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

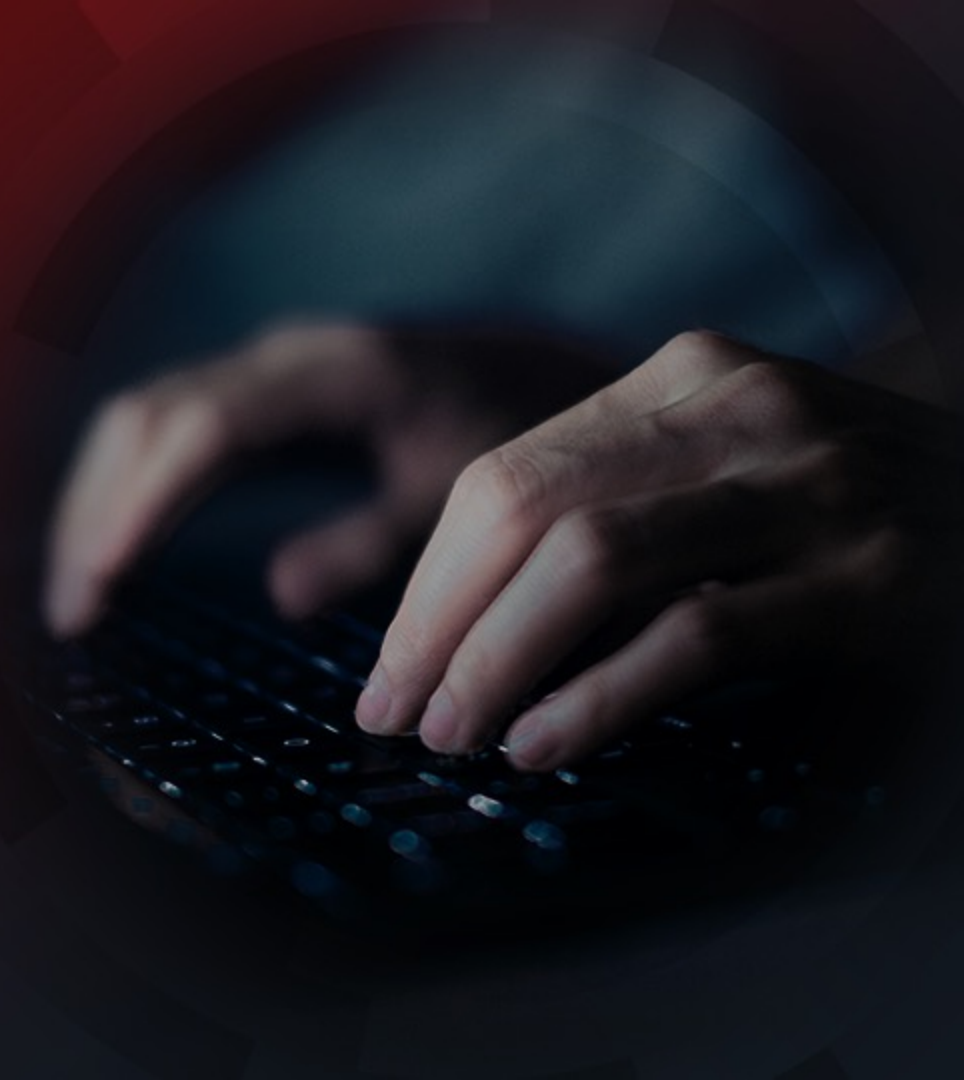
2024年9月10日

タニウム合同会社

TANIUM

TANIUM

会社概要



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 (Executive Chairman)
　　Dan Streetman (CEO)
従業員数：約2,000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

事業開始：2014年
代表：原田 英典 (日本法人代表執行役社長)
従業員数：約110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

3,300万
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）

- 株式会社JTB
- 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
- 住友生命保険相互会社
- 積水化学工業株式会社
- 積水ハウス株式会社
- 全日本空輸株式会社
- 双日株式会社
- ダイキン工業株式会社
- 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
- パナソニック ホールディングス株式会社
- 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
- 株式会社マクニカ
- 株式会社みずほフィナンシャルグループ
- 矢崎総業株式会社
- ヤマハ発動機株式会社
- ローム株式会社

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：683名）
- 調査方法：Webアンケート
- 実施期間：2024年6月3日～2024年6月13日

TANIUM

単体調査

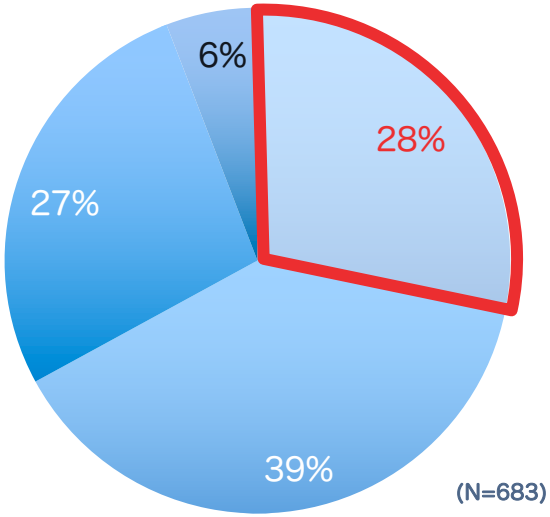
【単体調査#1】サイバーハイジーンの認知度

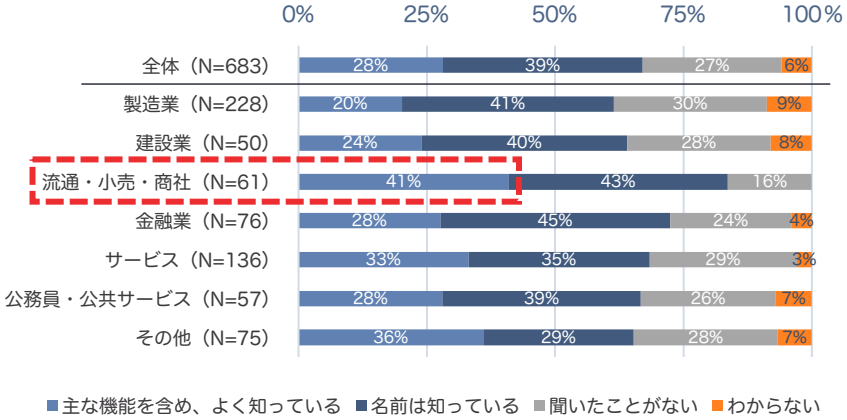
業種別/規模別

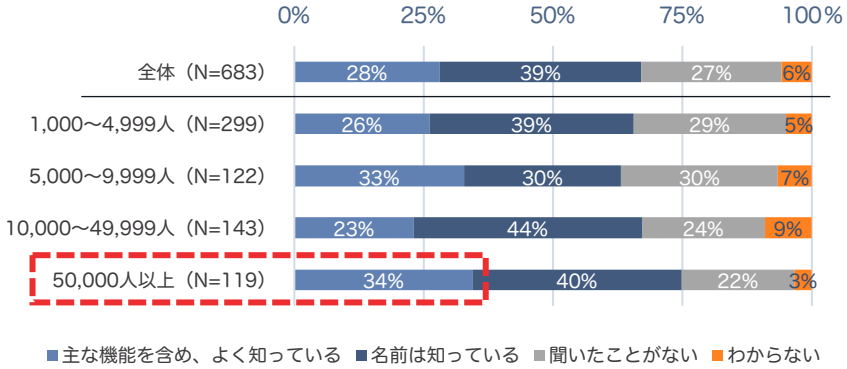
大企業での認知度が高い傾向が見られる。

数値としては昨年とほぼ横ばい(2023年調査では27%)。

2024年





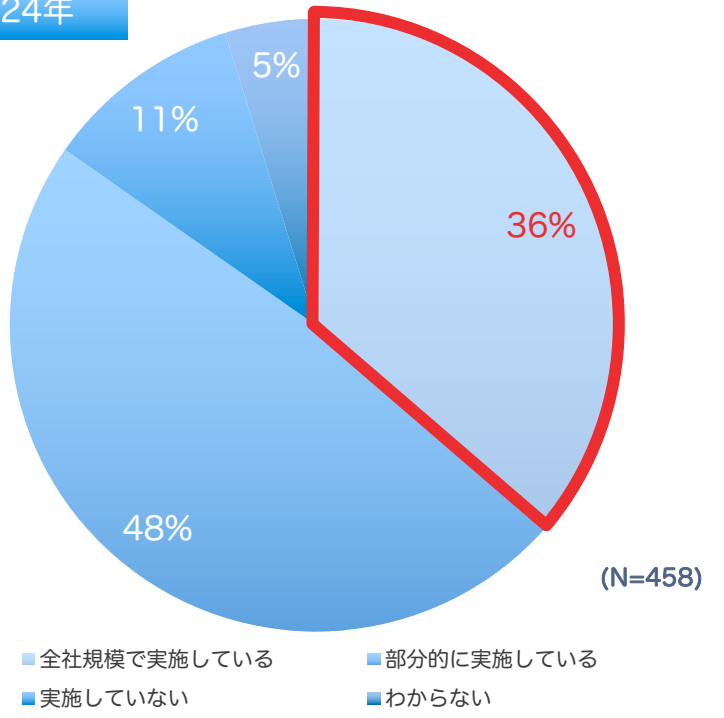


【単体調査#2】サイバーハイジーンの実施範囲

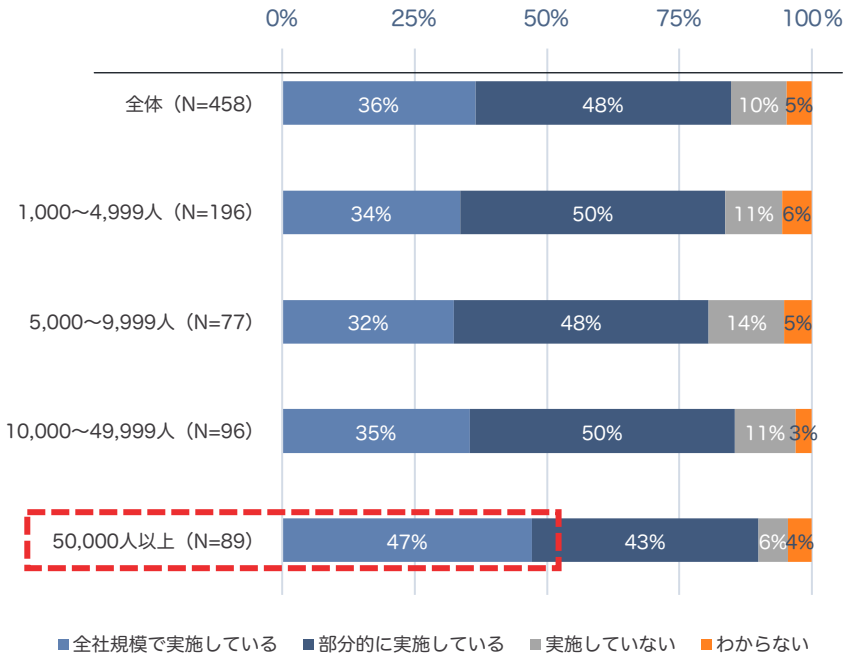
昨年と比較して、大きな変化は見られず。36%強の組織で全社対応。

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(2023年調査では32%) 。

2024年



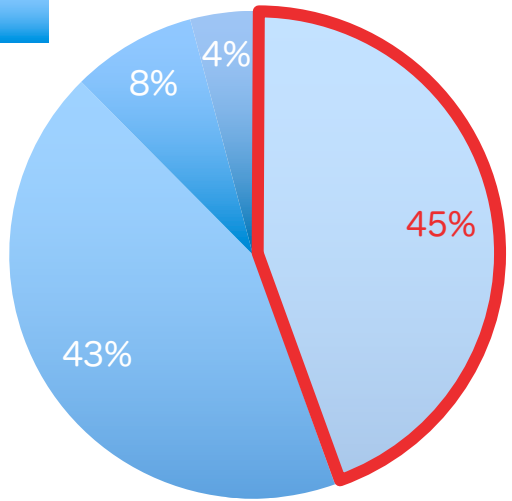
規模別



【単体調査#3】サイバーハイジーン実現におけるIT資産管理の認識

今年新たに追加した調査事項。リアルタイムな鮮度の高い情報が必要という人の割合が全体の45%強。
規模の大きい組織ほどリアルタイムに資産情報を取得できることに対する認識が強い。

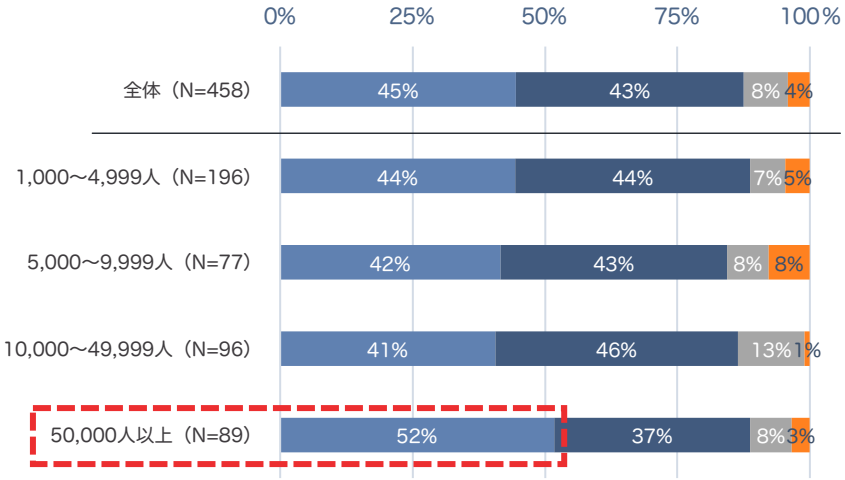
2024年



(N=458)

- 組織内のIT資産構成管理の状況をリアルタイムに把握していること
- 組織内のIT資産構成管理の状況を定期的に把握すること
- 組織内のIT資産構成管理は特定の部門からの依頼に応じて都度情報収集すること
- わからない

規模別

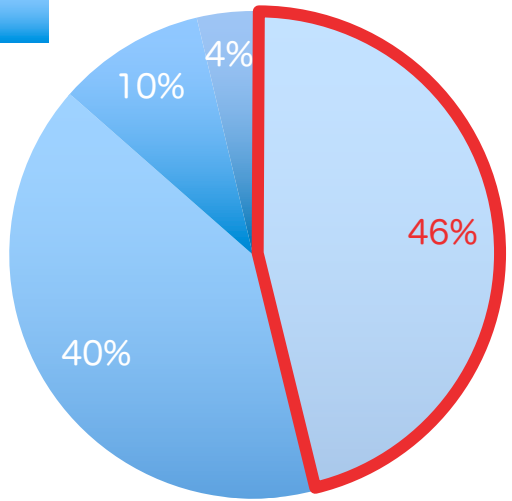


- 組織内のIT資産構成管理の状況をリアルタイムに把握していること
- 組織内のIT資産構成管理の状況を定期的に把握すること
- 組織内のIT資産構成管理は特定の部門からの依頼に応じて都度情報収集すること
- わからない

【単体調査#4】サイバーハイジーン実現における脆弱性管理の認識

今年新たに追加した調査事項。脆弱性情報をリアルタイムに把握が必要という人の割合が全体の46%強。
規模の大きい組織ほどリアルタイムに脆弱性情報取得できることに対する認識が強い。

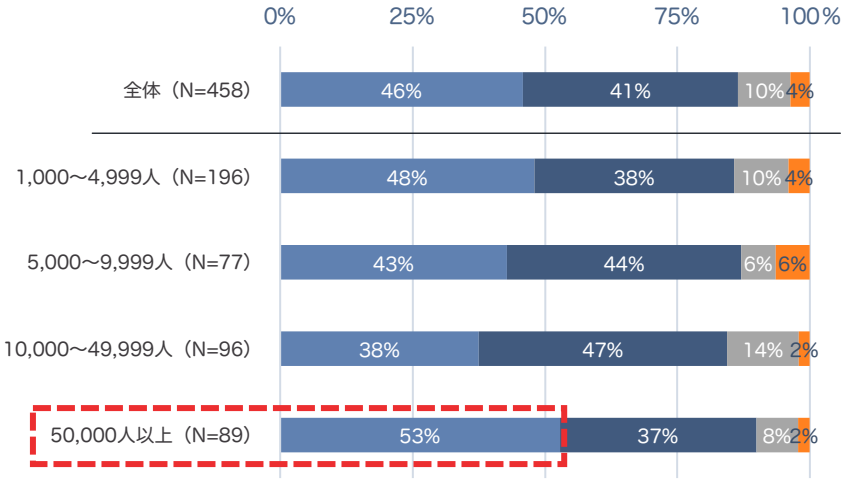
2024年



(N=458)

- 組織内の脆弱性情報をリアルタイムに把握していること
- 組織内の脆弱性情報を定期的に把握すること
- 組織内の脆弱性情報は特定の部門からの依頼に応じて都度情報収集すること
- わからない

規模別

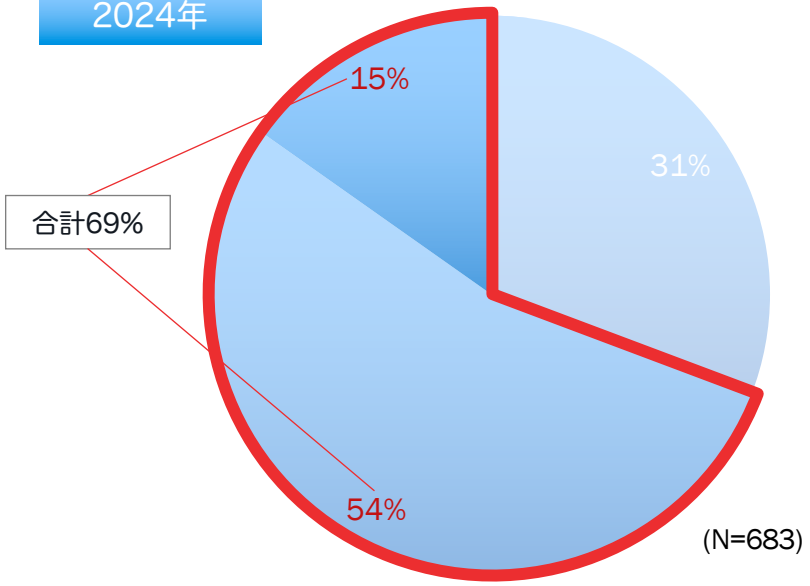


- 組織内の脆弱性情報をリアルタイムに把握していること
- 組織内の脆弱性情報を定期的に把握すること
- 組織内の脆弱性情報は特定の部門からの依頼に応じて都度情報収集すること
- わからない

【単体調査#5】非管理端末（野良端末）の把握

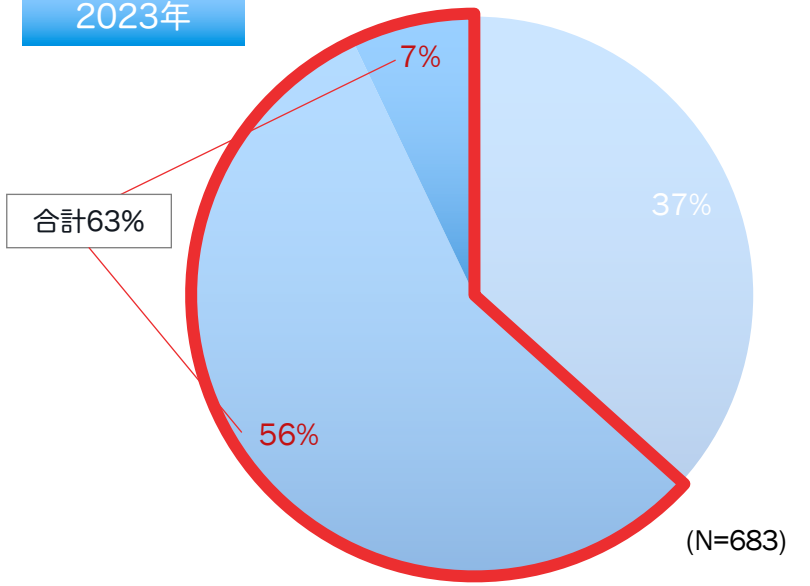
完全に把握できていると回答した組織は4割に満たず、7割弱の組織で非管理端末が存在。
昨年と比較して非管理端末の割合が増えてきている。非管理端末の漬し込みが難しいことが分かる。

2024年



- 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

2023年

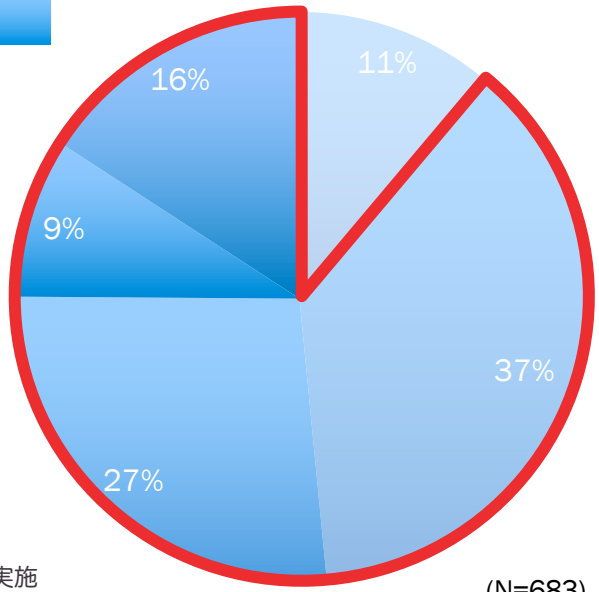


- 完全に把握している（非管理端末数：ゼロ）
- IT部門としては非管理端末の存在は認知しているものの、管理は担当者に任せているので正確な台数は把握していない
- IT部門として、そもそも非管理端末の存在を認知していないため不明

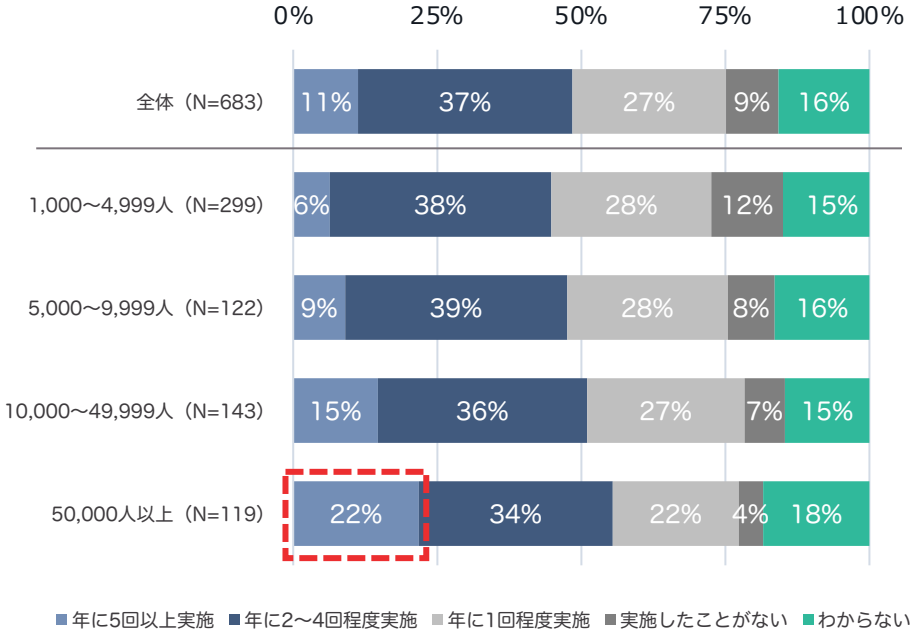
【単体調査#6】脆弱性対応の頻度

89%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。
昨年と比較して、大きな変化は見られず(2023年調査では87%) 。

2024年



規模別

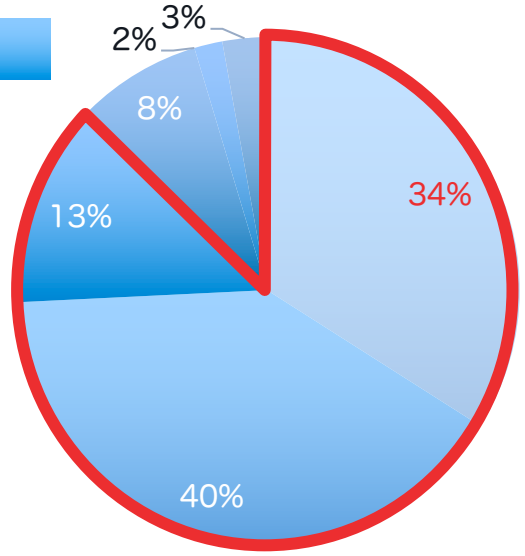


【単体調査#7】サイバーハイジーン管理の運用におけるKPI設定の有無

今年新たに追加した調査事項。サイバーハイジーン管理の運用において指標となるKPIを定めている人の割合が87%。

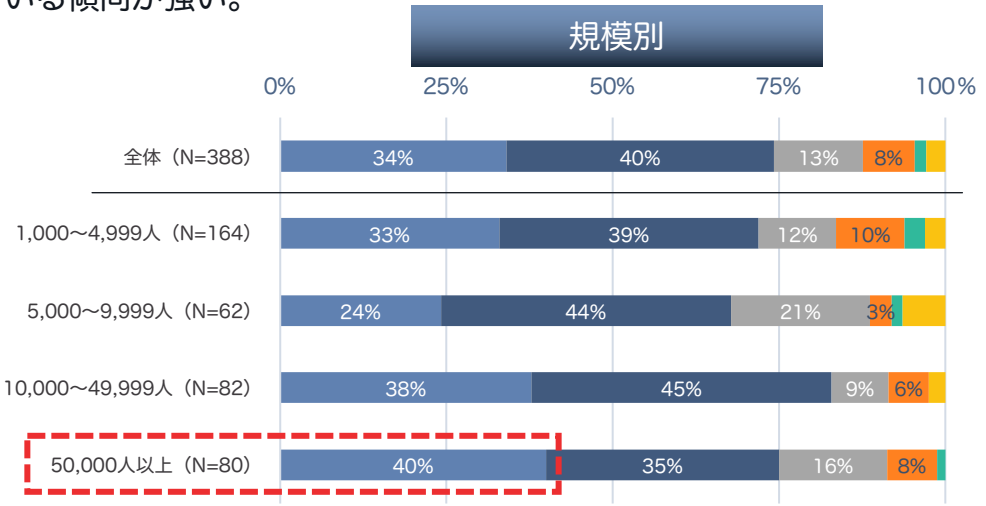
規模の大きい組織ほどKPIを設定し定期的に計測し評価している傾向が強い。

2024年



(N=388)

- KPIを定めており、定期的に計測し評価している
- KPIを定めており、計測している
- KPIは定めているが、特に計測はしていない
- KPIとしては明確に定めてはいないがサイバーハイジーン管理は行っている
- サイバーハイジーンの管理は行っていない
- わからない



- KPIを定めており、定期的に計測し評価している
- KPIを定めており、計測している
- KPIは定めているが、特に計測はしていない
- KPIとしては明確に定めてはいないがサイバーハイジーン管理は行っている
- サイバーハイジーンの管理は行っていない
- わからない

絞り込み調査

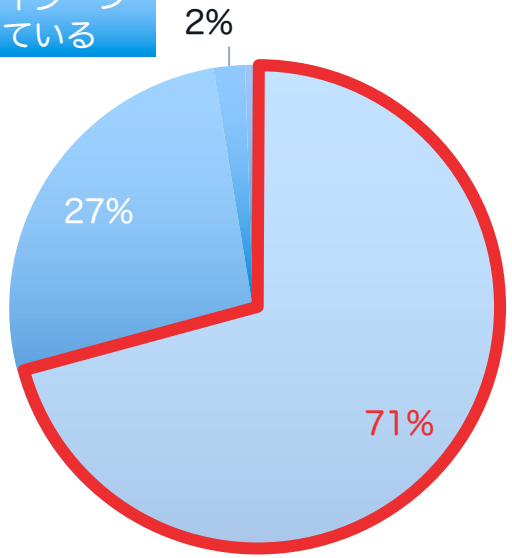
【単体調査#1】
サイバーハイジーンの認知度

を元にした意識調査

【絞り込み調査#1】サイバーハイジーンの認知度に基づく資産管理の意識

サイバーハイジーンの機能をよく知っている人ほどIT資産構成管理のリアルタイムに把握する意識を持っている。

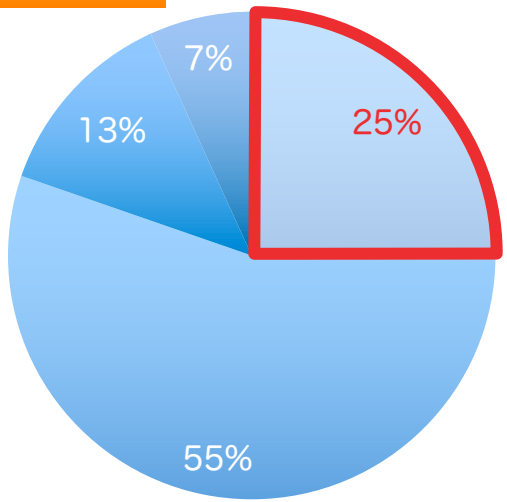
サイバーハイジーン
よく知っている



(N=192)

- 組織内のIT資産構成管理の状況をリアルタイムに把握していること
- 組織内のIT資産構成管理の状況を定期的に把握すること
- 組織内のIT資産構成管理は特定の部門からの依頼に応じて都度情報収集すること
- わからない

サイバーハイジーン
よく知らない



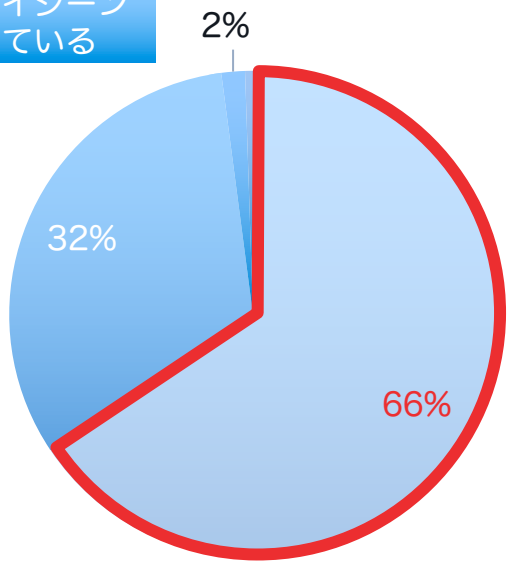
(N=266)

- 組織内のIT資産構成管理の状況をリアルタイムに把握していること
- 組織内のIT資産構成管理の状況を定期的に把握すること
- 組織内のIT資産構成管理は特定の部門からの依頼に応じて都度情報収集すること
- わからない

【絞り込み調査#2】サイバーハイジーンの認知度に基づく脆弱性管理の意識

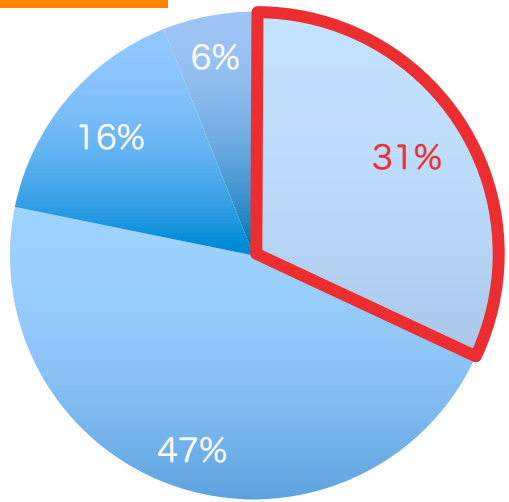
サイバーハイジーンの機能をよく知っている人ほど脆弱性情報を**リアルタイムに把握する**意識を持っている。

サイバーハイジーン
よく知っている



(N=192)

サイバーハイジーン
よく知らない



(N=266)

- 組織内の脆弱性情報をリアルタイムに把握していること
- 組織内の脆弱性情報を定期的に把握すること
- 組織内の脆弱性情報は特定の部門からの依頼に応じて都度情報収集すること
- わからない

絞り込み調査

【単体調査#1】
サイバーハイジーンの認知度
【単体調査#3】
サイバーハイジーン実現におけるIT資産管理の認識

を元にした運用の実態調査

絞り込みのフィルタ条件

本章の絞り込み調査は以下の4象限に分けてサイバーハイジーンの運用実態調査を実施する。

サイバーハイジーン：理解 リアルタイム重要性：認識	サイバーハイジーン：理解 リアルタイム重要性：未認識
サイバーハイジーン：未理解 リアルタイム重要性：認識	サイバーハイジーン：未理解 リアルタイム重要性：未認識

絞り込みのフィルタ条件

本章の絞り込み調査は以下の4象限に分けてサイバーハイジーンの運用実態調査を実施する。

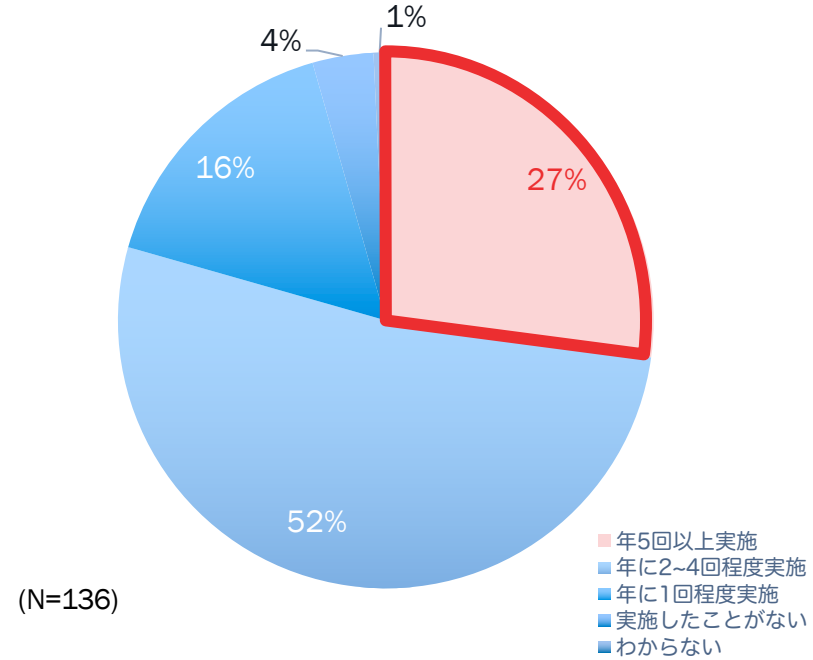
サイバーハイジーン：理解 リアルタイム重要性：認識	サイバーハイジーン：理解 リアルタイム重要性：未認識
サイバーハイジーン：未理解 リアルタイム重要性：認識	サイバーハイジーン：未理解 リアルタイム重要性：未認識

【絞り込み調査#1】脆弱性対応の頻度

サイバーハイジーン：理解 リアルタイム重要性：認識 | サイバーハイジーン：理解 リアルタイム重要性：未認識
サイバーハイジーン：未理解 リアルタイム重要性：認識 | サイバーハイジーン：未理解 リアルタイム重要性：未認識

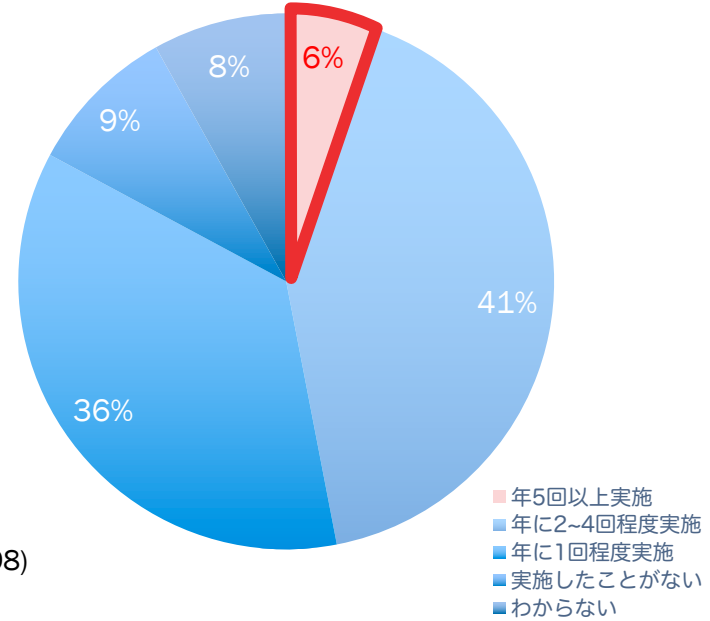
リアルタイムの重要性を認識していない組織は脆弱性対応頻度が顕著に落ちている

サイバーハイジーン理解 & リアルタイムの重要性認識



(N=136)

サイバーハイジーン未理解 & リアルタイムの重要性未認識



(N=198)

【絞り込み調査#2】脆弱性対処時間

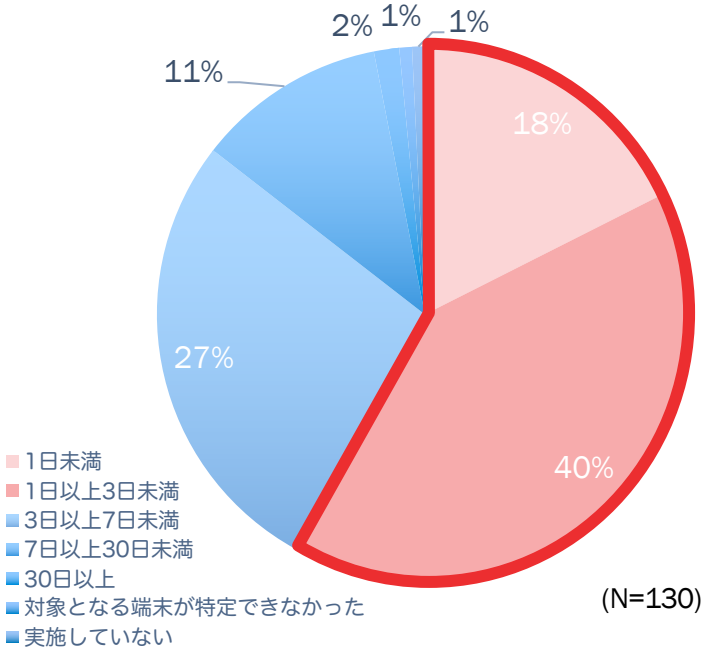
（脆弱性発見後、必要な監査やアップデートなどの是正措置を対象全台に実施するのにかかった時間）

サイバーハイジーン：理解 リアルタイム重要性：認識 | サイバーハイジーン：理解 リアルタイム重要性：未認識

サイバーハイジーン：未理解 リアルタイム重要性：認識 | サイバーハイジーン：未理解 リアルタイム重要性：未認識

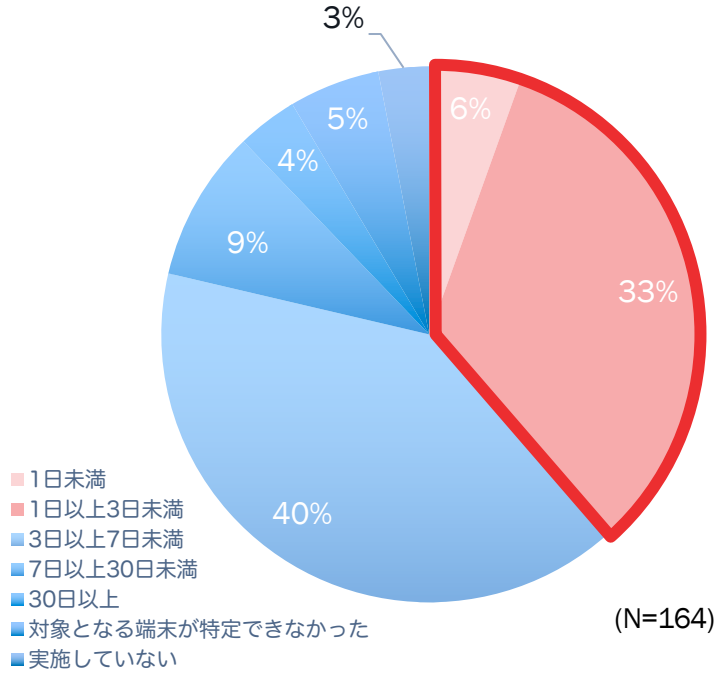
3日未満の結果に顕著な差異が見られる。リアルタイム重要性を認識している組織は5割以上が3日未満で対処完了

サイバーハイジーン理解 & リアルタイムの重要性認識



(N=130)

サイバーハイジーン未理解 & リアルタイムの重要性未認識



(N=164)

【絞り込み調査#3】安全性確認に要した時間

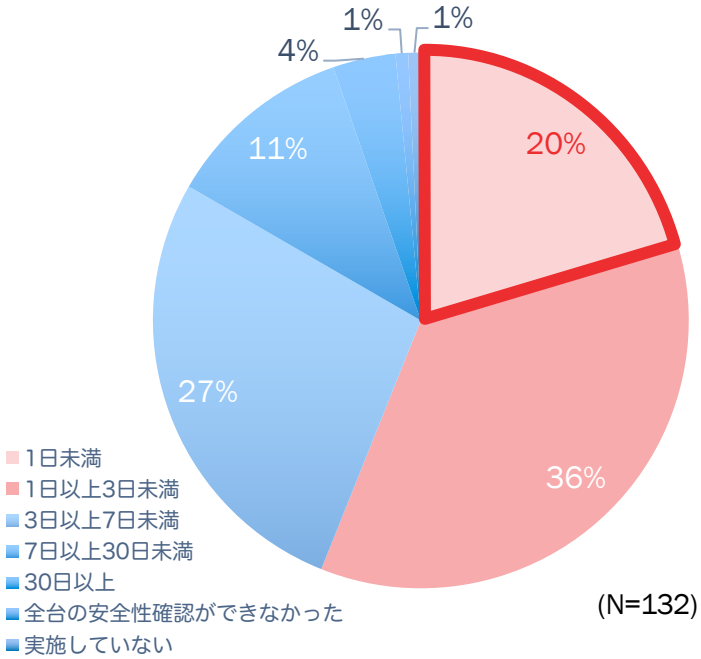
（インシデント発生後に端末全ての安全性確認にかかった時間）

サイバーハイジーン：理解 リアルタイム重要性：認識 | サイバーハイジーン：理解 リアルタイム重要性：未認識

サイバーハイジーン：未理解 リアルタイム重要性：認識 | サイバーハイジーン：未理解 リアルタイム重要性：未認識

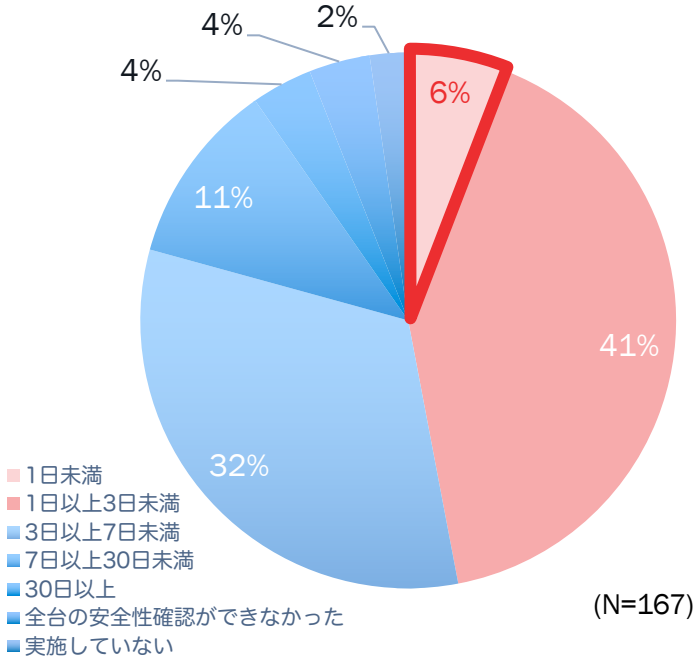
特に短期間での完了に顕著な差異。リアルタイム重要性を認識している組織では20%が1日以内に安全性確認完了

サイバーハイジーン理解 & リアルタイムの重要性認識



(N=132)

サイバーハイジーン未理解 & リアルタイムの重要性未認識



(N=167)

絞り込み調査

【単体調査#1】
サイバーハイジーンの認知度
【単体調査#7】
サイバーハイジーン管理の運用においてKPI設定の有無

を元にした運用の実態調査

絞り込みのフィルタ条件

本章の絞り込み調査は以下の4象限に分けてサイバーハイジーンの運用実態調査を実施する。

サイバーハイジーン：理解 KPI設定/定期評価：実施	サイバーハイジーン：理解 KPI設定/定期評価：未実施
サイバーハイジーン：未理解 KPI設定/定期評価：実施	サイバーハイジーン：未理解 KPI設定/定期評価：未実施

絞り込みのフィルタ条件

本章の絞り込み調査は以下の4象限に分けてサイバーハイジーンの運用実態調査を実施する。

実行が伴っていることから、本調査では
「サイバーハイジーン徹底組織」とする

サイバーハイジーン：理解
KPI設定/定期評価：実施

サイバーハイジーン：理解
KPI設定/定期評価：未実施

サイバーハイジーン：未理解
KPI設定/定期評価：実施

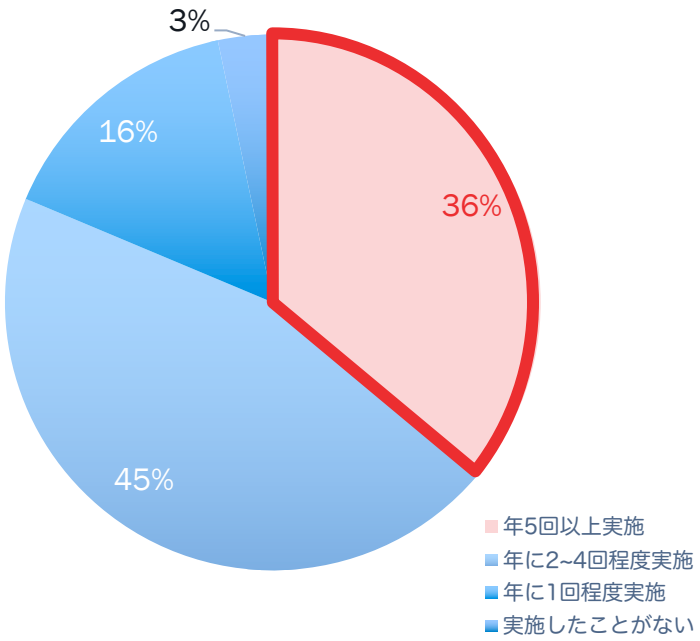
サイバーハイジーン：未理解
KPI設定/定期評価：未実施

【絞り込み調査#1】脆弱性対応の頻度

サイバーハイジーン：理解 KPI設定/定期評価：実施 | サイバーハイジーン：理解 KPI設定/定期評価：未実施
サイバーハイジーン：未理解 KPI設定/定期評価：実施 | サイバーハイジーン：未理解 KPI設定/定期評価：未実施

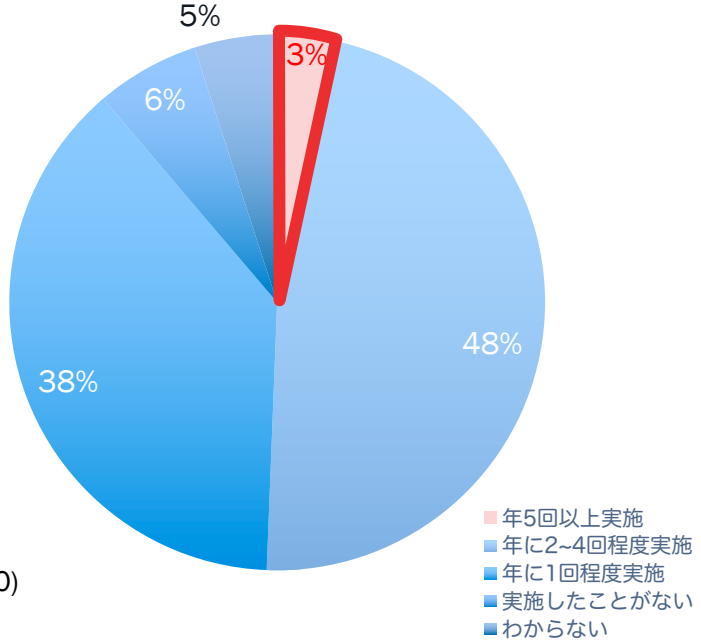
年5回以上実施できている組織の割合に顕著な差異。サイバーハイジーン徹底組織においては36%。

サイバーハイジーン理解 & KPI設定/定期評価実施



(N=91)

サイバーハイジーン未理解 &KPI設定/定期評価未実施



(N=160)

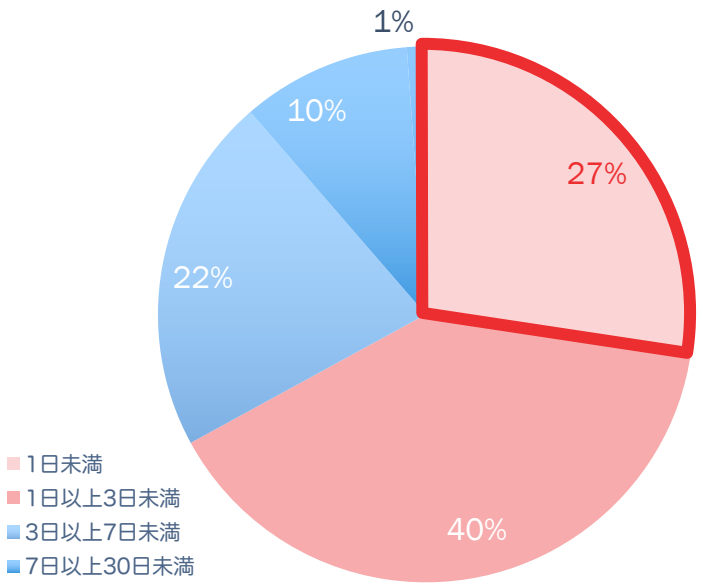
【絞り込み調査#2】脆弱性対処時間

(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)

サイバーハイジーン：理解 KPI設定/定期評価：実施 | サイバーハイジーン：理解 KPI設定/定期評価：未実施
サイバーハイジーン：未理解 KPI設定/定期評価：実施 | サイバーハイジーン：未理解 KPI設定/定期評価：未実施

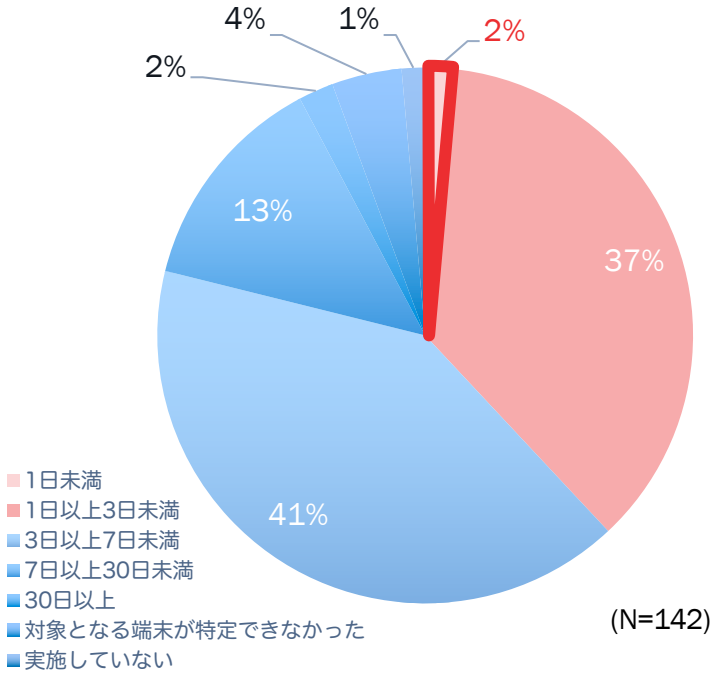
1日未満の結果に顕著な差異が見られる。サイバーハイジーン徹底組織は3割弱が1日未満で対処完了。

サイバーハイジーン理解 & KPI設定/定期評価実施



(N=88)

サイバーハイジーン未理解 &KPI設定/定期評価未実施



(N=142)

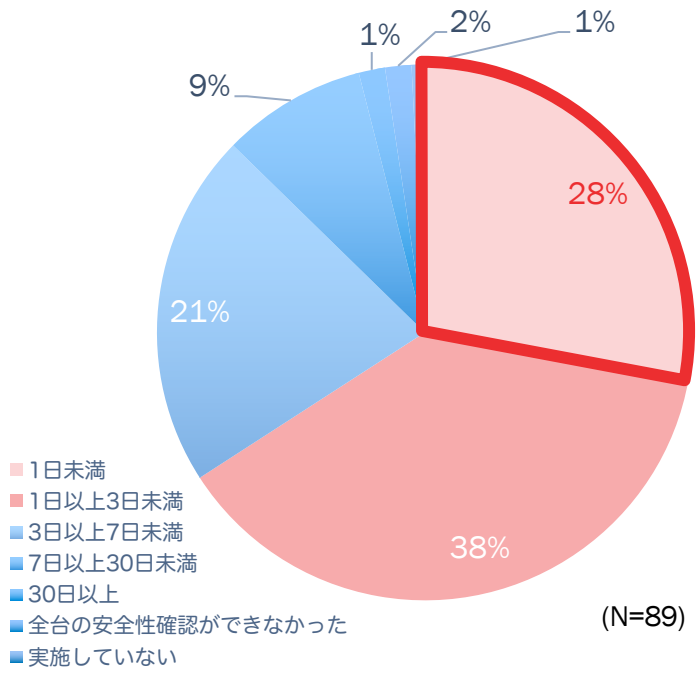
【絞り込み調査#3】安全性確認に要した時間

（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）

サイバーハイジーン：理解 KPI設定/定期評価：実施
サイバーハイジーン：理解 KPI設定/定期評価：未実施
サイバーハイジーン：未理解 KPI設定/定期評価：実施
サイバーハイジーン：未理解 KPI設定/定期評価：未実施

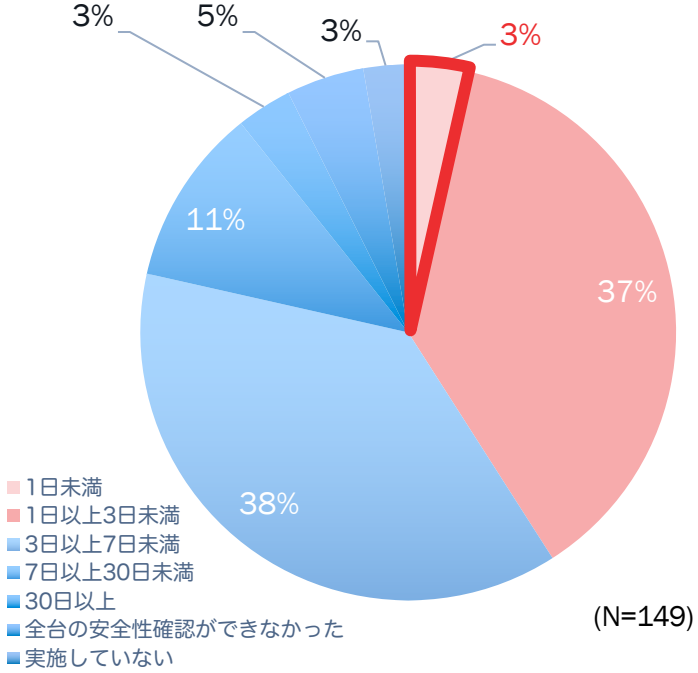
特に短期間での完了に顕著な差異。サイバーハイジーン徹底組織において、 3割弱が1日未満で安全性確認完了。

サイバーハイジーン理解 & KPI設定/定期評価実施



(N=89)

サイバーハイジーン未理解 &KPI設定/定期評価未実施



(N=149)

今回の調査結果について

サイバーハイジーンの認知度

例年と大きな差分はなし

リアルタイム対応の必要性

サイバーハイジーンの認知度に応じ、
IT資産管理と脆弱性管理の調査結果で
2倍以上の差が確認された

野良端末管理

完全把握できている割合が6%減少
（昨年比）

サイバーハイジーン徹底組織

脆弱性対応、脆弱性対処時間、
安全性確認に要する時間の三点で有意な
差異（最大で12倍程度の開き）が存在

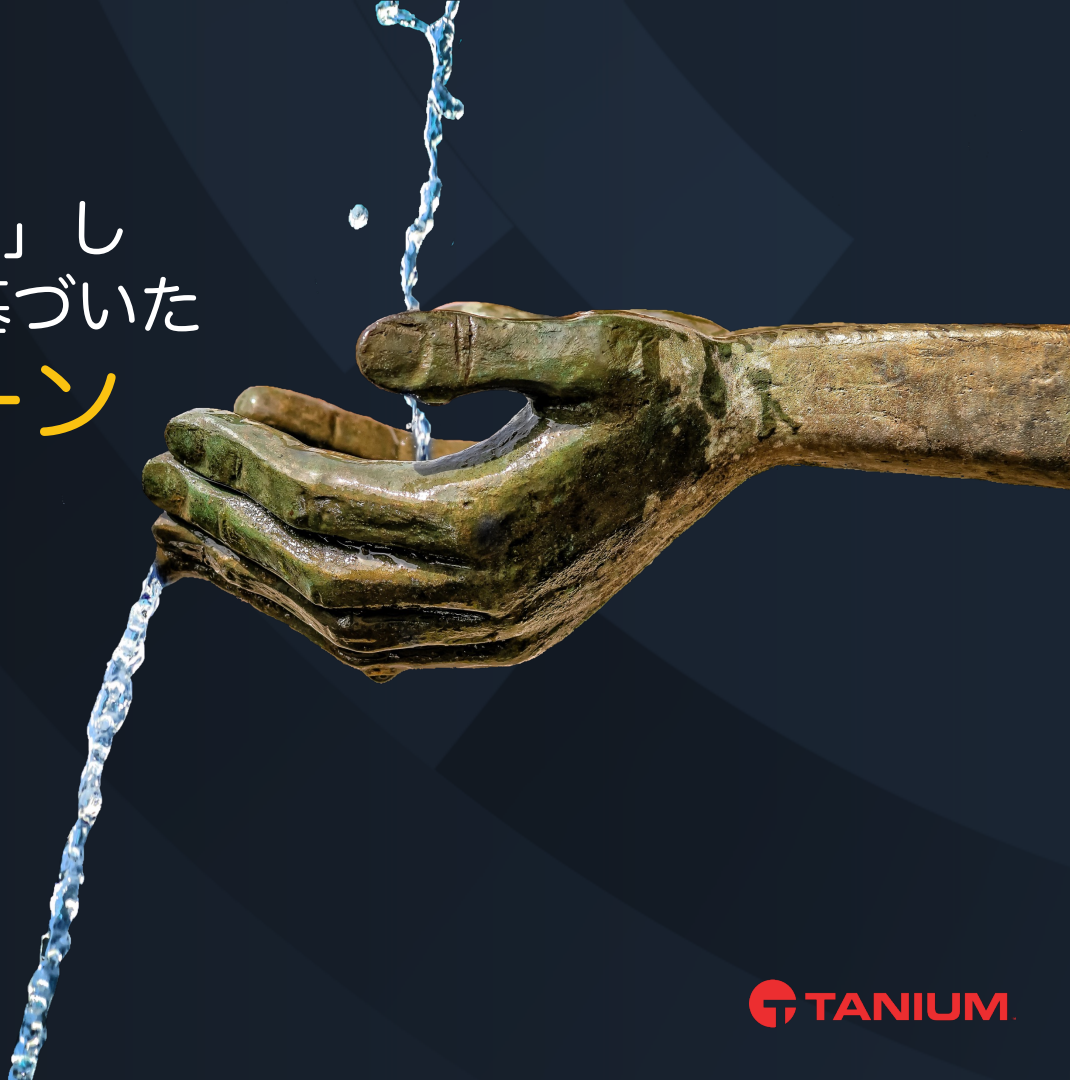
調査結果を踏まえてタニウムからの提言

2024年09月10日

タニウム合同会社

TANIUM

タニウムは、「KPIを設定」し
「リアルタイムな情報」に基づいた
サイバーハイジーン
の運用を推奨します



TANIUM

2023~2024年の主なサイバー攻撃

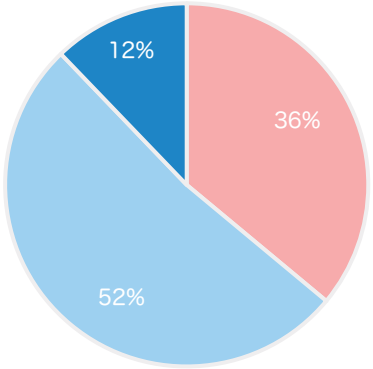
サプライチェーンのセキュリティ、脆弱性の残置などがセキュリティ対策の課題に

1	事例A 港湾業	➢ 全サーバがランサムウェアに感染 ➢ 侵入経路は一部許可していた関連事業者が利用していた機器の脆弱性 ➢ バックアップシステムも被害を受け、3日間の事業停止
2	事例B 医療業	➢ 約4万件の個人情報漏洩の恐れ、ダークウェブへの情報公開被害 ➢ 侵入経路は機器の脆弱性 ➢ 約1週間の重要システムの停止
3	事例C サービス業	➢ 約150万件の個人情報漏洩の遅れ ➢ 全国の自治体や企業など、50にわたる組織情報が流出 ➢ ランサムウェア感染により、ダークウェブへの情報公開被害

ランサムウェアによる被害の企業規模と業種、被害原因

規模や業種に関係なく被害が広がっており、被害原因の大半がサイバーハイジーン運用の未徹底

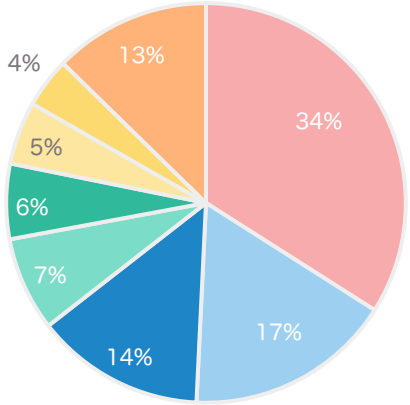
ランサムウェア被害の企業規模



(N=197)

大企業　中小企業　団体等

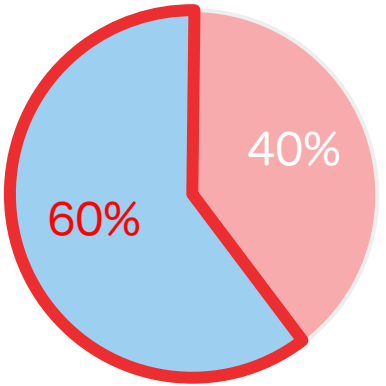
ランサムウェア被害の企業業種



(N=197)

製造業　卸売・小売業
サービス業　情報通信業
建設業　医療・福祉
金融業・保険業　その他

ランサムウェアの侵入経路とされる機器のセキュリティパッチの適用状況



(N=86)

最新のセキュリティパッチを適用済み
未適用のセキュリティパッチがあった

警察庁「令和５年における サイバー空間をめぐる脅威の情勢等について」よりグラフ作成
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

求められるサイバーハイジーン運用のイメージ

KPIを設定し、達成基準を明確化することで、セキュリティ対策の意識向上につながる

	運用項目	管理によるリスク低減	KPIの策定
1	IT資産可視化	全数管理	管理端末 100%→ "今"の実態に即した台帳管理
2	非管理端末可視化	非管理端末削減	非管理端末 0% →不正端末侵入の排除
3	脆弱性可視化	脆弱性削減	公開脆弱性の存在 0% →緊急リスクの把握/対応
4	パッチ管理	OS脆弱性対策の徹底	重要パッチ対応 100% →パッチ未適用率/パッチ適用工数の減少
5	ソフトウェア管理	不要ソフトウェア削減	ソフトウェア数の把握/ver.管理 100% →違反S/Wの排除、S/W投資の最適化
6	ポリシー管理	パスワード、 外部デバイスポリシー徹底	ポリシー準拠の可視化 100% →非準拠デバイスへの強制

Taniumの貢献

全デバイスの
"リアルタイム"
可視化

全デバイスに
内在する
リスクの
可視化と排除

KPIを定期的に評価しサイバーハイジーン運用コミットを徹底

Taniumでは鮮度の高い情報を元にサイバーハイジーンダッシュボードで運用コミットを支援

"リアルタイム"な全社状況の見える化/自社のセキュリティレベル理解/GAPの洗い出し

全社で遵守すべき
セキュリティポリシー

- 達成基準明確化でセキュリティ意識向上
- 相互監視による透明性向上
- 競争意識向上によるセキュリティ啓発

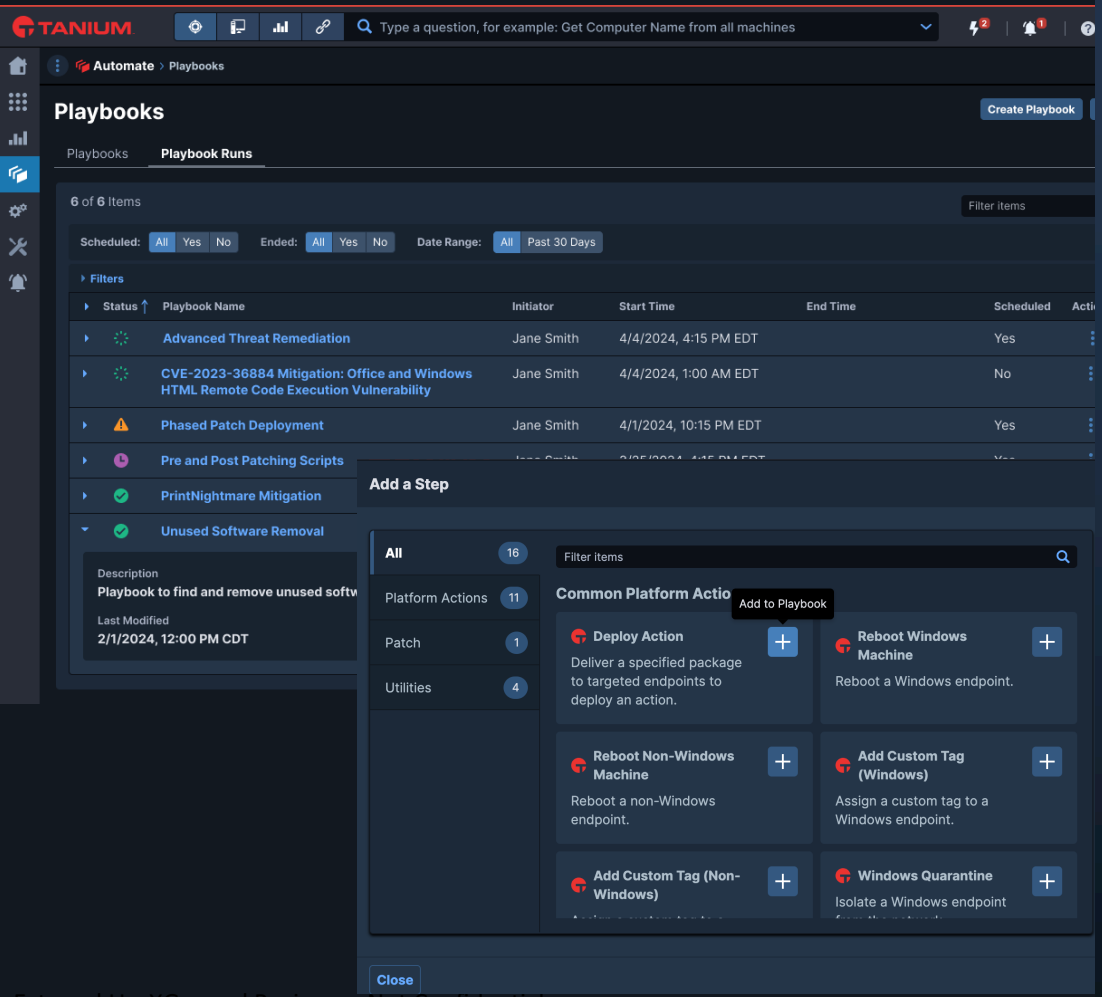
サイバーハイジーン運用をサプライチェーンまで展開

サイバーハイジーン運用の徹底には平時有事問わず、サプライチェーン全体のモニタリングが重要

	サイバーハイジーン運用項目例	管理によるリスク低減
1	IT資産可視化	全数管理
2	非管理端末可視化	非管理端末削減
3	脆弱性可視化	脆弱性削減
4	パッチ管理	OS脆弱性対策の徹底
5	ソフトウェア管理 SBOM管理	不要ソフトウェア削減 ソフトウェア最新化徹底
6	ポリシー管理	パスワード、 外部デバイスポリシー徹底

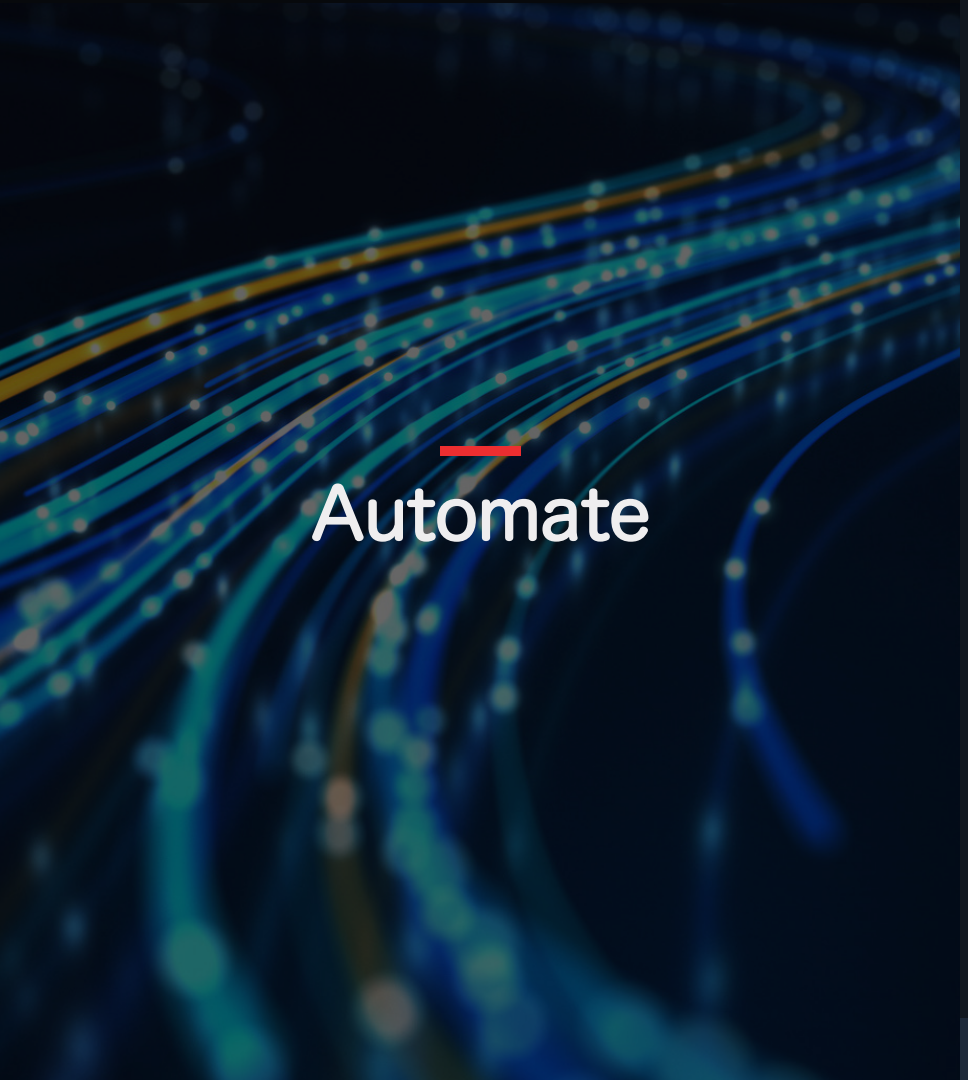
平時/有事の
モニタリング

新機能リリースについて



Tanium Automate

組織のエンドポイント管理を
自立型へ導くFirst Step



Automate

- 様々なプロセスをPlaybookとして自動化
- 作業ミスを減らし効率的な運用を実現
- 動作状況の可視化や各種制御も実現

ご清聴いただきありがとうございました。

TANIUM

補足資料

絞り込み調査完全版

TANIUM

絞り込み調査

【単体調査#1】
サイバーハイジーンの認知度
【単体調査#3】
サイバーハイジーン実現におけるIT資産管理の認識

を元にした運用の実態調査

絞り込みのフィルタ条件

本章の絞り込み調査は以下の4象限に分けてサイバーハイジーンの運用実態調査を実施する。

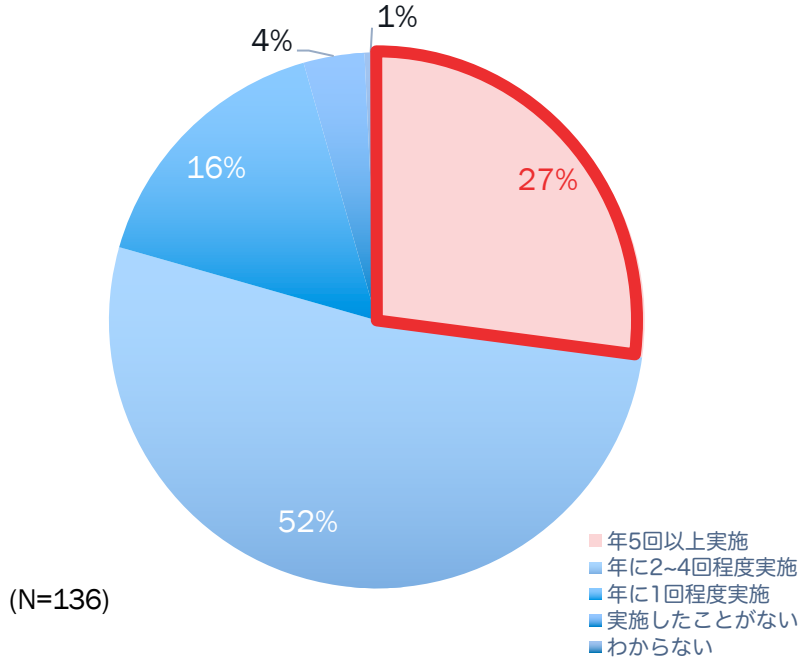
サイバーハイジーン：理解 リアルタイム重要性：認識	サイバーハイジーン：理解 リアルタイム重要性：未認識
サイバーハイジーン：未理解 リアルタイム重要性：認識	サイバーハイジーン：未理解 リアルタイム重要性：未認識

【絞り込み調査#1-1】脆弱性対応の頻度

サイバーハイジーン：理解 リアルタイム重要性：認識	サイバーハイジーン：理解 リアルタイム重要性：未認識
サイバーハイジーン：未理解 リアルタイム重要性：認識	サイバーハイジーン：未理解 リアルタイム重要性：未認識

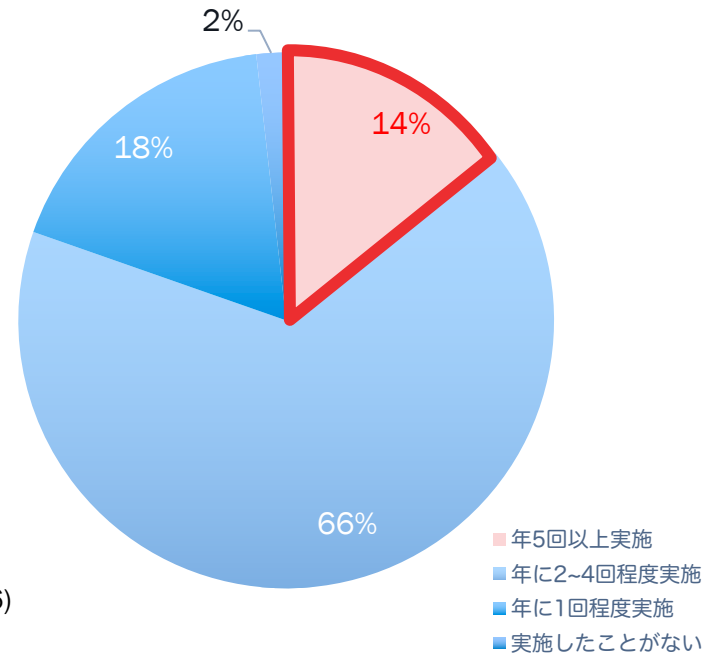
サイバーハイジーンの機能をよく理解していても、リアルタイムの重要性を認識していない組織は脆弱性対応頻度が落ちる。

サイバーハイジーン理解 & リアルタイムの重要性認識



(N=136)

サイバーハイジーン理解 & リアルタイムの重要性未認識



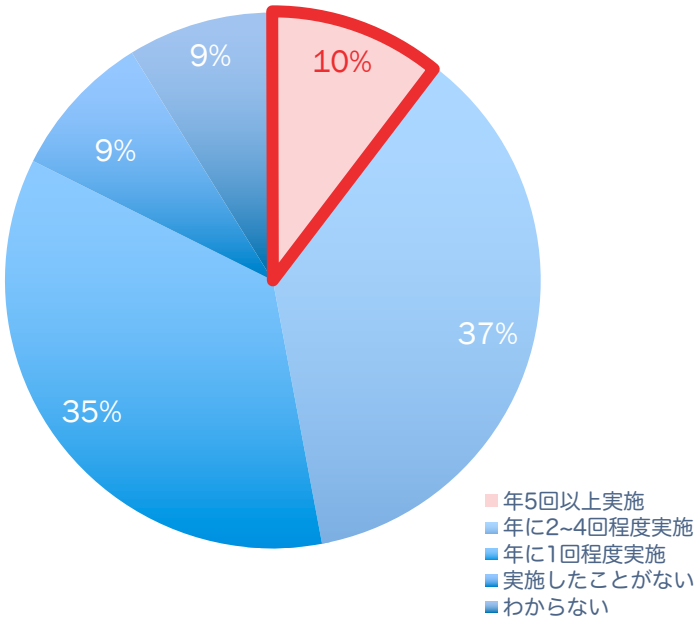
(N=56)

【絞り込み調査#1-2】脆弱性対応の頻度

サイバーハイジーン：理解 リアルタイム重要性：認識 | サイバーハイジーン：理解 リアルタイム重要性：未認識
サイバーハイジーン：未理解 リアルタイム重要性：認識 | サイバーハイジーン：未理解 リアルタイム重要性：未認識

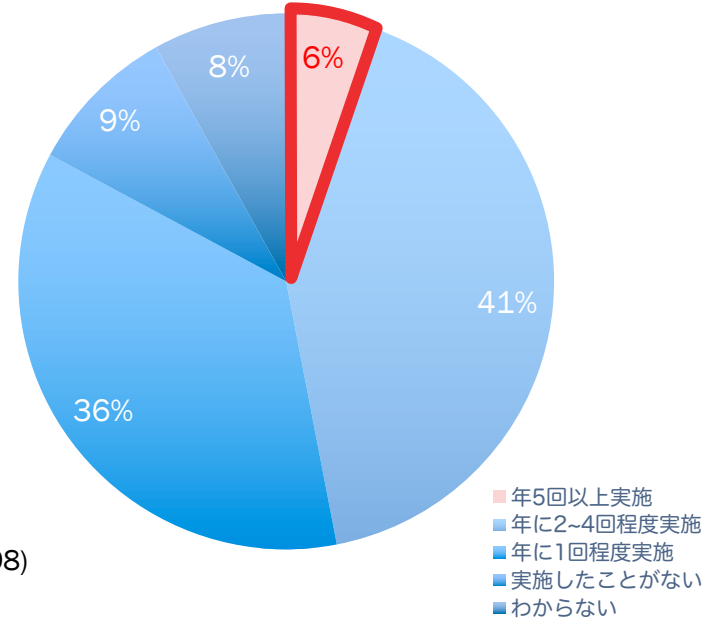
サイバーハイジーンの機能を含め理解していない人は脆弱性対応頻度が総じて低い傾向となる。

サイバーハイジーン未理解 & リアルタイムの重要性認識



(N=68)

サイバーハイジーン未理解 & リアルタイムの重要性未認識



(N=198)

【絞り込み調査#2-1】脆弱性対処時間

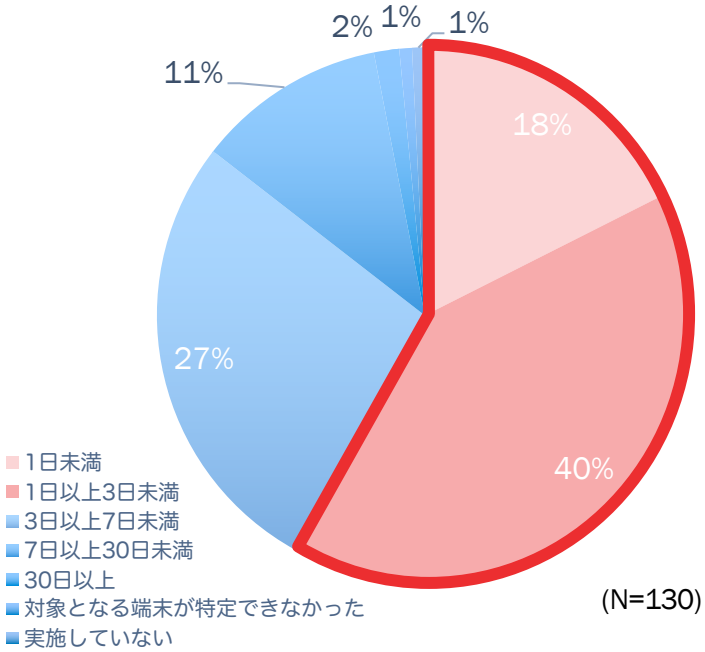
（脆弱性発見後、必要な監査やアップデートなどの是正措置を対象全台に実施するのにかかった時間）

サイバーハイジーン：理解 リアルタイム重要性：認識 | サイバーハイジーン：理解 リアルタイム重要性：未認識

サイバーハイジーン：未理解 リアルタイム重要性：認識 | サイバーハイジーン：未理解 リアルタイム重要性：未認識

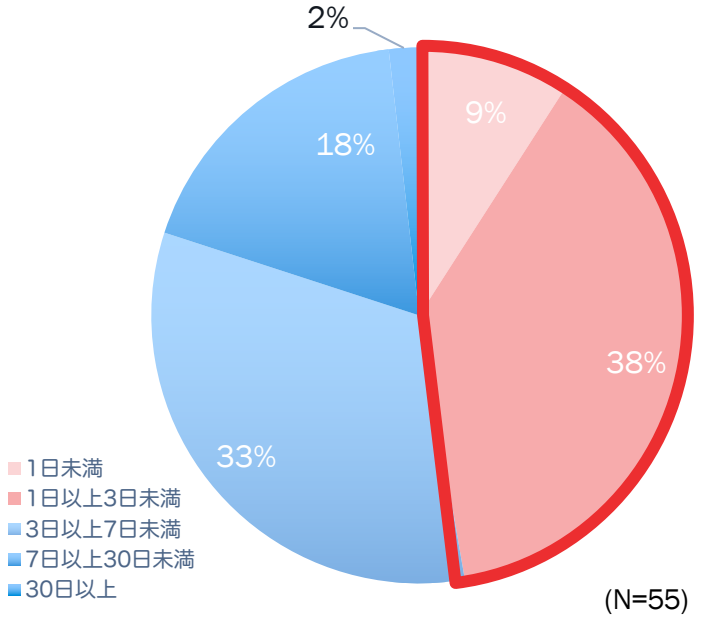
3日未満の結果に顕著な差異が見られる。サイバーハイジーン徹底組織は5割以上が3日未満で対処が完了。

サイバーハイジーン理解 & リアルタイムの重要性認識



(N=130)

サイバーハイジーン理解 & リアルタイムの重要性未認識



(N=55)

【絞り込み調査#2-2】脆弱性対処時間

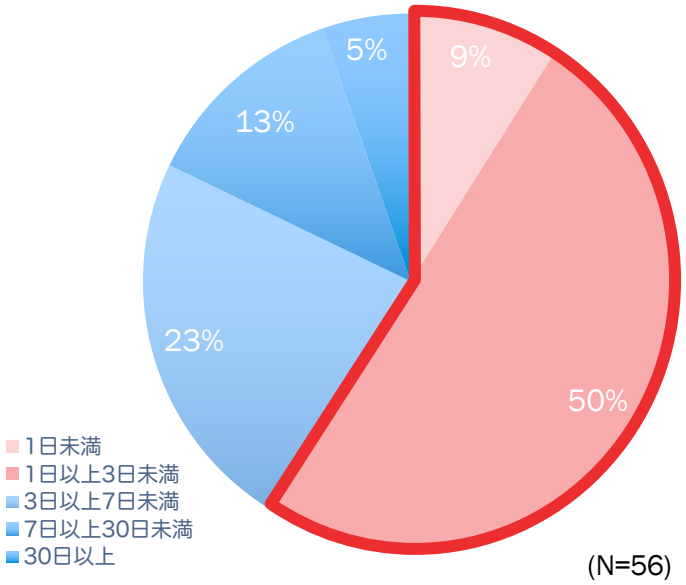
(脆弱性発見後、必要な監査やアップデートなどの是正措置を対象全台に実施するのにかかった時間)

サイバーハイジーン：理解 リアルタイム重要性：認識 | サイバーハイジーン：理解 リアルタイム重要性：未認識

サイバーハイジーン：未理解 リアルタイム重要性：認識 | サイバーハイジーン：未理解 リアルタイム重要性：未認識

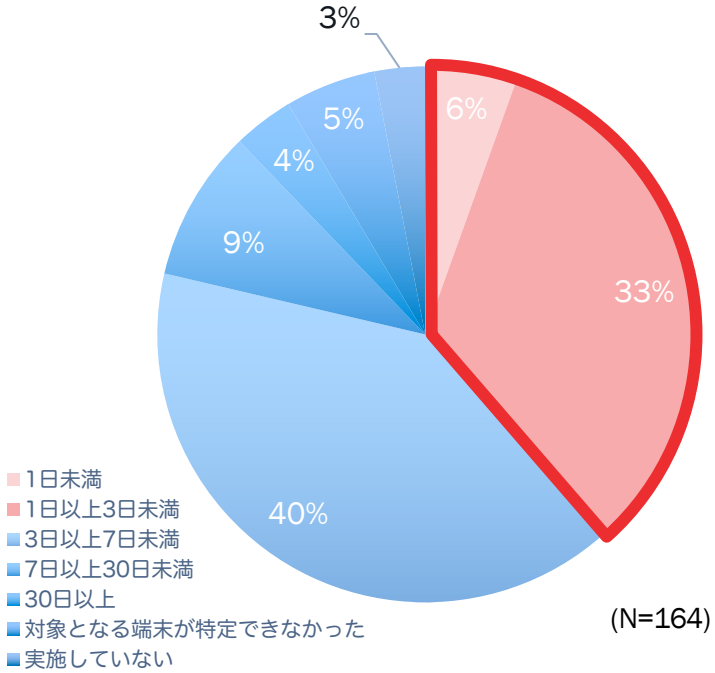
3日未満の結果に顕著な差異が見られる。リアルタイム情報の重要性を認識している組織は5割以上が3日未満で対処完了。

サイバーハイジーン未理解 & リアルタイムの重要性認識



(N=56)

サイバーハイジーン未理解 & リアルタイムの重要性未認識



(N=164)

【絞り込み調査#3-1】安全性確認に要した時間

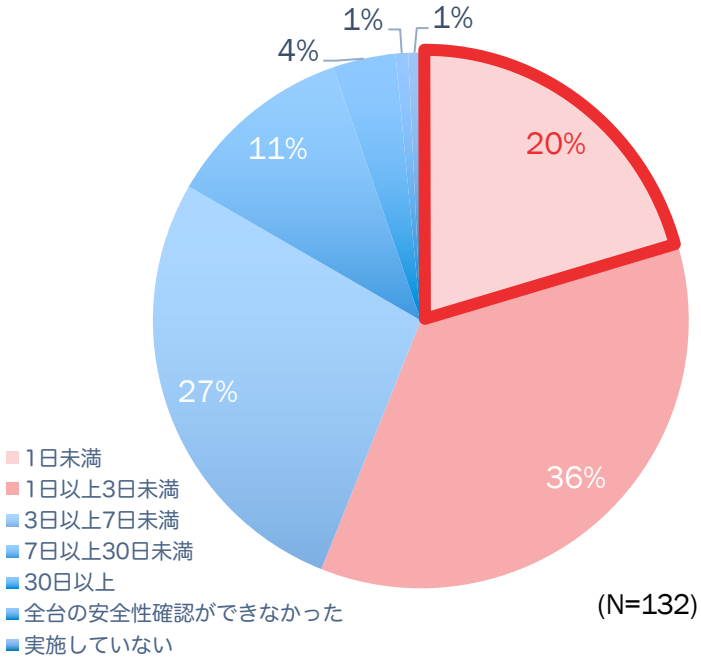
（インシデント発生後に端末全ての安全性確認にかかった時間）

サイバーハイジーン：理解 リアルタイム重要性：認識 | サイバーハイジーン：理解 リアルタイム重要性：未認識

サイバーハイジーン：未理解 リアルタイム重要性：認識 | サイバーハイジーン：未理解 リアルタイム重要性：未認識

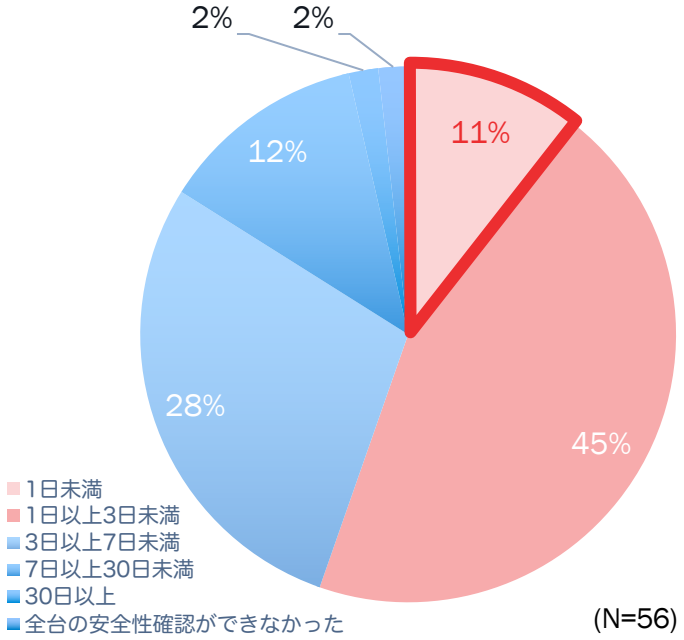
特に短期間での完了に顕著な差異。サイバーハイジーン徹底組織においては20%が1日以内に安全性確認完了。

サイバーハイジーン理解 & リアルタイムの重要性認識



(N=132)

サイバーハイジーン理解 & リアルタイムの重要性未認識



(N=56)

【絞り込み調査#3-2】安全性確認に要した時間

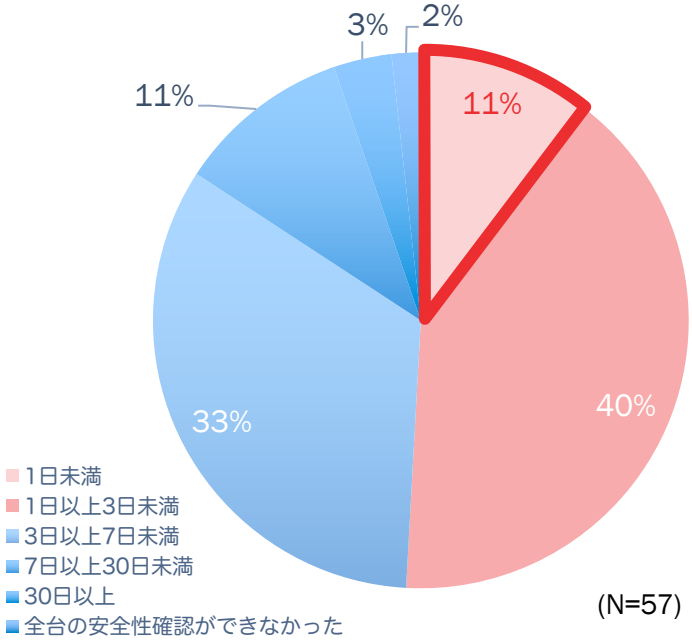
（インシデント発生後に端末全ての安全性確認にかかった時間）

サイバーハイジーン：理解 リアルタイム重要性：認識 | サイバーハイジーン：理解 リアルタイム重要性：未認識

サイバーハイジーン：未理解 リアルタイム重要性：認識 | サイバーハイジーン：未理解 リアルタイム重要性：未認識

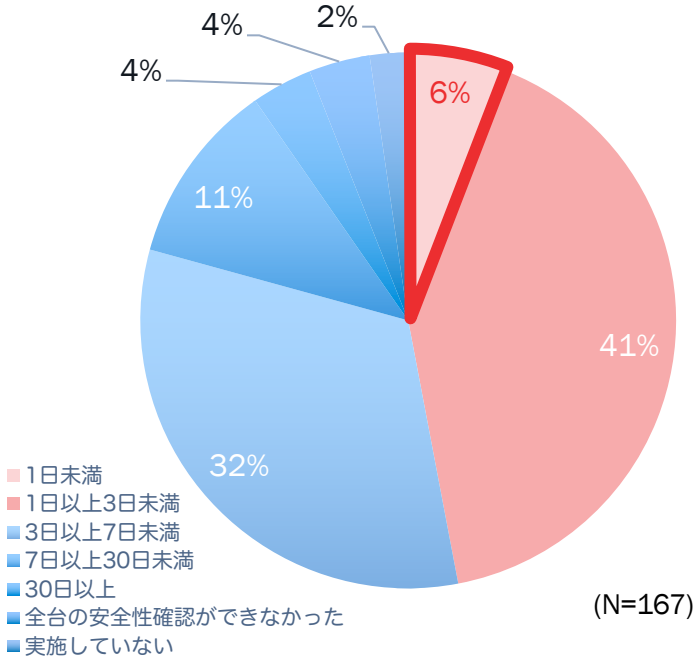
特に短期間での完了に顕著な差異。リアルタイム情報の重要性を認識している組織は10%強が1日以内に安全性確認完了。

サイバーハイジーン未理解 & リアルタイムの重要性認識



(N=57)

サイバーハイジーン未理解 & リアルタイムの重要性未認識



(N=167)

絞り込み調査

【単体調査#1】
サイバーハイジーンの認知度
【単体調査#7】
サイバーハイジーン管理の運用においてKPI設定の有無

を元にした運用の実態調査

絞り込みのフィルタ条件

本章の絞り込み調査は以下の4象限に分けてサイバーハイジーンの運用実態調査を実施する。

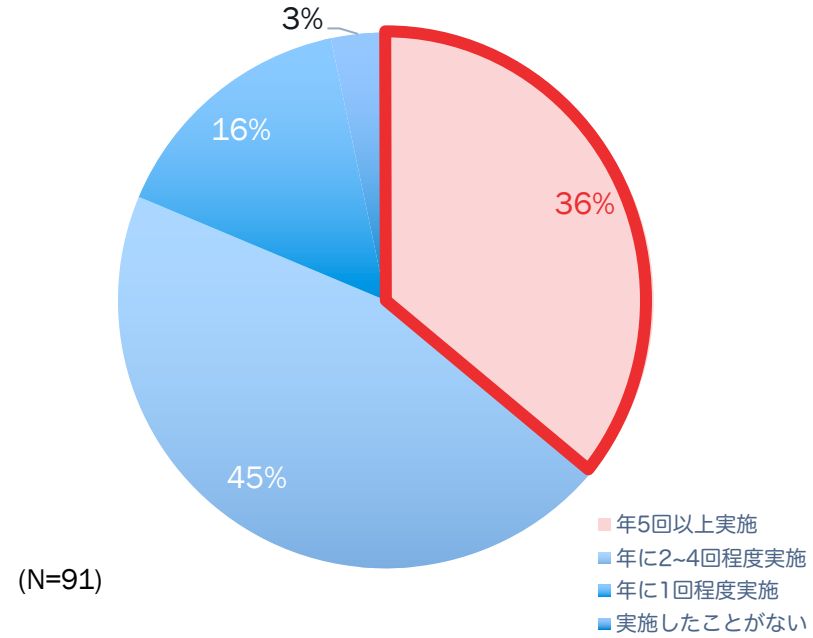
サイバーハイジーン：理解 KPI設定/定期評価：実施	サイバーハイジーン：理解 KPI設定/定期評価：未認識
サイバーハイジーン：未理解 KPI設定/定期評価：認識	サイバーハイジーン：未理解 KPI設定/定期評価：未認識

【絞り込み調査#1-1】脆弱性対応の頻度

サイバーハイジーン：理解 KPI設定/定期評価：実施 | サイバーハイジーン：理解 KPI設定/定期評価：未実施
サイバーハイジーン：未理解 KPI設定/定期評価：実施 | サイバーハイジーン：未理解 KPI設定/定期評価：未実施

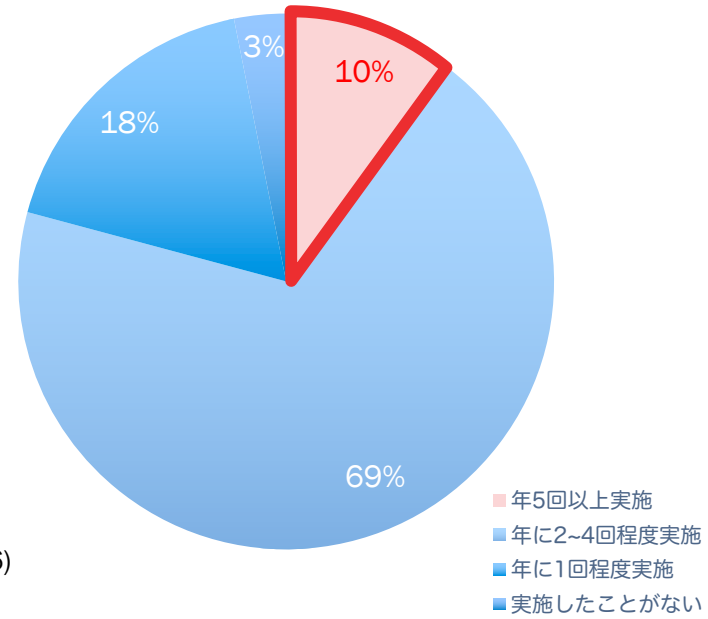
年5回以上実施できている組織の割合に顕著な差異。サイバーハイジーン徹底組織においては36%。

サイバーハイジーン理解 & KPI設定/定期評価実施



(N=91)

サイバーハイジーン理解 & KPI設定/定期評価未実施



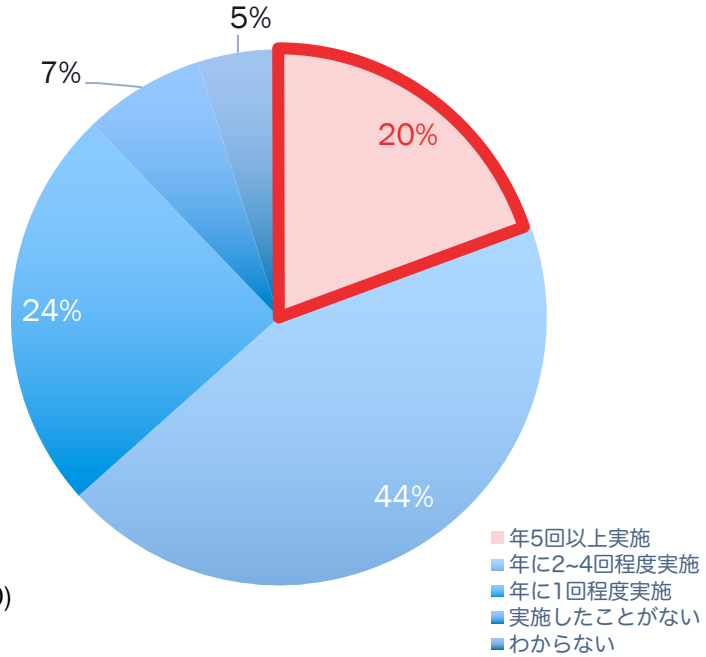
(N=96)

【絞り込み調査#1-2】脆弱性対応の頻度

サイバーハイジーン：理解 KPI設定/定期評価：実施	サイバーハイジーン：理解 KPI設定/定期評価：未実施
サイバーハイジーン：未理解 KPI設定/定期評価：実施	サイバーハイジーン：未理解 KPI設定/定期評価：未実施

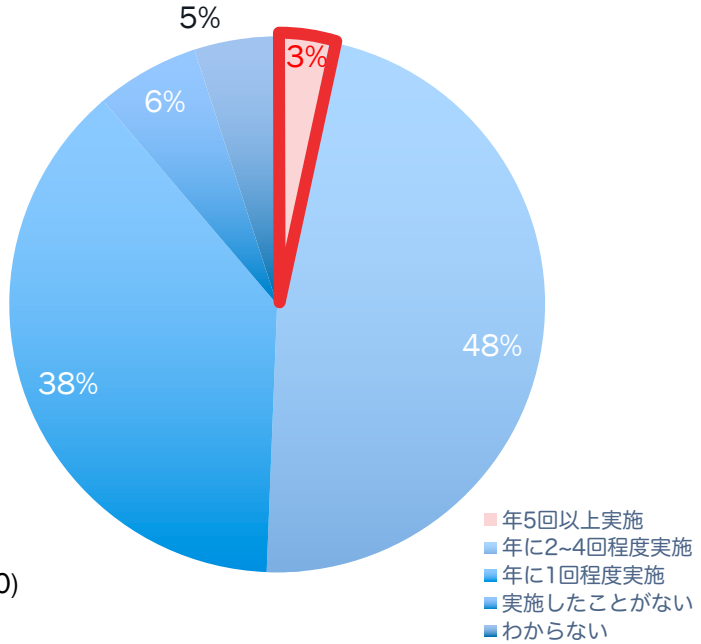
年5回以上実施できている組織の割合に顕著な差異。KPI徹底組織においては20%超。

サイバーハイジーン未理解 &
KPI設定/定期評価実施



(N=210)

サイバーハイジーン未理解
&KPI設定/定期評価未実施



(N=160)

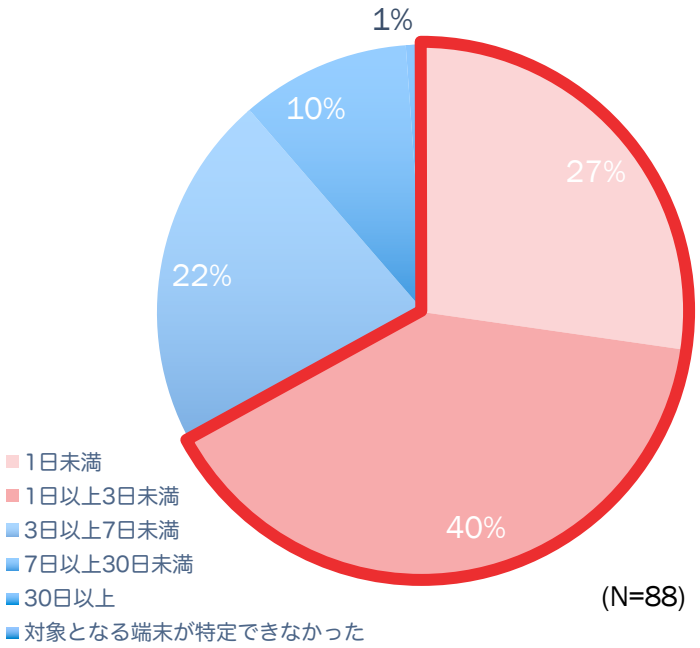
【絞り込み調査#2-1】脆弱性対処時間

(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)

サイバーハイジーン：理解 KPI設定/定期評価：実施 | サイバーハイジーン：理解 KPI設定/定期評価：未実施
サイバーハイジーン：未理解 KPI設定/定期評価：実施 | サイバーハイジーン：未理解 KPI設定/定期評価：未実施

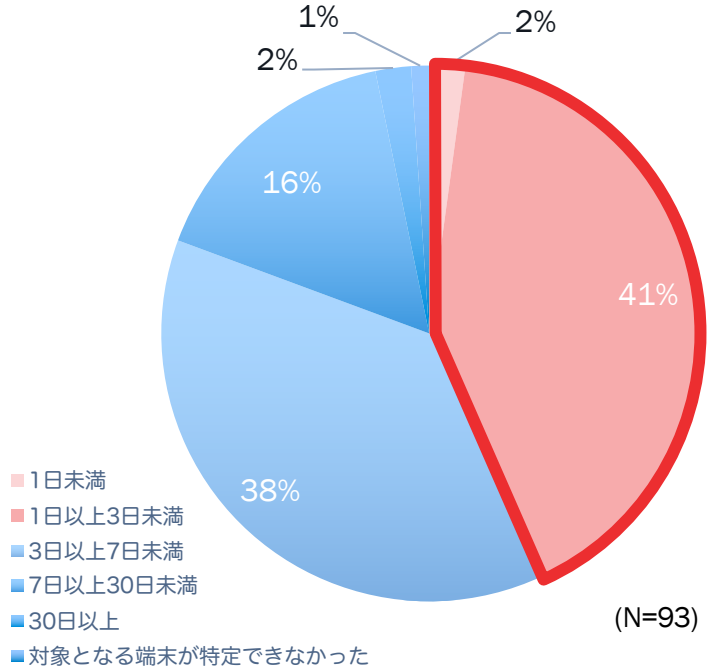
3日未満の結果に顕著な差異が見られる。サイバーハイジーン徹底組織は7割弱が3日未満で対処が完了。

サイバーハイジーン理解 & KPI設定/定期評価実施



(N=88)

サイバーハイジーン理解 & KPI設定/定期評価未実施



(N=93)

【絞り込み調査#2-2】脆弱性対処時間

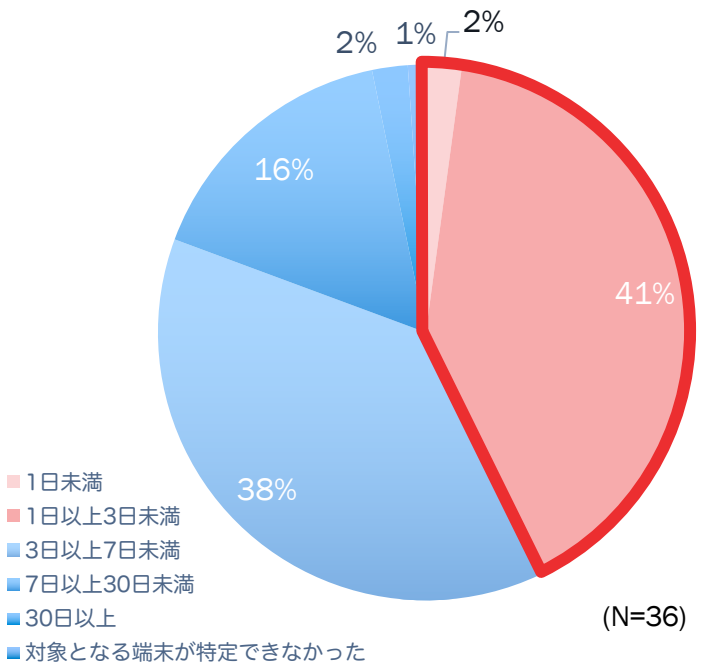
(脆弱性発見後、必要な監査やアップデートなどの是正措置を対象全台に実施するのにかかった時間)

サイバーハイジーン：理解 KPI設定/定期評価：実施 | サイバーハイジーン：理解 KPI設定/定期評価：未実施

サイバーハイジーン：未理解 KPI設定/定期評価：実施 | サイバーハイジーン：未理解 KPI設定/定期評価：未実施

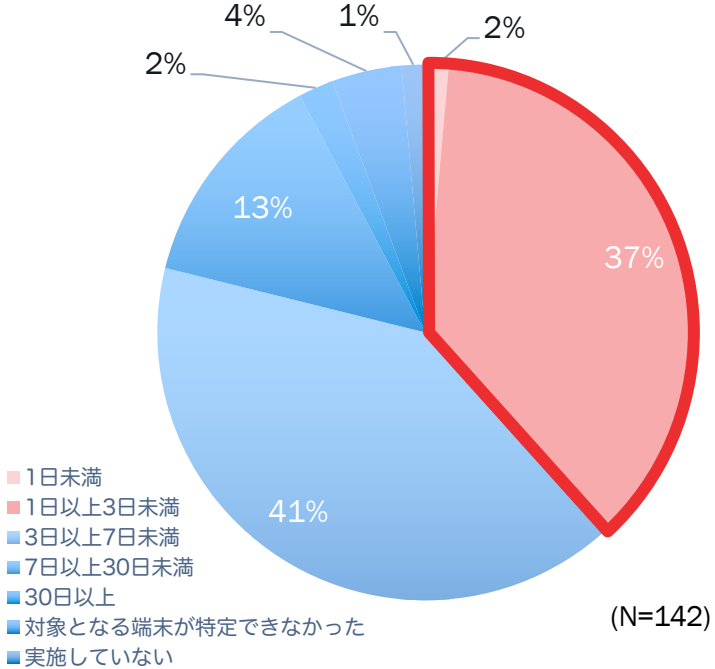
サイバーハイジーンをあまり知らない人の運用の結果には大きな差異は見られない。

サイバーハイジーン未理解 & KPI設定/定期評価実施



(N=36)

サイバーハイジーン未理解 &KPI設定/定期評価未実施



(N=142)

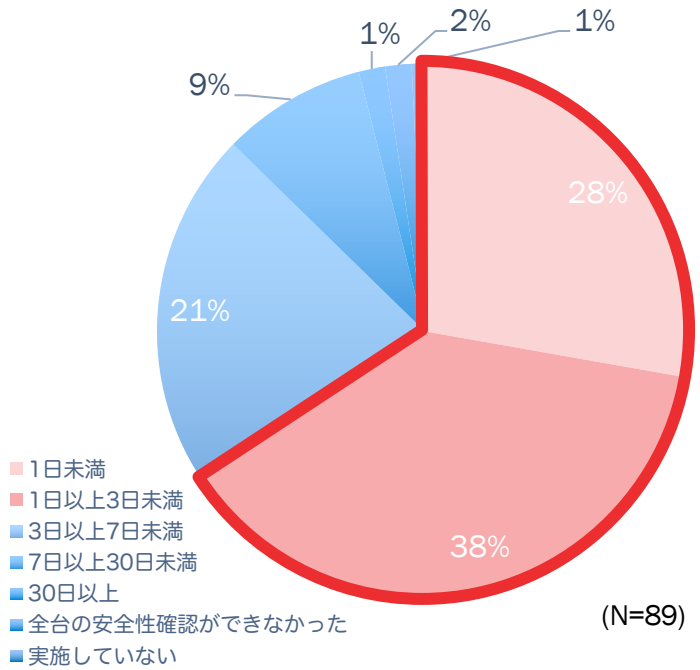
【絞り込み調査#3-1】安全性確認に要した時間

（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）

サイバーハイジーン：理解 KPI設定/定期評価：実施 | サイバーハイジーン：理解 KPI設定/定期評価：未実施
サイバーハイジーン：未理解 KPI設定/定期評価：実施 | サイバーハイジーン：未理解 KPI設定/定期評価：未実施

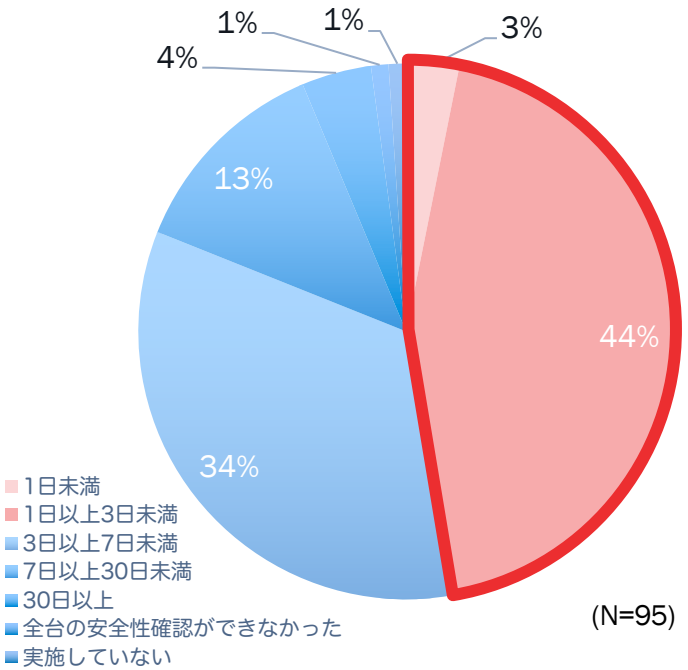
特に短期間での完了に顕著な差異。サイバーハイジーン徹底組織においては70%弱が3日以内に安全性確認完了。

サイバーハイジーン理解 & KPI設定/定期評価実施



(N=89)

サイバーハイジーン理解 & KPI設定/定期評価未実施



(N=95)

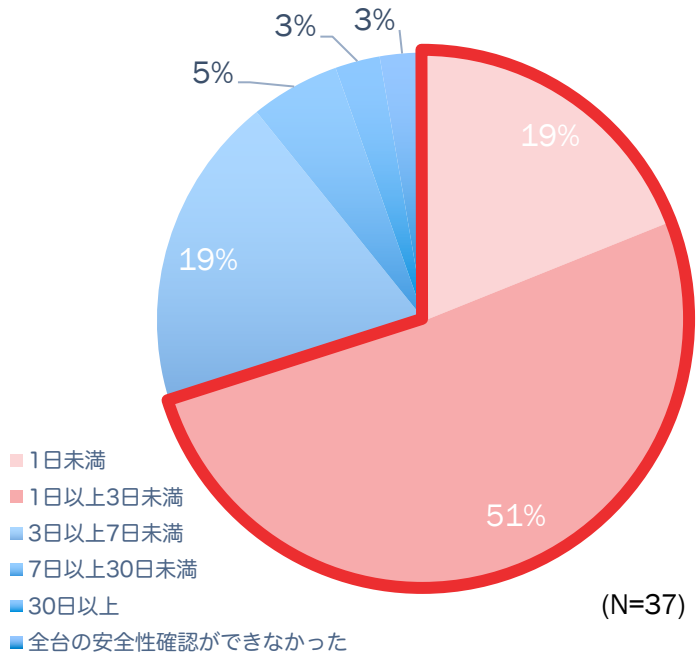
【絞り込み調査#3-2】安全性確認に要した時間

（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）

サイバーハイジーン：理解 KPI設定/定期評価：実施	サイバーハイジーン：理解 KPI設定/定期評価：未実施
サイバーハイジーン：未理解 KPI設定/定期評価：実施	サイバーハイジーン：未理解 KPI設定/定期評価：未実施

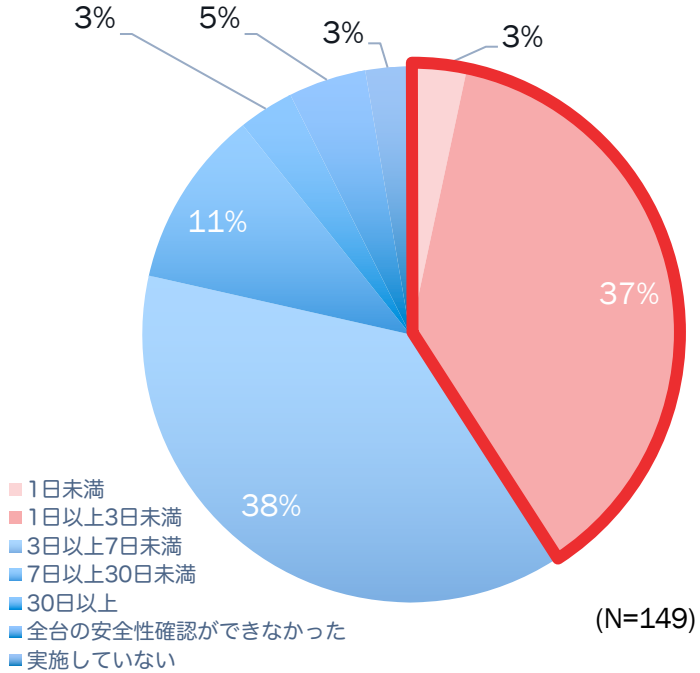
特に短期間での完了に顕著な差異。 KPI徹底組織においては70%が3日以内に安全性確認完了。

サイバーハイジーン未理解 & KPI設定/定期評価実施



(N=37)

サイバーハイジーン未理解 &KPI設定/定期評価未実施



(N=149)