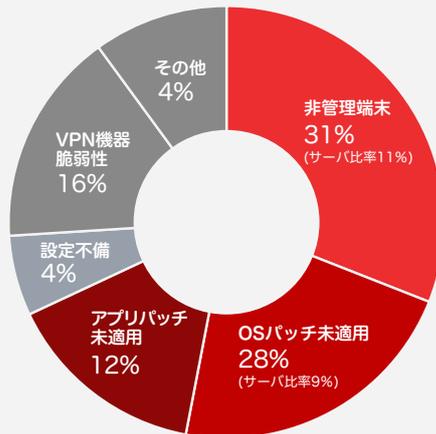


いま脆弱性管理に求められる サイバーハイジーンの実現

脆弱性の管理 できていますか？

近年発生するサイバー事故の約99.6%は「既知の脆弱性」が悪用されています。言い換えれば、日常的なパッチ適用とサーバを含む全資産管理を徹底することで、ほとんどのサイバー・セキュリティ・インシデントは抑止できるということです。しかし実際にこれを実現できている企業は決して多くはありません。そこには、情報システム部門やセキュリティチームにとって悩ましいとも言える課題があります。



サイバー事故
(事案)要因は
99.6%が
既知の脆弱性

(サーバが初期攻撃の対象となることも)

※出典：2019年～2022年4月末：
25組織(政府機関/自治体/民間企業)の国内の
セキュリティ機関と弊社の合同調査結果より

管理者が向き合う脆弱性対策の課題

サイバー攻撃の増加

昨今では国防課題にもなっているランサムウェアを始め、脆弱性を狙ったサイバー攻撃は増加の一途を辿っており、対応する側にも頻度と工夫が求められ管理負荷が大きくなっています。

グローバル機関が公開した 頻繁に悪用された脆弱性 TOP15の内訳*

Windows関連	9件
アプリケーション関連	2件
SaaS/ISP(基盤)関連	2件
ネットワーク機器関連	2件

※引用: Alert (AA22-117A) 2021 Top Routinely Exploited Vulnerabilities
(<https://www.cisa.gov/uscert/ncas/alerts/aa22-117a>)

資産の分散・多様化

リモートワークの拡大やDX推進、ビジネスのオープン化など環境の変化に伴い企業のIT資産やロケーションも分散・多様化し、一貫したリスク評価での資産全体管理が困難になってきています。

実際の企業のケース

そもそも 非管理の端末*	管理下の 脆弱性保有端末*
約 10%	約 87%

※タニウムのリアルタイムセンサーを導入した実環境調査より
(端末全数330台)

対策の遅延・タイムラグ

さまざまなソフトウェアのパッチ配布や導入済EDRの正常稼働、端末の各種設定など、恒常的且つ膨大な環境健全化をリアルタイムで行うことは業務負担が大きく、正確性の維持が困難です。

実環境における測定

Windows FUの適用率*	セキュリティツール 利用率の可視化
6か月で 約 60%	不可能

※実環境(2万台/150拠点)における効果測定に基づく

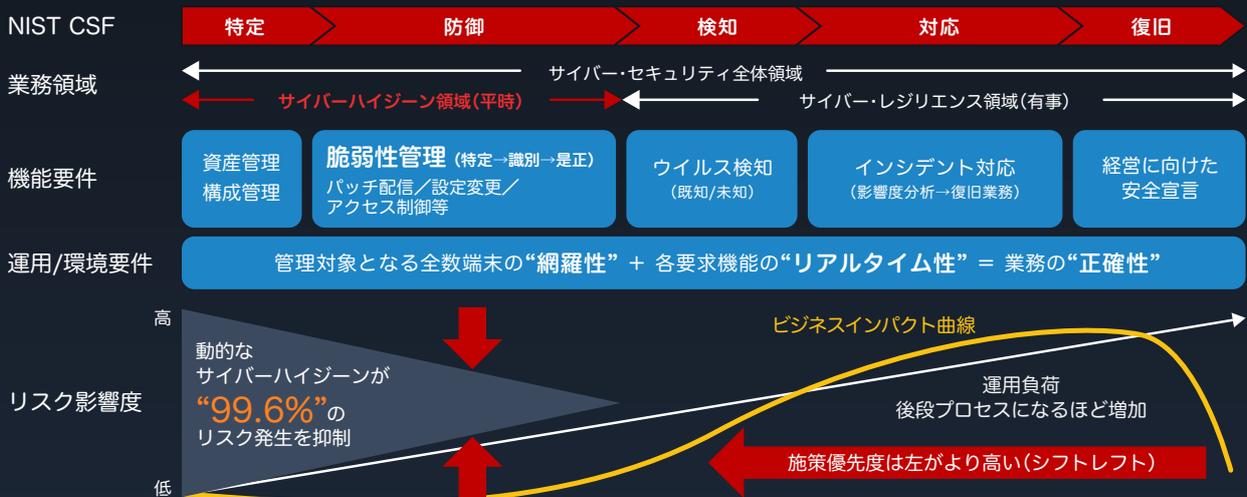
このような脆弱性対策における課題はサイバーハイジーンに取り組み「**モダン脆弱性管理**」を実現することで最小化できます！

網羅性・リアルタイム性・業務の正確性を備えた運用

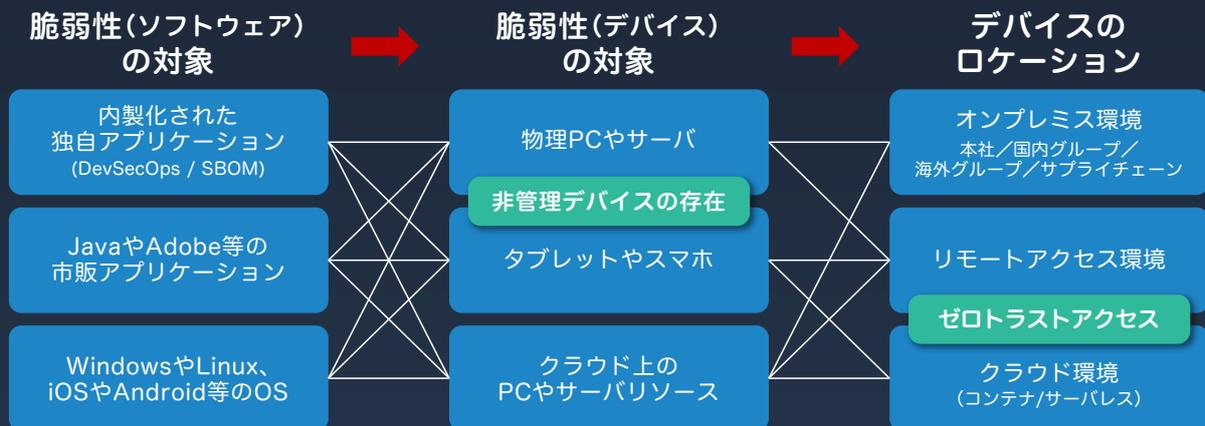
サイバーハイジーンで実現する”点から面へのシフト” = “モダン脆弱性管理”

既知の脆弱性を可能な限り排除し、衛生的なIT資産環境を継続的に維持するサイバーハイジーンは、近年国際的な機関でも強く提唱されており、セキュリティ・フレームワークの初期段階でリスクを大幅に抑制する取り組みとして優先度の高い施策とされています。Taniumは、多様化、分散化が進む企業のIT資産環境に対し、網羅性とリアルタイム性を備え、管理業務の正確性を担保できる、より高度なサイバーハイジーンによる「モダン脆弱性管理」を推奨しています。

リスク母数を抑えビジネスへの影響と運用負荷を軽減する サイバーハイジーン



“モダン脆弱性管理”においては脆弱性対象を
“点”から“面”へシフトすることが重要”



脆弱性の管理対象となる「ソフトウェア」「デバイス」「ロケーション」を網羅し、管理者の指示に対して“リアルタイム”な特定と識別、そして是正を可能にできるかがポイントとなる。

リアルタイム・プラットフォーム「Tanium」が
“モダン脆弱性管理”を実現します！

独自の特許技術で企業のサイバーハイジーンを支える

Taniumのプラットフォーム

「Tanium」は、1クラウド、1エージェントで統合エンドポイント管理 (UEM) と統合エンドポイントセキュリティ (UES) を備え高度なサイバーハイジーンを実現する革新的な統制プラットフォームです。5年の歳月を掛けて開発した唯一無二の特許技術をベースに、リアルタイム性と網羅性、その結果としての業務の正確性を提供し、企業のIT資産セキュリティに対する管理者ニーズ、経営ニーズ、現場ニーズに応えます。

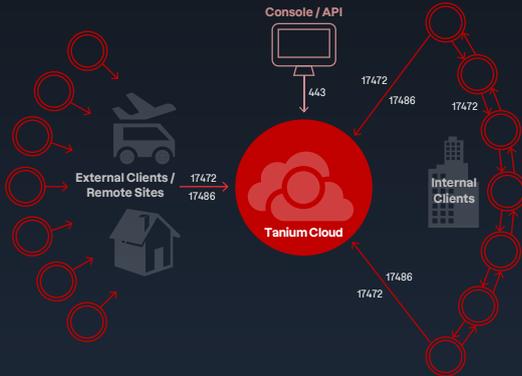
- NISTが求める端末管理機能の全てをシングル・エージェントでカバー
- 「全数端末」の可視化や制御を「リアルタイム」且つ「網羅的」に実現

TCO削減

ROI向上

高度化

5年の歳月を掛けて開発した唯一無二の特許技術



Taniumの独自技術

① リニアチェーン

オンプレミス環境なら統制されたセキュアなブロックチェーン構造を自動で形成しバクテリア方式で制御します。

② 専用プロトコル

リモートワーク環境では独自で開発した通信プロトコルにより、リモートアクセスVPN経由やローカルブレイクアウトしていても高速通信が可能となります。

従来のハブ & スポークモデルとは根本から異なるアルゴリズムを採用

特長① シンプル

1クラウド1エージェントの究極のシンプルさ

特長② 低負荷

大容量配信でもトラフィックを圧迫しない配信技術

特長③ 高速

可視化(特定/識別)と制御が数分、数秒の脅威の高速化

特長④ カバレッジ

オンプレもクラウドもリモートも全て管理統制下

タニウム提供機能の優位性

管理対象: マルチOS対応
(Windows, Linux, Mac, Solaris, AIX, Windows Embedded)

提供機能: 管理者権限でコマンドラインで実現出来る機能をリアルタイム且つ網羅的に実現

管理機能: 管理端末台数に関係なく、Tanium Cloud(管理サーバ式)のみで管理を実現

特許技術: これらの特長的な機能は5年の歳月を掛けて開発し特許を取得

タニウムご利用の条件は3つのみ

- ① Tanium-Cloudをご契約 (別途、IdP認証が必要)
- ② Tanium(エージェント)を管理対象端末にインストール
- ③ Tanium⇔Tanium、Tanium⇔Tanium-Cloudの疎通のため、TCP17472と17486をオープン

タニウムのソリューション

Tanium Core Platform(タニウム・エージェント)

拡張モジュール(サブスクリプションで提供)

	Asset	Discover	Provision
デバイス	オフライン端末を含めたエンドポイント情報を管理するモジュール	非管理のIPデバイスを検出・特定するモジュール	Windowsのペアメタルプロビジョニングを行うモジュール
ソフトウェア	Patch	Deploy	Enforce
リスク	Threat Response	Comply	Benchmark
端末状態	Reveal	Performance	Impact

Tanium Core Platform (タニウム・エージェント)

管理対象となる全ての端末にインストールし、管理者権限、コマンドラインで実行する全ての機能を提供可能

拡張モジュール (サブスクリプション)

必要な機能を必要なタイミングで柔軟に導入できる用途別の拡張モジュール

タニウムの実績

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

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

タニウムの特設サイトがオープン!

Taniumの特長や機能、お役立ち資料、
動画をわかりやすくまとめた
特設サイトをご用意しています。
ぜひ、ご覧ください。



<https://next-security.tanium.jp/lp>

見えないものは、守れない!
サイバーハイジーンで
サイバーセキュリティの
悩みを解決

詳細を見る >

リアルタイム性や網羅性、
直感的な操作性を実感いただける
動画をご用意しています。
ぜひご覧ください。
(外部サイトになります)



Movie

<https://youtu.be/BWoZ3M-7OHg>

最新情報や
企業の脆弱性対策に関する情報を
Blogでご紹介しています。



Blog

<https://www.tanium.jp/blog/>

製品および本誌に
掲載されている情報に関する
お問い合わせはこちらまで。



Contact us

<https://www.tanium.jp/contact-us/>



タニウム合同会社

〒100-0004 東京都千代田区大手町2-6-4 常盤橋タワー25F