国内におけるサプライチェーンセキュリティ実態調査結果について

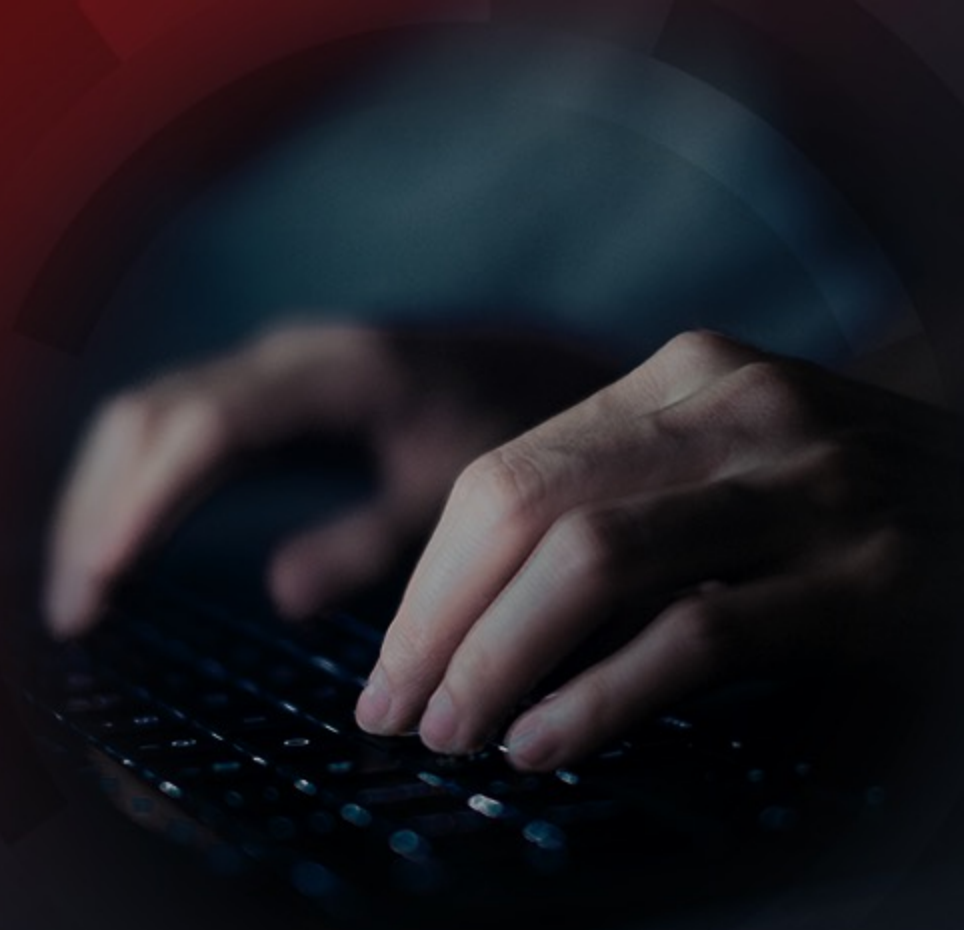
2022年8月24日

タニウム合同会社

TANIUM

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：Orion Hindawi (Co-Founder/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：2014年
代表：古市 力 (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

国内における採用実績（抜粋）

- 伊藤忠テクノソリューションズ株式会社
- 株式会社 荏原製作所
- 株式会社エヌ・ティ・ティ・データ
- 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
- 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
- 日本製鉄株式会社
- 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

（五十音順）

2023 年度 3 つの注力戦略領域

Realize Hyper-Growth

1. Tanium Cloud 1st の徹底的な推進

2. お客様の DX 施策を強力に保護する XEM の提供

3. パートナー協業強化による顧客基盤の拡大

サプライチェーンをとりまくセキュリティ課題

3位
2022年度版のランキング

4年連続
2019年度版～

Source :
独立行政法人 情報処理推進機構 セキュリティセンター : 情報セキュリティ10大脅威(2019-2022)

飛躍的に増加するサプライヤーへの攻撃

攻撃者のターゲットはより脆弱なシステム環境へ

66%

12,000件
昨対比650%

Source : European Union Agency for Cybersecurity, 2021/7/29付 プレスリリース
https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

Source: IPA 情報セキュリティ10大脅威2022
組織編、簡易説明資料

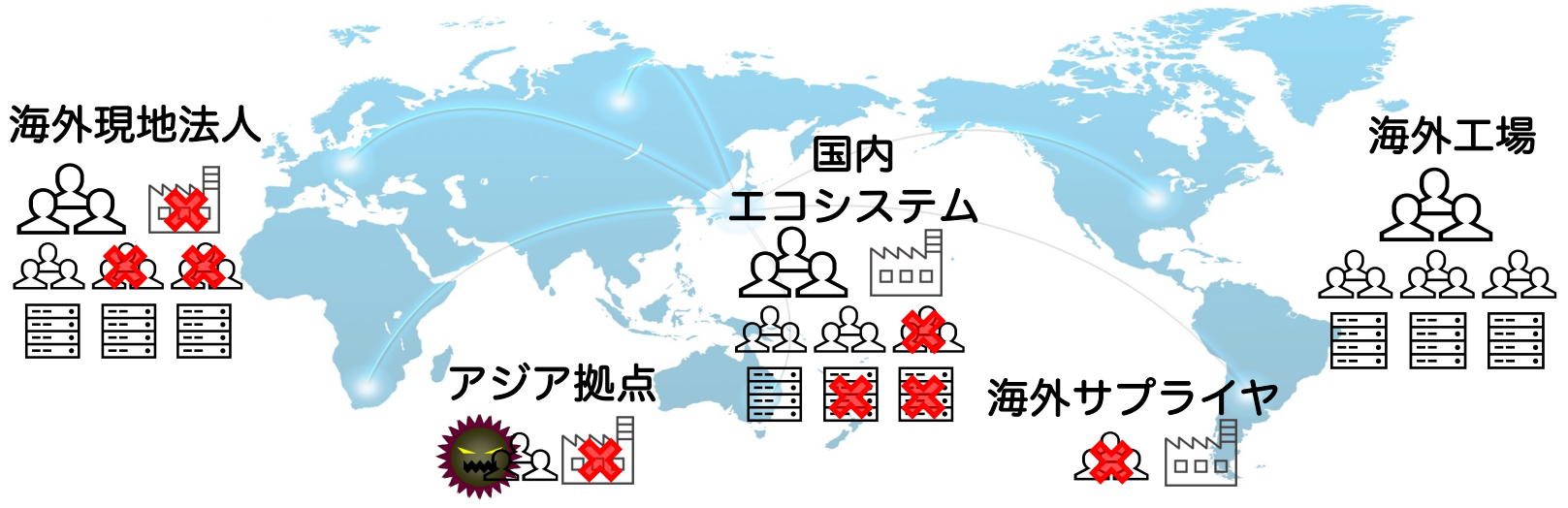
サプライチェーン・リスク等の新たな脅威を
先取りした対応を推進し、組織の壁を越えた
サプライチェーン全体でセキュリティを
向上するための方策を講じていく

Source :
内閣サイバーセキュリティセンター： 重要インフラのサイバーセキュリティに係る行動計画(2022/06/17版)より抜粋
https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf

TANIUM

なぜサプライチェーンが狙われるのか？

脆弱性対策の「穴」がねらわれる現実＝攻撃者は攻撃しやすい箇所から侵入してくる



①弱いところから初期侵入を許す
②重要拠点への展開
③情報漏洩、工場停止など重大事案化

経営責務としての
（グローバル）ガバナンス

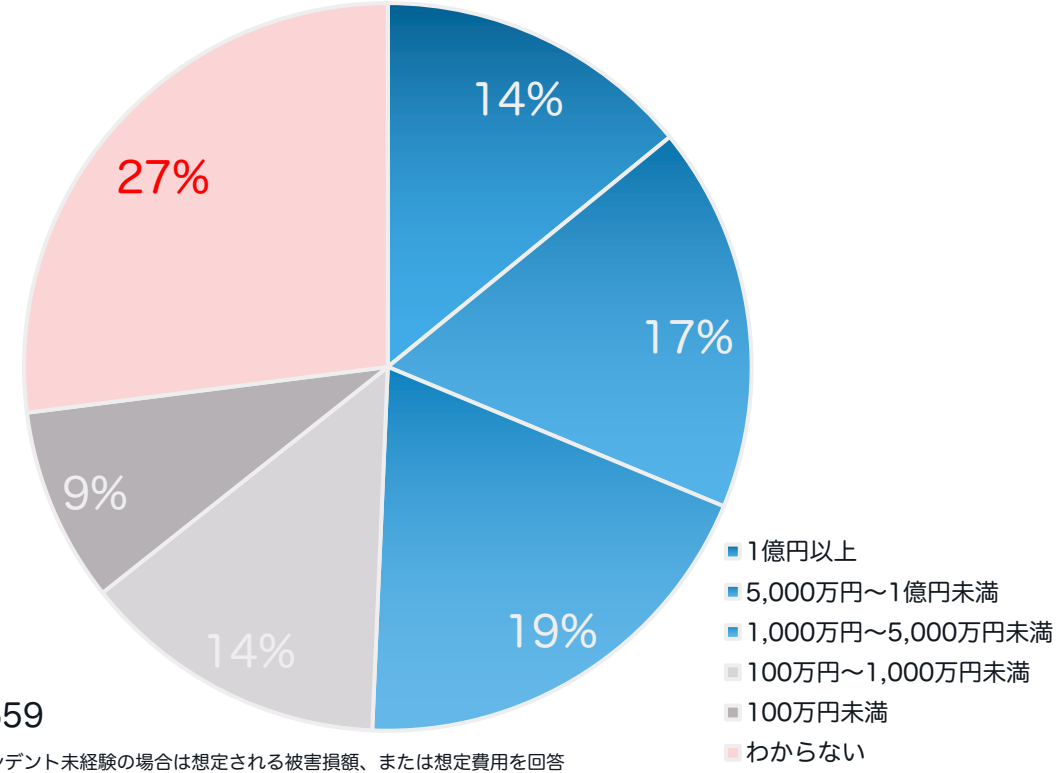
サプライチェーンリスクに関する市場調査

- 調査対象：大企業のサイバーセキュリティ意思決定者659名
- 調査方法：Webアンケート
- 実施期間：2022年6月1日～2022年6月20日

TANIUM

セキュリティ インシデント発生時の被害総額

被害総額は100万円未満から１億円以上まで幅広く分散。３割の組織は「わからない」



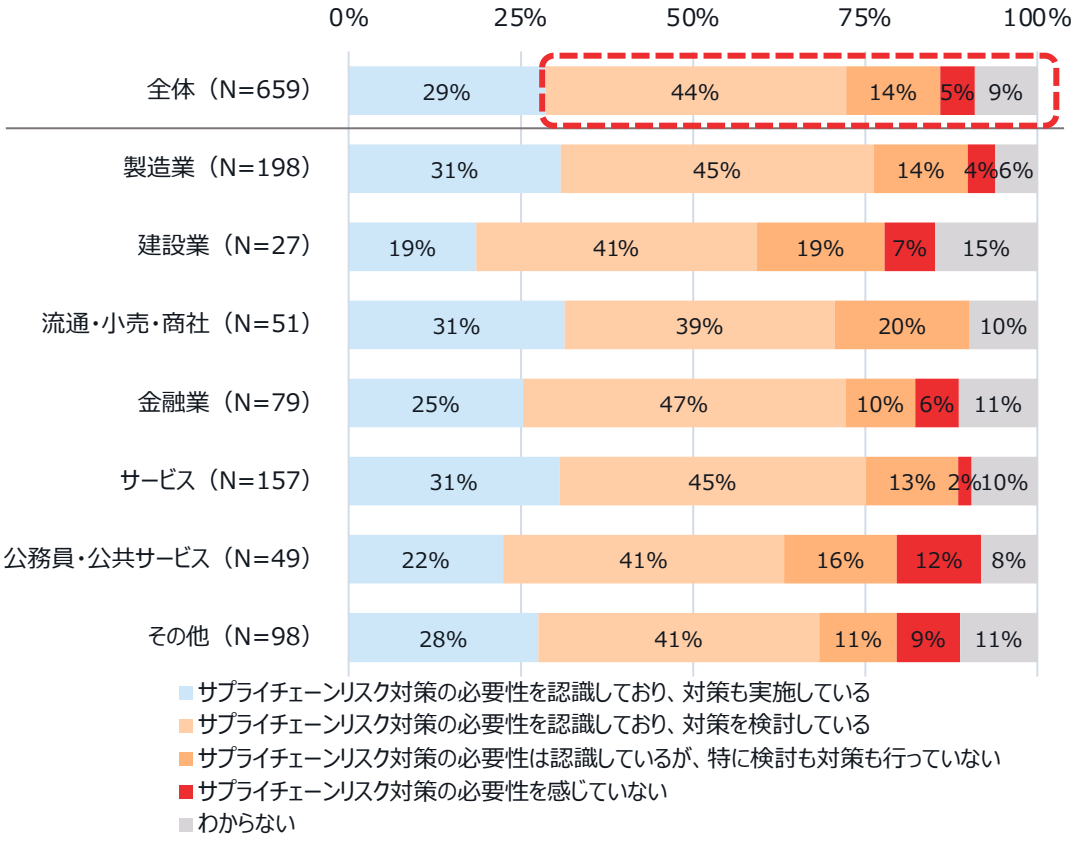
N=659

＊インシデント未経験の場合は想定される被害損額、または想定費用を回答

タニウム考察

- 約半数の組織が1,000万円以上を被害総額として経験・想定している
- 1億円以上の被害総額を回答している企業が14%にのぼり、昨今のランサムウェア被害等による金銭的な負担は組織にとって大きな重石になっている
- ３割の組織は被害を想定できていない

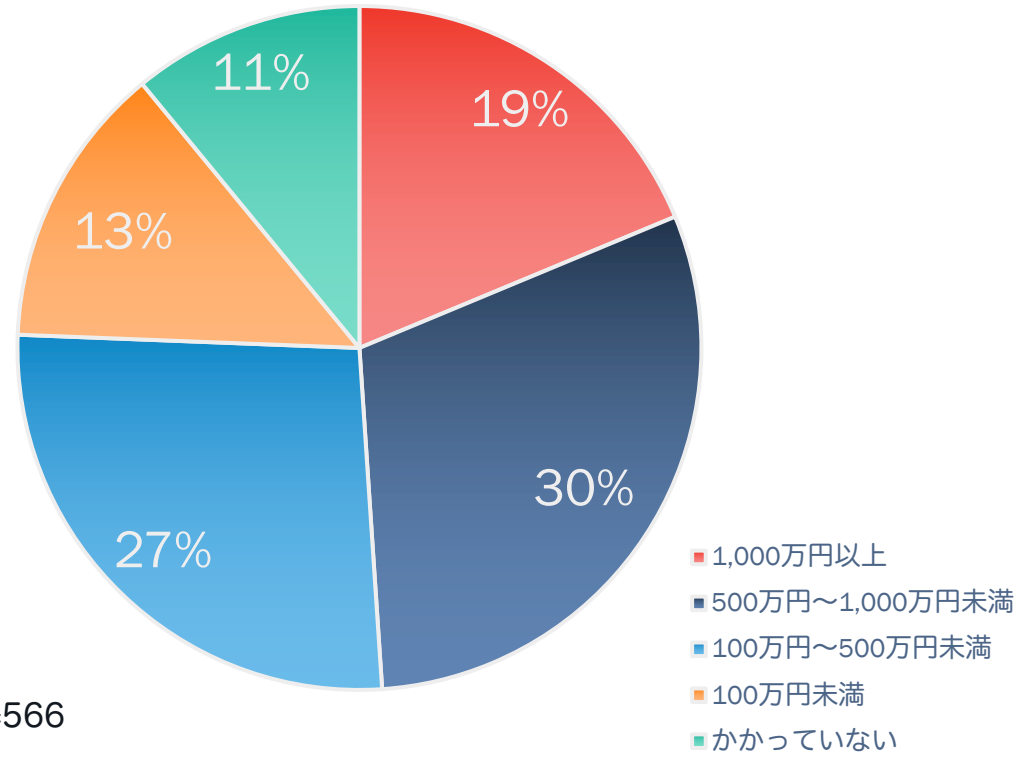
サプライチェーンリスクは７割強の環境で放置されている



タニウム考察

- サプライチェーンリスク対策の必要性は業種を問わず認知されており、全体では9割弱の組織が認知している
- 一方で、「わからない」と回答した組織も含めると７割以上の回答者はサプライチェーンに対して具体的な対策まで行えておらず、実質リスクが放置されている

サプライチェーンリスク対策にかかるコスト



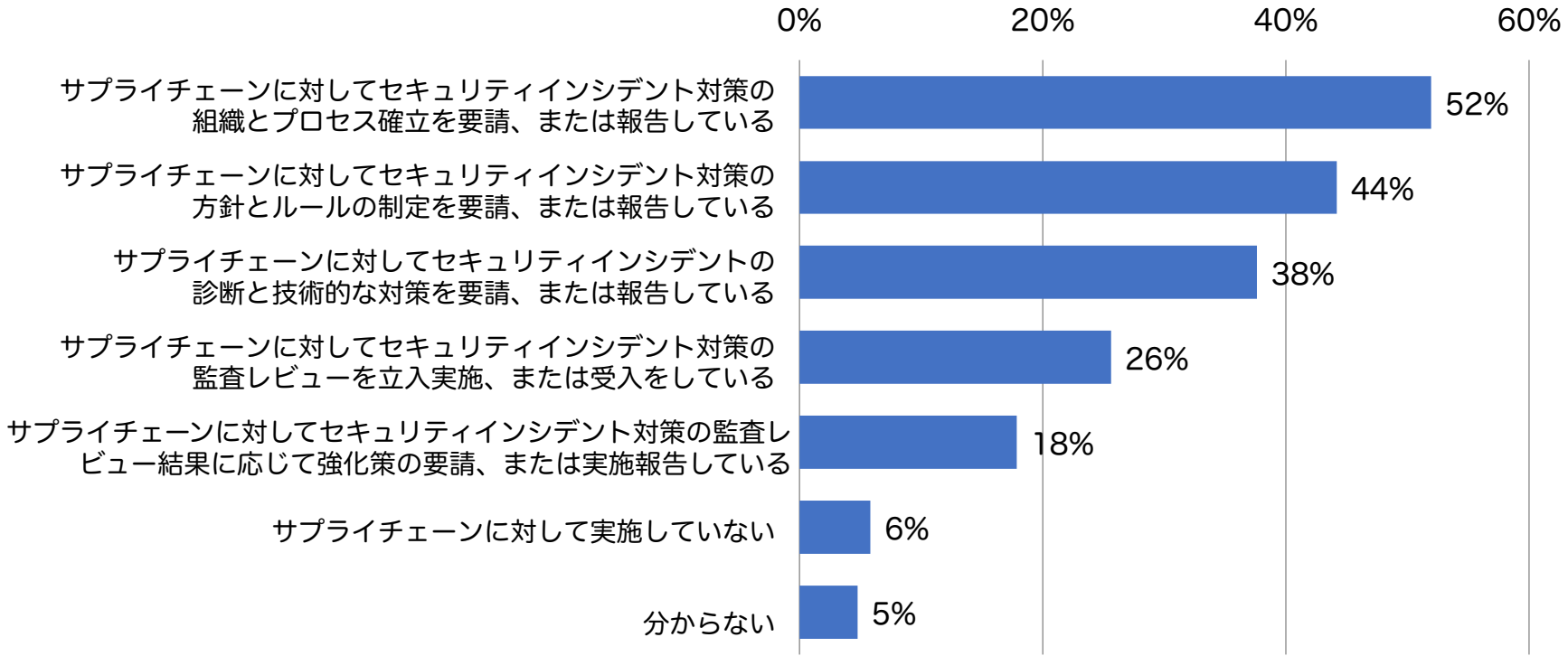
N=566

タニウム考察

- 調査対象組織に対してセキュリティチェック等にかかる1社あたりの年間の管理コストを訪ねたところ、500万円以上と回答した割合が約半数にのぼった
- 被害総額の回答と照らし合わせると、サプライチェーンセキュリティ対策にかかるコストは少ないとは言えず、組織が対策を明確化できない一つの要因となっていることが推察される

取引先に対して実施していること

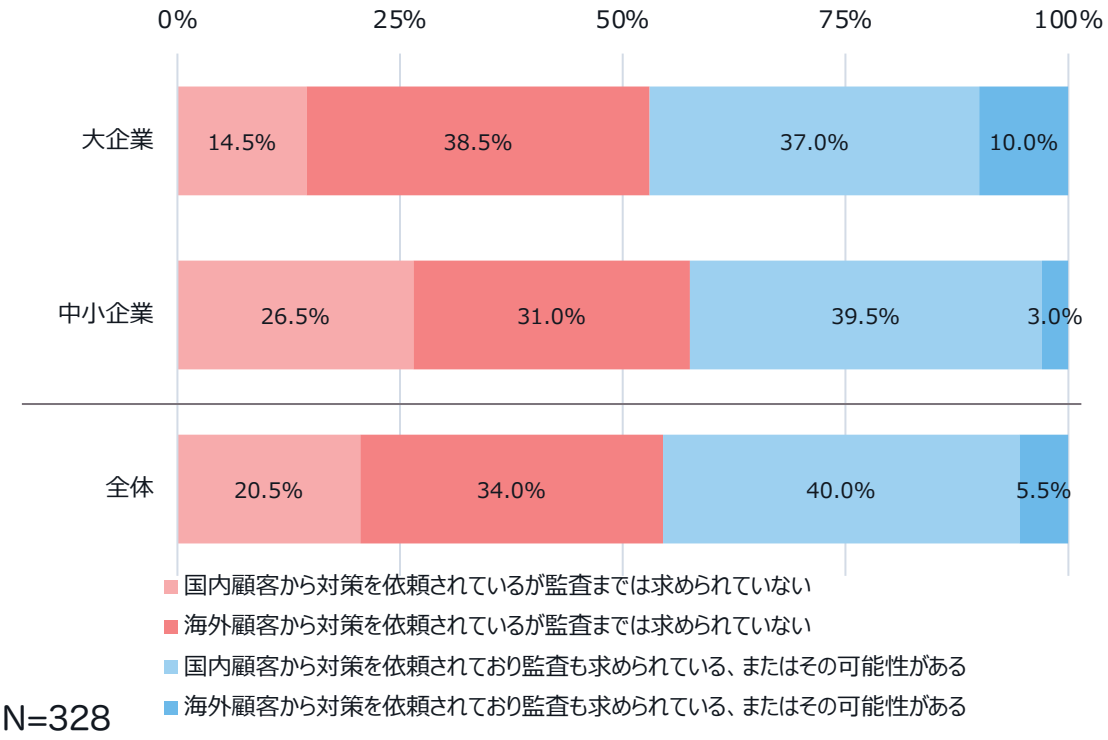
一応の要請を行っている組織が多いが、「要請や報告」をどのように行うかは課題が多い



N=566

サプライチェーンリスクにおける監査の重要性

過半数の組織は、サプライヤーにたいして「監査」を求めていない



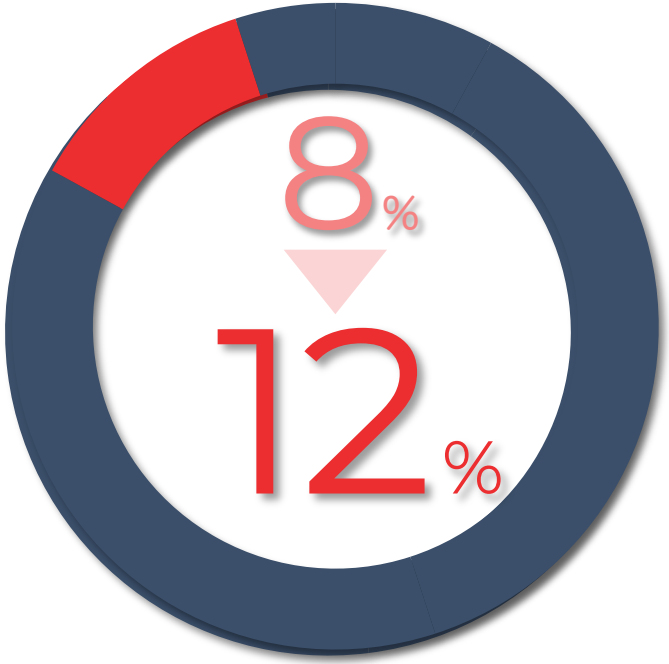
N=328

タニウム考察

- 調査回答者のサプライチェーンリスク対策における立場は＜依頼する＞＜依頼を受ける＞＜その両方＞が約３割ずつで、大企業、中小企業による差分は殆ど無かった
- 全体を通じて、納品先から監査を求められていると回答した組織は45%にとどまる
- 第三者監査のない対策への信頼度をどう担保するかはバイヤーにとっての大きな課題

ガバナンス対象にサプライチェーンを含めている組織は極小

サプライチェーンリスクが増大するなか、バイヤー側からのガバナンスは自社グループにとどまる



タニウム考察

- 今回の回答組織全体のうち、サプライチェーンをガバナンス対象に含めている割合は8%にとどまった
- 業種別では「流通・小売・商社」のみ当該割合が14%と２桁を超えたが、それ以外の業種はすべて10%未満
- 今後３年のうちにサプライヤーへのガバナンス強化を検討している割合もわずか4%と非常に少ない

調査結果を踏まえてタニウムからの提言

TANIUM

サプライチェーン攻撃に対し、今一度リスクの見直しが必要

被害の予防

- 業務委託や情報管理における規則の徹底
- 報告体制等の問題発生時の運用規則整備
- 信頼できる委託先、取引先組織の選定
- 複数の取引先候補の検討 -納品物の検証
- 契約内容の確認
- 委託先組織の管理
- 取引先や委託先の情報セキュリティ対応の確認、監査
- 情報セキュリティの認証取得
  (ISMS, Pマーク、SOC2, ISMAPなど)

被害を受けた後の対応

- 影響調査および原因の追究、対策の強化
- 被害への補償
- 関係各所への報告、相談体制の確立
  (上司、CSIRT, 関係組織、公的機関など)

タニウムが推奨する
サプライチェーンリスク対策は
サイバーハイジーン

TANIUM

サイバーハイジーンの考え方

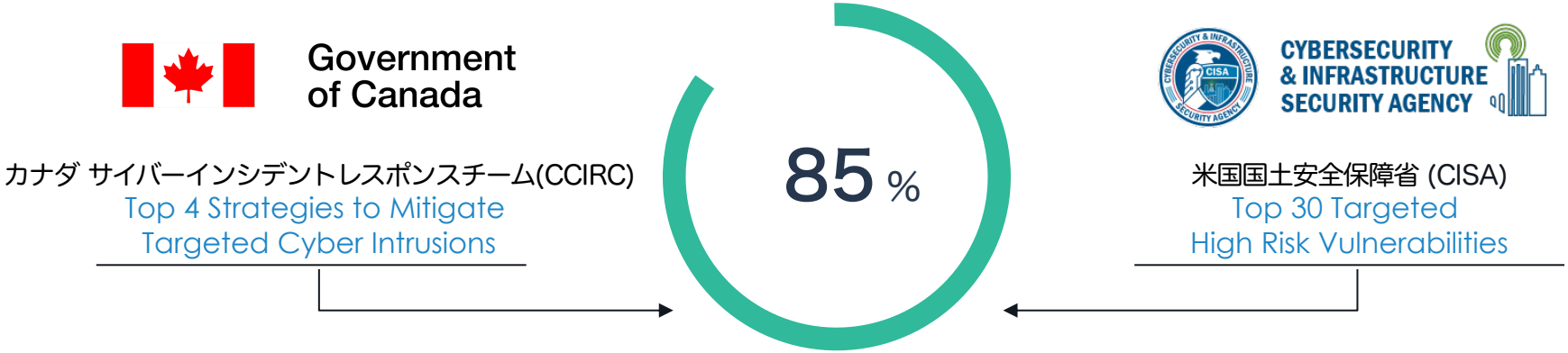
サイバー・レジリエンス

- セキュリティ侵害の迅速な検出
- インシデント発生時の侵入経路と影響範囲の特定、把握
- セキュリティ侵害の影響軽減
- 影響範囲全体の早急な復旧

サイバーハイジーン

- 保有端末資産の把握と状態の定期的な監視
- 該当する脆弱性の把握
- 未適用パッチの可視化
- 不許可資産の排除
- パッチの適用
- ソフトウェアの更新

サイバーハイジーンによるリスク低減効果

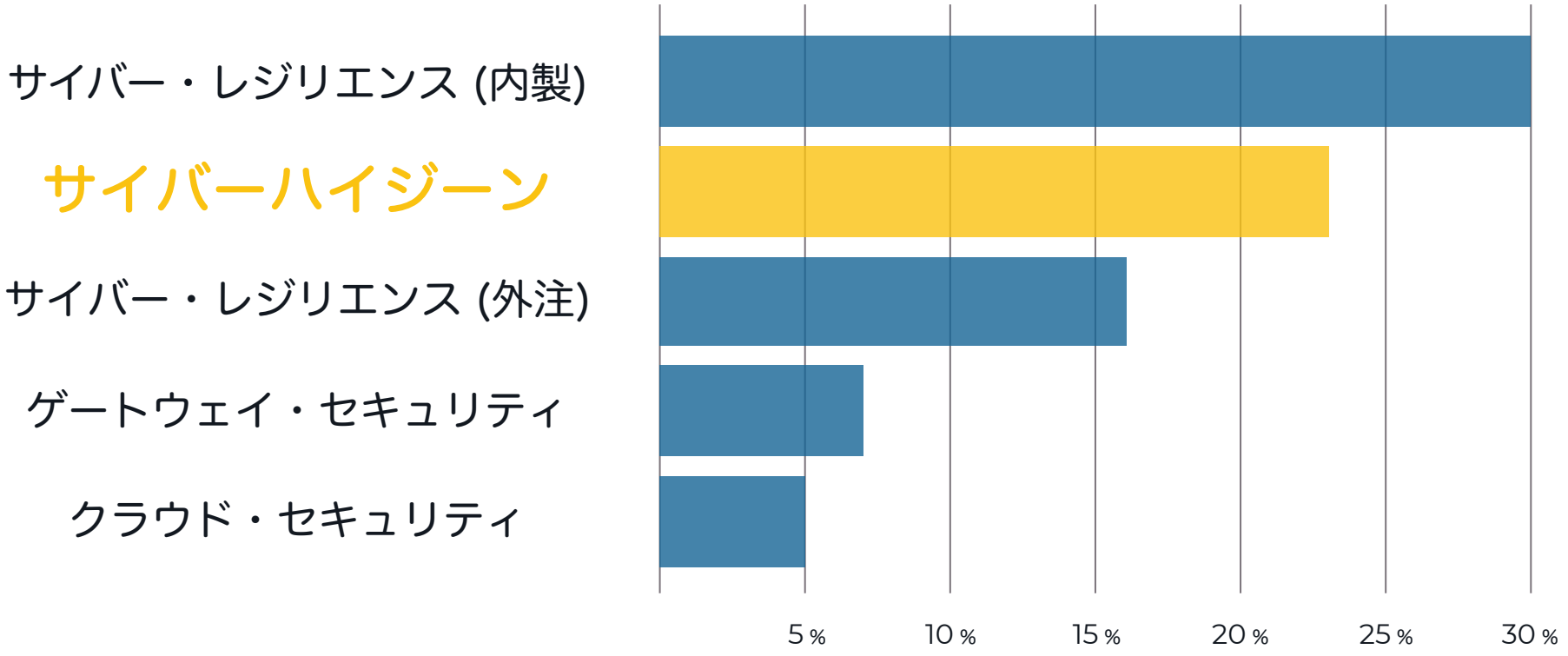


何かが起きてからでは遅い
平時の対策こそが先進諸国の公的機関から推奨されている

Source :
CCIRC: Top 4 Strategies to Mitigate Targeted Cyber Intrusions より抜粋
https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tp-strtgs-en.aspx

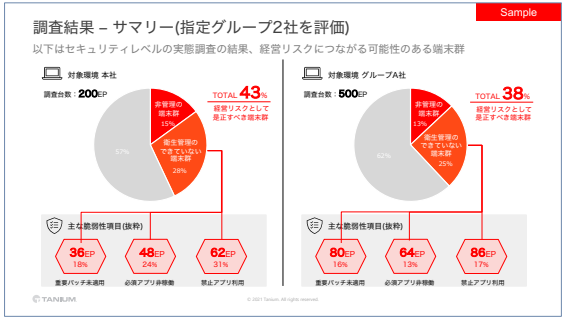
CISA: Top 30 Targeted High Risk Vulnerabilities より抜粋
https://www.cisa.gov/uscert/ncas/alerts/TA15-119A

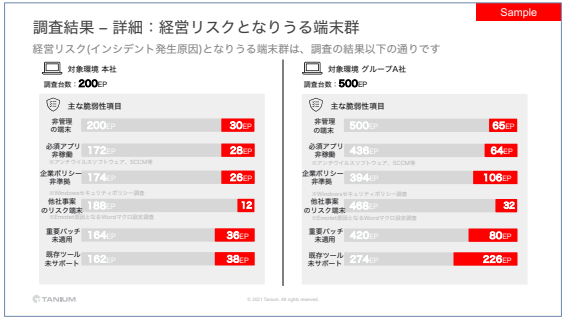
国内でも優先投資領域として存在感を増すサイバーハイジーン

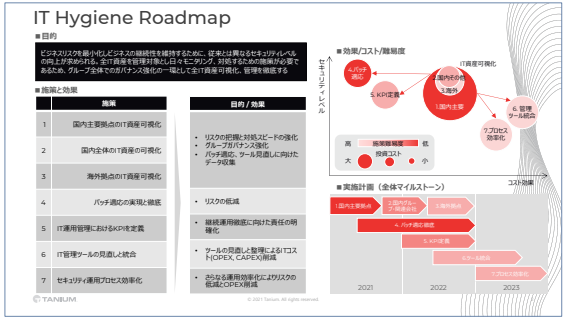


Source: 本調査
従業員10,000名以上の企業 N=253

ハイジーン・アセスメントのすすめ







衛生状態の可視化 → 課題の整理 → 優先順位と方向性検討 → 実施計画の策定支援

60+社

アセスメントを体験されたお客様

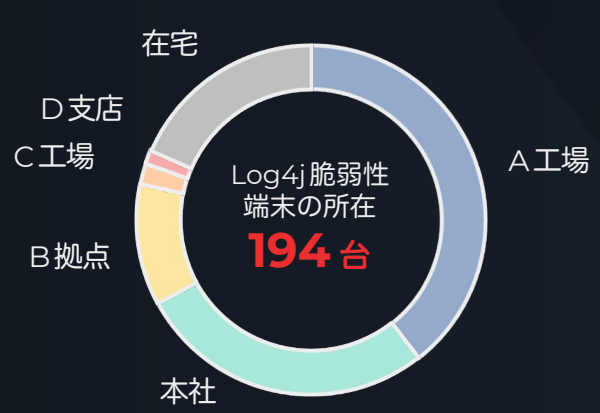
ソフトウェア・サプライチェーンセキュリティも課題

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

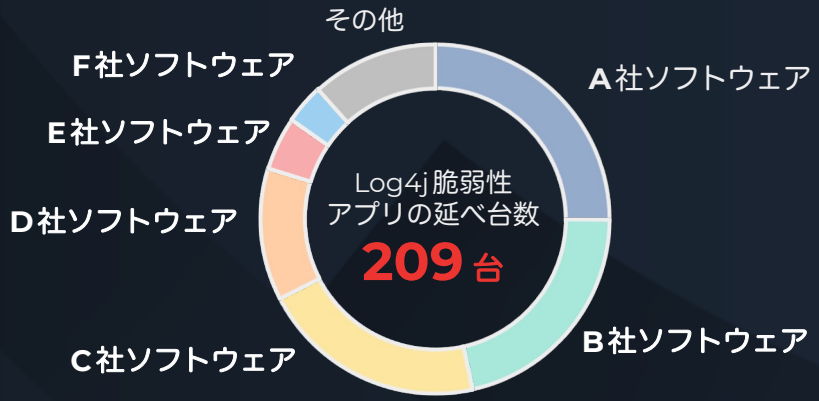
調査端末
3,534 台

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

TANIUM

ご静聴ありがとうございました

お問い合わせ先：
マーケティング本部 jpmarketing@tanium.com

TANIUM