国内におけるサイバーハイジーン実態調査結果について

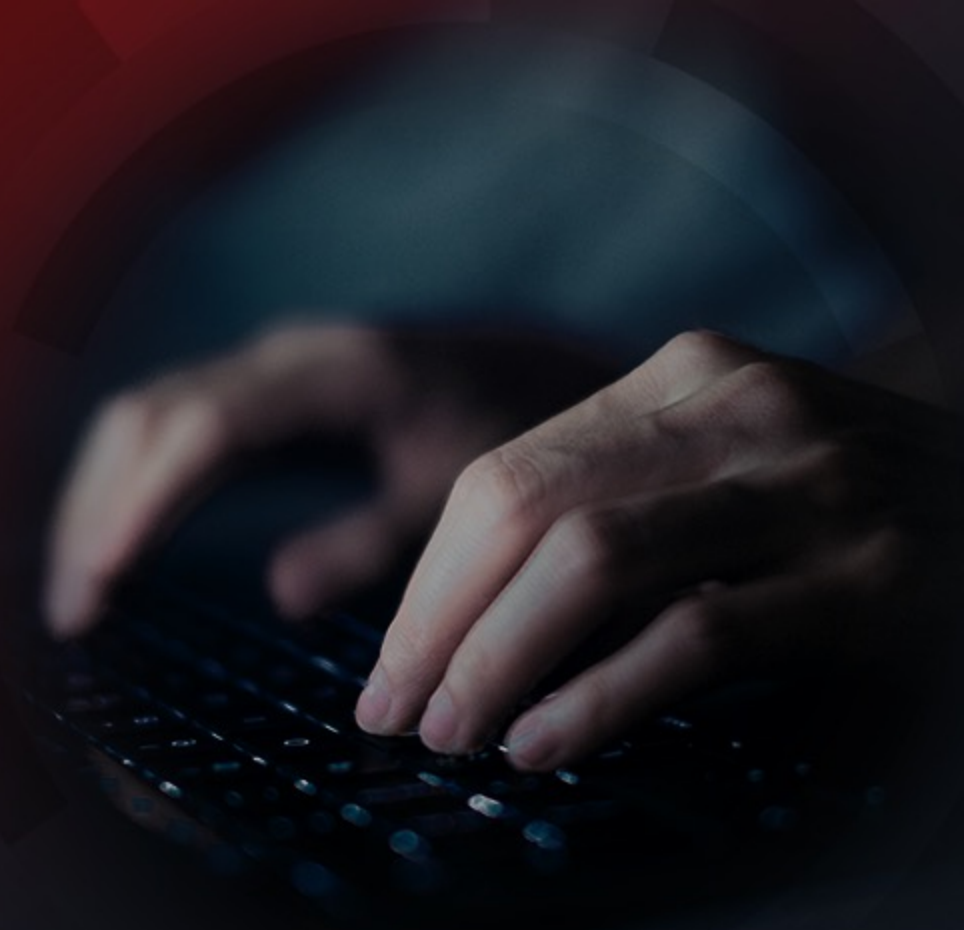
2023年3月3日

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：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：2014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

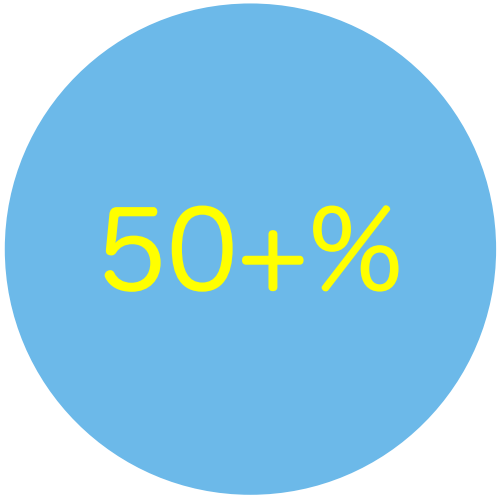
5
米国軍組織における採用数

3,000万
グローバルで管理しているエンドポイント数

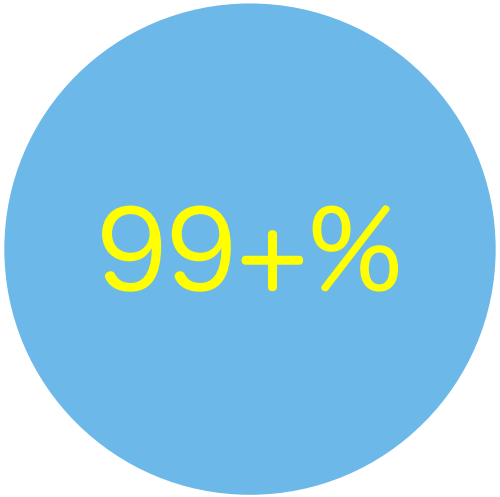
国内のお客さま（公開可能企業のみ。五十音順）

- 伊藤忠テクノソリューションズ株式会社
- 株式会社 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
- 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

タニウム国内ビジネスアップデート（2022年2月～2023年1月）



国内売上成長率



更新率

＊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

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

サイバー攻撃プロセスとセキュリティ対策の優先度

サイバー攻撃プロセス

犯罪組織

非管理端末の存在 “20%以上”

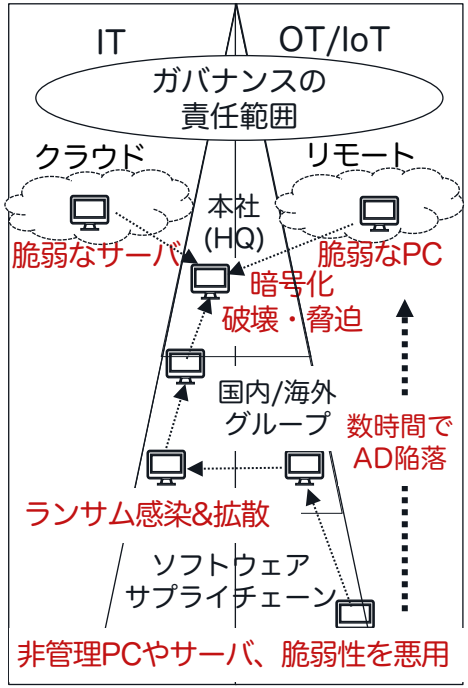
OS/アプリ脆弱性の存在 “40%以上”

不正アクセスやランサムの高速拡散

段階的に管理者権限まで昇格
”ADの陥落”

EPPやEDR機能の無力化やログ消去

サーバを暗号化し破壊・脅迫
”事業停止“や”情報漏洩“



攻撃プロセスを踏まえた対策の優先度

最優先施策

サイバー・ハイジーン
(プロアクティブ・ディフェンス)

サイバー・レジリエンス
(リアクティブ・ディフェンス)

共通要件

・ガバナンス責任範囲の“網羅性”を確保
・各IT運用業務の“リアルタイム性”を確保
動的なエンドポイント管理が必須要件に！

IPAが公開した情報セキュリティ10大脅威 2023※の考察

順位	組織
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	標的型攻撃による機密情報の窃取
4位	内部不正による情報漏えい
5位	テレワーク等の ニューノーマルな働き方を狙った攻撃
6位	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
7位	ビジネスメール詐欺による金銭被害
8位	脆弱性対策情報の公開に伴う悪用増加
9位	不注意による情報漏えい等の被害
10位	犯罪のビジネス化 （アンダーグラウンドサービス）

サイバー・ハイジーン

グループITガバナンス

動的なサイバー・ハイジーンと
グループITガバナンスの
重要性を裏付ける

※https://www.ipa.go.jp/security/vuln/10threats2023.html

サイバーハイジーンに関する市場調査

- 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：2022年12月19日～2022年12月31日

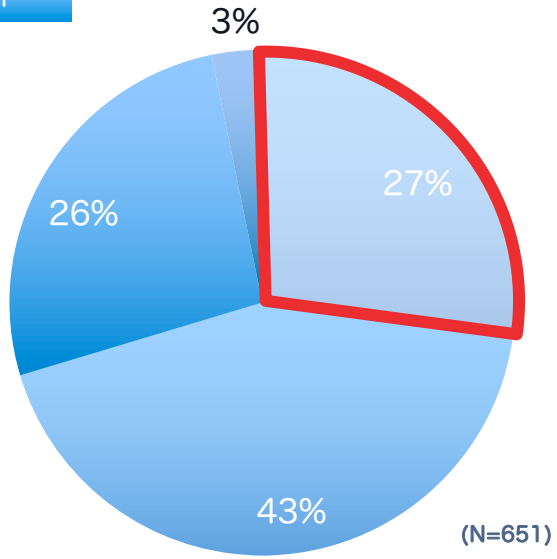
TANIUM

【調査#1】サイバーハイジーンの認知度

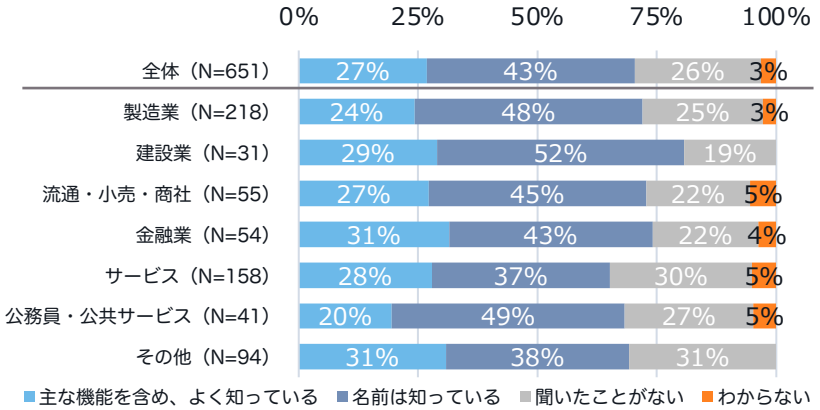
大企業での認知度が高い傾向が見られる。

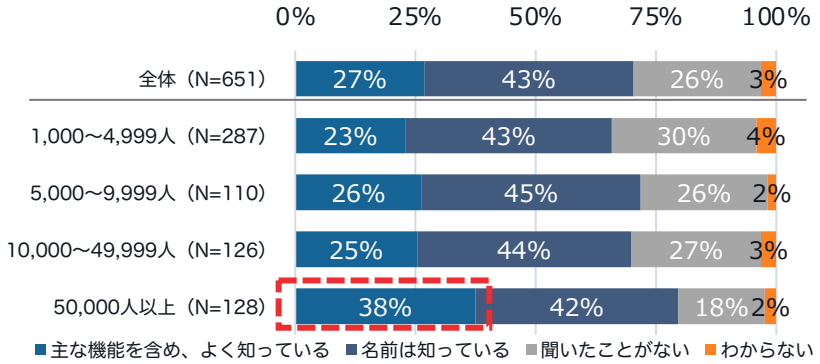
数値としては昨年とほぼ横ばい。

2022年



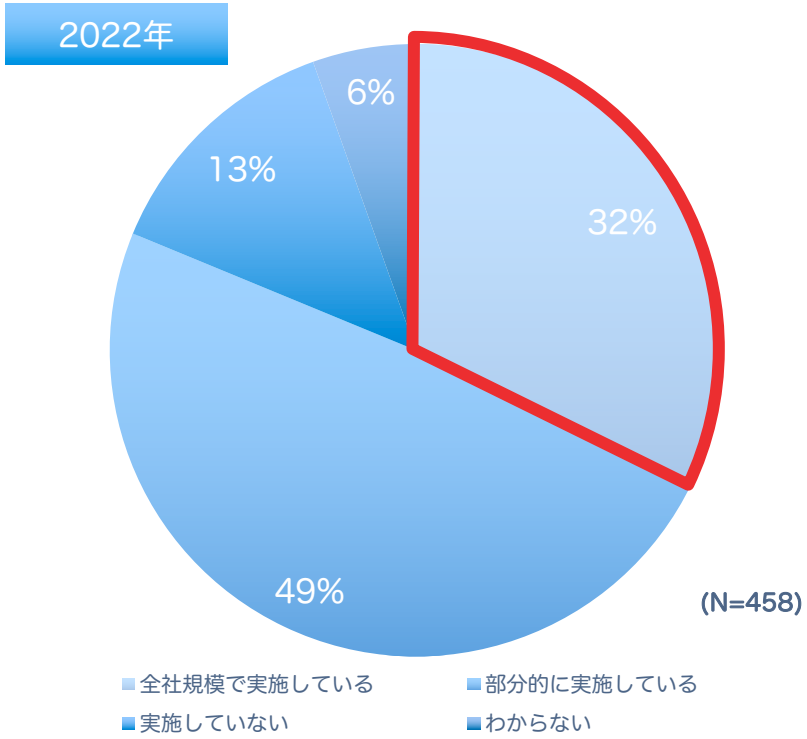
業種別/規模別

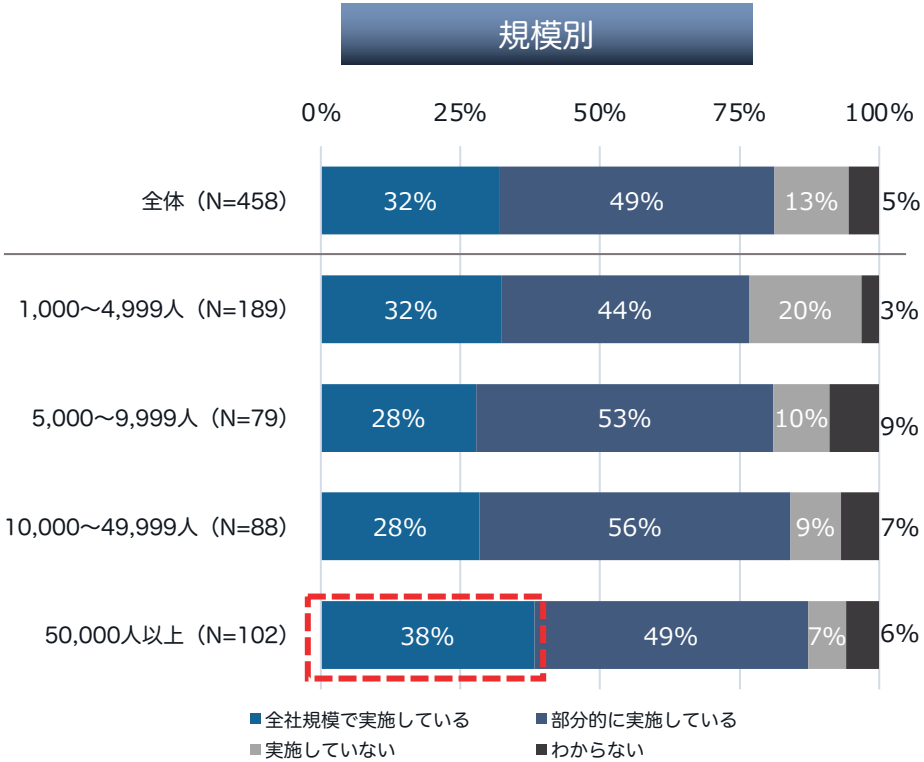




【調査#2】サイバーハイジーンの実施範囲

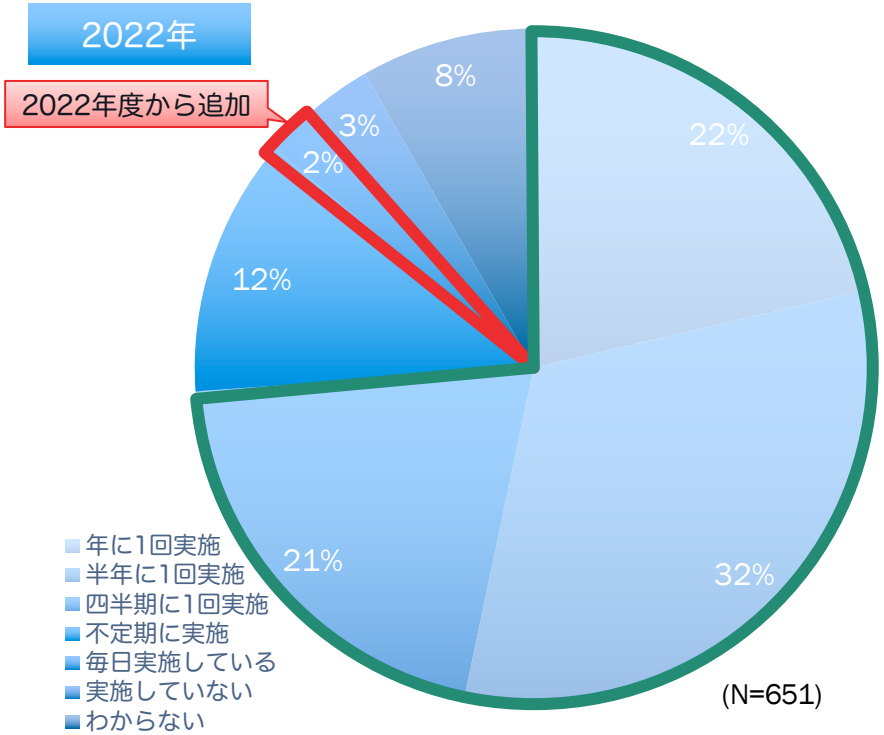
昨年と比較して、大きな変化は見られず。32%強の組織で全社対応。
規模の大きい組織ほど全社規模で実施している割合が高い。





【調査#3】IT資産の棚卸頻度

毎日実施している企業は全体のわずか 2.3% であり、サイバーハイジーンの徹底が浸透しているとは言えない。定期的な棚卸が実態となっているのも昨年から大きく変わらず。



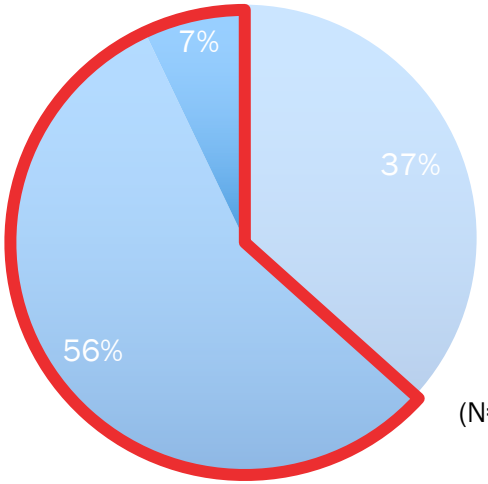
[考察]

- サイバーハイジーン実施においては、資産の状態を常に把握することが基本となる
- IT資産の棚卸とは別にサイバーハイジーンの一環で資産可視化をおこなっている組織は一定数存在する 可能性はある

【調査#4】非管理端末（野良端末）の把握

完全に把握できていると回答した組織は4割に満たず、６割を超える組織で非管理端末が存在。
業種別では公共と流通で非管理端末の比率が高い。

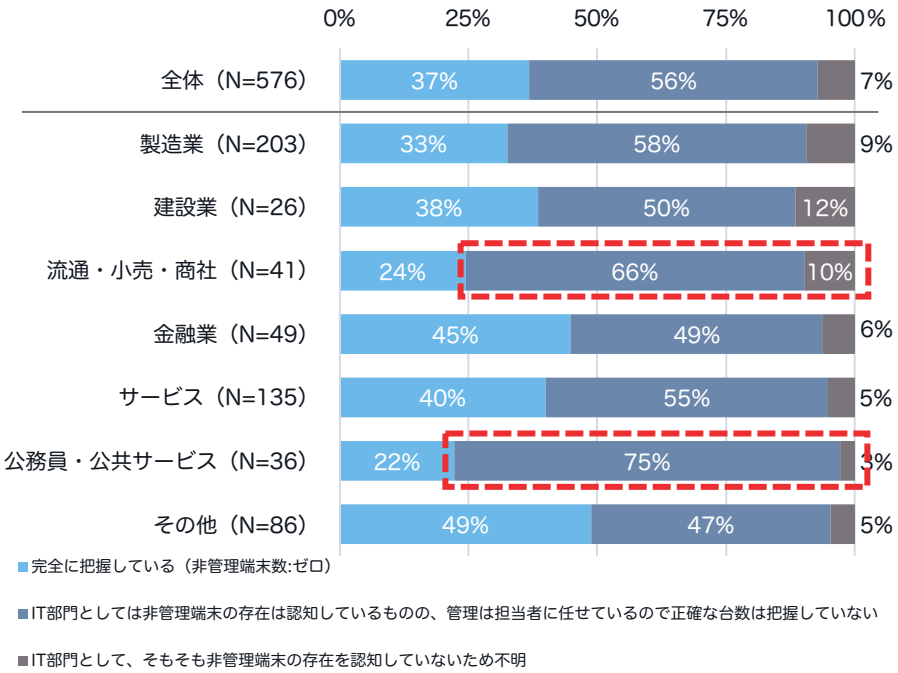
2022年



(N=576)

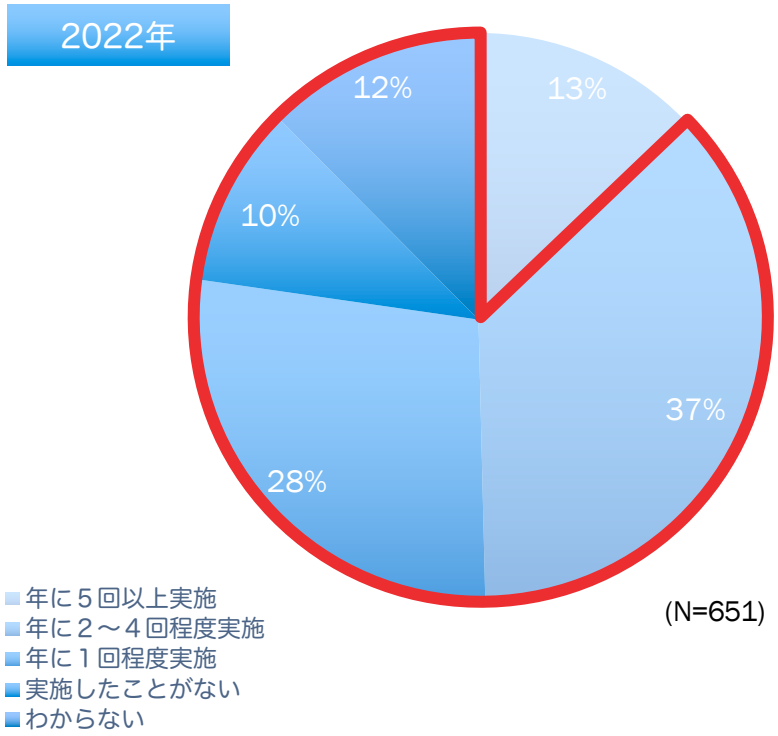
- 完全に把握している（非管理端末数：ゼロ）
- IT部門としては非管理端末の存在は認知しているものの、管理は担当者に任せているので正確な台数は把握していない
- IT部門として、そもそも非管理端末の存在を認知していないため不明

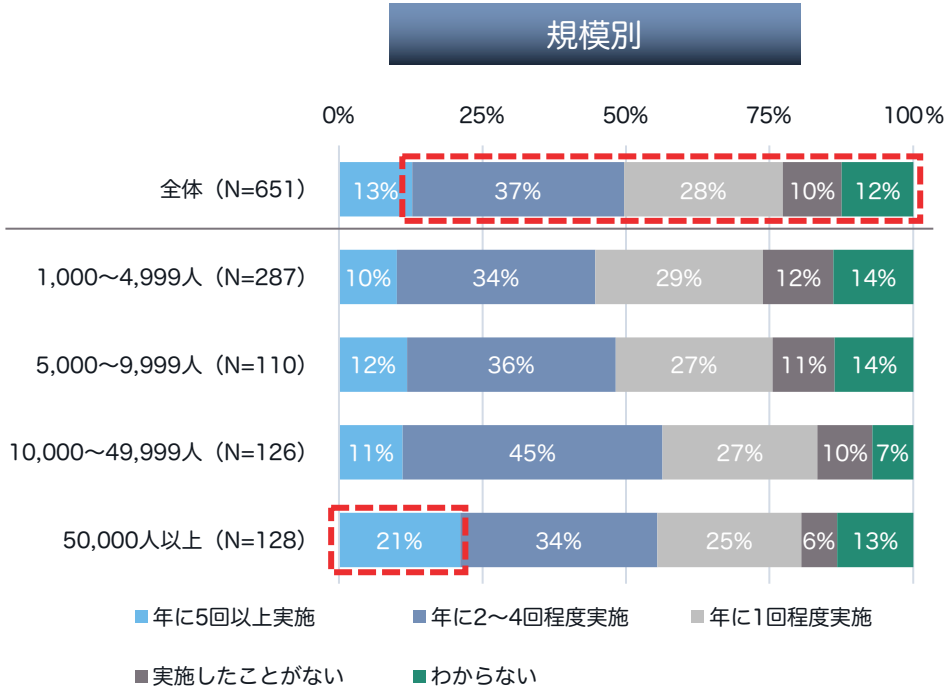
業種別



【調査#5】脆弱性対応の頻度

87％強の組織が四半期に一回以下の脆弱性対応実施にとどまる。規模別では大企業の実施頻度が高い傾向にある。

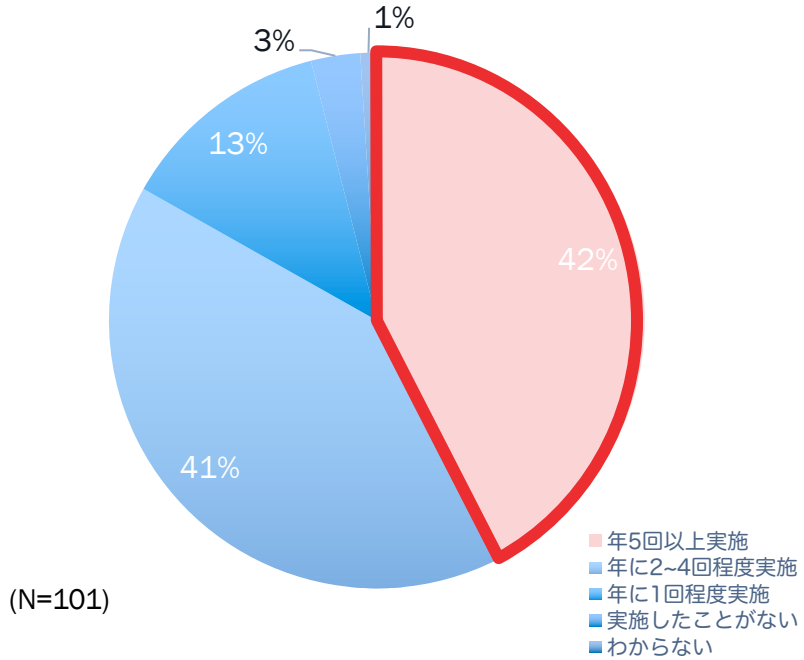




【絞り込み調査#1】脆弱性対応の頻度

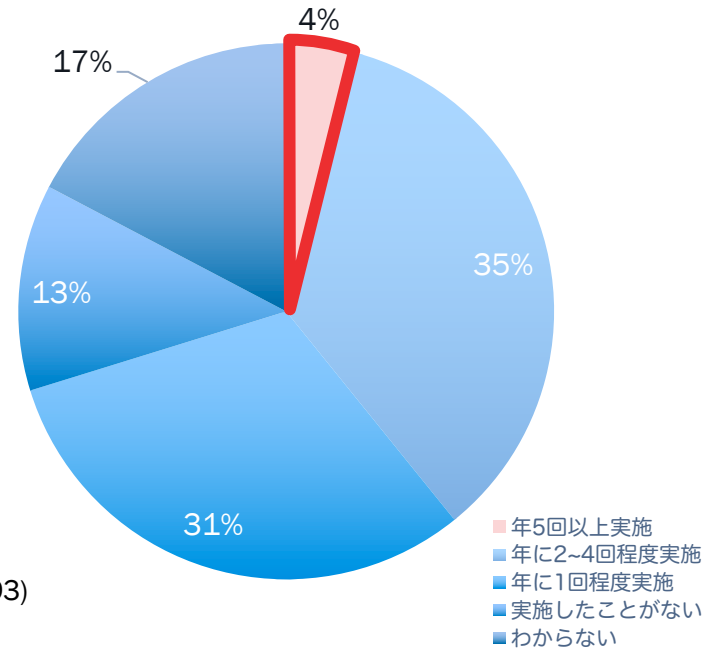
年5回以上実施できている組織の割合に顕著な差異。サイバーハイジーン徹底組織においては40%超。

サイバーハイジーン徹底



(N=101)

サイバーハイジーン
これから



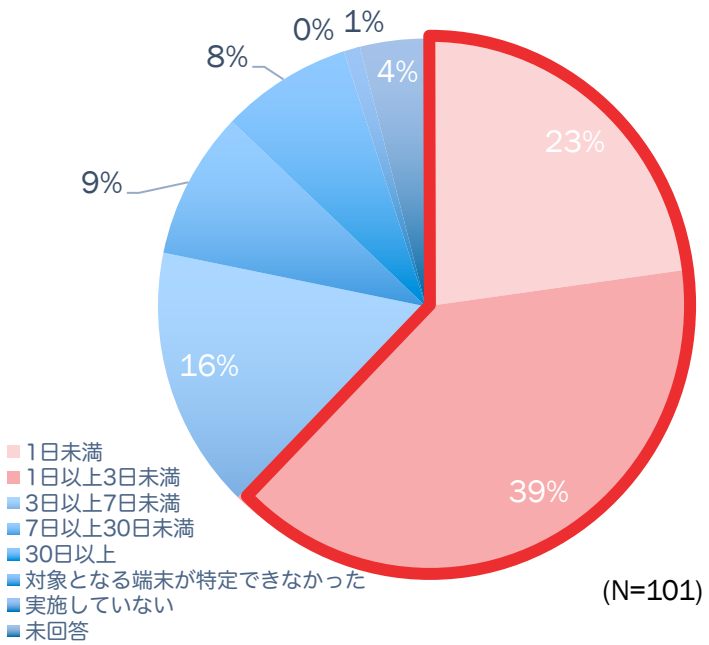
(N=393)

【絞り込み調査#2】脆弱性対処時間

(脆弱性発見後、必要な監査やアップデートなどの是正措置を対象全台に実施するのにかかった時間)

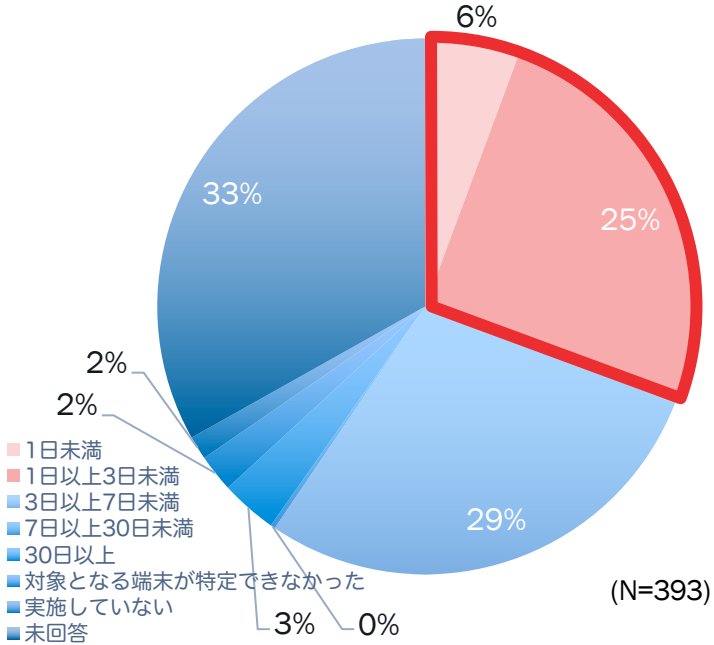
3日未満の結果に顕著な差異が見られる。サイバーハイジーン徹底組織は6割以上が3日未満で対処が完了。

サイバーハイジーン徹底



(N=101)

サイバーハイジーン これから



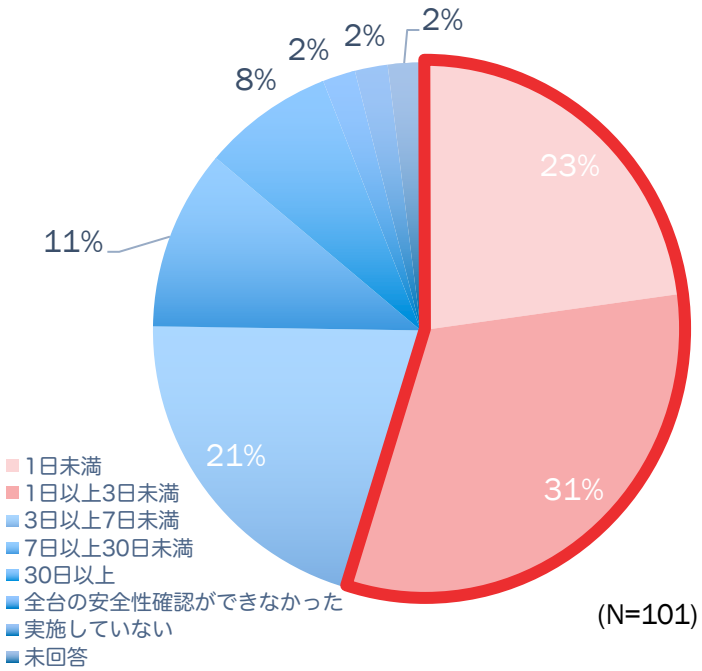
(N=393)

【絞り込み調査#3】安全性確認までにかかった時間

（インシデント発生後に端末全ての安全性確認にかかった時間）

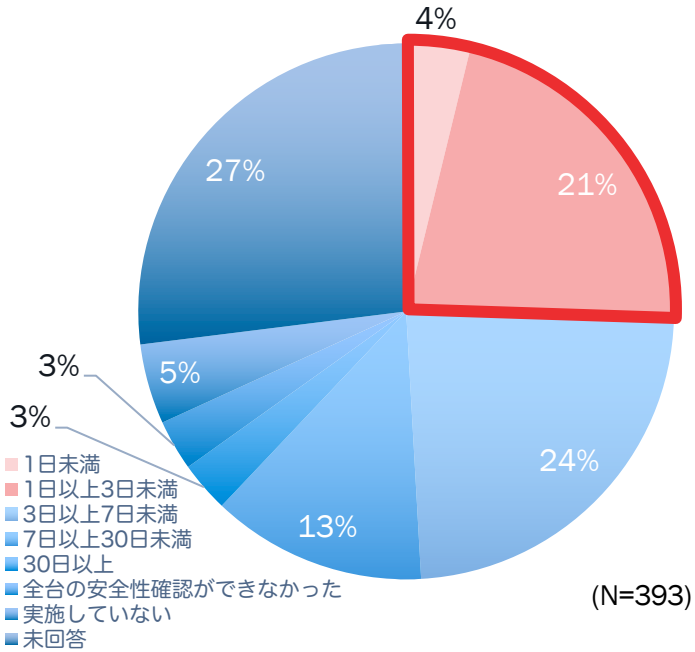
特に短期間での完了に顕著な差異。サイバーハイジーン徹底組織においては50%強が3日以内に安全性確認完了。

サイバーハイジーン徹底



(N=101)

サイバーハイジーン
これから



(N=393)

調査結果を踏まえてタニウムからの提言

2023年3月3日

タニウム合同会社

TANIUM

タニウムは

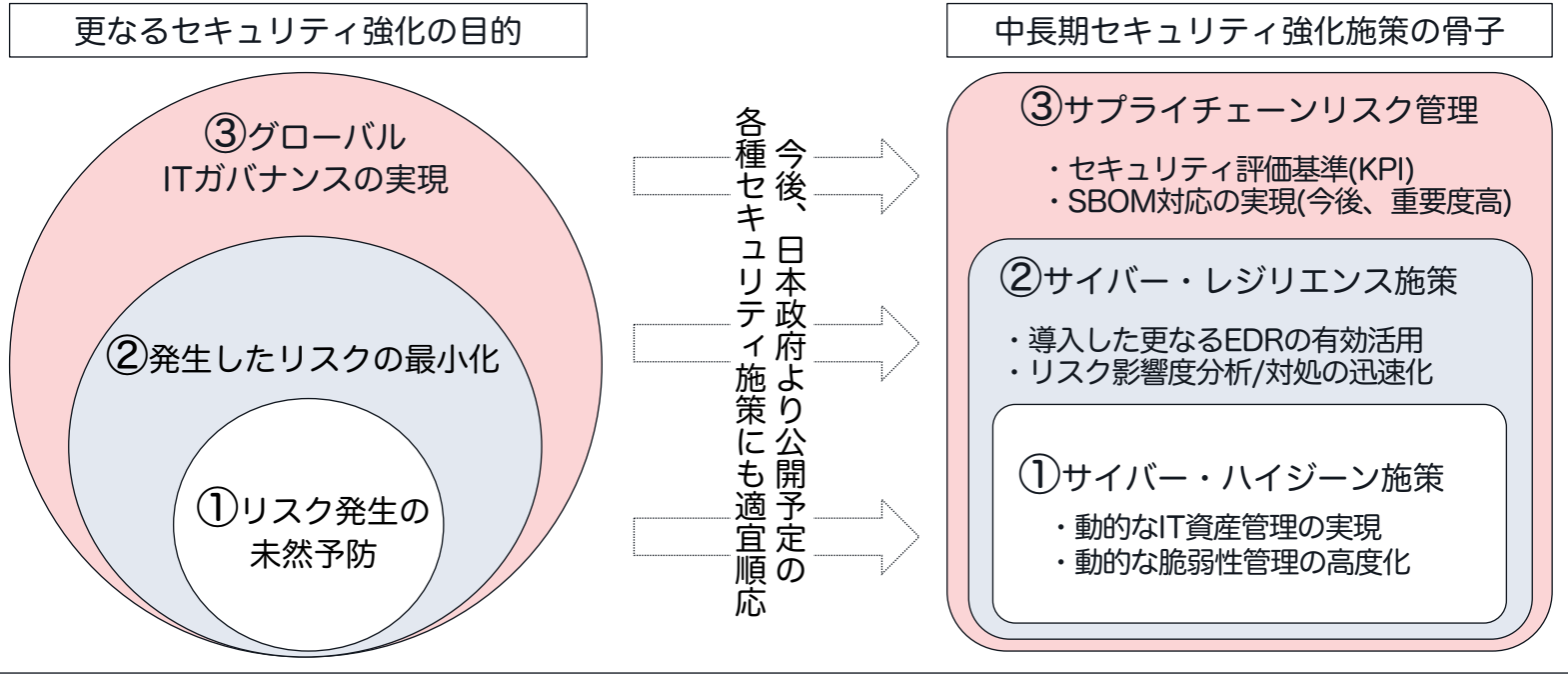
サイバーハイジーン

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)

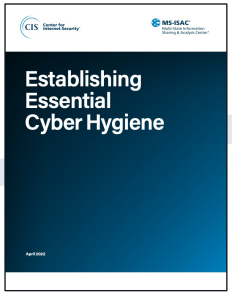


グローバルで加速化するサイバー・ハイジーンの最新動向

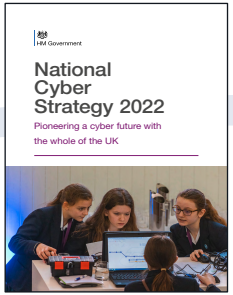
明示的にサイバー・ハイジーンを言及する 法令/戦略/ガイドライン/フレームワーク等

CISA：Cyber Hygiene Service

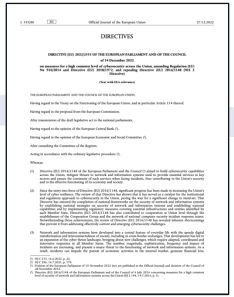
CIS：Essential Cyber Hygiene



NCSC：National Cyber Strategy

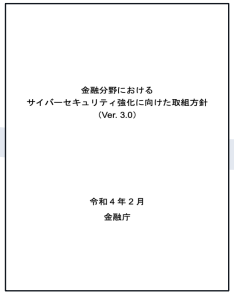


EU：NIS 2 Directive (2023年1月施行)

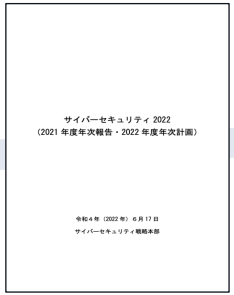


グローバルにおいては、
ITに先進的な諸外国が一斉に指示

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

次回はSBOMに関する調査発表を予定です。
乞うご期待ください。

TANIUM