国内サイバー・ハイジーン（衛生管理）調査結果について

タニウム合同会社

2021年12月7日

© 2021 Tanium. All rights reserved.

タニウムについて

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：2,000+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

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：東京都品川区
営業拠点：東京、大阪、名古屋

- 2% Give Backイニシアチブを通じた社会貢献を実践
- Fortune Best Workplaces In Technology 2021 に選出
- SC Awards Europe 2021において
  Best Enterprise Security および
  Best Customer Service を受賞

© 2021 Tanium. All rights reserved.

タニウムの採用実績

50%
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

5/6
米国軍組織
における採用数

2,760万
グローバルで管理している
エンドポイント数

日本国内における主な採用実績（例） *50音順. 法人格略

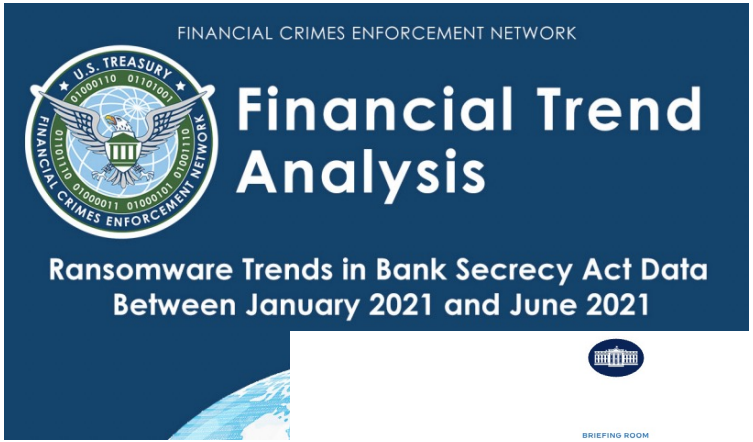
- NTTデータ
- 川崎重工業
- 京セラ
- 資生堂
- セガサミーホールディングス
- 福井県
- 全日本空輸
- 東急不動産
- 東芝デジタルソリューションズ
- 西日本電信電話
- 日本電気
- ベネッセホールディングス
- みずほフィナンシャルグループ
- 三井物産セキュアディレクション
- ローソン
- ヤンマー

© 2021 Tanium. All rights reserved.

サイバーセキュリティをめぐるトレンド - 1

倍増するランサムウェア被害

- 米国財務省 金融犯罪取締ネットワーク（FinCEN)のレポート *1によると、2021年上期（1月～6月）に
  - 635件のSARs(疑義のある案件)が報告
    - 2020年通期で報告された487件を既に30%上回る
  - 被害総額590百万ドル(約670億円)
    - 2020年通期の被害総額は416百万ドル(474億円)で、これを上期のみで42%上回る
- 2021年10月には、米国大統領官邸主導で30以上の国が参加しランサムウェア対策に対する多国間協議を2日間に渡って実施*2



*1 https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf
*2 https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

TANIUM
© 2021 Tanium. All rights reserved.

サイバーセキュリティをめぐるトレンド – 2

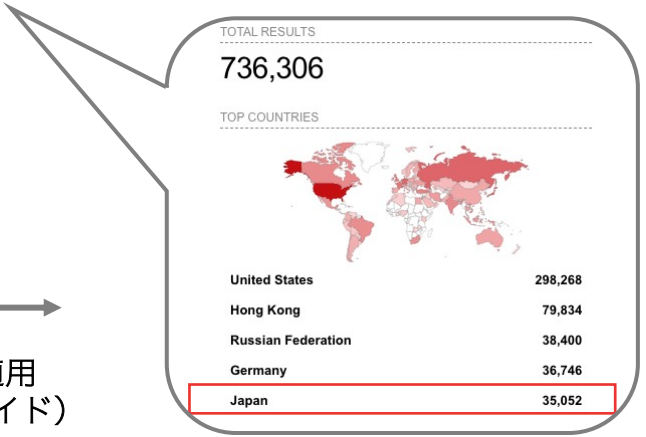
*1 IPAとは、情報処理推進機構の略称で、経済産業省管轄の独立行政法人。日本のIT国家戦略を技術面・人材面から支えるために設立された。

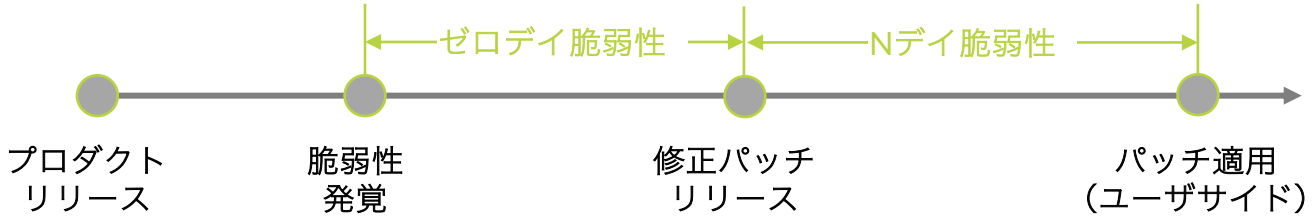
高まるNデイ攻撃のリスク

- IPA[*1]が本年8月に発表した「情報セキュリティ10大脅威2021」では「脆弱性対策情報の公開に伴う悪用増加」がランクイン
- Nデイ攻撃とは、既にソフトウェアに脆弱性が発見され、パッチが公開されているものの、当該パッチが適用されていない脆弱性（Nデイ脆弱性）を狙った攻撃
  - Nデイ攻撃は既に脆弱性が明確になっているので攻撃者にとって障壁が低い

【Nデイ脆弱性の具体例】

- 2017年5月に世界を席巻したWannaCryはそれ以前にマイクロソフト社が公開していたSMBv1の脆弱性を悪用したもの（通称EternalBlue, CVE:2017-0144）
- 2021年11月1日時点にオンライン検索エンジン「Shodan」で当該脆弱性(SMB v1)を内包している国内Windows端末は3万台以上存在





© 2021 Tanium. All rights reserved.

高まる外部脅威に対して組織が取るべき対策とは

バズワードは次々にうまれるが、基本方針は変わらない

IPAは2015年以来、情報セキュリティ対策の基本の第一項目として、脆弱性を解消し攻撃によるリスクを低減する目的のためにソフトウェア更新を行うことを一貫して提唱している

実現するためには

全ての対象端末の存在を把握していること（シャドーITの撲滅）

対象端末の資産情報（ソフトウェアバージョン等）をリアルタイムに監視できること

対象端末に対してソフトウェア更新を実施、かつその成否を確認できること

サイバー・ハイジーン（衛生管理）

© 2021 Tanium. All rights reserved.

システム更新を行わなかったことによる最近の情報漏洩

14,000名の個人情報が理化学研究所から流出

2021年11月5日
理化学研究所

← 前の記事　↑ 一覧へ戻る　→ 次の記事

学習管理システムからの情報流出の可能性について

このたび、理化学研究所（理研）が職員などの教育・研修に利用している学習管理システム（学習教材の配信や成績などを統合して管理するシステム）に対して不正アクセスがあり、登録されていたサービス利用者の個人情報が流出した可能性が高いと考えられ、所要の対応をとっております。

関係者の皆様にご迷惑とご心配をおかけする事態になりましたことを心よりお詫び申し上げます。

現時点で判明している事実等につきまして、下記の通りご報告いたします。

経緯

9月24日（金）13時頃、理研が利用している学習管理システムのサービス提供業者より「サーバーに対し外部から不正アクセスがありファイルが改ざんされた」との報告がありました。調査報告を受けた結果、理研からサービス提供業者に改善を要求していた既知の脆弱性を突かれ、ファイルの改ざんだけでなく何らかの命令が実行されたことが判明しました。

ファイル改ざんによる命令実行によって学習管理システムのデータベースに登録されている約1万4000件の個人情報が流出した可能性が高いと認識しております。

9月の事案の発表が11月にずれ込んだことを、理研は「被害状況の調査に時間がかかっていた。結局、流出の可能性があるというところまでしか分からなかった」と説明[*1]

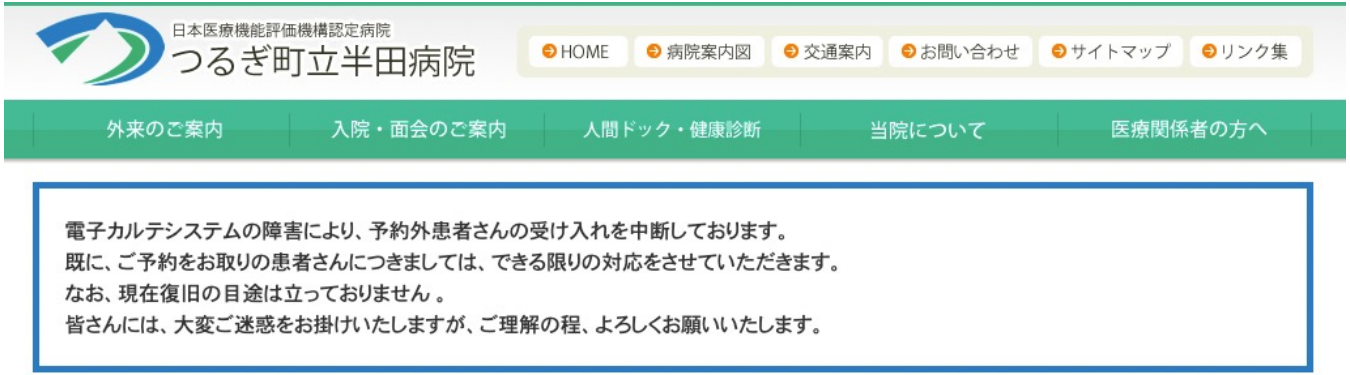
全端末をリアルタイムに監視・管理できていれば被害は最小化した可能性

*1 ITmedia news (https://www.itmedia.co.jp/news/articles/2111/05/news157.html) 2021/11/6 last access

© 2021 Tanium. All rights reserved.

いま、そこにある脅威

大企業ばかりが狙われるわけではない、脅かされる市民生活

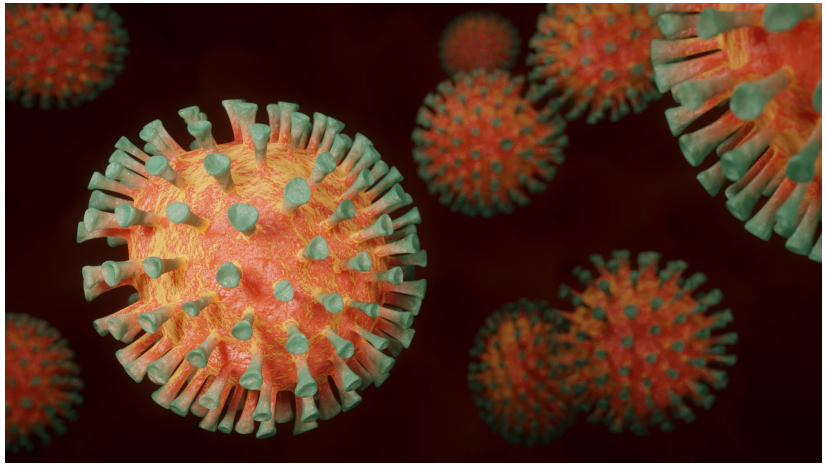


- 徳島県 つるぎ町立半田病院は2021年10月31日、ランサムウェアに感染したと発表
  - 8万5千人の電子カルテシステムの利用中止
  - 感染以降、新規患者受付中止が続く
  - 美馬市内の休日診療や救急患者の搬送などに影響
  - 11月3日の休日に一日かけて復旧にあたるもシステムは回復せず
- 身代金は支払わず、新システム構築を決定（2億円規模の投資）
- VPN（ネットワーク機器）の既知の脆弱性をつかれた攻撃の可能性が判明

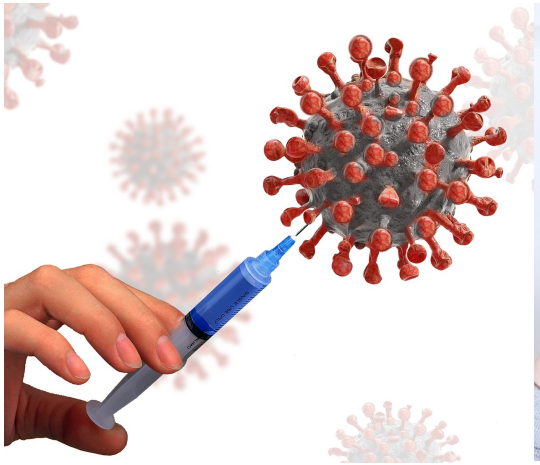
© 2021 Tanium. All rights reserved.

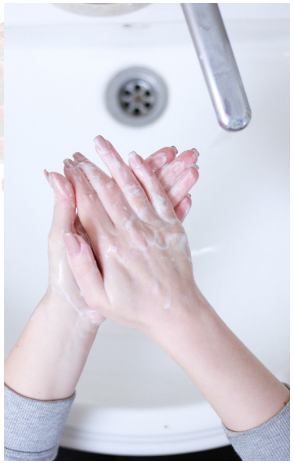
サイバー空間において習慣化すべきこと＝ハイジーン

脆弱性というウイルスが蔓延：不衛生な状態



脆弱性への耐性を強化する：衛生的な状態





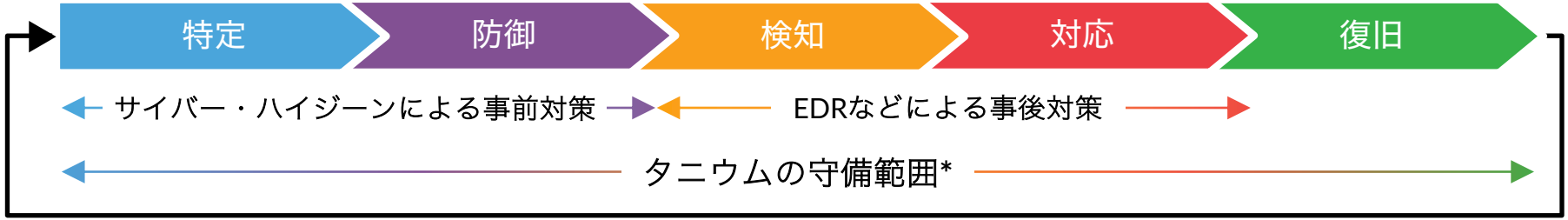
サイバー・ハイジーン（衛生管理）こそが組織耐性（免疫）を高める

※ 対処療法（例：治療薬）は、何かしらの被害が発生してしまう

© 2021 Tanium. All rights reserved.

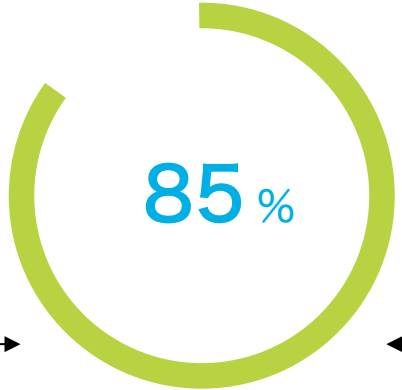
サイバー・ハイジーンの実証されている効果

米国標準技術研究所が定義するサイバーセキュリティフレームワーク (NIST CSF)



Government of Canada

カナダ サイバーインシデントレスポンスチーム(CCIRC)
Top 4 Strategies to Mitigate
Targeted Cyber Intrusions



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

米国国土安全保障省 (CISA)
Top 30 Targeted
High Risk Vulnerabilities

サイバー・ハイジーンの防御効果

© 2021 Tanium. All rights reserved.

*EPP機能を除く

サイバー脅威への堅牢な対策はガバナンス強化そのもの

ESG経営が叫ばれる昨今、”Governance”で検討すべきは
グループ企業ガバナンスとグローバル・ガバナンス
従来サイバーセキュリティを高い次元で実現してきた本社機能に加えて
サプライチェーンまで視野に入れ、リアルタイムかつ網羅的な
資産ならびに脆弱性の可視化ならびに管理・対処が不可欠

サイバー・ハイジーンの先進国であるアメリカ合衆国では、
20年以上にわたって、サイバー・ハイジーンの重要性を
連邦政府が主導しながら、民間企業を含めて確立してきた

© 2021 Tanium. All rights reserved.

米国におけるサイバー・ハイジーンを取り巻く歴史 - 1

- **2000年　サイバー・ハイジーン[Cyber Hygiene]という言葉が公の場で初めて提唱される**
  - 「インターネットの父」として有名なヴィンセント・グレイ・サーフ氏が提唱
  - 同年2月に開催された合衆国議会(上下両院合同経済委員会)においてセキュリティの状態を幅広く常に”衛生的な状態“にあるようにするためのプロセスならびに、ベストプラクティスとして言及
- **2013年　重要インフラのサイバーセキュリティ強化に向けた法令の公表**
  - 大統領令13636号（Executive Order：EO-13636）「重要インフラのサイバーセキュリティの向上」
  - 大統領指令21号（Presidential Decision Directive：PPD-21）「重要インフラのセキュリティと回復力」
- **2014年　重要インフラを対象にCyber Security Framework (CSF) version1.0が公開**
  - NIST (National Institute of Standards and Technology：米国国立標準技術研究所) が上述のEO-13636の具現化措置としてフレームワークを公表
- **2015年　CSF version1.0をもとに、SP800-171が策定**
  - SP800の一連の文書はNIST内でコンピュータセキュリティを担当するCSD (Computer Security Division) が発行するコンピュータセキュリティ関係のレポート
  - 米国政府機関がセキュリティ対策を実施する際に利用することを前提にしつつも、政府／民間を問わ参照される
  - SP800-171では民間企業が取り扱うべき「CUI（Controlled Unclassified Information）」の指針が示される
  - 国防総省がいち早く取引先企業（米国外企業であっても）にSP800-171への準拠を要求

© 2021 Tanium. All rights reserved.

米国におけるサイバー・ハイジーンを取り巻く歴史 – 2

- **2017年　アメリカ議会両院に対して”Promoting Good Cyber Hygiene Act”法案が提出される**
  - 超党派の支持をもって、両院に対してITシステムを衛生的に保つことを目的に法案が提出
    - NISTが重要インフラ以外の政府機関、民間、個人に向けたサイバーセキュリティに関連するベストプラクティスを取りまとめること
    - DHS (Department of Homeland Security: 米国国土安全保障省)に対して、行政機関にたいして行われるサイバー攻撃ならびにそれらへの対処方針を策定すること
- **2018年　CSF version1.1が策定・公開**
  - CSF version1.0との互換性を担保しながら、対象を重要インフラ以外に拡張
  - サプライチェーンにおけるリスク管理について増補
- **2018年　DHSがAWAREリスク管理ツールを公開**
  - 政府関係機関が準拠すべきセキュリティ管理のプロセスを標準化し、組織をまたいでセキュリティ管理方式の底上げを図る
- **2021年　バイデン大統領が「国家のサイバーセキュリティ向上に関する大統領令」を発令**
  - 攻撃に対する事後対応から予防へとサイバーセキュリティの重点を移行させる方針
  - ITだけではなくOTも対象に含まれ、システム構成もオンプレミス・パブリッククラウド・ハイブリッドクラウドを問わない
  - 2020年のSolarWinds社へのハッキングや21年5月のコロニアル・パイプラインへのランサムウェア攻撃などを踏まえた対応
  - 米国国家安全保障局の報道官は発令にあたって「端的に言って、把握していないものは修復しようがない」と発言[*1]

*1 ロイター EXCLUSIVE-Software vendors would have to disclose breaches to U.S. government users under new order -draft | Reuters (Last access Oct 22)

© 2021 Tanium. All rights reserved.

日本におけるサイバー・ハイジーンへの取組

タニウムは2014年の東京オフィス設立以来、一貫してサイバー・ハイジーンの重要性を提唱

- **2015年　サイバーセキュリティ基本法施行**
  - サイバーセキュリティ戦略本部発足
  - 内閣サイバーセキュリティセンター（NISC）設立
- **2018年　我が国における最初の「サイバーセキュリティ戦略」を閣議決定**
- **2019年　改正サイバーセキュリティ基本法施行**
  - TOKYO2020開催を視野に改正実施
  - リオやロンドンでのサイバー攻撃事例を踏まえ、民間を巻き込んだ体制＝サイバーセキュリティ協議会発足
- **2021年　次期サイバーセキュリティ戦略を閣議決定**
  - サイバー犯罪への対策としては、（中略）サイバーハイジーンを実践出来る環境を構 築するため、各主体を対象として、サイバーセキュリティに関する意識・知識の向上（中略）広報啓発活動を実施する
  - 民間分野を含めたサイバーハイジーンの確保に資する産官学連携による実務的な協力活動の充実を進めることが求められる

© 2021 Tanium. All rights reserved.

国内におけるサイバー・ハイジーン（衛生管理）に関する調査結果

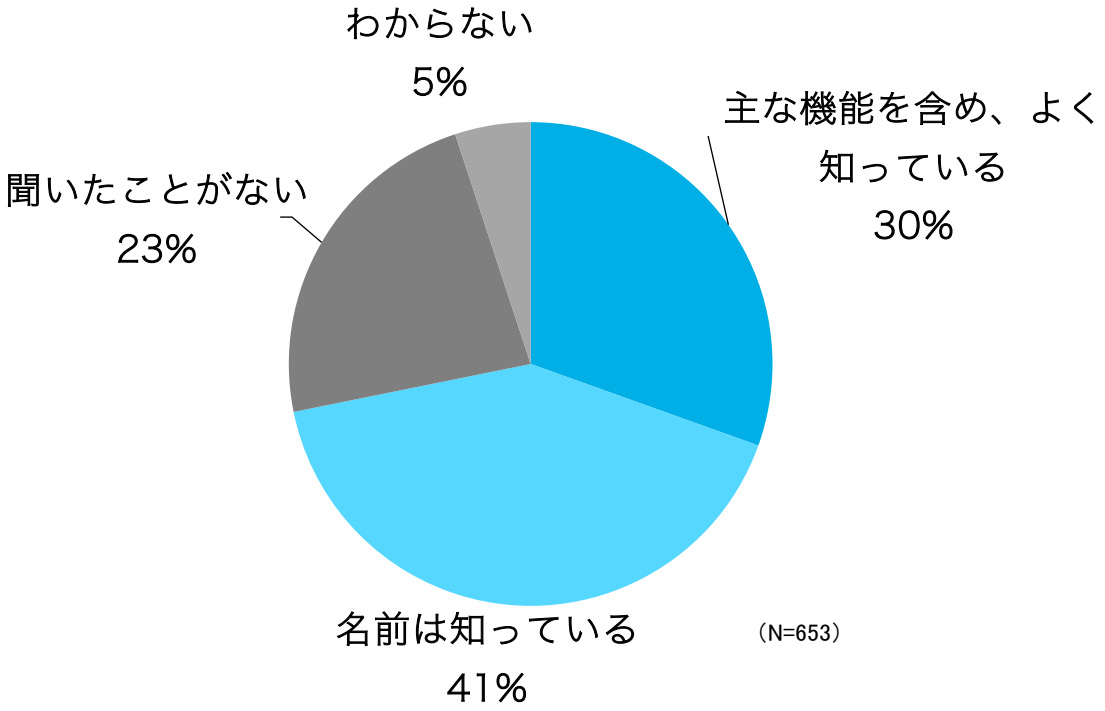
調査対象：大企業のサイバーセキュリティ意思決定者6,711名（有効回答数653件）

調査方法：Webアンケート

実施期間：2021年9月13日～2021年9月14日

国内におけるサイバー・ハイジーンの認知度

用語の浸透度は7割に達するも、まだ市場の理解は成熟していない

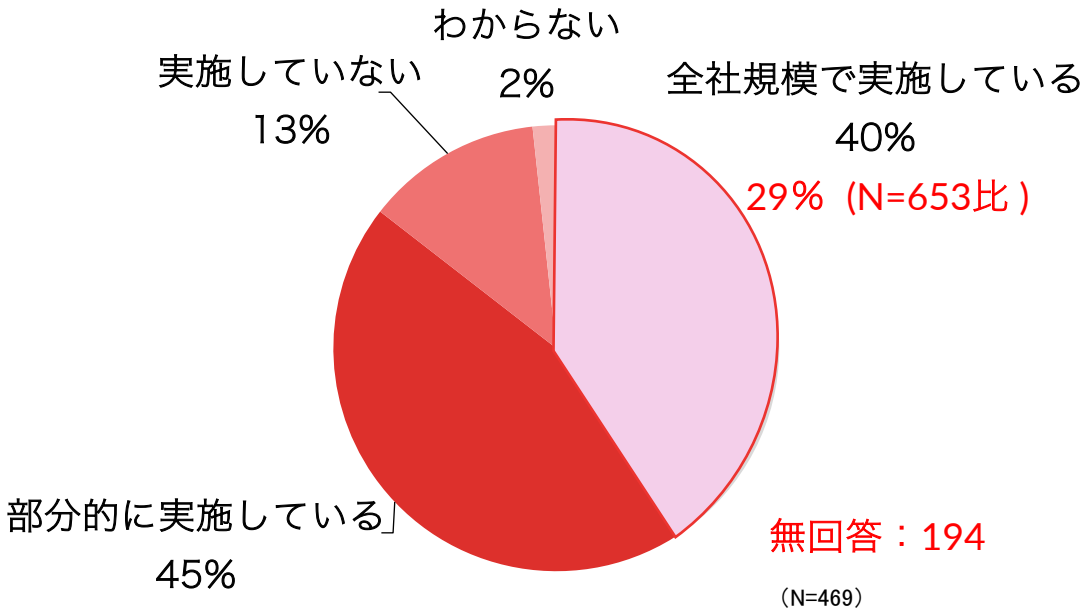


タニウム考察

- ソフトウェア更新、脆弱性管理など、サイバー・ハイジーンを構成する従来から存在する手法は理解されていると想定
- サイバー・ハイジーンの全体像をしっかりと理解できている組織はまだまだ少ないと想定される
- ポイントは全数管理ならびに、リアルタイム管理

© 2021 Tanium. All rights reserved.

国内におけるハイジーンの実施割合

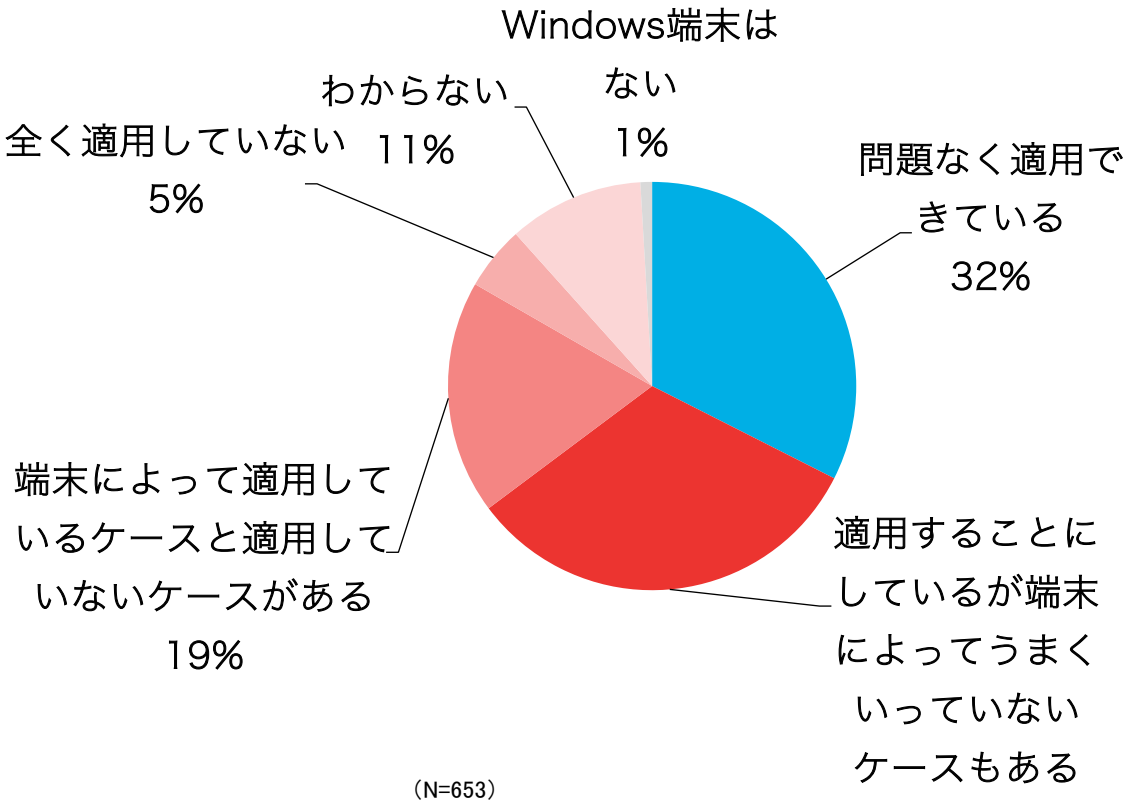


タニウム考察

- ハイジーンを実施出来ていない組織が6割強
- 当設問への回答は全体の7割にとどまる
- アンケート実施母数に対して全社規模でハイジーンを実施している組織の割合は29%にとどまる
- 本来、組織全体でハイジーンを行わない限り、ハイジーンの効果は限定的

© 2021 Tanium. All rights reserved.

国内におけるWindows 10 FUの適用状況



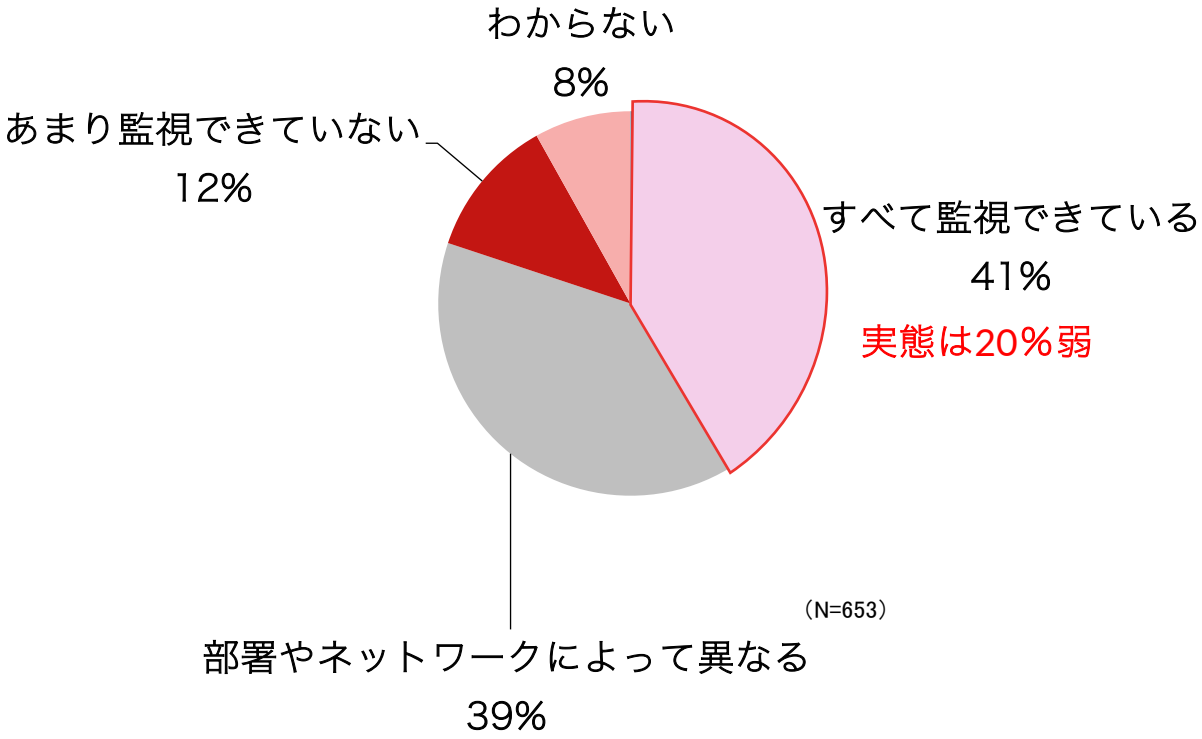
タニウム考察

- 多くの組織で採用されているWindowsのFeature Updates (機能更新プログラム）を問題なく適用できているのは3割
- うまく適用できていないと答えた組織が3割
- 結果、約7割の端末群がNデイ脆弱性を抱えたまま組織内で活用されていることが明らかに

© 2021 Tanium. All rights reserved.

クライアントPCへの自社指定必須ソフトの導入状況

4割の組織がすべて監視できていると回答するものの、実態との乖離が存在する可能性



タニウム考察

- 回答者の約4割が「すべて」監視できていると回答
- 別調査から、組織のIT部門が管理できている端末群は全体の45%に過ぎないという結果（次ページ参照）
- 総合的に組織端末の20%弱程度にしか、自社指定ソフトの導入状況を監視できていないことが本調査結果とあわせ明らかに

© 2021 Tanium. All rights reserved.

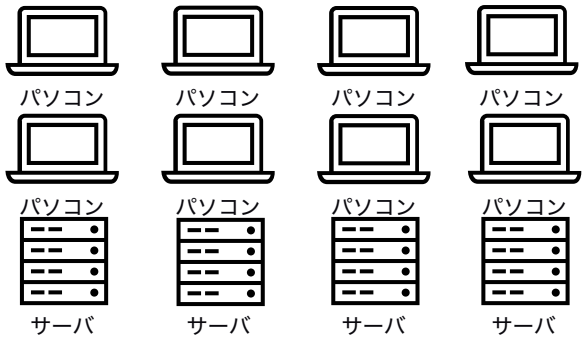
見えないものは守れない

自社の端末を100%見える化出来ている企業はほとんどないという事実

脆弱性の温床となる不衛生な端末が半数以上の実態*

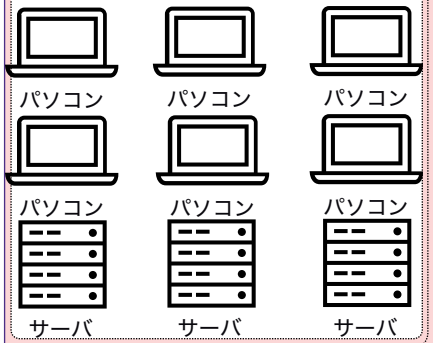
ハイジーン出来ている端末群
約45%

資産管理は出来ている端末群
約85%

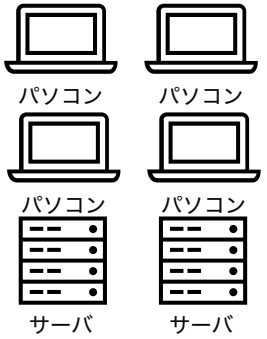


ハイジーン出来ていない不衛生な端末群
約55%

パッチ等の低い適用率
約40%



非管理端末群
約15%

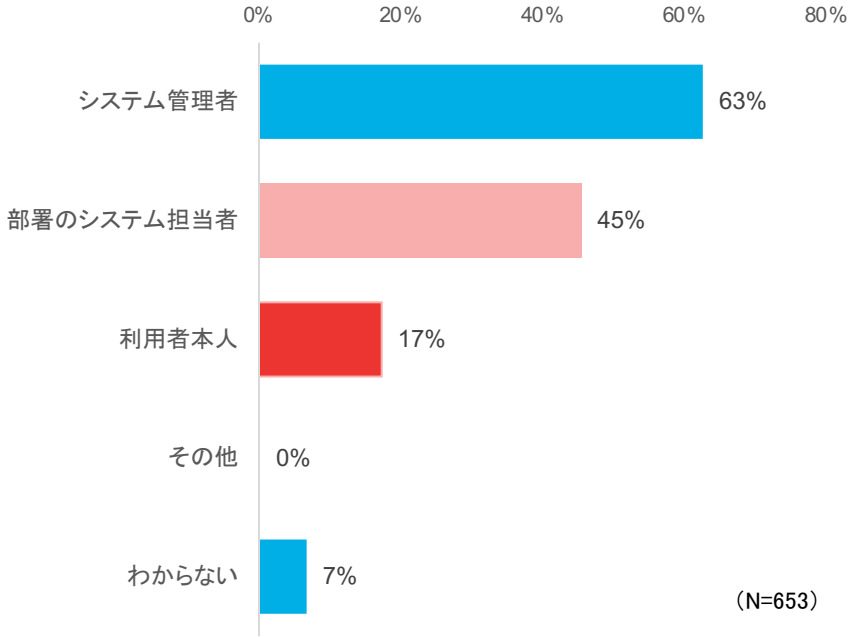


*タニウム 日本国内での独自調査 (2021)

© 2021 Tanium. All rights reserved.

管理者権限の付与状況

約2割の組織が利用者本人に管理者権限を付与　（複数回答設問）



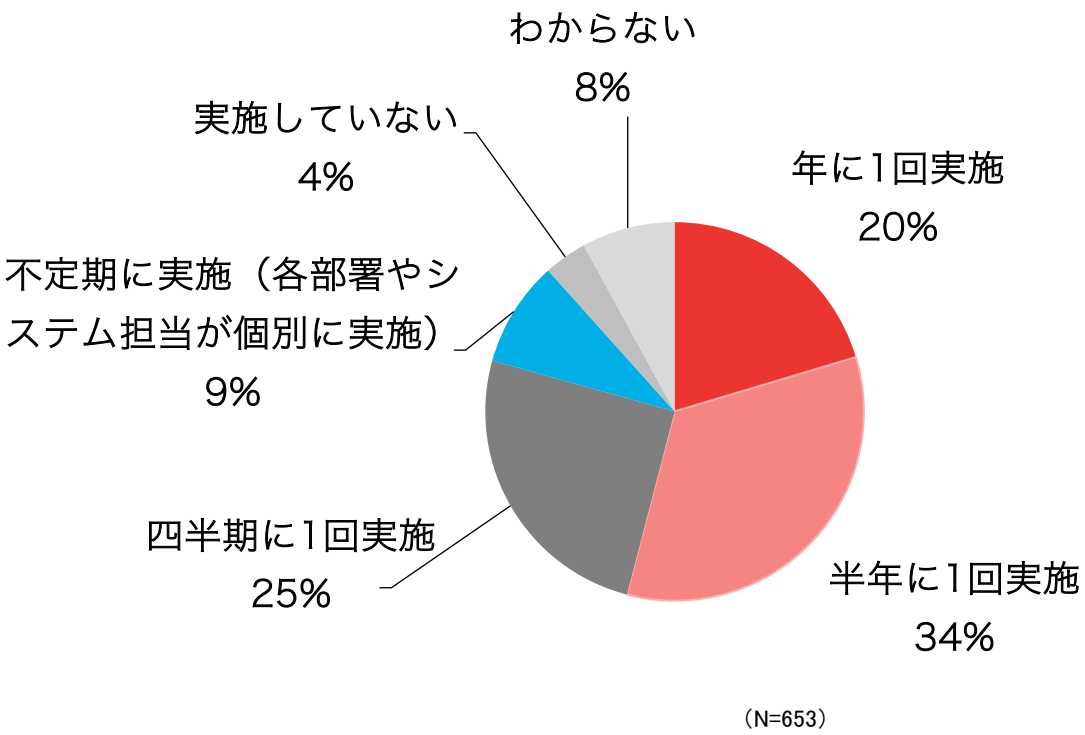
*1 ラテラルムーブメントとは、攻撃者がセキュリティレベルの低い端末等からシステムに侵入し、その後組織内システム内で各種機密リソースにアクセスし、最終的に特権ID等を乗っ取り組織システムの根幹（たとえば、ドメインコントローラーなど）の制御を奪ってしまうこと。企業システムの停止、ビジネスオペレーションの停止が発生することから、企業への財務的損失も大きくなる

タニウム考察

- 部門ごとや、利用者本人に特権ID／管理者権限を付与している企業が約6割
- 特権IDを活用した各種セキュリティリスク（例：標的型攻撃、内部不正による情報漏えい）に対して改善機会が多く存在
- 昨今課題となっているラテラルムーブメント*1による特権ID昇格等への対策も急務

© 2021 Tanium. All rights reserved.

資産管理（IT資産の棚卸し）の頻度



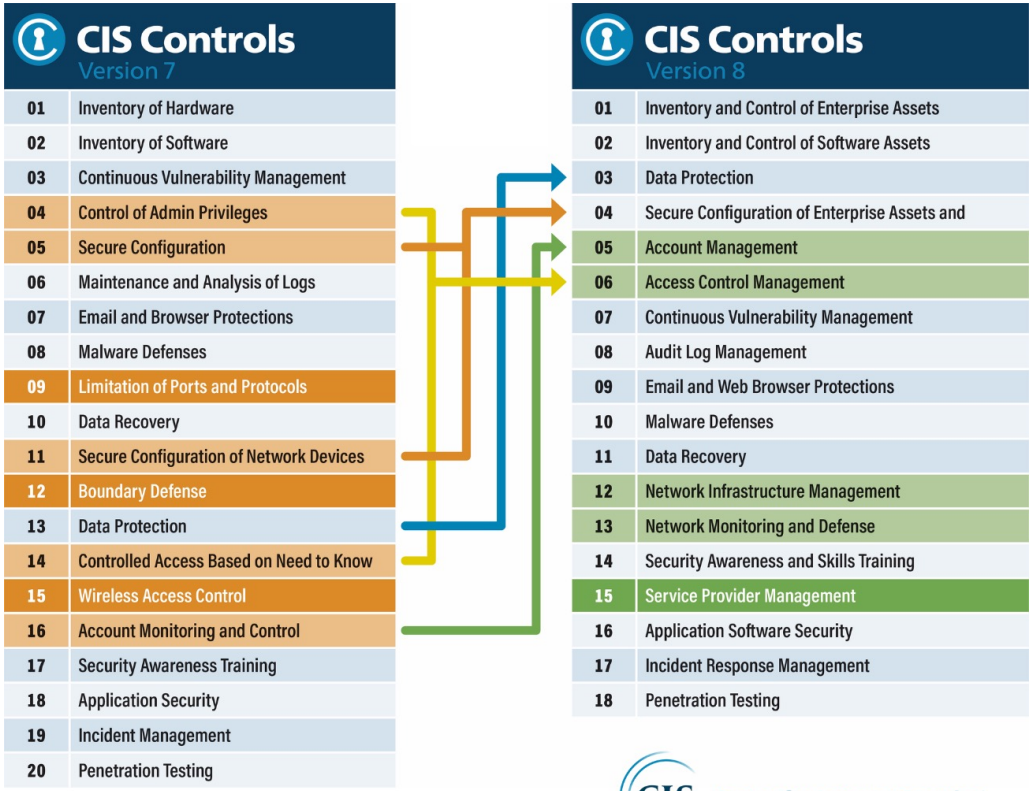
（N=653）

タニウム考察

- 半数以上の企業は半年に1回ないし、年に1回のみの実施
- これらの組織において、資産管理は会計上の固定資産管理の枠組みで実施されているものと想定
- P16のサイバー・ハイジーン実施状況（総数の29%）と比較しても、リアルタイム性をもって実施している組織は少なく、実態に課題

© 2021 Tanium. All rights reserved.

CIS Controls v8でも資産管理が最重要項目として規定



CIS Controls Version 7	
01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

CIS Controls Version 8	
01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

CIS Center for Internet Security®

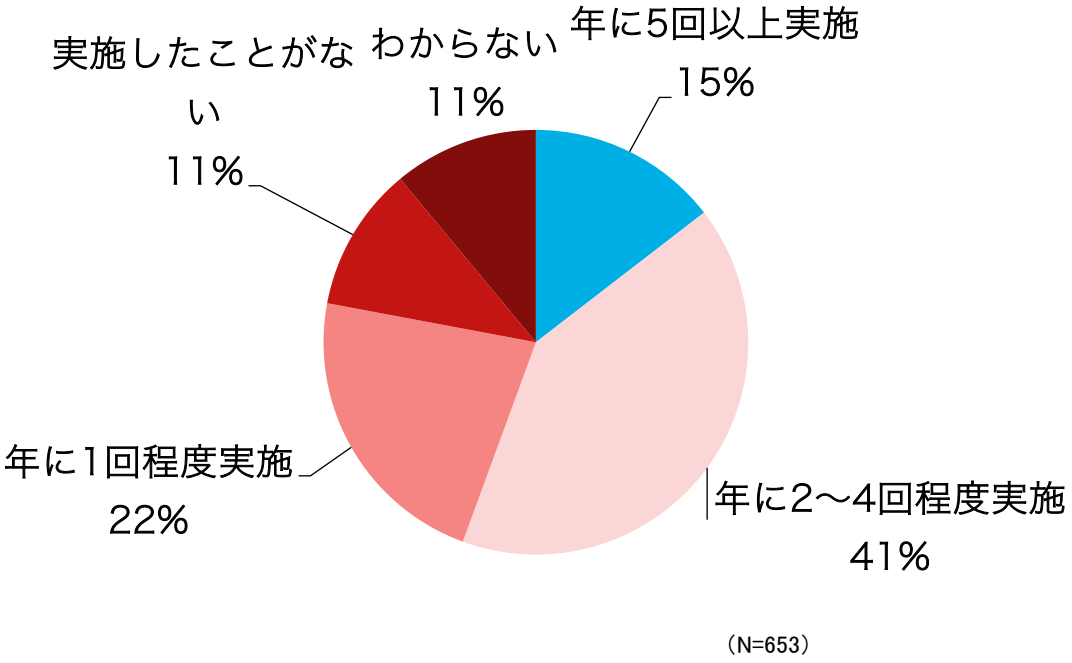
(引用) https://www.sans.org/blog/cis-controls-v8/

- 米国CIS （Center for Internet Security）がNISTが規定するSP800-53のサブセットとして「最初に最低限実施すべきこと」としてまとめたフレームワーク
- 2021年5月に最新のVersion8が公開
- Version7からいくつかの変更が行われているが、重要度の最も高い上位2項目は引き続き、ハードウェア資産管理と、ソフトウェア資産管理

© 2021 Tanium. All rights reserved.

脆弱性対応の頻度

コンスタントに脆弱性対応を実施できている組織は15%にとどまる



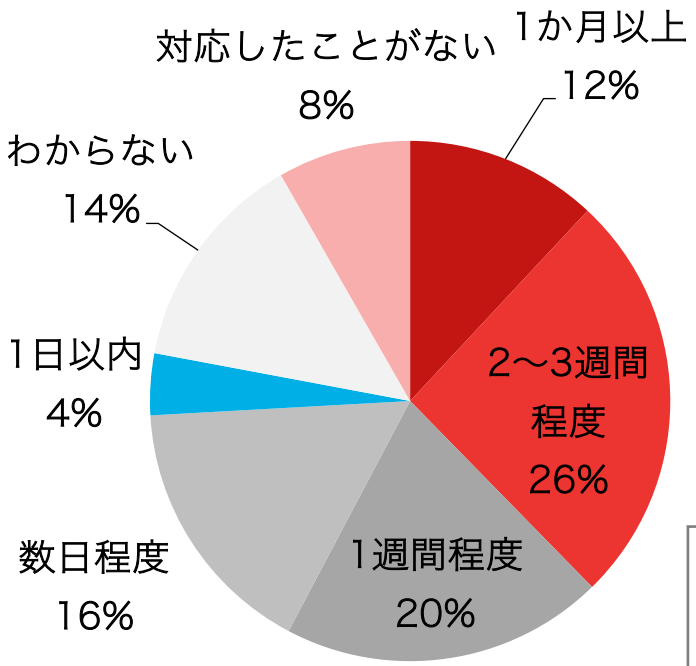
（N=653）

タニウム考察

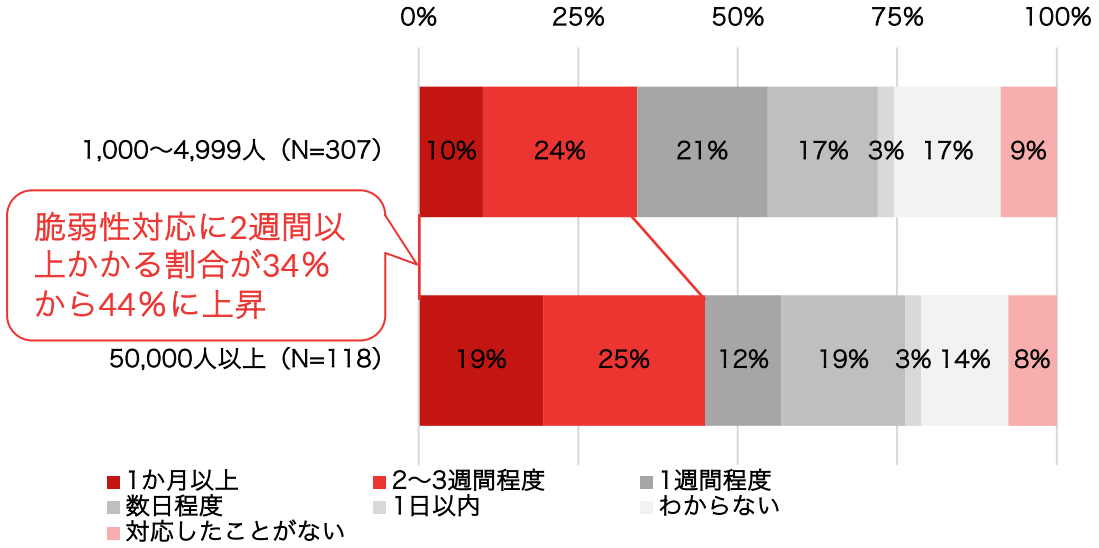
- 85%の組織は脆弱性対応は四半期に1回以下の頻度
- CIS Controls v8では重要度7位に継続的な脆弱性管理があげられている
- 「パッチ適用でシステム影響が出るのは怖いので塩漬け」という発想から「セキュリティパッチは適用、システムに影響が出た場合は改修を検討」への変更が必要

© 2021 Tanium. All rights reserved.

脆弱性対応にかかる日数のトレンド



（N=653）

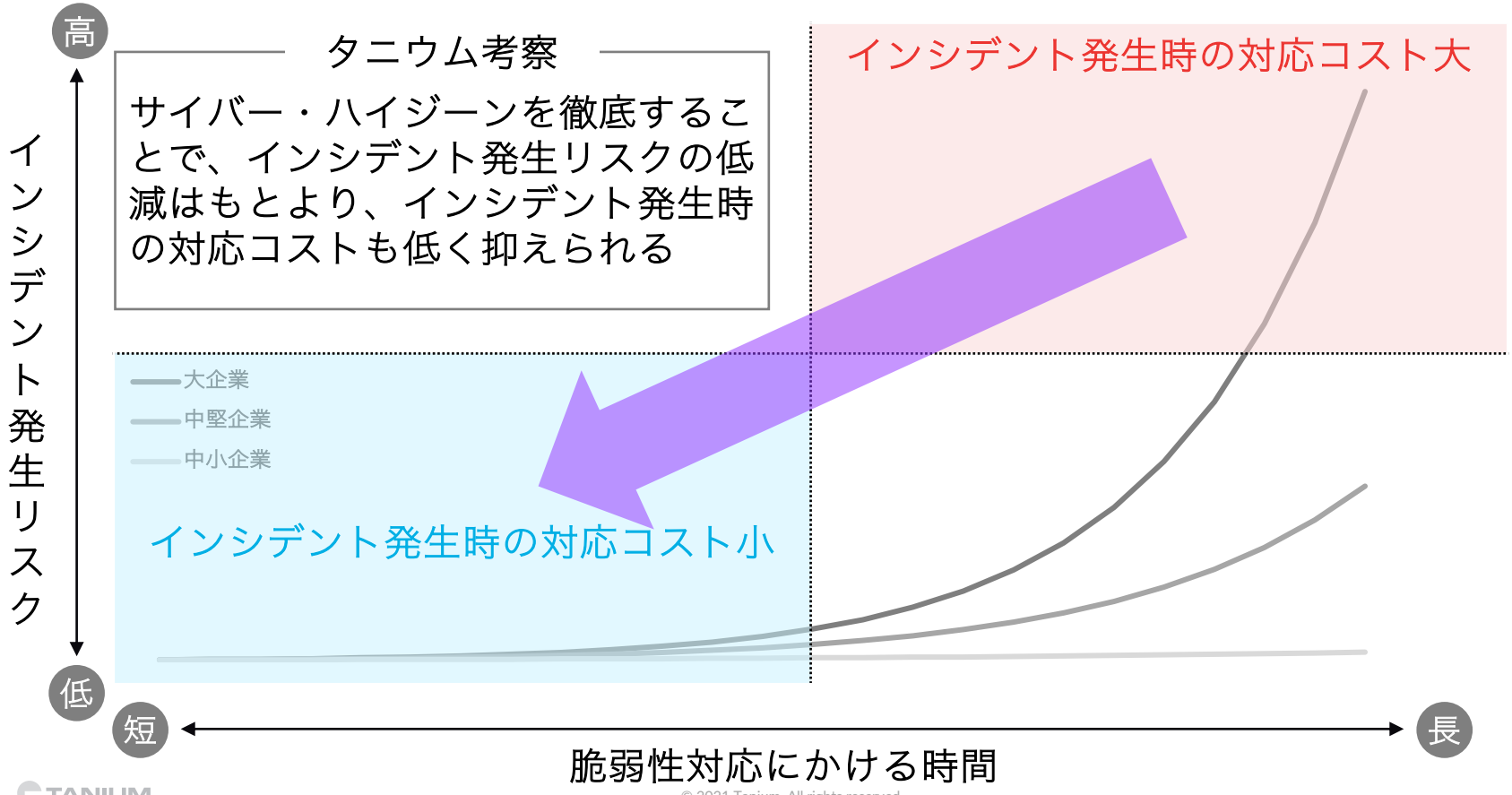


タニウム考察

- 約4割の組織が脆弱性対応に2週間以上かける
- 企業規模が大きくなるほど、脆弱性対応に日数が必要
- 即日対応できている組織は全体の4%にとどまる

© 2021 Tanium. All rights reserved.

脆弱性を放置することでリスクは指数関数的に増大



© 2021 Tanium. All rights reserved.

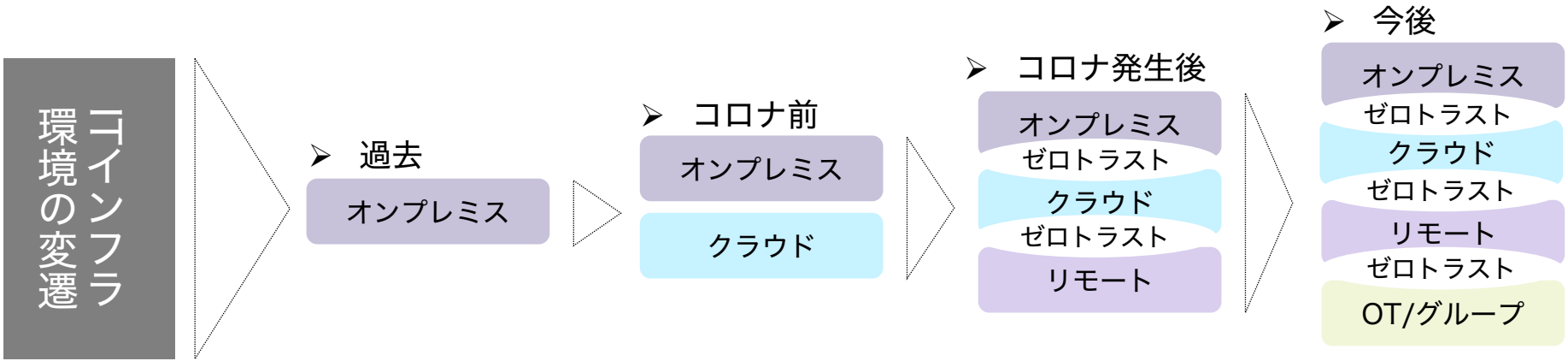
市場調査結果を踏まえてタニウムからの提言

セキュリテイ対策の第一歩

サイバー・ハイジーンの徹底を！

加速的に重要度が増すサイバー・ハイジーン対応

HQのガバナンス(責任)範囲は、全数拠点＋全数端末のマルチドメイン



➢ セキュリティ境界	1箇所	2箇所	2＋PC/サーバ台数分	2 ＋PC/サーバ台数分
➢ HQのガバナンス範囲	1箇所	2箇所	3箇所	3＋グループ/OT数分
➢ 重要情報資産分布	PC/サーバ台数分	PC/サーバ台数分	PC/サーバ台数分	PC/サーバ台数分

© 2021 Tanium. All rights reserved.

サイバー・ハイジーンを徹底することで得られるメリット

経営者

うちは大丈夫か？

ガバナンス範囲を母数とした
リアルタイムで網羅的な情報

迅速な意思決定

経営が常に求められる
安全宣言や説明責任の責務

システム部門

パッチあたった？

全ての資産状況を
リアルタイムに確認

俊敏な対応と修繕

新たな脆弱性が発見される度
自社への影響度を正確に把握
かつ、対応策を実施可能

ユーザー部門

在宅続けていい？

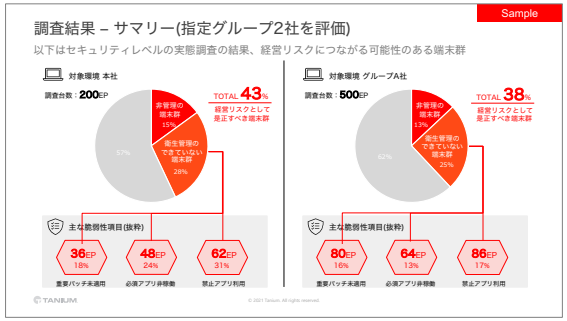
リモートワーク等の
新しい働き方を安全に実装

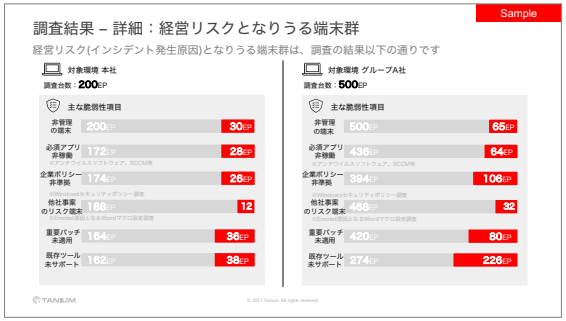
高い市場からの評価

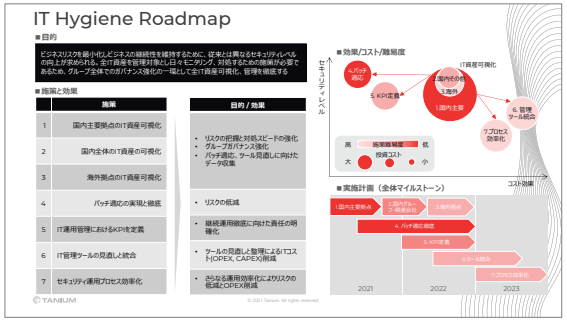
従業員満足度を向上させ
市場からの格付け評価等を
向上させていくことが可能

© 2021 Tanium. All rights reserved.

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

50+社

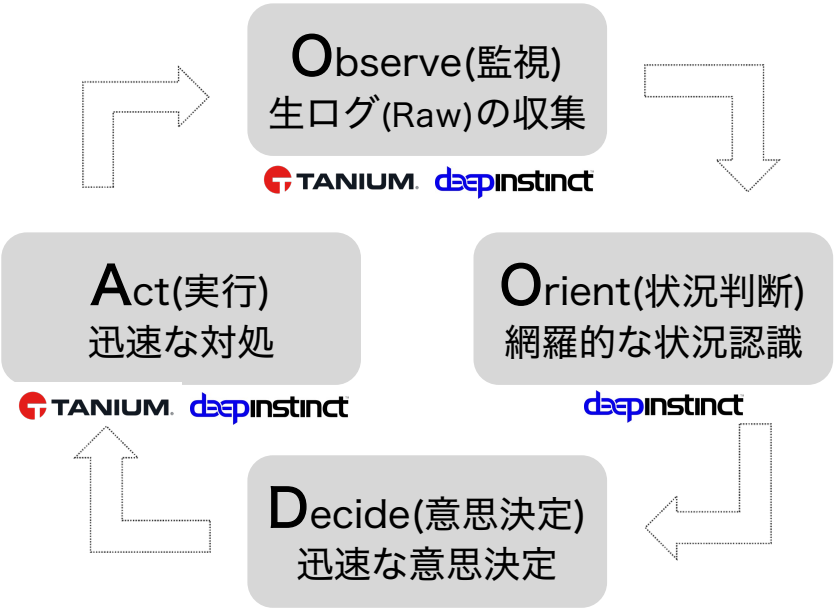
アセスメントを体験されたお客様

© 2021 Tanium. All rights reserved.

ハイジーンを実現した次に考えるべきこと

サイバーセキュリティ対策における後工程（サイバー・レジリエンス）の強化＝OODAループの採用

米空軍で提唱された「軍事行動における指揮官の迅速な意思決定」の理論



- エンドポイントに求められること
  - 状況把握に必要な生ログ、Rawデータをリアルタイム且つ網羅的に収集出来る
  - HQがダッシュボードで、グローバルの実態を常にモニタリングが出来る
  - 意思決定された対処策を全数端末に対しリアルタイムに制御が出来る

高度なレジリエンスを実現する

© 2021 Tanium. All rights reserved.

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