ivanti

IT部門と企業に

統合化されたIT

がもたらすメリット

統合化されたITのパワー

IT部門が管理しているのは、企業の中で最も急速に変化しているIT事業です。

テクノロジーの急速な発展によってもたらされる課題と可能性は、ユーザーがコンシューマー向けサービスのように企業のリソースをいつでもすぐに利用できることの要求の増加、そして企業の大きな失敗の原因ともなるセキュリティの脅威の増大が伴います。

IT部門には、新たな技術や方法を導入し、企業の成長を支援しつつ、わずかな労力と時間で多くの業務を遂行することが求められています。IT部門は、この種の課題やリスクもリターンも大きい問題を解決することの技能を最も求められています。

IT運用部門、セキュリティ部門、資産管理部門が交差するポイントをスタート地点にするとよいでしょう。

常に先手を打つために、IT部門は常に改善する方法に目を向けています。IT部門は、スタッフの知識やスタッフが難なく利用できる技術を新たな目的のために活用できる可能性についてだけでなく、自社のIT環境を最適化するためには今以上に可視化、速やかなフィードバック、事業運営上の情報がIT部門に必要なことにも気付いています。

IT運用部門、セキュリティ部門、資産管理部門が交差するポイントをスタート地点にするとよいでしょう。

例えば、ほんの数年前まで、ハードウェアとソフトウェアのインベントリ（目録）をソフトウェアの配布と組み合わせることが重要である理由を誰もが疑問に思っていました。ところが今では、企業の環境に存在するデバイスとソフトウェアを把握することは、正確な拠点位置にソフトウェアの配布にとって極めて重要なだけでなく、デバイスに最新のパッチを適用し、セキュリティの脅威に対してリアルタイムの対応を行う基盤を提供する上でも役立っています。この情報は、IT部門が監査や規制の要求事項に対応する際や、企業がソフトウェアライセンス、リース、ITに関連する支出を主体的に最適化するためにも役立つ可能性があります。

ただし、多くの企業がそうであるように、これらのツールとプロセスが様々な部門に分散されている場合、誰もが自らの業務に追われ、これらすべてを集約化することなど思い付きもしないのです。異なるツールや異なる部門間でデータとプロセスが共有されていれば、どれだけ報告、連絡、対応にかかる時間が短縮されるか考えてみてください！

他部門のIT機能やツールと連携を取り、可視化を強化し、対応を自動化すれば、目の前にある可能性がはっきりと見えるようになるはずです。この可能性をもたらすものをIvantiは「統合化されたITのパワー」と呼んでいます。

「統合化されたIT」の導入例をいくつかご紹介いたします。

オンボーディング＆オフボーディング

新入社員のオンボーディングとオフボーディングは一筋縄ではいかないことがあります。多くのIT部門にとって、オンボーディングとオフボーディングとは手動で行う必要のある数多くの作業を伴うプロセスで、予定通りにいかないことや、ミスが起きることは避けられないプロセスとなっています。

ただし、統合化されたアプローチを導入すれば、プロビジョニングとデプロビジョニング（プロビジョニング解除）プロセスを簡易化し、自動化することができます。新入社員が入社すると、IT部門には新入社員の上司にあたる社員や人事部門の社員から、新入社員に必要なハードウェアとソフトウェアを支給することを使いやすいポータル経由で依頼できます。ハードウェアが届いたら、ネットワークに接続します。そして、ハードウェアが認識されると、システムが自動的にデバイスのプロビジョニングを実行し、新入社員の職務に適切な権限とアクセス権に従って企業のシステム上に新規アカウントを作成します。社員の職務が変わると、システムは以前の職務の権限を取り消し、新しい職務に合わせて権限を更新します。

もちろんすべての作業が自動で実行されます。また、ツール、プロセス、データを連携することで、コンプライアンスに関するレポートを簡単に作成し、各社員に付与されているアクセス権や、各社員がアクセス権を取得した方法や時期を実証できます。セキュリティの観点から考えると、社員が退職する場合に、すべての権限が確実に取り消されるという安心感を得ることができます。

統合化されたアプローチを導入すれば、プロビジョニングとデプロビジョニング（プロビジョニング解除）プロセスを簡易化し、自動化することができます。

プロビジョニングとアイデンティティのワークフローを資産管理、セキュリティ管理、サービス管理のITプロセスと統合することにより、ユーザーは問題なく作業を開始し、生産性を維持することができ、企業は安全をさらに強化できます。

「市販されている自動化のためのソフトウェアは他にもあります。IVANTIが他のソフトウェアと決定的に違うのは、社員の職務が変わった場合、リアルタイムで調整できる機能が装備されている点です。今ではダウンストリーム・システムに社員による作業や手動の作業を一切必要とせずに、ユーザー設定や権限の変更を実行できるようになっています。行われた作業は人事部門が社員の役職名を変更することだけでした。変更は、IDENTITY DIRECTORによって認識され、自動的にダウンストリーム・システムすべてに変更が適用されました」

MATTRESSFIRM®

Windows 10への移行

インプレースアップグレードとして実行するかハードウェアリプレースの一部として実行するかを問わず、大規模なOSの移行は、IT部門が取り組む作業の中で最も業務への支障が大きい作業です。企業は依然として、Windows 10への移行および更新の計画を立て、安全に実行する方法を見出せず苦戦しています。

ユーザーは新しいデバイスを注文し、自動的にプロファイルとデータをすべて保存し、デバイスを受け取り、設定、カスタマイズすることができます。

「統合化されたIT」のアプローチを導入することで、「ゼロタッチ」モデルのプロビジョニングでサービス管理のワークフローが使用されるため、ユーザーは新しいデバイスを注文し、自動的にプロファイルとデータをすべて保存し、デバイスを受け取り、設定、カスタマイズすることができます。しかもこの一連のプロセスにIT部門の関与は一切不要です。企業はネットワークの帯域幅に過度の負担をかけることなく、Microsoftの頻繁な更新プログラムを自動化し、段階的に実施することもできます。

また、セキュリティ機能がオンに設定され、正常に機能していることを保証し、同じプロセスの一環としてサードパーティー製アプリも保護できます。さらに、システムとプロセスが集約化されているため、ビジュアルダッシュボード経由でWindows 10へのアップグレード状況を抜かりなく追跡することができ、後に行われる監査を簡素化できます。

（100の施設に学生のデバイスが65,000台）

「プロジェクトには絶対に遅れられない期日が設定されていました。期限は、展開開始から約8週間後の7月31日でした。

入念な計画、社員の素晴らしい仕事ぶり、計画の進行状況を確認できる機能のおかげで、

期日の1週間前に65,000台以上のマシンをWINDOWS 10に移行することができました」

CYPRESS FAIRBANKS
INDEPENDENT SCHOOL DISTRICT

「ゼロタッチ」のITソフトウェアのリクエスト&再取得

社員の継続的な生産性を保証するため、企業はセルフサービスポータル経由でITを統合し、ソフトウェアのリクエストと関連のプロセスを自動化できます。ここではその仕組みを説明させていただきます。

社員がアプリストアのようなセルフサービスポータル経由で必要なソフトウェアをリクエストすると、

手動操作を一切必要とせず、社員が使用しているデバイスに対応した適切なソフトウェアが自動展開されます。IT部門は、統合化された承認ワークフロー、ライセンスの可用性、コンプライアンスチェックからメリットを得られます。また、所有しているIT資産と各IT資産がどのように使用されているかを把握しているため、企業は未使用のソフトウェアを再取得し、ソフトウェアのコストを最適化し、いつでも自信を持って監査にのぞめる態勢を整えることができます。

社員がアプリストアのようなセルフサービスポータル経由で必要なソフトウェアをリクエストすると、デバイスに対応した適切なソフトウェアが自動的に展開されます。

これこそまさに、ITサービス管理、資産管理、エンドポイント管理プロセスが連携して機能している環境です。

このシナリオでの「統合化されたITのパワー」とは、IT部門がサービスリクエストを自動化し、自由に使えるリソースを増やし、監査にのぞめる態勢を整える対策を提供し、結果的に少ないコストで業務を最適化することを可能にすることです。

「使用されていないソフトウェアを自動的に特定し、削除するためのソリューションを導入後わずか3ヶ月で、ライセンスにかかっていたコストを$958,000節約することができました。また、ユーザーの問題に対応するために利用できる時間が大幅に増え、ソリューションも劇的に改善されました。当社はユーザー重視の姿勢に誇りを持っており、IVANTIは当社のそのような姿勢をさらに強化してくれています」

Sealed Air

多層防御のセキュリティ

ハードウェアとソフトウェアのインベントリ（目録）についてお話したことを覚えていらっしゃいますか？ハードウェアとソフトウェア資産に関する情報を把握していれば、

社内に存在するセキュリティのギャップを特定し、パッチ適用やホワイトリスティング 、管理者権限管理などのソリューションでそのギャップを埋めることができますが、セキュリティを潜り抜けることに成功した脅威に対してはどのような対策を取り、阻止することができるでしょうか？プロセスを自動化するために社員とツールを確実に連携できるシナリオであれば、それだけで十分なセキュリティ対策となります。ここでは、ITの統合化が進んでいる企業における防御の仕組みをご紹介いたします。

企業の環境において悪意のあるコードの存在が検出された場合、すぐにネットワークから悪意のあるコードが存在するエンドポイントを自動的に隔離できます。隔離した後、信頼できるコンソールから、簡単なマウスクリック操作で隔離されたマシンを遠隔操作し、状態に関する情報を取得し、イメージを再適用するためのプロセスを実行できます。

プロセスを実行すると、ユーザーの設定とアプリケーションが自動的に再インストールされ、バックアップされていたドキュメントすべてが復元されます。エンドポイントにイメージを再適用中、デバイスの状態に関する情報を使用し、脆弱性がある他のデバイスのために環境を速やかにスキャンし、すぐに脅威に対応するため他のデバイスを更新することもできます。これで防御は万全となり、再び安心して重要な事業目標に集中できるようになります。

社内に存在するセキュリティのギャップを特定し、そのギャップを埋めることもできます。

「IVANTIのおかげで、当社は自社の環境について理解を深められることができ、500以上のサーバーにパッチ適用が必要であることを特定することができました。しかも非常に短期間で…IT部門は、様々な種類のオペレーティングシステムに素早く簡単にパッチを適用できるようになりました。また、IT部門はパッチを適用するために当社の環境に存在するすべてのオペレーティングシステムに関する詳細な情報を理解する必要がなくなり、単一のコンソールから複数のオペレーティングシステムにパッチを適用できるようになりました。これまでよりもはるかに短い時間でパッチ適用の要件を満たすことができるようになったため、IT部門が他のプロジェクトにあてられる時間が各段に増えました」

SWIN BUR NE
SWINBURNE UNIVERSITY OF TECHNOLOGY

統合化されたITのパワー

本書で紹介したのは、社員が日々直面している問題を解決する上で、ITを統合することがいかに役立つかを示す一例にすぎません。自社の環境において組み合わせられるIT関連の機能を検討することに加え、事業にプラスの影響をもたらし、コストを削減し、エンドユーザーの満足度を向上できる可能性がどの程度あるのかを検討すれば、企業は状況を一変できます。**そしてIvantiはそのために必要なソリューションを提供できます。**

当社のミッションは明確です。Ivantiは、「統合化されたITのパワー」を通してお客様が市場で成功できるよう支援することを目指しています。

IVANTI誕生の経緯

2017年1月LANDESKとHEAT Softwareの統合に伴い、新たな会社名が必要となりました。LANDESKとHEAT Softwareは30年近く、ITセキュリティのリスクを軽減しつつユーザーの生産性を上げるユーザー重視のITソリューションを提供してきました。

LANDESKは、「クライアント管理」、「エンドポイント保護」、「ITサービス＆サポート」、「エンタープライズモビリティ管理」の4分野において、調査会社Gartnerによって高く評価されていた唯一のベンダーでした。

LANDESKとHEAT Softwareは時代と共に変化を遂げてきました。LANDESKは、Wavelink、Shavlik、Xtraction Solutionsなどの企業を買収してきた企業で、最近ではAppSenseを買収しています。HEATは、FrontRangeとLumensionを統合して誕生した企業でした。このように両社の傘下にはたくさんの企業が名を連ねています。この数ある企業名をひとつのブランド名にまとめるためIvantiが誕生しました。以来、ConcordeとRESはIvantiの傘下に入っています。

詳細はこちら：www.ivanti.co.jp | 03-5226-5960


ivanti