BSIA x CIO賢人倶楽部 シンポジウム2022

DXの実現を支えるセキュリティ変革の最前線

タニウム合同会社
Chief IT Architect
CISSP, CISA
楢原 盛史(ならはら もりふみ)

TANIUM

Agenda

① タニウムの会社概要と主な実績

② 現場が言いずらいDX投資の“足枷”とは？

③ DXの実現に向けたSXの考え方

④ 現下の情勢を踏まえたサイバー攻撃の最新動向

⑤ グローバル組織が優先的に取り組むセキュリティ施策

⑥ タニウムが提供する機能とは？

⑦ タニウムの活用事例

⑧ 日本初：IOT/OTリスクアセスメントのご紹介

①タニウムの会社概要と主な実績

TANIUM

タニウムの企業概要と主な実績

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：東京都品川区
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）

米空軍(US. AIR FORCE)での採用事例

U.S. AIR FORCE

米国空軍は、
自動修復および資産の
可視化プロジェクトに
タニウムを選択

TANIUM

- **43分**
  アラート検知から修復完了までの時間
- **99%以上**
  全世界の全数端末へのパッチ適用率

・米国空軍は、組織全体のリアルタイムな可視性の実現にタニウムを採用

・タニウムの単一のプラットフォーム利用により運用者は資産の特定と最適化、脆弱性の管理、脆弱性診断、及びインシデント対応の各業務を数秒で実施することを実現

タニウムのパートナー

国内販売パートナー*

AZURE PLUS co.,ltd
CEC
CP-SOL
CTC
FUJITSU
HITACHI Inspire the Next 株式会社 日立システムズ
iSopra
JBS
LAC 株式会社ラック
MACNICA
MBSD
NEC
net one
NTT DATA NTTデータ 先端技術株式会社
NTTビジネスソリューションズ
NTT Communications
SB C&S
TechMatrix
TIC

ソリューション・パートナー

aws
cisco
CYWARE
deepinstinct
Flexera
FORESCOUT
Google Cloud
IBM Cloud
Microsoft
okta
ORACLE
paloalto NETWORKS
salesforce
servicenow
snow*
splunk>

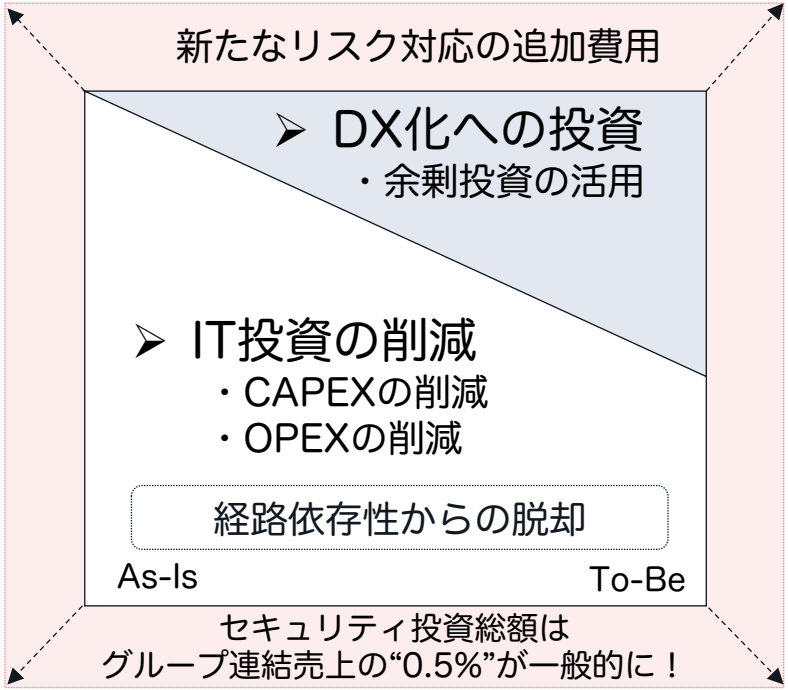
※ https://www.tanium.jp/partners/technology-alliances-jp/ (50音順。2022年5月時点)

②現場が言いずらいDX投資の”足枷”とは？

TANIUM

連続的な ”DX投資” をどのように生み出し続けるのか？

➢ ITインフラの投資総額



➢ ITチームが抱えている経路依存性

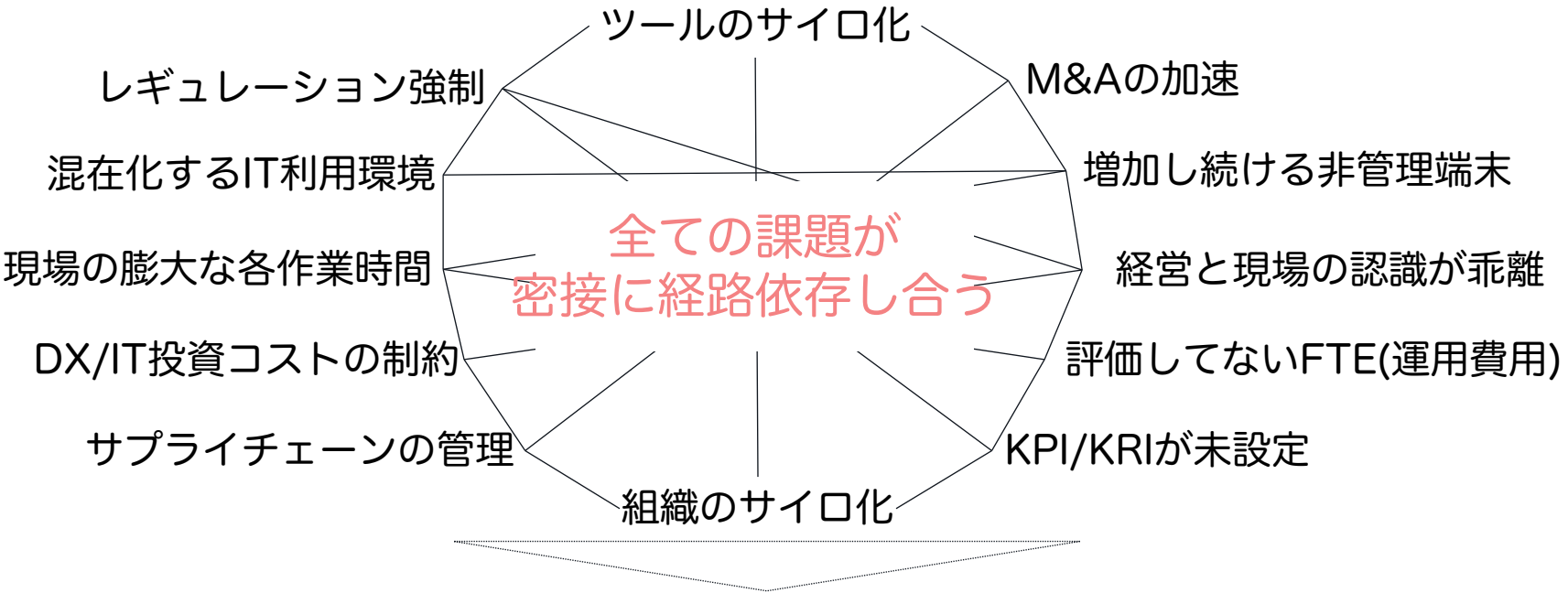
- 資産把握やパッチ適用等の単純業務に忙殺
- 各業務のKPIベースの運用が不可能に近い
- 導入ツールのサイロ化、運用組織のサイロ化
- ユーザー部門からの多発するクレーム対応
- チームメンバーの離脱、個人稼働率の増加

増加する(計上されない)運用コスト

“技術革新”によって、
“攻めのIT投資”を連続的に創出

先進的グローバル組織が取り組む ”経路依存性” からの脱却

DX実現の足を引っ張るIT目線の“経路依存性”とは？



全ての課題を一斉に解決する方法 ＝ 技術革新

経営サイドが“安全宣言”を迅速に出せない理由とは？

- 経営
- 現場の実情
- あるべき運用の姿
- 求められる運用要件

うちは大丈夫か？

可視化？

把握？

ちゃんと出来てる？

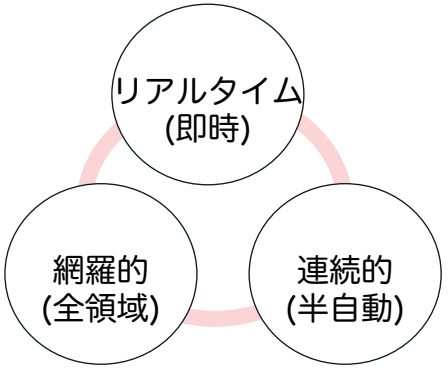
定性的で常に曖昧な情報

〇〇の特定や識別

〇〇台や〇〇%

〇〇時間以内に修復

定量的で常に正確な情報



経営サイドはいつまでも安全宣言が出せない

経営サイドは迅速に安全宣言を出せる

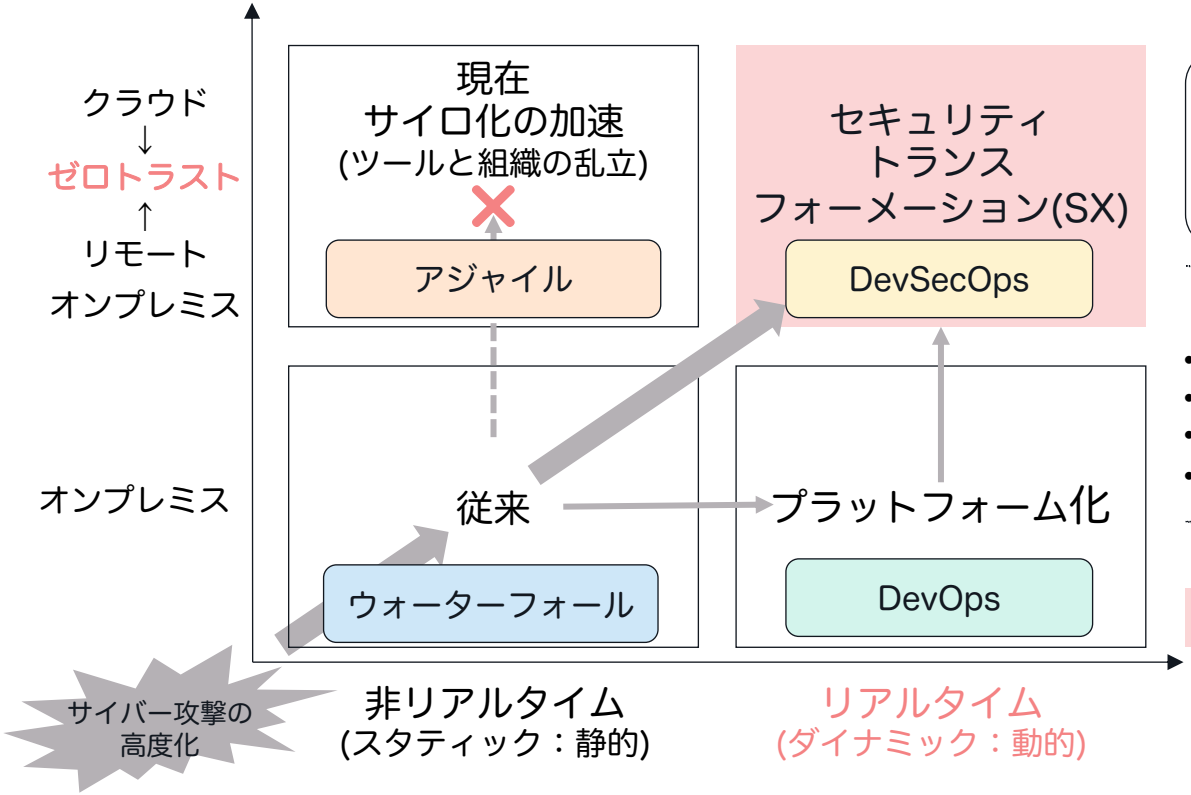
動的なエンドポイント管理の実現

③DXの実現に向けたSXの考え方

TANIUM

セキュリティ・トランスフォーメーション(SX)

今、取り組むべき「サイロ化」→「プラットフォーム化」に向けた変革とは？



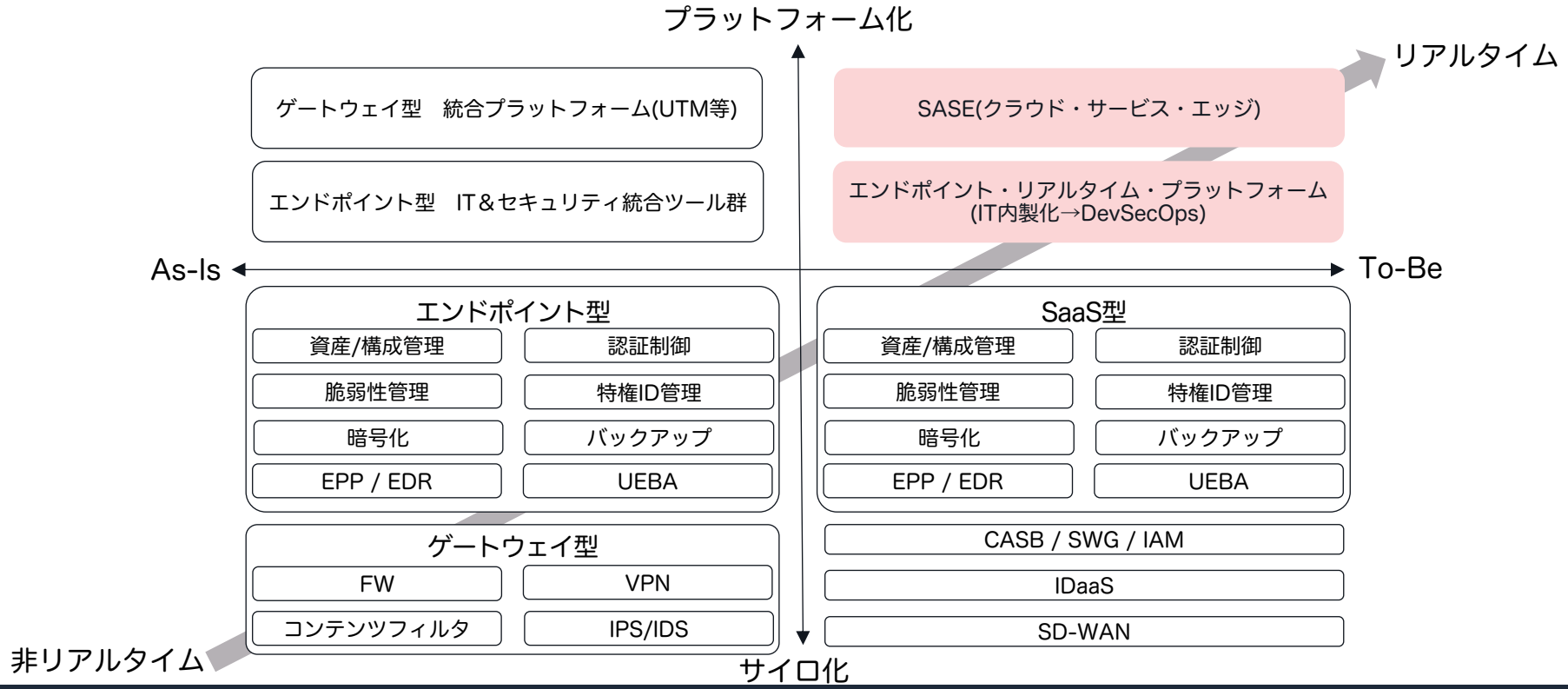
「SX」とは、IT＆セキュリティの
組織/技術/運用が融合し高度化し続ける
サイバー攻撃に対し、常に迅速で順応
した対応が実現可能な変革を図ること

- DXの成功には「SX」の実現が鍵に
- DevSecOpsによるIT内製化の加速
- マルチOSとオンプレ･ゼロトラの網羅性
- 全ての業務にリアルタイム性の確保

革新的な技術の活用

セキュリティ・トランスフォーメーション(SX)に向けて

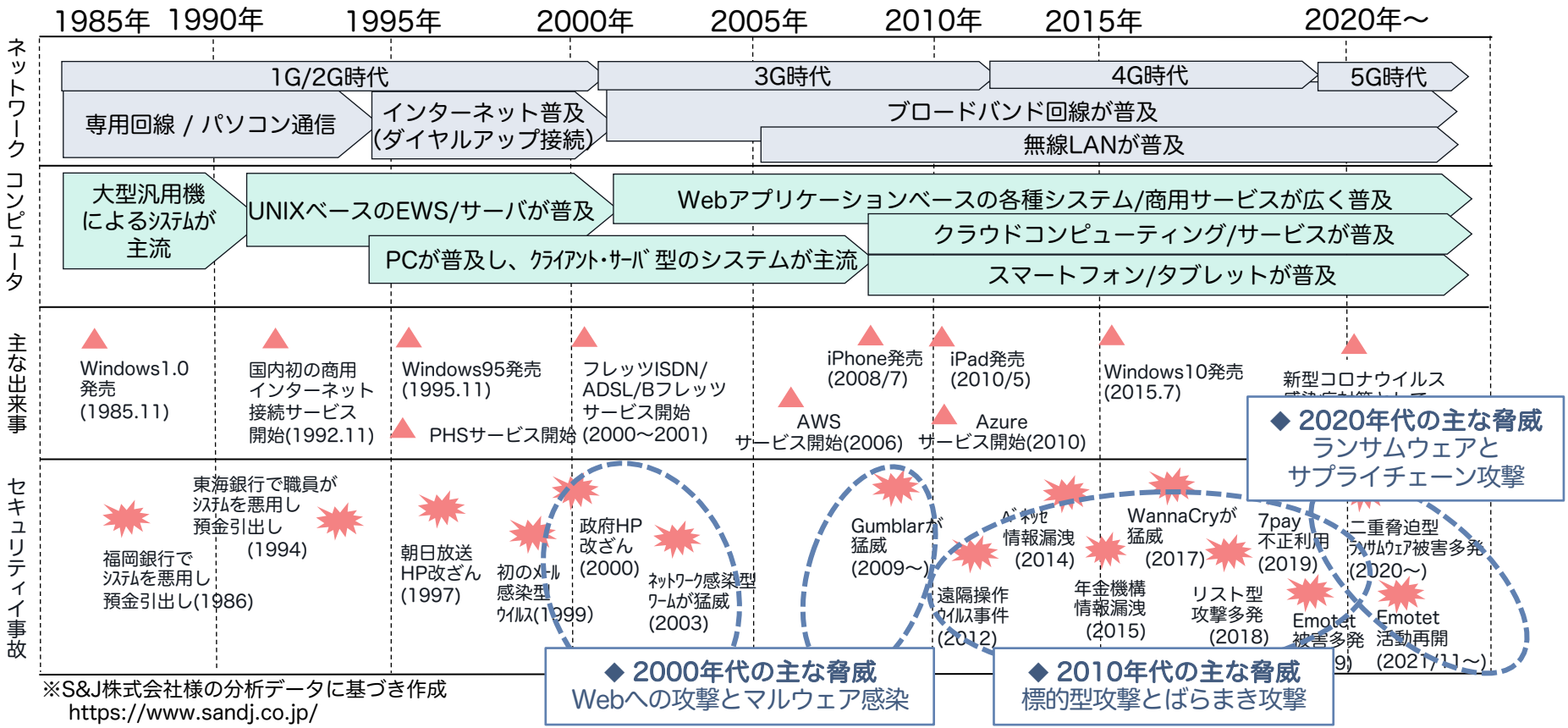
As-IsからTo-Beを見据えた主たるアーキテクチャのマッピング



④現下の情勢を踏まえたサイバー攻撃の最新動向

TANIUM

時代の変遷を踏まえた“IT”と“サイバー攻撃”のトレンド※



※S&J株式会社様の分析データに基づき作成
https://www.sandj.co.jp/

現下の情勢を踏まえた最新のサイバー攻撃トレンド

破壊的なサイバー攻撃の頻発と国際問題化で、リスクの深刻度は確実な増加へ！

➢ サイバー攻撃トレンド

- ウクライナ侵攻で見られる ハイブリッド戦
- サイバー犯罪と捜査の グローバル化
- 米中対立で深まる サイバー空間の分断
- ソフトウェアサプライチェーンの セキュリティ

“実地戦”のタイムライン

2.21　分断地域の独立承認

2.24　ウクライナ侵攻開始

3.2　国際緊急特別総会決議
3.10　ウクライナEU加盟申請
3.12　ロシアSWIFT排除

4.13　フィンランドNATO加盟意向

融合するハイブリット戦

“サイバー攻撃”のタイムライン

1.13　ウクライナ複数組織にワイパー攻撃
1.14　ウクライナ政府サイト改ざん
1.15　ウクライナ軍、銀行にDDoS
1.24　ベラルーシ鉄道にサイバー攻撃
2.12　ウクライナハイブリット戦に注意喚起
2.16　米国：ロシアのAPT攻撃に注意勧告
2.22　米欧：ウクライナへのサイバー支援表明
2.24　欧州衛星サービスへの妨害攻撃
2.27　アノニマスによるロシアTVハイジャック
3.21　米英日：経済制裁への報酬サイバー攻撃へ注意喚起
3.25　米国：カスペルスキー製品の調達を制限
3.28　ウクライナ通信会社へサイバー攻撃
4.8　フィンランド政府機関へDDoS攻撃
4.8　ウクライナ電力システムへ破壊的naサイバー攻撃
4.13　米国：産業システム向けマルウェアに注意喚起

6.16　米国司法省：各国法執行機関と連携しロシアのボットネットを解体

セキュリティ事故が “経営” にもたらすインパクト※と責務とは？

情報漏洩

機密情報
個人情報

- 漏洩顧客数×@500の賠償金(損害賠償請求)
- 株価が平均6.3%の下落、ESG評価の格下げ
- 善管注意義務、改正個人情報保護法への抵触
- 提供サービス自体の“廃止”リスク

事故の責任は“取締役”が問われる！
謝罪会見や引責辞任、そして監視対象へ

事業停止

システム停止

- 年間売上 ÷ 365日 × 停止日数 ＝ 売上損害
- 影響度調査～復旧(安全宣言)の膨大な作業工数
- ランサムウェア修復費用は“約2.1億円”
- レピュテーションの著しい低下

リスク発生を徹底して抑制する
サイバー・ハイジーン施策の優先度

※参考引用：https://www.j-cic.com

⑤グローバル組織が優先的に取り組むセキュリティ施策

TANIUM

侵入“される”ことを前提としたセキュリティ

サイバー・レジリエンス(減災：発生したリスクの最小化)

防災  減災

侵入“されない”ことを“大”前提としたセキュリティ

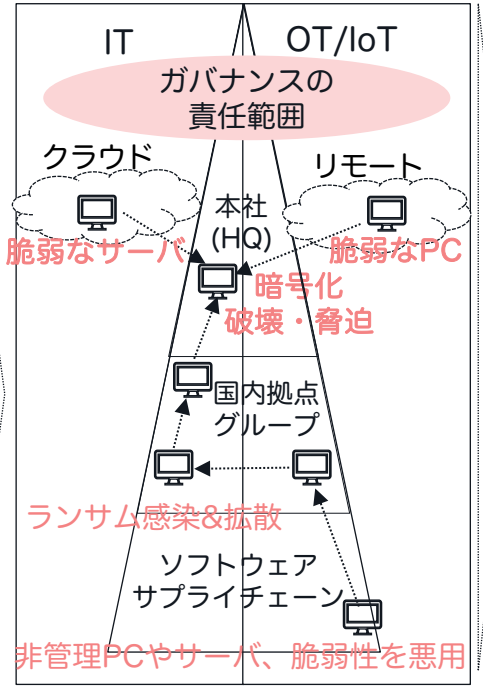
サイバー・ハイジーン(防災：リスク発生自体の未然予防)

サイバー攻撃ステップを踏まえたセキュリティ高度化の要件

サイバー攻撃のステップ

犯罪組織

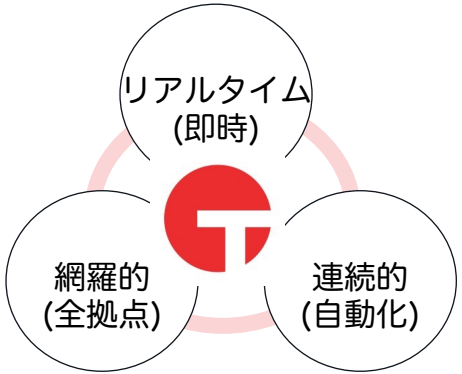
- 非管理端末(PCやサーバ)
- PCやサーバの脆弱性を悪用
- ランサムウェアを感染&拡散
- 段階的な管理者権限の窃取
- 既存セキュリティを無力化
- サーバを暗号化し破壊・脅迫



セキュリティ高度化の要件

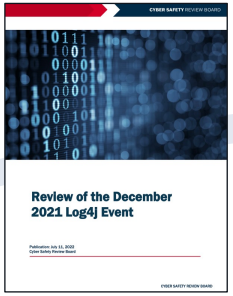
①全数端末の特定/識別(動的なIT資産管理)
②脆弱性管理(調査/パッチ適用/設定変更)
③発生リスクの最小化(影響度分析→復旧)

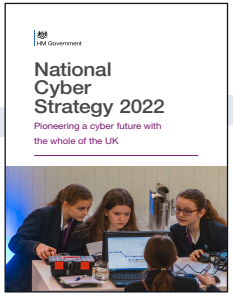
共通の運用要件

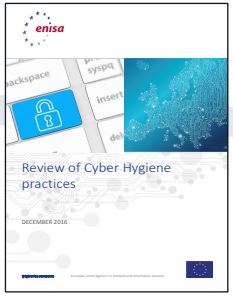


グローバルで加速化するサイバー・ハイジーンの最新動向

明示的にサイバー・ハイジーンを指示する 法律/戦略/ガイドライン/フレームワーク等

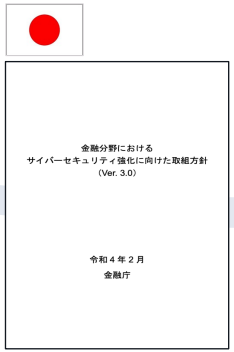


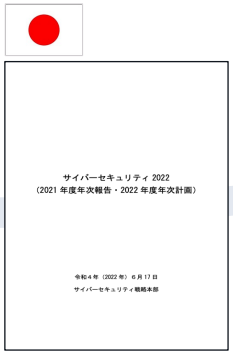




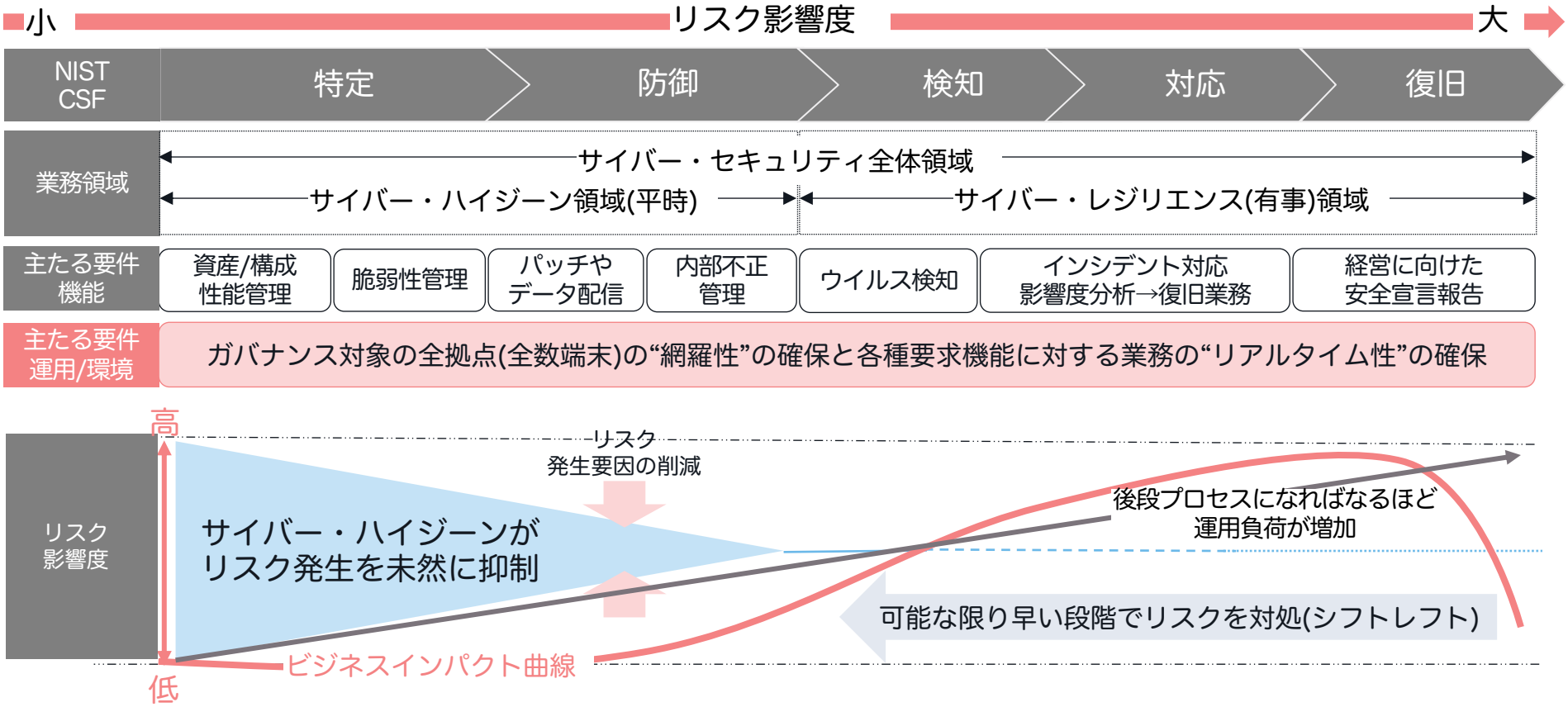
グローバルにおいては、
ITに先進的な諸外国が一斉に指示

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





サイバー・セキュリティの全体領域の施策優先度の考察



⑥タニウムが提供する機能とは？

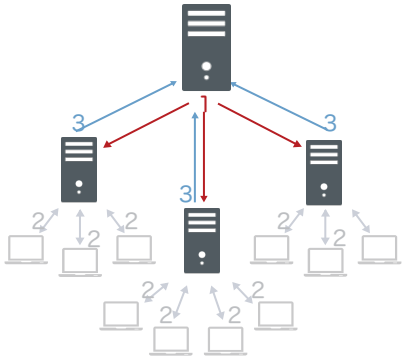
TANIUM

サイバー・セキュリティの全体領域の施策優先度の考察

小 ← リスク影響度 → 大

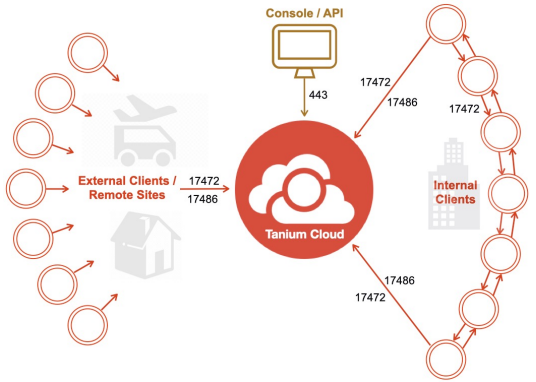
NIST CSF	特定	防御	検知	対応	復旧
主たる要件 機能	資産/構成 性能管理	脆弱性管理	パッチや データ配信	内部不正 管理	ウイルス検知	インシデント対応 影響度分析→復旧業務	経営に向けた 安全宣言報告
主たる要件 運用/環境	ガバナンス対象の全拠点(全数端末)の“網羅性”の確保と各種要求機能に対する業務の“リアルタイム性”の確保						

他社製品
ハブ & スポークモデル



アルゴリズムが
根本から異なる

TANIUM
専用プロトコル & リニアチェーン

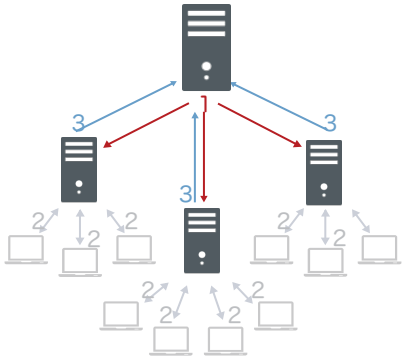


サイバー・セキュリティの全体領域の施策優先度の考察

小 ← リスク影響度 → 大

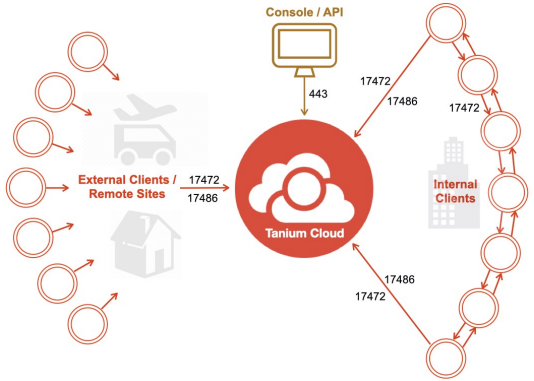
NIST CSF	特定	防御	検知	対応	復旧
主たる要件 機能	TANIUM				
主たる要件 運用/環境	リアルタイム・プラットフォーム(シングル・エージェントで全ての領域をカバー)				

他社製品
ハブ & スポークモデル



アルゴリズムが
根本から異なる

TANIUM
専用プロトコル & リニアチェーン



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)

管理対象	拡張モジュール(サブスクリプションで提供)		
デバイス	Asset 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	Discover 非管理のIPデバイスを検出・特定するモジュール	Provision Windowsのベ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 Microsoft/Linux/mac OSのパッチをスキャン・配信するモジュール	Deploy ソフトウェアのインストール、更新、削除を行うモジュール	Enforce エンドポイントのポリシ、防御機能を管理するモジュール
リスク	Threat Response リアルタイムの検知、過去情報の探索、対応までを行うEDRモジュール	Comply セキュリティ監査と脆弱性診断を実行するモジュール	Risk エンドポイントのサイバーリスクを可視化・制御するモジュール
端末状態	Reveal センシティブデータの存在を特定するモジュール	Performance エンドポイントの状態や利用状況を可視化するモジュール	Impact ADユーザやコンピュータのつながりを可視化するモジュール

エンドポイント管理の高度化を見据えたAs-IsとTo-Be

As-Is：サイロ化

ソフトウェア

- サイバー・ハイジーン(資産/構成/脆弱性管理 等)
- データ配信(FU/QU/各種アプリやソフト 等)
- 内部犯行対策(特権ID管理/DRM/DLP/操作ログ管理 等)
- EDR(インシデントレスポンス支援ツール 等)
- EPP(統合型ウイルス対策製品)
- 各社独自のバッチ処理(プログラム/スクリプト等)
- Windows 新旧OS

1台あたりのコンピューティングリソース

To-Be：リアルタイムプラットフォーム化

もたらす効果

TCO削減 | ROI向上 | 高度化

ソフトウェア

TANIUM

リアルタイム・プラットフォーム
(既存ツールも管理高度化を実現)

Windows 新旧OS

1台あたりのコンピューティングリソース

実環境(2万台/150拠点)におけるタニウムの効果測定

➢ 代表的なIT運用業務の「実施時間」と「実現率」の比較

サイバー・ハイジーン領域 ⟷ サイバー・レジリエンス領域

全数端末状態の可視化	Windows FUの適用率	特定CVEの全数調査	レジストリの一斉変更
既存ツール → TANIUM	既存ツール → TANIUM	既存ツール → TANIUM	既存ツール → TANIUM
2日 / 75% → 1分以内 / 100%	6ヶ月 / 60% → 2週間 / 97%以上	1日 / 80% → 1分以内 / 100%	1日 / 100% → 1分以内 / 100%

非管理端末の可視化	ツール利用率の可視化	特定リスクの影響度調査	リスク端末の一斉隔離
既存ツール → TANIUM	既存ツール → TANIUM	既存ツール → TANIUM	既存ツール → TANIUM
6ヶ月 / 50% → 5分毎 / 100%	不可 / 不可 → 1分以内 / 100%	3日 / 70% → 1分以内 / 100%	1日 / 100% → 1分以内 / 100%

“リアルタイム性と網羅性”により“機能要件 ＋ 運用要件 ＋ 環境要件”を同時に満たし
”TCO削減 ＋ ROI向上 ＋ 業務の正確性向上“を実現

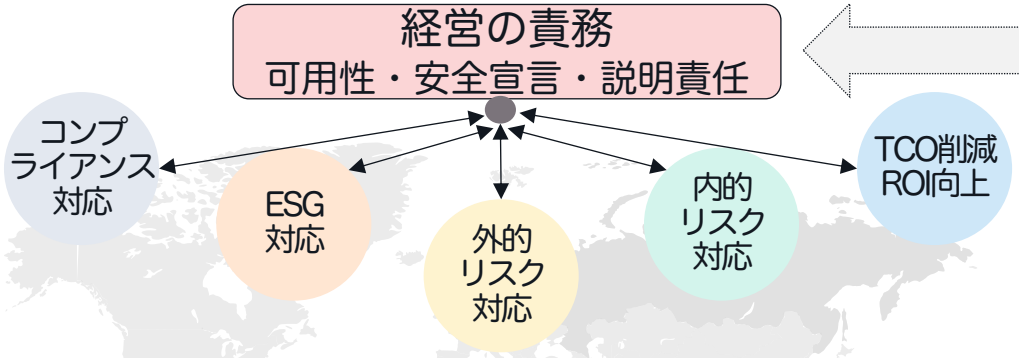
定量的指標(KPI)ベースのCIO/CISOダッシュボード

月次レポートのカテゴリ(例)		KPI (網羅性)	実績① (前回)	KPI (時間軸)	実績② (前回)	KRI	動向
サービス/ライセンス利用率	Adobe	100%	98% (92%)	3分	3分 (5分)		
	Office 365	100%	100% (95%)	3分	80時間 (94時間)		
利用ツール稼働率	EPP/EDR	100%	75% (62%)	3分	10分 (5分)		
	資産管理(A)	100%	99% (100%)	5分	5分 (5分)		
IT資産把握率	PC/サーバの総数	98%	90% (85%)	3分	5分 (5分)		
	非管理端末の総数	2%以下	5% (8%)	5分	5分 (5分)		
パッチ適用率	Windows 10	100%	98% (95%)	14日	14日 (30日)		
ポリシー違反	不正ソフトウェア利用	0件	3件 (0件)	1分	1分 (1分)		
	未許可USBの利用	0件	1件 (3件)	1分	1分 (1分)		
ESG(TCFD)	サーバのCO2削減率	15%	10% (5%)	180日	180日 (180日)		

リスク対応
• 主要ツールの利用率、稼働率が　低く緊急の改善が必要。 • パッチ適用率は良好な状態であり、次月も維持する。 • IT資産把握率は順次で増加しているものの、改善を実施する。 • ポリシー違反は複数観測され、社員に対するポリシーの周知徹底を実施する。 • ESG対応は順次実現。

“ガバナンス”と“エンドポイント”の密接な関連性

ガバナンスの目的：ステークホルダーの権利/利益を守り続ける



ITチームが求められる業務

本社は全数端末管理の網羅性を確保し、
リアルタイムな特定/識別/是正業務が必要に！

実現出来ない場合

事業停止、特別損失、機会損失、ブランド価値低下、
株価の下落、善管注意義務違反、株主代表訴訟 等

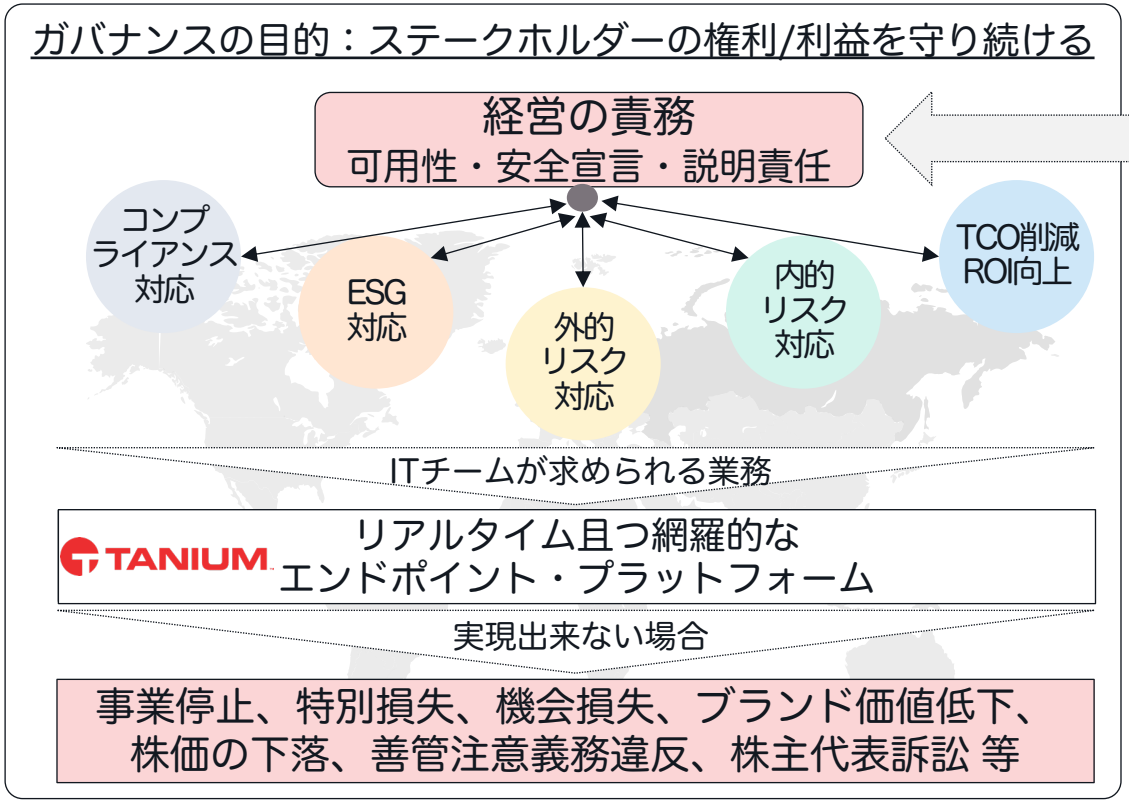
➢ 経営の意思決定プロセス

常に正確な情報を元に
迅速で正確な意思決定

全てのIT運用業務は
リアルタイム且つ網羅的

平時も有事も
うちは大丈夫か？

“ガバナンス”と“エンドポイント”の密接な関連性



➢ 経営の意思決定プロセス

常に正確な情報を元に
迅速で正確な意思決定

全てのIT運用業務は
リアルタイム且つ網羅的

平時も有事も
うちは大丈夫か？

⑦タニウムの活用事例

TANIUM

東急不動産ホールディングス

Win10FUの配布、
累積パッチの配布、
適用状況のリアルタイム可視化

TechMatrix
テクマトリックス株式会社

インベントリ情報把握と、Windows10パッチマネジメントに活用

Windows10への切り替えでパッチマネジメントの課題が顕在化

- 関連会社や遠隔地の拠点を含めグループ全体で2万台を超える端末が管理対象
- WSUSと資産管理ツールを組み合わせて毎月パッチ配信をしていたが、9割ほどの適用率にとどまっていた
- WSUSではパッチの再プッシュが難しい為、端末側での操作が必要になるなど運用面でも課題が顕在化、グループ全体で集中管理が可能なパッチマネジメント手法が必要となっていた

数日かかっていたインベントリ情報の収集が数分で実施可能に

- 4GB程度のファイルを複数拠点に配布するテストを実環境で実施したところ、ネットワーク負荷やトラフィック量、端末での適用状況を鑑み、従来のツールで行う場合よりも4倍ほど早く配信できることがわかった
- 適用できていない端末をリアルタイムで可視化、事業会社の担当者に催促している
- 各事業会社ごとに10台を超える資産管理サーバの運用担当者にパッチの適用状況やインベントリ情報を確認依頼、各担当者は1時間程度かけて調べて返答をしていたが全体で数日かかっていた、Tanium導入後これら一連の確認作業をわずか数分で実施可能になった
- ネットワーク負荷を考え、拠点やフロアごとにグループを分けて配信時間を分散する調整をしていたが、送信の効率が向上したことでそういった調整が不要になった

「タニウムは柔軟性がありながら、正確性とスピードを兼ね備えている」　お客様からのコメント

AutoNation

リアルタイムの
可視化とコントロール

99.9%のパッチ適用率

300拠点,30,000EPに対するサイバー・ハイジーンの実現とエンドポイントセキュリティの向上

タニウム導入前のエンドポイント管理における課題

- 全EPの状況を把握する為に数週間必要だった(全てかどうかはツール依存)
- クリティカルパッチの全数適用に数ヶ月必要だった(全てかどうかはツール依存)
- SCCMのパッチ適用率が74%、SCCMのインストール率が80%だった
- EPに問題があった際は常に現地へ駆けつけ対応が必要だった

PoCによって顕在化された課題

- 未適用パッチの数が10,000以上(古くは2007年から)
- 多くのEPが6つ以上のクリティカルパッチを未適用
- SCCMエージェントが未インストール且つ壊れているEPを多数発見
- 91%のEPでAdobeFlashのサポートが終了していた

タニウム導入によって実現した事

- 300拠点,30,000EPに対し初回でパッチ適用率を99%、インストールが98%
- SCCMの中継サーバ(260台)が不要に(Taniumサーバの1セットのみへ)
- 3rdパーティアプリケーション(アンチウィルス)の展開が4日で完了
- 未適用パッチをリアルタイムにリスト化し、即時のパッチ適用が可能に

⑧日本初：IOT/OTリスクアセスメントのご紹介

TANIUM

IOT/OT領域でセキュリティ施策が求められる背景

サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに
対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する
超スマート社会“Society5.0”が推進され、日本政府よりセキュリティ対策強化が示唆

- 日本政府が示すサイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)
  - ・サプライチェーン(バリュークリエイションプロセス)全体のサイバーセキュリティを確保
  - ・産業に求められるセキュリティ対策の全体像を整理
  - ・サイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)が策定

CPSFの実現で求められること

環境変化に伴う
事業継続

体系立った
ガイドライン策定

脅威に対する
対策情報の把握

CPSFの対応に向けたサービスの実施ステップ(S&J社連携)

①CPSF対応評価
日本政府並びに国際的な
ガイドラインの準拠状況を評価

②CPSF脅威シナリオ評価
自社環境に合わせた脅威シナリオを
基にした机上での課題評価

③CPSアーキテクチャ評価
外部/内部脅威やネットワーク設計
ミス/操作ミスの有無を実査で評価

主なサービス目的とスコープ

実施ステップ	①CPSF対応評価	②CPS脅威シナリオ評価	③CPSアーキテクチャ評価
目的	・セキュリティ対策状況を広く把握するために、日本政府や国際的なガイドラインへの準拠状況を可視化 ・課題点への対応ができるようにする ・評価対象となるIOT/OTデバイスの可視化(Discoverモジュール利用)	・環境に合わせた脅威シナリオを定義して、サイバー攻撃への対策充足度だけでなく、内部要員の過失や悪意によるインシデントを想定し、既存の規定類、管理資料等をもとにマネジメントの観点からの対策の充足度も評価 ・改善に向けたプランニング	・ガイドラインや机上調査では可視化できない外部/内部脅威やネットワーク設計ミス/操作ミス等のリスクの有無を実査で可視化 ・具体的な技術的な課題に対しての対策計画を作成
調査スコープ	・CPSF/IEC62443/NIST SP800-171に定義されている事項	・前提：お客様のIoT/OT環境 ・サイバー攻撃への対策充足度 ・内部不正、過失によるインシデントへの対策充足度 ・マネジメント（管理体制、規程文書類、リカバリ計画）のセキュリティ評価）におけるセキュリティ評価	・制御機器 ・内部ネットワーク ・インターネットとの境界

最後に・・ガバナンス・プラットフォームのTo-Be像

To-Be：企業(組織)に関わる全てのステークホルダーの“利益や権利”を守る

本社(HQ)集中統制によるグループを包含したガバナンス・プラットフォーム化

ご清聴いただきまして、ありがとうございました。

TANIUM