

A woman with long, curly hair is looking down at a tablet computer she is holding. She is wearing a light blue shirt and a necklace. The background is a blurred office environment with windows.

ivanti

強固なIT・セキュリティ 基盤の構築

あなたの会社のIT資産を把握することで得られる3つの付加価値

ハイブリッドワークの時代には、すべての人の日常業務がITに依存しています。オンラインで仕事をする人や部署が増えれば増えるほど、企業のIT資産は複雑化します。



今日、従業員は平均2.6台のデバイス^[1]を使用して仕事をしています。

マップ作成、監視、保護、およびプロアクティブな保守が必要な多くのエンドポイントがあります。さらに、IDCnpredict^[2]は、2025年までにエッジで接続するデバイスが79.4ゼタバイトのデータを生成すると予測しています。

ITとセキュリティの実践には、企業のIT資産を完全に把握することが不可欠です。知識は、単なる、欠点のないCMRD（構成管理データベース）以上に多くの利益をもたらす力です。

1 従業員のデジタル体験管理 (DEX) 向けの進化していく諸要件、EMA, 2022

2 世界各国のグローバルDataSphere IoTデバイスとデータの予測、2019-2023、IDC



01 サポートとサービス管理の向上

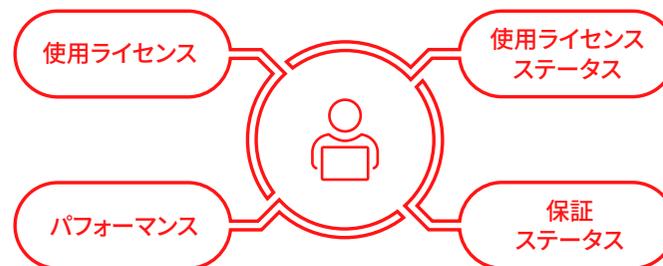
02 可視性と情報セキュリティの向上

03 コスト管理の管理性向上

01 サポートとサービス管理 の向上

IT環境が複雑になればなるほど、会社のサービスチームは、より多くのデバイスをサポートする必要があり、中にはネットワークにアクセスしていることにさえ気づかないデバイスもあります。その結果、より多くの問題が発生し、雪崩のようにサポート依頼を引き起こす可能性があります。

そこで、IT資産 を完全に把握することが、第一線のサポートチームとサービス管理チームにメリットをもたらすのです。使用状況、パフォーマンス、ライセンス、保証のステータスなど、すべての資産に関するデータを一元管理することで、よりプロアクティブなアプローチに移行でき、エンドユーザーの業務に影響を与える前に問題を解決することができるようになります。



しかし、仮にカスタマーサポートへの依頼があったとしても、すべての資産情報が1つの場所にあることで、サービスデスクは、問題をさらにエスカレートさせることなく、より迅速に解決するための完全なコンテキストを持つことができます。

ITサポートチームとサービス管理チームに、IT資産全体に関して、深い、コンテキストに基づいたデータを提供することができます。これらのチームのスマートで迅速な意思決定を可能にしより良い従業員の経験を実現し、生産性を高めることとなります。



02

可視性と情報セキュリティの向上

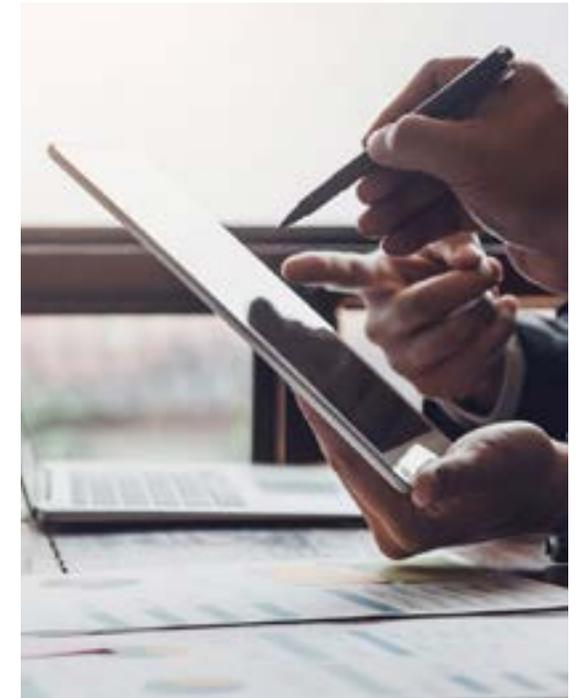
知らないものは保護できません。しかし、接続されたデバイスの量が増えているため、手動での監視や監査は、少なくともリアルタイムでは事実上不可能です。

データ侵害の平均コストは 435 万ドルに 達します^[1]。

情報漏えいの平均コストは435万ドルに達し、ダウンタイムは年々増加しているため、ITセキュリティ・チームは、会社の企業ネットワークにアクセスする対象を常に把握する必要があります。すべての資産の情報を一元的に把握することで、従業員のデジタル体験に影響を与えることなく、コンプライアンスとデータセキュリティを維持することがはるかに容易になります。

米国に本拠を置くインターネットセキュリティセンター(CIS)^[2]は、18の重要なセキュリティコントロールを定義しており、その最初の2つは、企業資産のインベントリーとコントロール、ソフトウェア資産のインベントリーとコントロールです。B31そのうちの最初の5つに対処することで、サイバー攻撃の85%を防ぐことができます。

EU に拠点を置く ENISA^[3]も同様の範囲をカバーしており、27 の管理領域に分かれています。これらの管理が満たされてはじめて、管理者は、データ保護やアクセス制御管理など、さらに重要なセキュリティ管理を適用するための十分な能力を備えることができます。



この2つの基本的なセキュリティ管理は、モバイル機器などの物理的資産、オペレーティングシステムやアプリケーションなどのソフトウェア資産を含む、すべての企業資産の棚卸し、追跡、修正を網羅するものです。会社のIT環境全体を把握することで、許可されたソフトウェアのみをインストールおよび実行できるようにし、ネットワークに接続された新しい資産は自動的に識別および分析されるようにすることができます。

1 [データ侵害のコスト 2022年レポート、IBM](#)

2 [18のCIS重要セキュリティコントロール、センター・フォー・インターネット・セキュリティ](#)

3 [デジタルサービスプロバイダのための最小限のセキュリティ対策の実施のための技術的ガイドライン、ENISA](#)

03 コスト管理の管理性向上

IT支出の管理はかつてないほど難しくなっています。測定可能性と敏捷性はビジネスの決定的に重要な要素であり、ITはその中心に位置していますが、今日のマルチクラウド・アーキテクチャは統治が困難であることは否めません。

IT専門家の **32%** は、IT支出の10-25%が未使用、不十分な使用、未管理、未計上なソフトウェアに浪費されていると考えています^[1]。

会社の資産の利用状況 データを会社のIT環境全体のコンテキストに置いて把握することにより、会社のIT予算とチームをより上手に管理して、会社の資産の使用を最適化できます。たとえば、ソフトウェアのライセンスや保証契約、物理的および仮想的な資産、クラウドサービスを知ることで、マシンを修理するべきか、引退させるべきかを迅速に判断することができます。

コスト管理強化のためのもう一つの領域はライセンス管理の最適化。サブスクリプション型IT資産への大きな依存、キャンセル可能な未使用のライセンスやクラウドのサブスクリプション、または欠けているライセンスを把握することにより、コストを削減し、罰金を招くリスクを減らすのに役立ちます。



これらの情報がすべて一箇所に集まることで、サービスデスクは、例えばアプリケーションのアクセス要求を解決する際に、十分な情報に基づいた意思決定を行うことができるようになります。別のアクセス権を購入する代わりに、既に支払っているが使用されていないアクセス権を再割り当てすることができます。

1 [Modern ITAM in the Digitally-Transformed Enterprise, Enterprise Management Associates, 2022](#)

単なる可視化以上

IT資産全体の把握は、会社のネットワーク上の資産の発見と可視化だけにとどまりません。IT資産全体の把握を、ITサポートとサービス管理の強化、セキュリティ体制の強化、より良い従業員体験の提供、IT支出の最適化のための基盤として扱うことで、真のメリットが得られます。Everywhere Workplace (場所にとられない働き方) を円滑に行い、かつ成功させるためには、IT環境に関するすべての情報が集約された単一の場所が不可欠です。



強固なIT・セキュリティ基盤の構築

あなたの会社のIT資産を把握する
ことで得られる3つの付加価値

ivanti

ivanti.com/ja

03-6432-4180

contact@ivanti.co.jp