刻の情報

※経済産業省：参考資料 SBOM（Software Bill of Materials）の導入に関する手引（案）より抜粋
※https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/009_s01_00.pdf

© 2023 Tanium. All rights reserved.

ユーザー企業にとってのSBOM管理の難しさ

一言にSBOMといってもユーザー企業にとっては多岐にわたる検討が必要



© 2023 Tanium. All rights reserved.

SBOMを取り巻く背景

企業経営に直結するソフトウェア・サプライチェーンに対する脅威が増大

+742%

Apache Log4j等のソフトウェア・サプライチェーン攻撃の年間増加率※1

−11%

SolarWindsのサイバー攻撃を受けた年間収益額の平均損害額※2

・世界が増大する脅威に対し、ソフトウェア管理手法のSBOMに注目
・SBOMにより脆弱性やライセンスの管理のリスク及びコストを低減

・2021年：大統領令(EO 14028)にてソフトウェア・サプライチェーンセキュリティ強化を発表
・2022年：CISA、NSA、ODNIは共同で、ソフトウェア・サプライチェーンのセキュリティ保護に関するガイダンスを発表

・2022年：サイバーレジリエンス法にてSBOM作成や更新プログラム提供等を含む、製品ライフサイクル全体でのセキュリティ対応を発表

・2019年：経済産業省よりサイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースが発足
・2023年：経済産業省よりSBOMの導入に関する手引(案)が公開

*1: Sonatype, 8th Annual State of the Software Supply Chain Report
https://www.sonatype.com/state-of-the-software-supply-chain/introduction

*2: IronNet, 2021 Cybersecurity Impact Report
https://www.ironnet.com/hubfs/IronNet-2021-Cybersecurity-Impact-Report-June2021.pdf

© 2023 Tanium. All rights reserved.

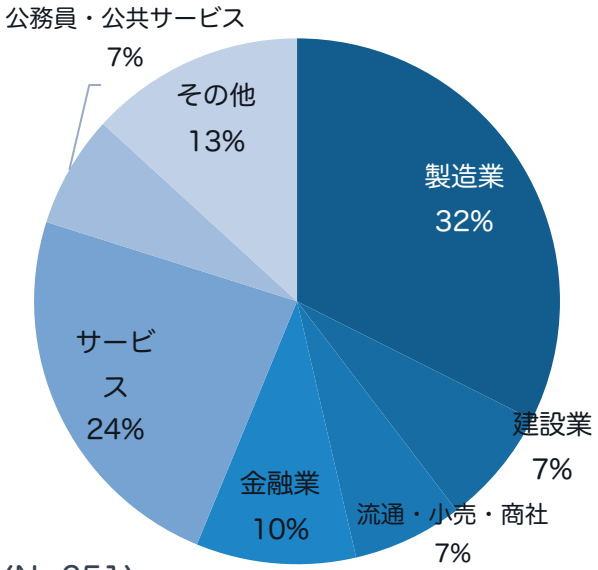
SBOM(ソフトウェア部品表) に関する市場調査

- 調査対象：主に大企業のＩＴ管理者と担当者（有効回答者：651名）
- 調査方法：Webアンケート
- 実施期間：2023年2月20日～2023年2月28日

TANIUM

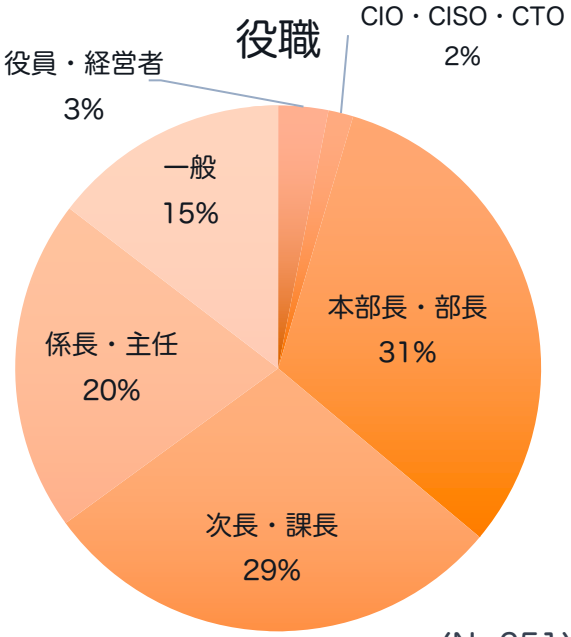
回答者プロフィール

業種



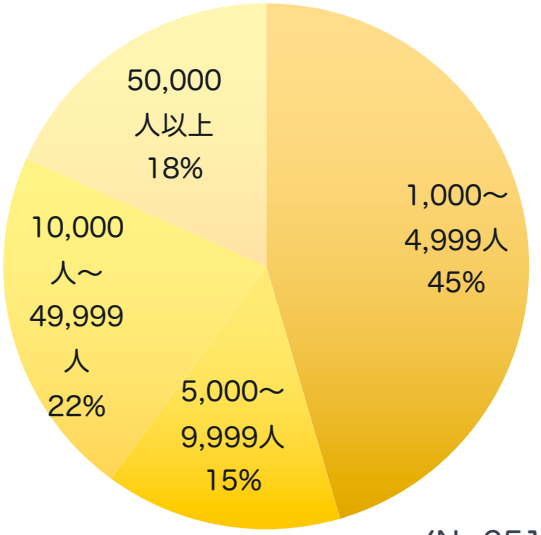
(N=651)

役職



(N=651)

規模



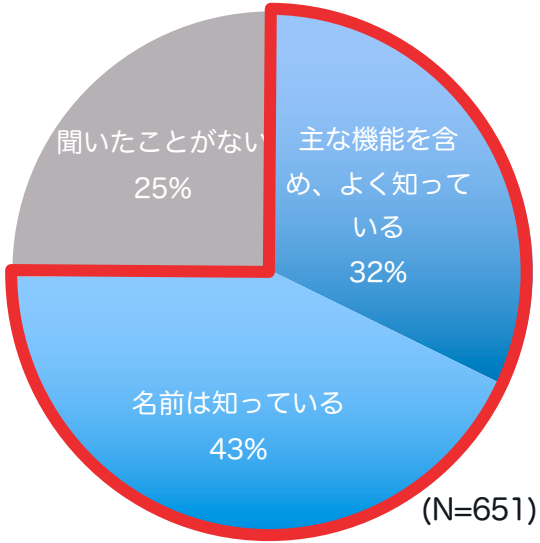
(N=651)

課長以上の役職者が65%、5,000名以上の大手企業が55%

© 2023 Tanium. All rights reserved.

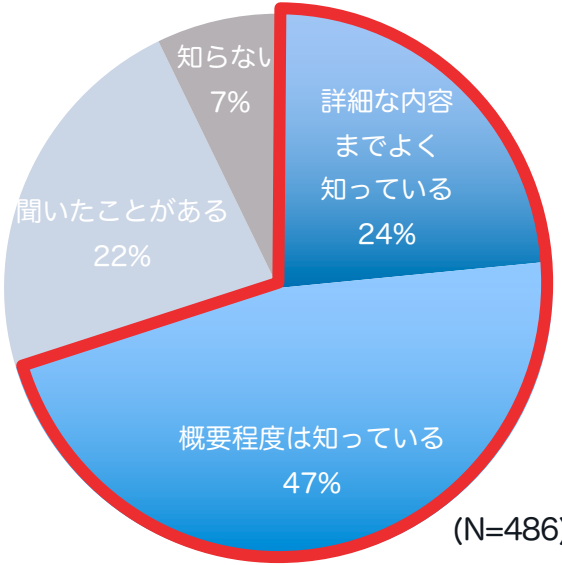
SBOMの認知度

SBOM（ソフトウェア部品表）



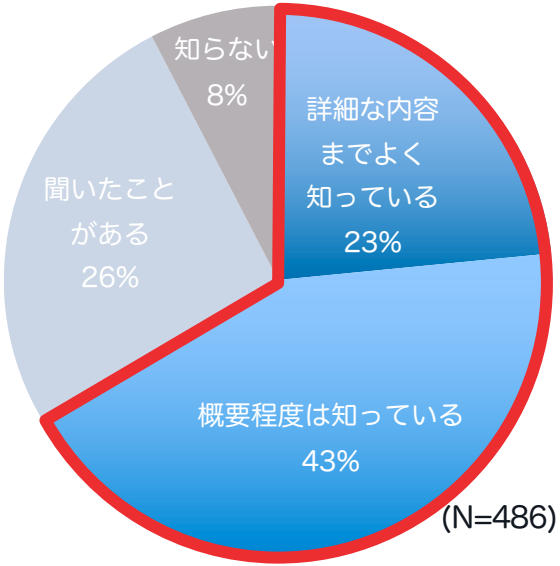
(N=651)

米国の大統領令で政府系システムに対してSBOMの構築が義務付けられたこと



(N=486)

経済産業省が“サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性”を公開していること

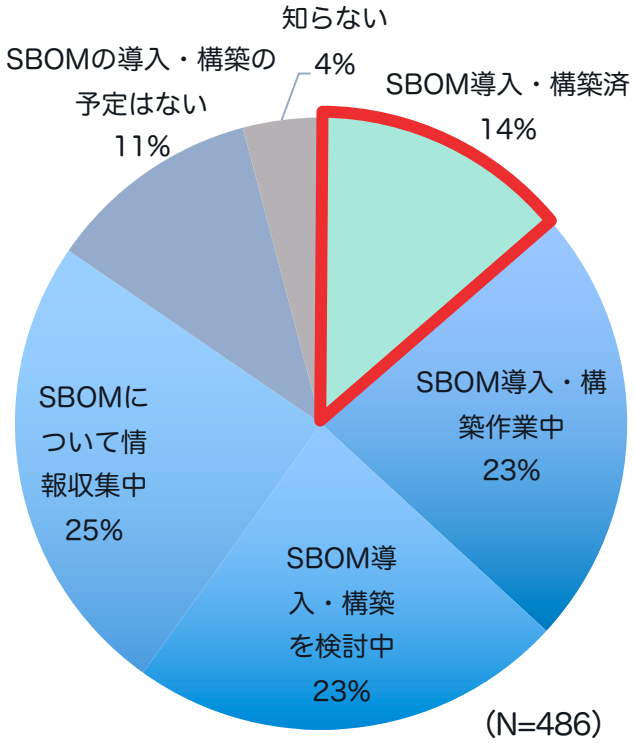


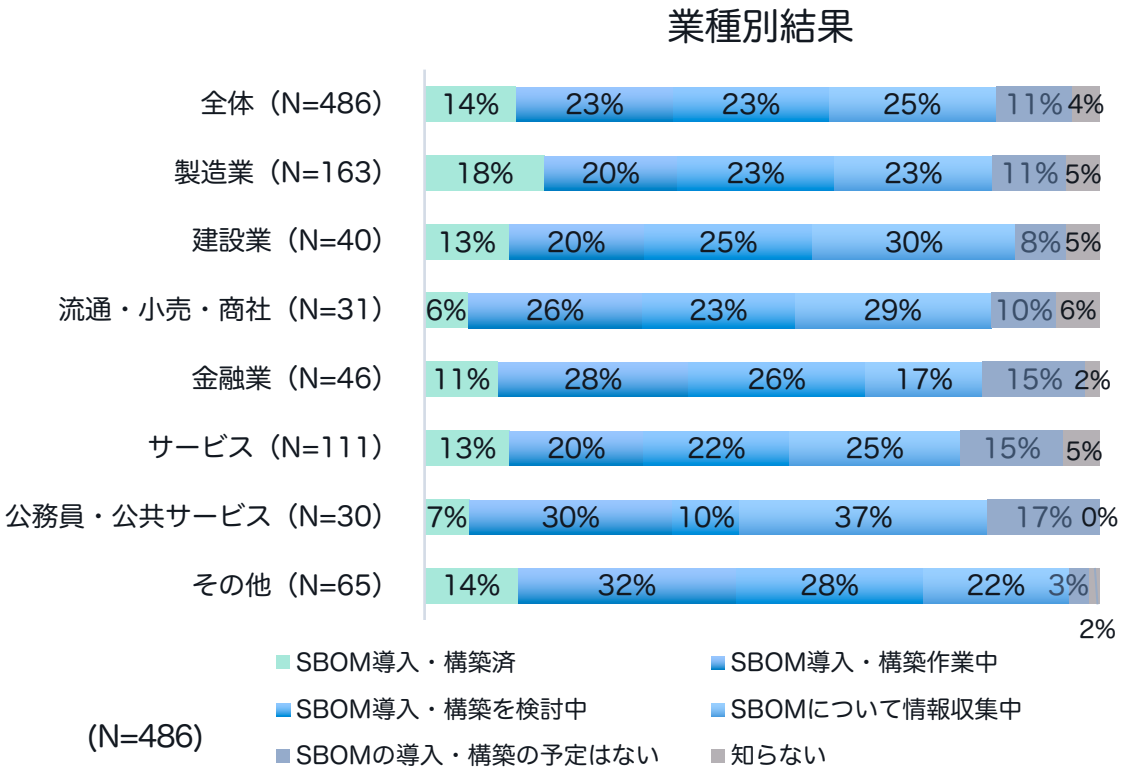
(N=486)

SBOMの認知度は75%に上り、国内外の動向も回答者の７割前後が認知していると回答した。

© 2023 Tanium. All rights reserved.

SBOMの導入状況

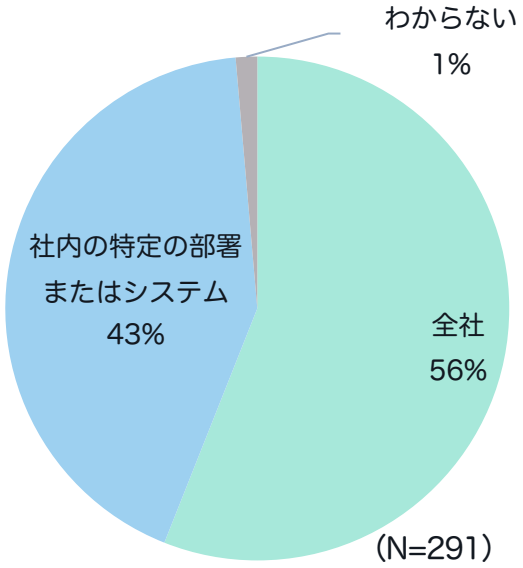




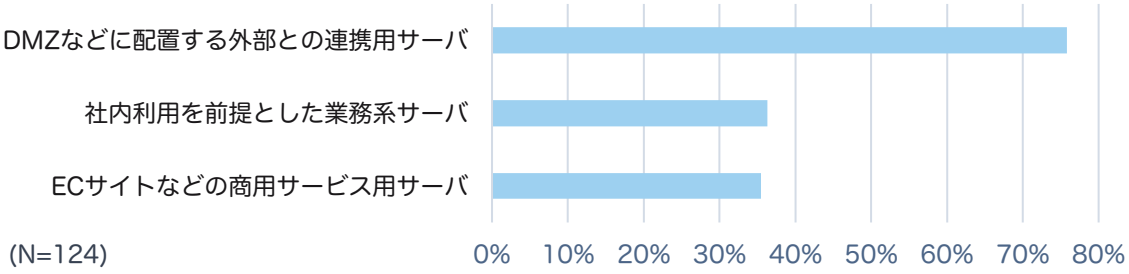
SBOM導入済みはわずか14%、ただしSBOM導入・構築検討中まで含むと６割が前向きな取り組みを実施中。業種別では製造業がトップとなり流通・小売の３倍の導入状況。

© 2023 Tanium. All rights reserved.

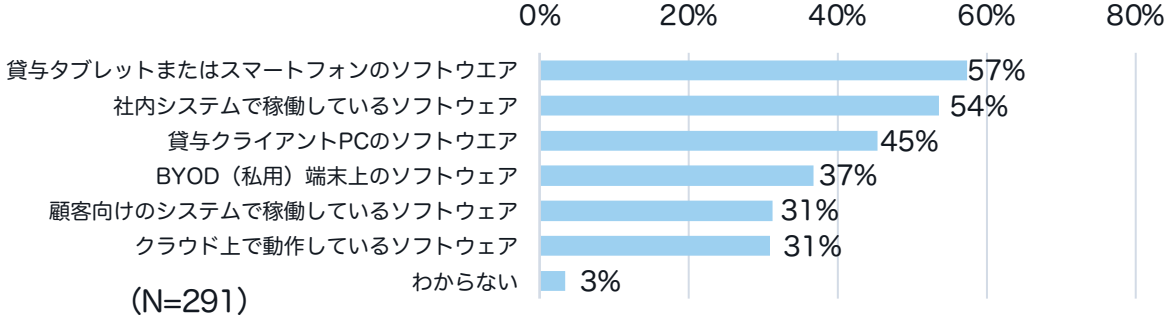
SBOMの対象領域



SBOM対象を特定システムに絞っている組織における
SBOM対象優先度の高いシステム



SBOM（ソフトウェア部品表）の対象となるエンドポイント

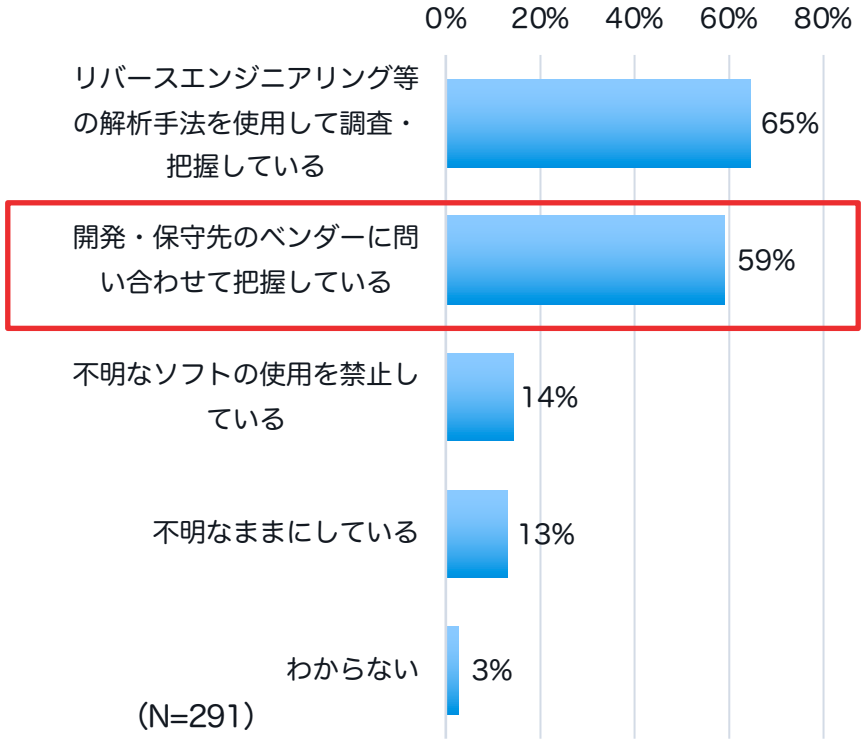


特定の部署やシステムをSBOM対象とする組織が４割強にとどまり、それらの組織の約８割がDMZ等外部と連携するシステムを対象としている。また、SBOM対象となるエンドポイントは幅広く分散しているが、設問にあげたすべてを対象としている組織は全体の10%にとどまる。つまり、全社でSBOM管理を徹底していると答えた組織においても一部のエンドポイントしか管理できてない組織が8割を超え、SBOM管理の徹底が難しいことが改めて浮き彫りになった。

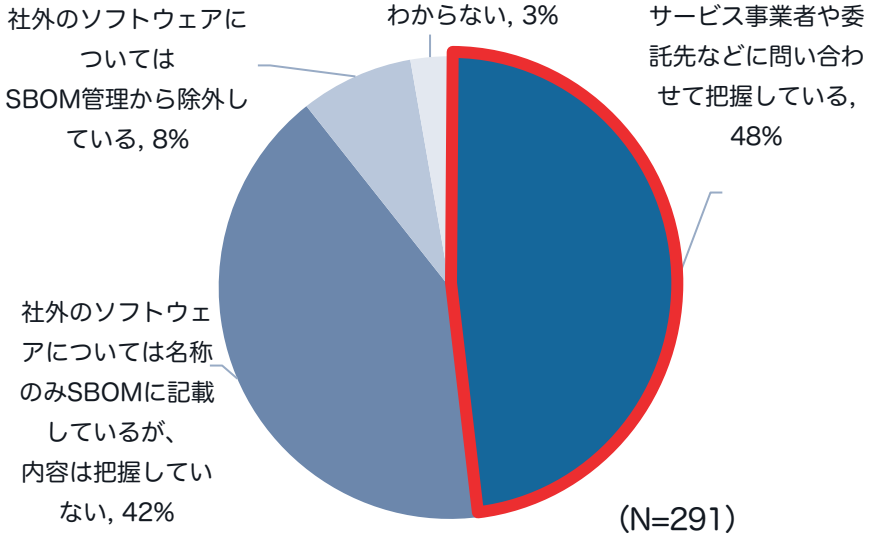
© 2023 Tanium. All rights reserved.

SBOM管理の実態

内部構造・依存関係が不明なソフトウェアがあった場合のSBOM管理



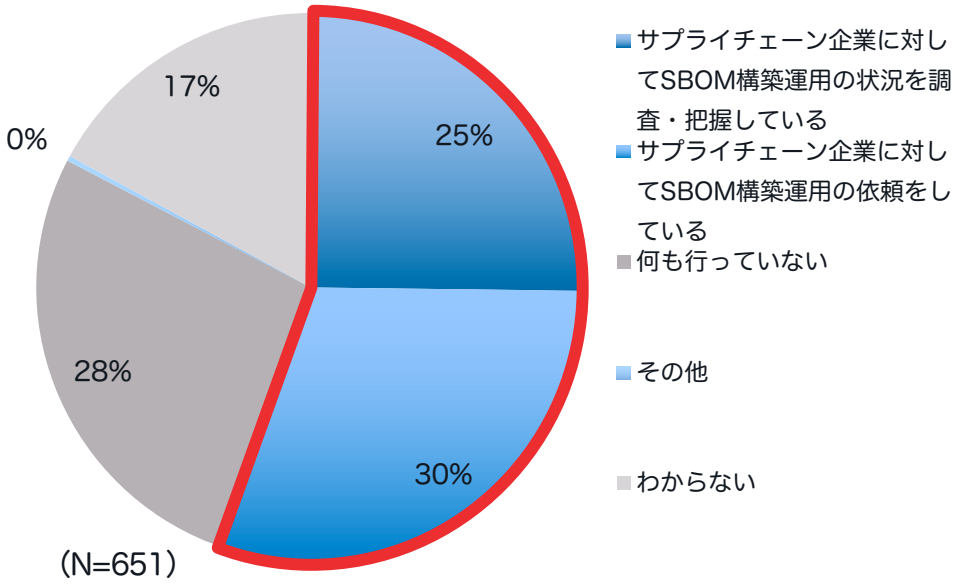
使用しているクラウドサービスや委託先等の社外のソフトウェアのSBOM管理

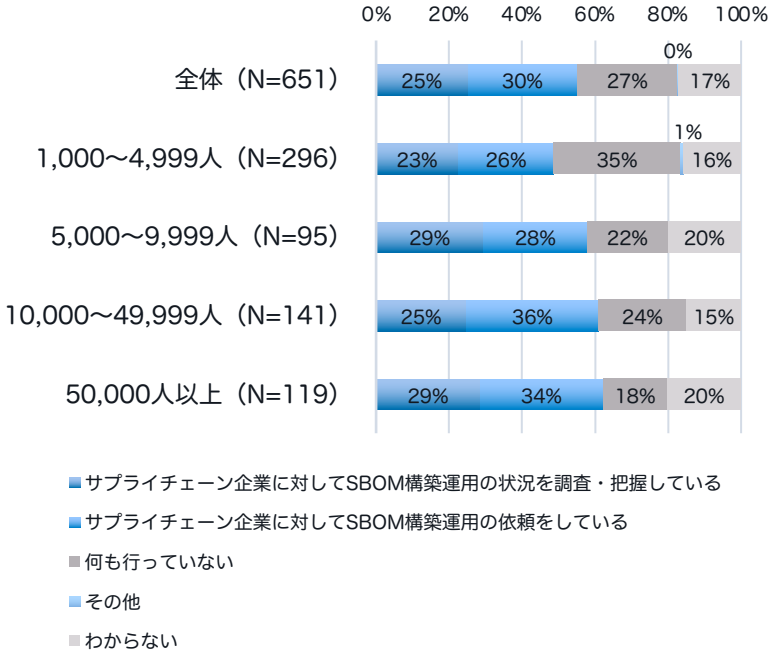


社外のソフトウェアやクラウドサービスなどについては問い合わせ対応が約半数、内部構造・依存関係が不明な場合も半数以上が問い合わせ対応と属人的な状況が明らかになった。

© 2023 Tanium. All rights reserved.

サプライチェーン企業に対するSBOM管理



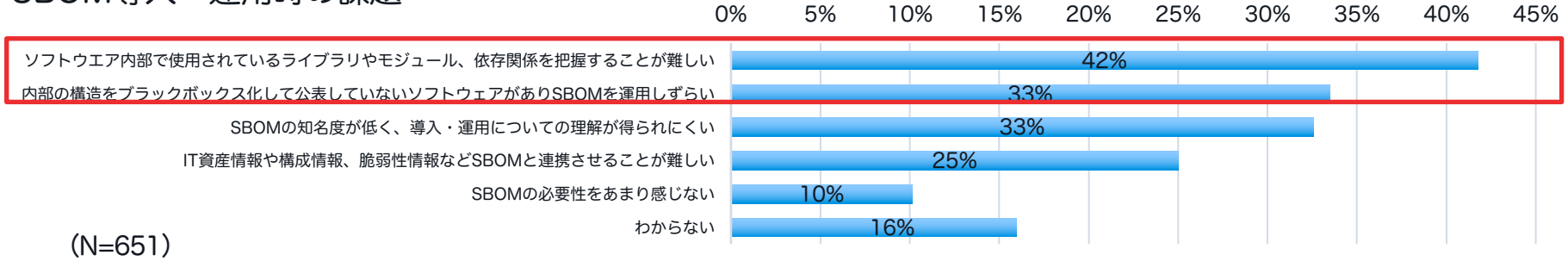


サプライチェーンのSBOMについては25%が調査・把握済、30%が依頼中となっている。
サプライチェーン企業に対するSBOM管理の需要が確認できた。

© 2023 Tanium. All rights reserved.

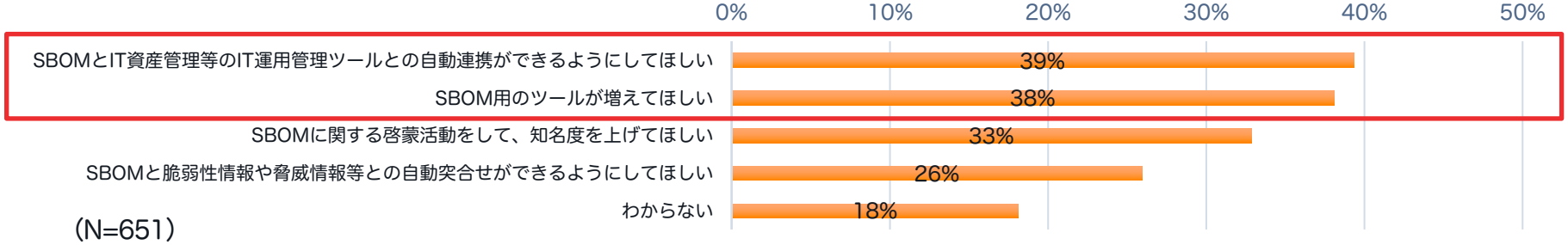
SBOM導入・運用時の課題と要望

SBOM導入・運用時の課題



（N=651）

SBOM導入・運用に関する要望



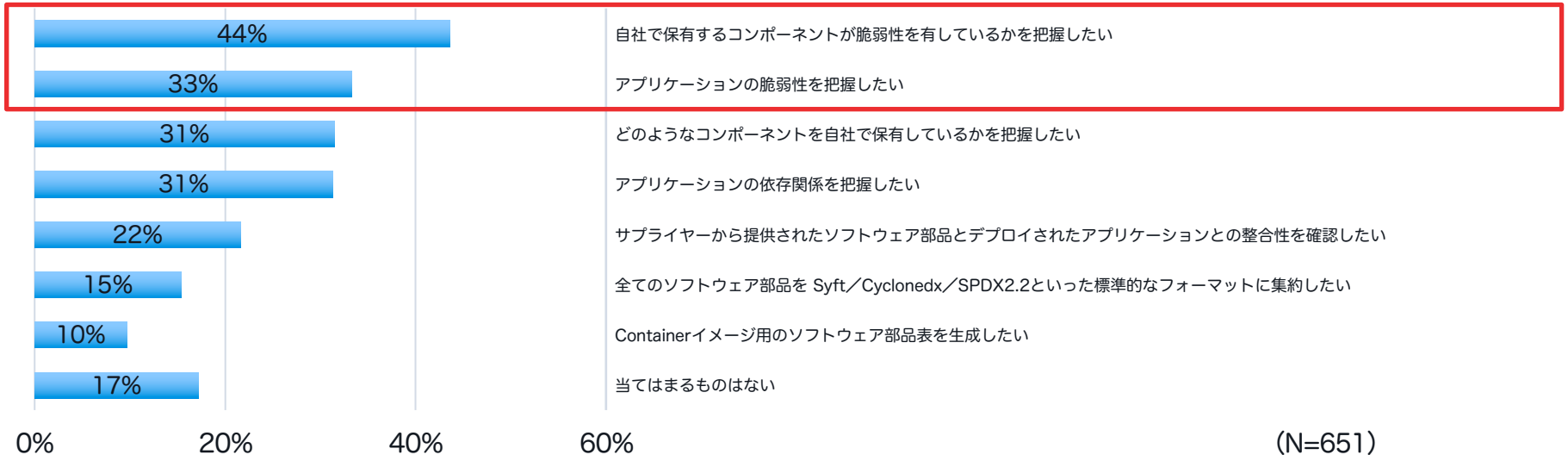
（N=651）

課題としては、詳細を把握しきれないという観点が上位を占める。
また、要望としては既存ツールとの連携、ツール不足と続く。

© 2023 Tanium. All rights reserved.

SBOMに期待する機能

SBOMに期待すること



- すでに自社で保有する脆弱性の把握に関する期待が最も高く44%となった
- 次点でアプリケーションの脆弱性把握に対する期待となり、脆弱性管理への期待値が高いことがわかる
  一方で全てのSBOMを標準フォーマットに集約したいという期待は15%にとどまる

© 2023 Tanium. All rights reserved.

SBOM実態調査のまとめ

SBOMの認知度は一定程度あるものの、具体的な対策までできている組織はわずか14%

社外のソフトウェアやクラウドサービス、内部構造・依存関係が不明な場合は問い合わせ対応が主な対応となり、属人的な運用に課題感

サプライチェーンまで包含したSBOM対応を視野に入れた検討が進む

既存環境向けのSBOM導入・運用には、既存のIT運用ツールを活用せざるを得ない状況であるがツール間のデータ連携に課題もあり、今後の連携、統合的ツールに期待

SBOM対応において脆弱性管理が最も検討優先度が高い

© 2023 Tanium. All rights reserved.

調査結果を踏まえてタニウムからの提言

2023年4月25日

タニウム合同会社

TANIUM

SBOM導入・運用の課題から見えてきたこと

ユーザー企業にとってSBOM管理を行う本来の目的とは？

自社環境に潜在する
脆弱性を把握すること

~~ソフトウェア製品を
SBOM標準フォーマットで管理すること~~

© 2023 Tanium. All rights reserved.

なぜ脆弱性を把握することが難しいのか

ソフトウェア内部で利用されているライブラリ、コンポーネントの把握する手段がないから

既存のIT資産管理ツール、脆弱性管理ツール、構成管理ツール単体ではソフトウェア内部の脆弱性までを把握することが難しいから

SBOM専用ツールは開発プロセスに特化していることが多く、運用プロセスにその機能を活用することが難しいから

アプリケーション実行環境は流動性があるため、納入時のSBOMを把握しているだけでは、現状と乖離がある可能性があるから

→ 流動性の高いIT環境でリアルタイムにソフトウェア内部まで脆弱性を把握できるツールの必要性

© 2023 Tanium. All rights reserved.

SBOM管理の課題解決に向けた取り組み

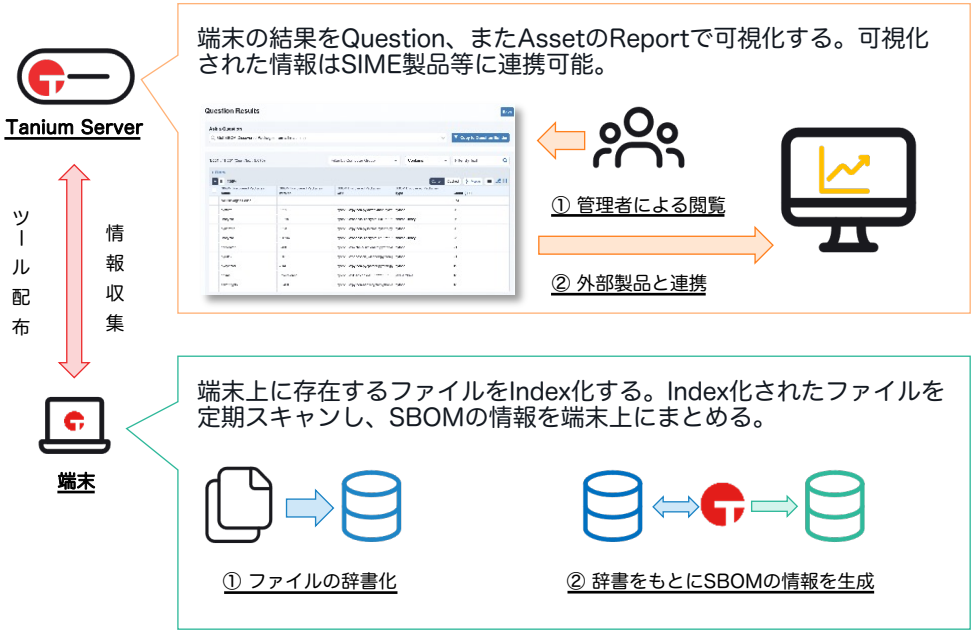
Taniumのアプローチ

調査結果からも明らかなようにユーザーのSBOMに対する興味は、開発のアプリケーション環境のみならず、既存環境の脆弱性を把握することにある。しかしながら、既存のITツールのみでインベントリ管理に加え、ソフトウェアのサプライチェーン、ライセンスコンプライアンス、セキュリティや品質などのリスクを完全に把握することは困難である。当社ではエンドポイントの網羅的なリアルタイム情報収集能力に長けた特徴を活かし、この課題解決に向け以下の機能提供を開始した。

- Tanium SBOM
  - パッケージソフトウェアで使われているライブラリを可視化
    例：OpenSSLのライブラリに脆弱性がでた時にどの製品がどのバージョンのライブラリを使っているか
  - SBOMの情報を取得・整形し、一覧で表示
  - 注視したいソフトをグラフ化しておくことも可能

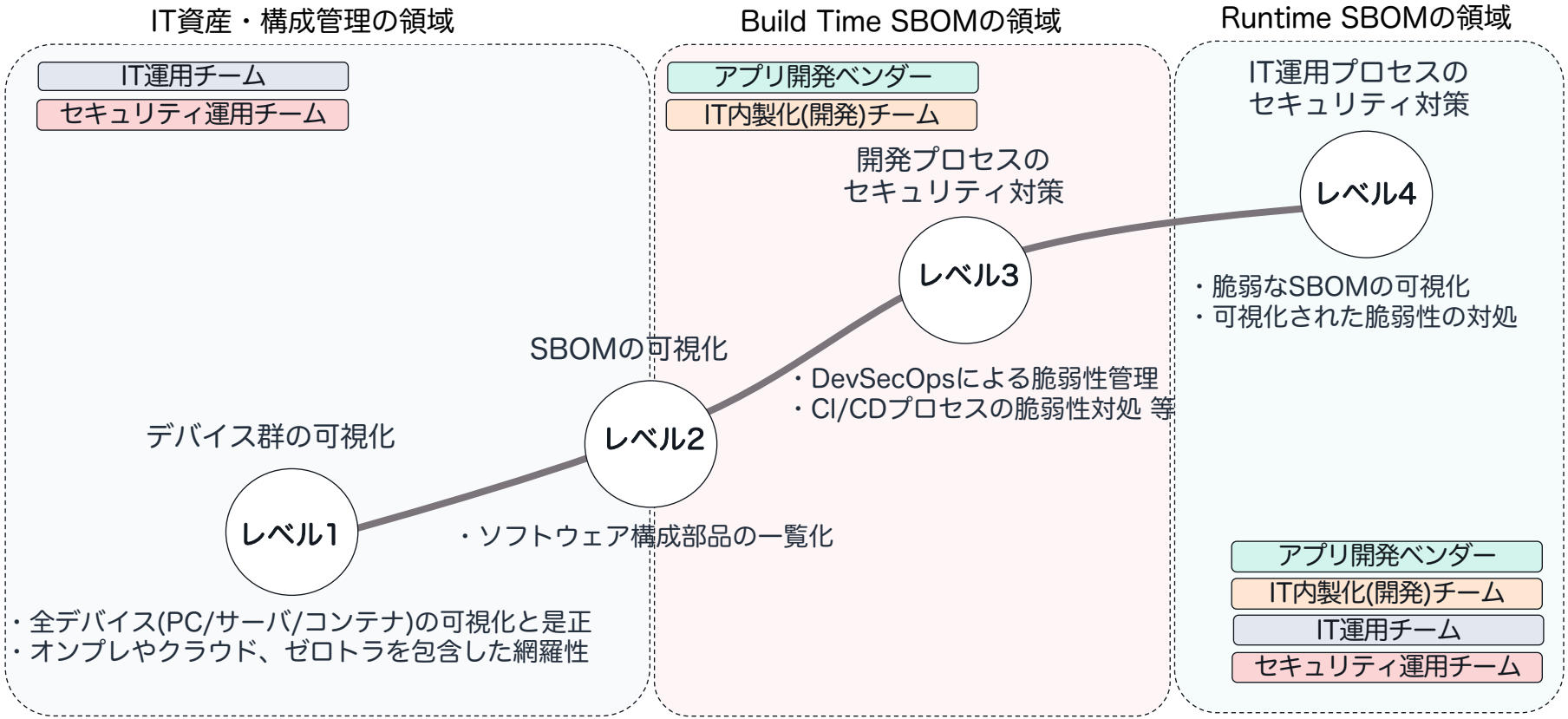
表示可能なバイナリの種類は以下の通り。

- Java (JAR, PAR, SAR, WAR, EAR, JHI, JPI, LPKG)
- JavaScript (NODE, NPM)
- Python
- PHP (Composer)
- Ruby (GEM)
- GoLang
- OpenSSL 共有ライブラリ



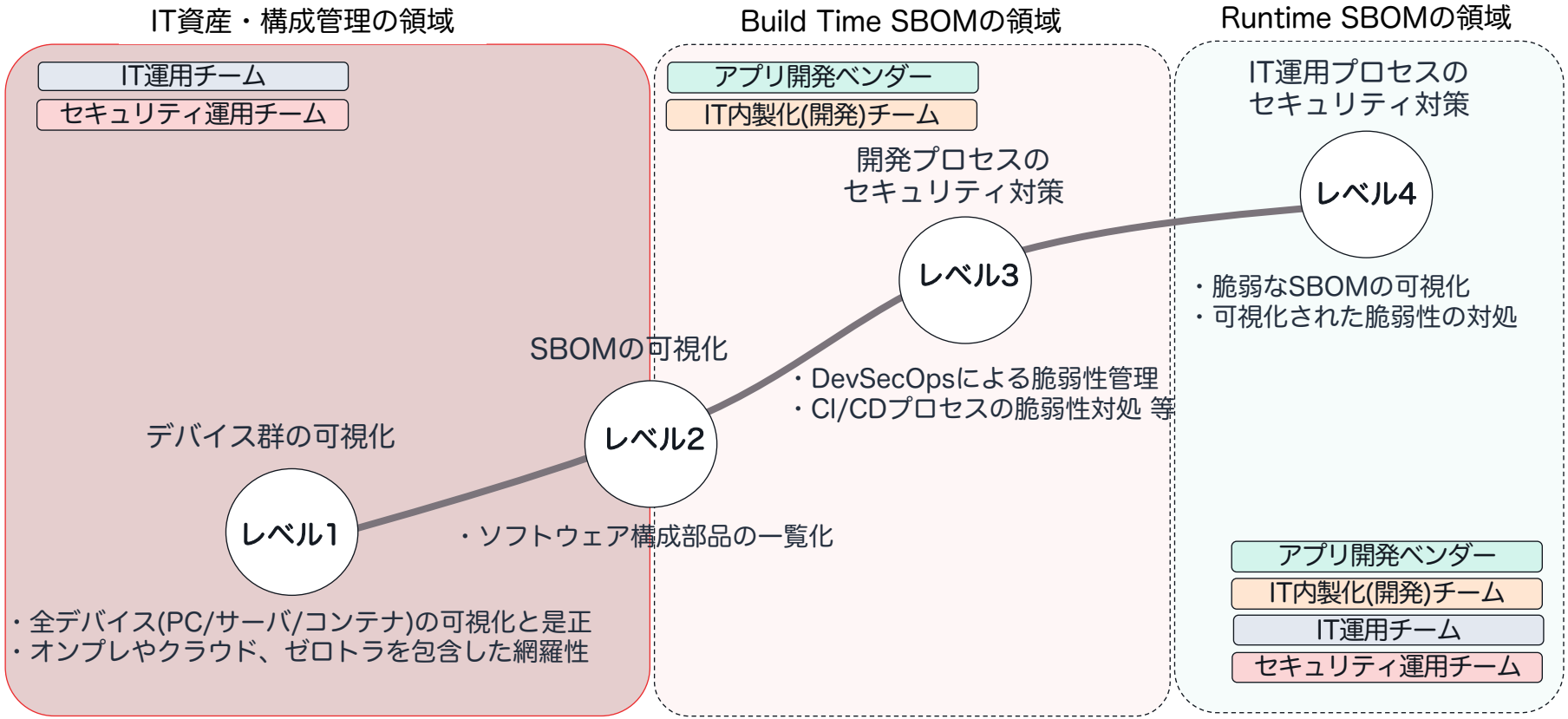
© 2023 Tanium. All rights reserved.

SBOM対応に向けたプレーヤー別の成熟度モデル



© 2023 Tanium. All rights reserved.

SBOM対応に向けたプレーヤー別の成熟度モデル



© 2023 Tanium. All rights reserved.

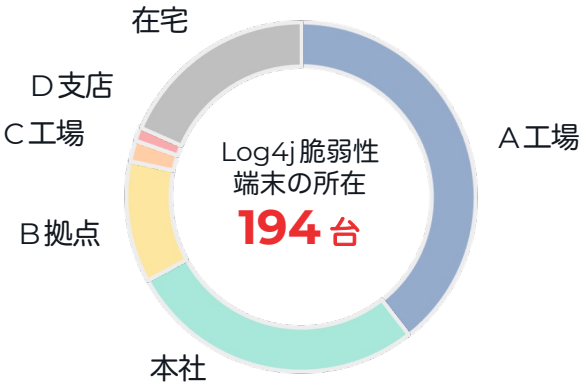
過去事例から読み解くSBOM管理

国内企業におけるLog4j脆弱性調査結果から浮き彫りになったSBOM（ソフトウェア部品表）管理の難しさ

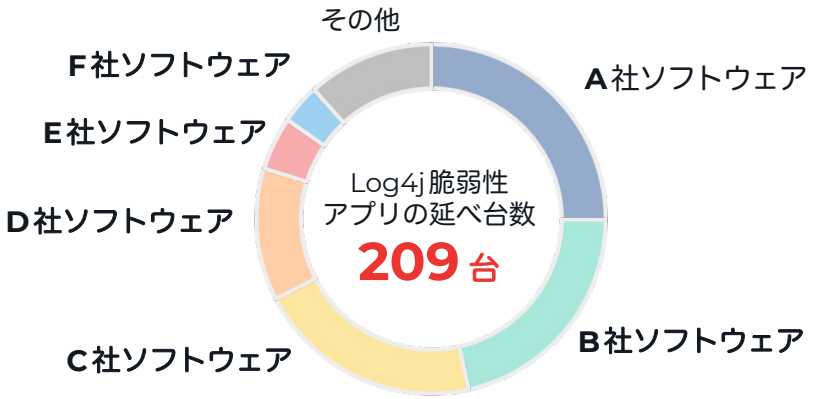
調査端末
3,534 台

Log4j 脆弱性の懸念がある端末数
194 台（5.5%）

Log4j 脆弱性の懸念があるアプリ
25 種類（14 ベンダー）



調査対象とした全ての拠点で Log4j の脆弱性を確認



ベンダーから得られた情報に基づく対処を実施したあとの調査にも関わらず、複数のソフトウェアで脆弱性を確認

Source: 当社調べ

© 2023 Tanium. All rights reserved.

タニウムは

サイバーハイジーン

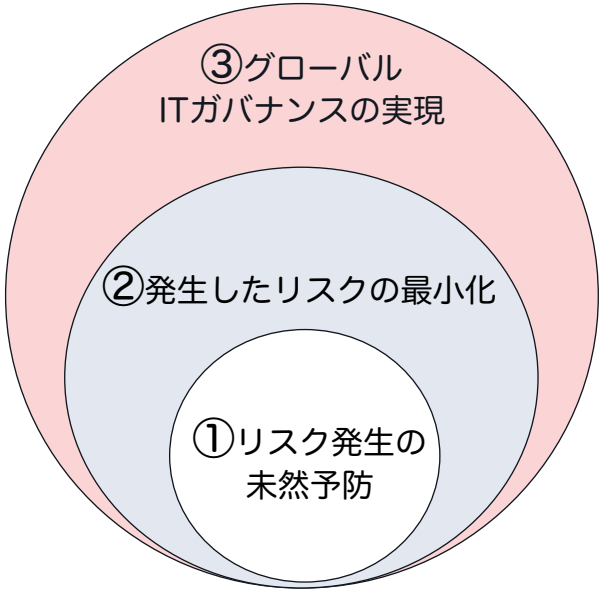
を推奨します

TANIUM

中長期セキュリティ戦略策定に向けた考察

NISTサイバーセキュリティフレームに基づく施策(グローバル・ベストプラクティスの活用)

更なるセキュリティ強化の目的



今後、日本政府より公開予定の各種セキュリティ施策にも適宜順応

中長期セキュリティ強化施策の骨子

③サプライチェーンリスク管理

・セキュリティ評価基準(KPI)
・SBOM対応の実現(今後、重要度高)

②サイバー・レジリエンス施策

・導入した更なるEDRの有効活用
・リスク影響度分析/対処の迅速化

①サイバー・ハイジーン施策

・動的なIT資産管理の実現
・動的な脆弱性管理の高度化

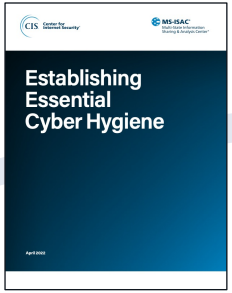
© 2023 Tanium. All rights reserved.

グローバルで加速化するサイバー・ハイジーンの最新動向

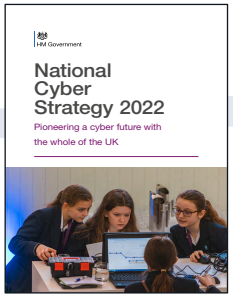
明示的にサイバー・ハイジーンを言及する 法令/戦略/ガイドライン/フレームワーク等

CISA：Cyber Hygiene Service

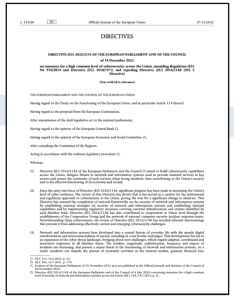
CIS：Essential Cyber Hygiene



NCSC：National Cyber Strategy

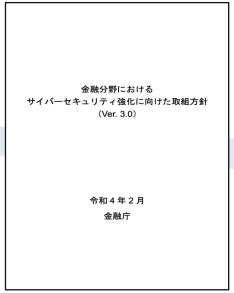


EU：NIS 2 Directive (2023年1月施行)

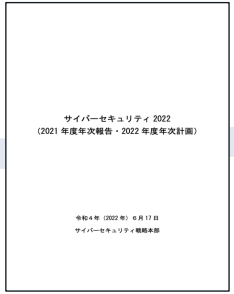


グローバルにおいては、
ITに先進的な諸外国が一斉に指示

金融庁



サイバーセキュリティ戦略本部



Singapore: Cyber Security Strategy

WORLD ECONOMIC FORUM Global Cybersecurity Outlook 2022

日本においては、金融庁や
サイバーセキュリティ戦略本部が指示

© 2023 Tanium. All rights reserved.

次回も面白い調査を企画中です。
乞うご期待ください。

TANIUM