



ivanti

可視性の改善、詳細な観察、 データに基づく行動

ビジネスで優れた成果を得るためには、
卓越したITインサイト(洞察)が必須

目次

はじめに	3
可視性の欠如:6つの使用例	4
1: 動きの遅いノートパソコン	4
2: 受け取り倉庫におけるルータ	5
3: コスト削減	7
4: メールの遅延	8
5: ノートパソコンのロックアウト	9
6: ITが知らない世界	10
Ivanti:頭の後ろの眼	11

このドキュメントは、あくまでもガイドとして提供されています。全ての場合において効果を保証するものではありません。このドキュメントには、Ivanti, Inc.およびその関連会社(総称して「Ivanti」と呼ばれます)の機密情報および/または所有財産が含まれており、Ivantiの事前の書面による同意なしに開示またはコピーすることはできません。Ivantiは、このドキュメントまたは関連製品の仕様と説明をいつでも予告なしに変更する権利を留保します。Ivantiは、このドキュメントの使用を保証するものではなく、ドキュメントに表示される可能性のあるいかなる誤りについても責任を負いません。また、本文書に含まれる情報を更新する義務を負いません。最新の製品情報については、ivanti.co.jpをご覧ください。

はじめに

IT資産、サービス、セキュリティ体制、プロセス、および結果の完全な情報を取得することは、IT資産を適切に管理、保護、および最適化するための基盤となります。より明確に把握し、よりデータに基づき行動し、より効果的にふるまう事ができます。したがって、コストと将来の予算を最適化し、顧客と従業員のエクスペリエンスを改善し、チームの生産性と効率性を高めることができます。

そして今日の高度に規制された産業とコンプライアンスが重要な世界においては、次のような内容が必ず求められます

。ー パッチ適用、コスト最適化、アプリケーション制御、および資産の場所に関する明確な情報。現在のIT部門はコストセンターではなく、イノベーションの中心になるという目標を持っています。

実は完全な可視性を得るためには最初のステップがあり、さらに多くのステップを踏まなくてはなりません。例えば：

- 出発点のベースラインを確立せずに、資産、セキュリティ、プロセス、および成熟度の観点から、またはIT業務に投入される作業の量と種類をどのように把握できるでしょうか？

- 認識されていないIT環境をどのように管理できるでしょうか？
- 同じ予算とITリソースで、企業により大きな価値を提供するにはどうすればよいでしょうか？
- 広範囲にわたるエンドポイントデバイスタイプに対する幅広いサポートを、可視性が低い状況で、経験が少ない手作業で提供するにはどうすればよいでしょうか？

Ivanti は企業のIT資産を隅々まで照らします

可視性の確保は基本的な戦術であり、Ivantiの実績のあるソリューションを用いればエンタープライズIT資産のあらゆる側面にスポットライトを当てられます。統合ITアプローチにより、ITサービス管理、IT資産管理、エンドポイントセキュリティ管理、およびエンタープライズサービス管理と統合エンドポイント管理の柱の下に組織されたユーザーおよびワークスペース管理のITチームを統合できます。より明確になり可視性が向上しているため、企業全体のユーザー、サービス、資産、さらにITのランドスケープ、セキュリティに対する姿勢、プロセスとデータとの同期が向上します。また、より多くの戦略目標を達成する余裕ができます。

このホワイトペーパーについて

このホワイトペーパーでは、6つの簡潔で例示的なユースケースと調査データポイントを提供してIT部門がどうやってより明確で可視性を高めることができるかを評価するのに役立てられます。





可視性の欠如:6つの使用例

次の6つのユースケースシナリオと、一般的な可視性の欠如に関連する問題点を検討してください。:

1

動きの遅いノートパソコン

ヘルプデスクの担当者は、ノートパソコンのパフォーマンスの低下に関するコールの増加に気が付きました。多くの時間をかけてサポートコールを終わらせたあと、ヘルプデスク担当は、1週間前にカンファレンスから戻った役員が「キラーアプリ」と考えたアプリを、彼が持ち込んだUSBメモリーからダウンロードするよう奨励していることを知りました。しかも、同一のライセンスを再利用していたのです。さらなる調査の結果、そのアプリがパソコンのリソースを大量に消費していることに気が付きました。しかし、現在アプリをインストールしているノートパソコンの数は不明です。

現在、多くのIT部門では全体的な可視性に乏しい状況で、未熟な、または手動のオペレーションを実行しています。可視性に欠けると、ハードウェアとソフトウェアを検出、管理、保護すること、およびソフトウェアの使用を効果的に管理することは

非常に困難です。

上記のシナリオには、複数の未知の内容が含まれています。:

- 使用されているライセンスのないソフトウェアによるコンプライアンス違反のリスク
- シャドウIT – ITを回避し、不正なソフトウェアをインストールする従業員
- 影響を受ける可能性のあるノートパソコンの台数
- 申告インシデントの総数
- 許可されていないソフトウェアのインストールと使用によって生じるセキュリティリスク
- 不明なライセンス利用リスク

自社が所有しているかわからない、または簡単に可視化できないものを管理、保護、および最適化できないということは強く申し上げます。Ernst & Young (EY)のホワイトペーパー「Data Validation the Best Practice for Data Quality in Fixed Asset Management (固定資産管理におけるデータ品質のベストプラクティス)」では、企業の56%のみが年に一度固定資産の場所を確認し、さらに10%~15%の企業が5年以上資産を確認していないと述べられています。

正式なIT資産管理 (ITAM) プログラムがないため、多くの場

43%

調査対象の組織の43%がまだ表計算を利用している

50%

の組織がエンドポイント管理ソリューションを使用している

45%

の組織がインベントリツールをリソースの1つとして使用している

合、チームはActive Directoryまたはエンドポイント管理ソリューションからの基本的なインベントリ情報のみに依存しています。資産の追跡に関するトピックについて、2019年12月にIvantiが委託したITXM調査の調査では、次のことがわかりました。ただし、ある組織が次のオプションを複数使用している可能性にご注意願います。:

ITSM、ITAM、SAMデータなど、一緒に結合しなければならない複数のデータソースは、必要な洞察と全体的な可視性を得るための速度を低下させます。Enterprise Management Associates (EMA) の調査によると、組織の50%には12個以上の検出ツールやインベントリツールがあり、11%には30個を超えるツールがあります。平均して、組織はデータ精度の問題を解決するために週に10時間費やし、32%は週に25時間以上費やしています。要するに可視性の欠如は、自分が持っていることがわからず、簡単に見ることができないものを管理、保護、最適化できないことを意味します。Ivantiソリューションは、表計算、IT資産管理ツール、バーコードスキャン、ディスクバリサービスなどの複数のソースからのデータを結合するのに役立つ強力なデータインポート機能を使用して、実際のデータと検出されたデータを比較し、不一致をレポートします。これらの情報により、意思決定者は仮定を検証し、資産情報が常に最新かつ正確であることを確認できます。

2

受け取り倉庫におけるルータ

ネットワーク運用チームに、受け取り倉庫から電話がありました。新しいルータのパレットが到着しましたとのこと。運用チームは、最初に新しいルータを注文した人が社内にはいないことに気付く前に、古いルータを置き換えるように新しいルータの構成を開始してしまいました。

可視性の欠如は多くの未知につながります。調達履歴はどうなっていますか？ 優先ベンダーと調達経路はどこでしょうか？ ネットワークに接続する許可されていないハードウェアによる潜在的なセキュリティリスクは何でしょうか？

前述のIvanti委託ITXM調査(2019年12月)では、組織がIT資産の購入データ、契約、および保証データを追跡および監視する方法について質問しました。調査の結果、次のことがわかりました。繰り返しますが、組織はこれらのオプションを同時利用している可能性があることに注意してください。

データとデータソースの可視性(存在するデータを把握し、すべてを1か所にまとめること)は、上記の苦痛を緩和するのに大いに役立ちます。一貫性があり、正確で、信頼できるデータにつながるはずで

39%

回答者の39%が複数のシステム
とリポジトリを使用

38%

が在庫を表計算を用いて
手動で追跡

37%

が資産管理リポジトリ/データベ
ースの一部として追跡

22%

が個別の契約管理シ
ステムを使用

「はじめに」で述べたように、エンタープライズサービス管理と統合エンドポイント管理が密接に連携、統合、および自動化されている場合:

- 資産発見のインサイトを使用して、問題のある資産の種類、モデル、ベンダー情報について予測を行い、定められたアクションを実行できます
- ベンダーの管理、コンプライアンス、保証の最適化を改善するために、より深いインサイトが得られます
- ITスタッフは、より戦略的なプロジェクトに集中するために、事後対応的または不必要な活動から解放されます
- 使用が許可されているハードウェアを知ることにより、セキュリティリスクが軽減されます。
- コストと管理の労力を最小限に抑えながら、より多くの成果を上げることができ、ビジネスにより多くの価値を直接提供できます

3 コスト削減

CIOは、今年度の予算削減の検討をスタッフに指示します。オペレーション担当副社長は、ノートパソコンの更新サイクルを延期できるかどうかを確認したいと考えていますが、ノートパソコンの台数、影響を受ける従業員、作成される可能性のある問題、実際に節約できる予算がわかりません。

このケースで浮上する可視性の問題点には、不明なノートパソコンのインシデントとベンダーの履歴、パソコン型番の正常性とパフォーマンスを判断するための資産ライフサイクル全体の一貫した追跡の欠如、不明なパッチ適用履歴が含まれます。また、どの従業員が影響を受ける可能性があるのかも不明です。

適切なインサイトの活用により、あるIvantiのお客様はハードウェア更新サイクルを6~12か月延長することができ、インシデント率向上を通じてエンドユーザのサービス品質に影響を与えたりすることなく、IT部門全体で150万ドルのコストを節約しました。

さらに、2019年12月のITXM調査の調査では、次のことが判明しました。

資産のライフサイクル、パフォーマンス、コンプライアンス、およびコストへの影響を理解することは、厳しく規制された業界で事業を行う企業にとって特に重要です。医療機器業界、政府のモバイルデバイス規制 (MDR)、および関連する欧州連合の医療機器に関する欧州データベース (EUDAMED) 規制がその例です。

28%

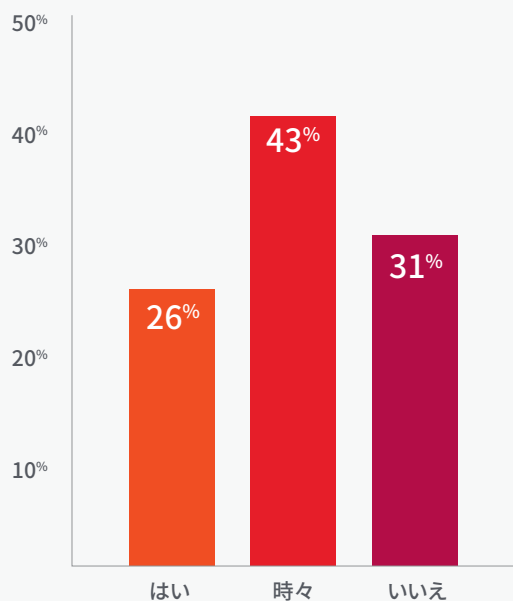
IT部門の28%が毎週、保証対象外/サポート対象外の資産をサポートするために時間を費やしている

20%

IT部門の20%は、古い資産の情報を持っていない

サーベイ: ITサービスにおけるIT資産管理プロセス適用の影響

御社のサービス管理プロセスと要求ワークフローによって、資産情報およびその関係性を自動的に可視化できていますか？



4 メールの遅延

ヘルプデスクのスタッフが出勤すると、大量の電話が鳴りだしました。メールが「機能しない」または「非常に遅い」というクレームです。他のITチームとの数回のミーティングの結果、IT運用チームは、誰かが昨夜メールアプリケーションを更新し、現在のサーバが新しい構成変更を処理できず、パフォーマンスの問題につながったと結論付けました。問題を軽減するために必要なハードウェアがあるかどうかはすぐにはわかりませんでした。

ここでの可視性欠如には、不明確な変更と構成の履歴、将来の変更のビュー、変更の影響とリスクの分析、不明なハードウェアインベントリが含まれます。

組織は、ITの達成目標を開発して成熟度を高め、自動化を採用して効率の向上を実現します。しかし、多くの人は、重要な最初のステップ、つまり最初からベースラインを確立することを忘却しています。このベースラインとは次のことを意味します。すなわち、1) 主要なサービスと、変更管理などの基礎となる資産に影響するプロセスとアクションを完全に可視化すること、ならびに 2) インシデントのパターン、停止の原因などを完全に理解して、改善するためのベースラインを提供することです。

実際、ITチームの最善の努力にもかかわらず、貧弱なシステムとリソースの不足により、戦術的で事後対応的なサービスお

よびサポート活動が行われるかもしれません。短期的な成果を超える体系的なアプローチは制約されており、問題は場当たりに解決されています。さらに次のことが指摘できます：

- 多くのプロセスが手動で行われ、一貫したITワークフローまたは標準が存在していない
- ステータスまたは影響の可視性が期待よりも低く、レポート機能が最小限またはまったく存在しない
- 継続的なコストとリスクが高く、解決のタイムラインが長くなることが多く、サービス品質が低い
- 上級管理職がサービスチームの影響を認識せず、より大きな投資をサポートすることはほとんどない

また、2019年12月のITXM調査から得られた以下の調査結果により、サービス管理プロセスとリクエストワークフローが資産情報と関係を自動的に可視化しているかどうか明らかにになりました。

ご覧のとおり、回答者の3分の1未満が資産情報の可視性を有していると答えましたが、残りの3分の2は時々かまったくないと答えました。

同じ調査によると、IT部門は、統合されたITサービス管理とIT資産管理プロセスおよびデータを用いて、以下の改善を期待しています。

- IT資産の可視性の向上- 63%
- ITスタッフの生産性の向上- 59%
- 最適化されたコスト- 54%
- サービス提供の改善- 53%

5

ノートパソコンのロックアウト

営業社員がヘルプデスクに電話をし、ノートパソコンからロックアウトされ、ロック解除するためにかけるべき電話番号が表示されていると申告しています。以前一緒に仕事をしたパートナーからと思われるメールのリンクをクリックしたところ、ノートパソコンがロックされたとのこと。はっきりしたことは不明ですが、他の従業員も同じメールを受け取っている可能性があります。

このユースケースにおいて、可視性の欠如はつぎのような問題を含んでいます。同じ電子メールを受信した他の従業員が不明、現在のパッチ適用範囲の更新時期、マシンの管理権限を持つ人の知識不足、さらに、感染したデバイスの数とそのステータスが不明、といったものです。

2019年のIvantiがスポンサーとなったWindows 10の調査では、回答者の最も重要なセキュリティ上の懸念の1つはデータ侵害リスク(41%)であり、その次はランサムウェア/マルウェアへの恐怖(20%)であることが判明しました。さらに、2019年4月に実施された別のIvanti主催の調査では、もしリアルタイム

の洞察を得ることができれば、70%の組織がセキュリティステータスについて最も知りたいと考えており、60%近くがアプリケーションデータの可視性を望んでいることがわかりました。

統合エンドポイント管理の観点から見ると、可視性の欠如はセキュリティインシデントへの取り組みにかかる時間を増やします。また、インシデントが組織のデータを侵害するリスクを高め、過労なチームに圧力を加え、組織に対する信頼を低下させます。これは、可視性の制限または統合データの不足の結果である可能性があり、資産データとセキュリティ情報の競合につながり、可視性のギャップが生じ、迅速な対応が困難になります。

一方、正確なパッチデータとユーザーアクセス情報を可視化することで攻撃に迅速に対応し、ネットワークを保護することができます。ランサムウェアなどの脅威を減らし、拡散を阻止します。また将来の攻撃に備えられます

さらに可視性がないため、再イメージングのニーズを効率的に管理して、上記の状況での修復をサポートすることが難しくなります。

サービスデスクアナリストの観点から見ると、環境内の資産、場所、使用者、使用方法を完全に可視化することは、面倒な表計算を利用せずに、解決時間の短縮などの効率的なジョブパフォーマンスを実現するために不可欠です。今回の使用例では、電子メールの疑いから生じる潜在的な脅威の可視性の範囲を広げることで、より迅速な修復が促進されます。



6

ITが知らない世界

ITアナリストは自社環境のセキュリティを評価していますが、自社内にどのマシンが存在するのか、それらが適切に管理されているのか、情報がありません。IT部門は自社環境内の75%しか把握できていません。さらに継続的なソフト更新などにより、マシンは管理されなくなりつつあります。サーバ側では適切な構成情報なしで仮想マシンが作成され、またパッチ更新で最新の状態に保たれていません。

このユースケースでは、企業環境内のエンドポイントとサーバの分析結果が存在しないため、実稼働レベルでパッチが適用されたのかは不明です。すべての組織においてIT資産の物理的または仮想的な場所を知ることは、サービスとサポートの観点からだけでなく、セキュリティの観点からも常に重要です。IT部門の管理外に放置され、最新のパッチが適用されていない資産は、データの整合性とコンプライアンス上のリスクに

なります。また、ITの脆弱性が増加しているため、すべてのデバイスを追跡することが重要になります。

「Data Validation the Best Practice for Data Quality in Fixed Asset Management (固定資産管理におけるデータ品質のベストプラクティス)」というタイトルの前述のEYホワイトペーパーでは、IT固定資産の30%が「幽霊」資産であり、見つけることができないと述べられています。多くの組織は保有資産を過小評価しているため、資産の可視性は重要な最初のステップです。組織が最初にIT資産管理を開始したとき、思っ



ていたよりも20~30%多くのデバイスを見つけることは珍しくありません。自分の知らないことを管理することはできません。これは重大なセキュリティリスクをもたらします。

統合エンドポイント管理ソリューションを使用すると、エンドポイントを完全に可視化および制御できるため、すべてを保護し、保護されていない管理対象デバイスから生じる脅威を回避できます。ITチームは、リアルタイムスキャンを実行し、ユーザーと場所の情報を突合する自動化されたプロビジョニング戦略の恩恵を受けます。仮想サーバの予想外の増加を回避するには、管理者権限を持つユーザーを確認して、他のITグループが運用レベルのセキュリティを備えた仮想マシンのみを起動できるようにすることが重要です。それでも、これらの新しいサーバを見つけてグループに追加する機能により、次のメンテナンスウィンドウを見逃すことはありません。

さらに、ライフサイクル全体を通して資産を管理することが重要です。パフォーマンス資産データ、問題、修正、パッチ情報、契約、およびライセンスを追跡することにより、ソフトウェアおよびハードウェアへの投資が最適なパフォーマンスで実行され、従業員の生産性に影響を与えないことを確認できます。

Ivanti:頭の後ろの眼

CIO、CISO、およびITの役員の眼が見えていなければ、高いレベルのリーダーシップと責任を達成できません。そのため、統合エンドポイント管理およびエンタープライズサービス管理ソリューションで体験できる拡張された可視性の確保により、チームの目標、業界の洞察、ビジネスの使命とビジョンを補完およびサポートできます。

IvantiがITの可視性をどのように改善するかをご覧ください。ユーザーのITエクスペリエンスの向上に向けて決定論的に行動し、組織の効率と生産性の向上を実現できます。詳細については右の連絡先へお問い合わせ願います。

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

[ivanti.co.jp](https://www.ivanti.co.jp)

contact@ivanti.co.jp