Windows 10 への移行に役立つ 10 の情報

最近 Dimensional Research によって世界規模で実施された調査では、IT 企業の 37%が来年内、35%が 2 年以内に Windows 10 への完全移行を予定しており、14%が移行のスケジュールを立てていないことが明らかとなりました。このいずれかに該当する場合、これまで様々な企業と連携して行った OS 移行の取り組みから得た当社の経験がまとめられた本書が役に立つでしょう。

役立つ情報 1：適切なブランチを選択する

Windows 10 の発表と共に、Microsoft は Windows 10 のエンドポイントを常に最新の状態に維持するため、これまでよりもはるかに頻度の多い更新プログラムを導入しました。Windows 10 の出現により、サービス提供モデルのオプション Current Branch for Business（CBB）および Long-Term Servicing Branch（LTSB）が、この年に 2 回更新プログラムがリリースされる「半期チャネル（Semi-Annual Channel）」に変更になります。

半期チャネルを展開しているエンドポイントには年に 2 回メジャーな更新プログラムが提供され、長期サービスチャネル（Long-Term Servicing Channel）を使用しているエンドポイントには、不定期（おそらく 2～3 年に 1 回）にメジャーな機能更新プログラムが提供される予定です。さらに Microsoft は、「長期サービスチャネルは店頭や産業デバイスのみを目的としている」という自社の姿勢を改めてはっきりとさせるため、半期チャネルに内蔵されている不必要な機能の多くを長期サービスチャネルから排除しています。これには、Windows Store アプリ、Cortana（コルタナ）機能、Microsoft Edge ブラウザが含まれます。

多くの企業が年に 2 回半期チャネルから更新プログラムを受け取ることになります。これにはセキュリティが強化され、機能更新プログラムが提供されるというメリットがある一方、頻繁に更新が提供されるため、IT チームが常に移行中の状態に陥るというデメリットもあります。

役立つ情報 2：OS 展開戦略を選択する

デスクトップの移行プロジェクトに取り組む際、いくつかのデバイス関連の注意点を考慮する必要があります。1 つ目の注意点は、サポートの問題です。一部のデバイスは単純に Windows 10 をサポートしません。2016 年後半以降、Windows 7 が事前にインストールされた PC は出荷されなくなり、最新のプロセッサは Windows 10 でのみサポートされるようになりました。既存のエンドポイントを交換、アップグレードもしくは既存のエンドポイントにイメージを再適用しましたか？

2 つ目の注意点は、「ステルス IT 移行」の問題です。独自の調査では、たとえ企業によって正式にサポートされていないとしても Windows 10 がインストールされた新しいデバイスを導入することを IT 部門がユーザーに許可する「ステルス IT 移行」の問題が、Windows 10 早期導入を後押しした最も大きな要因であることが確認されています。

冒頭で触れた Dimensional Research が実施した調査では、Windows 10 へ移行するために導入されている唯一にして最良のアプローチは存在しないことが明らかとなっています。回答者の 52%がシステム管理ツールを使用して既存のエンドポイントのイメージの再適用を予定していると回答しており、49%がハードウェアの移行、すなわち新しいデバイスの展開に合わせて Windows 10 へアップグレードを行

うことを検討していると回答しています。一方、コンピューターの入れ替え時期と OS の移行時期を一致させることにより、企業はインプレースアップグレードにまつわる時間とコストを節約できる可能性があります。

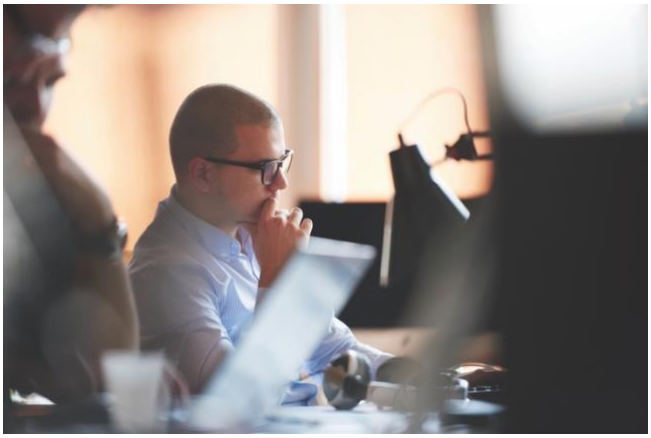
役立つ情報 3：アプリケーションを移行の障壁にしない

Windows 10 に移行する際に企業が直面する最大の障害のひとつが、アプリケーションの互換性の問題です。

幸運なことに、今は仮想化、階層化、もしくはストリーミングテクノロジー経由でお使いのデスクトップ環境にアプリをスムーズに統合することを可能にするアプリケーション提供プラットフォームがたくさんあります。アプリケーションを根底にある OS から切り離すことで、これらのテクノロジーは、Windows 10 など新しいオペレーティングシステムを使用する際、アプリケーションの互換性に関する問題を軽減できます。

以下の質問は、アプリケーションを提供する方法を選択する際、ご自身とユーザーのニーズに最も適したアプローチを見極める上で役立ちます。

- ユーザーはオフラインでアプリケーションにアクセスする必要があるか？
- ユーザーがこれらのアプリケーションを実行するために必要とする権限とは？
- どのような方法でこれらのアプリのライセンスを付与するか？
- IT 部門はどのような方法でアップグレードに対応するか？
- 上記の条件を踏まえ、自社にとって最もコスト効率に優れたアプローチとは何か？



また、Web アプリケーションも考慮する必要があります。現在互換モード、もしくは特定のバージョンの Java を使って IE9 上で問題なく社内の Web アプリを実行している場合、IE11 や Microsoft Edge に移行すると何が起きるでしょうか？自社専用の Web アプリケーションを開発していますか？もしくは、コストや時間がかかる可能性のあるサポートを続けるために社内の Web アプリケーションを仮想化していますか？もしくは、互換性の問題を解決するために、管理が難しくセキュリティの問題につながる可能性のある複数のブラウザ（例：Chrome、Firefox など）をインストールしていますか？

Ivaniti は移行前に、実行するために管理者権限が必要なアプリケーションに特に注意して Windows 10 上でビジネスクリティカルなアプリケーションを再検証することを推奨しています。

役立つ情報 4：究極のユーザーエクスペリエンスを作る

新しいワークスペースを受け入れられるかどうかの審査は、ログオンの時点で始まっています。初回ログオンに時間がかかる場合、新しいワークスペースをユーザーが好意的に受け入れる可能性は初日から低くなるでしょう。また、ログオンや実行に時間がかかったり、画面がフリーズしたり、アプリケーションが利用できなかったりする度に、ユーザーが受け入れる可能性、そしてユーザーの生産性は低下します。

新しいワークスペースの使いやすさとユーザーが受け入れる可能性を最適化するため、Ivanti は新しいワークスペースでのユーザーエクスペリエンスを評価するアナリティクスの実行を推奨しています。既存の環境を基準とし、ログオンにかかる時間やメモリ使用量、CPU 使用量、アプリケーションの利用状況、リソースを実行するために必要な権限などの指標を記録する必要があります。また、ユーザーが自分のデータを保存するために使用している方法や保存場所も慎重に確認する必要があります。これは、移行中および移行後にユーザーが満足できるユーザーエクスペリエンスを確保するために必要不可欠な情報となります。

このプラクティスにより、新しい環境でのサービス品質に影響を及ぼす可能性のある潜在的な障害や処理時間を遅くする機能を未然に防ぐことができます。さらに、このプラクティスは、ライセンス要件を把握し、不必要かつ安全ではない権限が付与されているユーザーを特定する場合にも役立ちます。

役立つ情報 5：ユーザーのワークスペースをパーソナライズする

Dimensional Research による最新の調査で、回答者の 90%以上がデスクトップを変更することについてどう思うかという問いに対して、迷惑や落胆といった感情を示していることが明らかとなりました。同調査では、回答者の 32%がすでに Windows 10 のインターフェースに困惑していることも明らかとなっています。Windows 10 へ移行後、ユーザー個人の設定が失われる場合、当然ユーザーは新たに提供された Windows 10 のワークスペースを受け入れることについて難色を示すでしょう。

このシナリオを避けるため、引き続き古いオペレーティングシステムとハードウェアについてユーザーのサポートを継続する必要があります。ただし、ユーザーが Windows 10 を実行する新しいハードウェアも必要としている場合、問題が生じます。それはなぜでしょうか？Windows 10 には、ユーザーが異なるデバイスとプラットフォーム間で切り替えを行う場合、ユーザー設定を維持することをさらに難しくする追加の移動プロファイルアーキテクチャが装備されています。

逆に、ユーザーが新しい（手強い）Windows 10 ワークスペースにログオンし、使い慣れた設定が表示されれば、未知への恐怖を最低限に抑え、受け入れることへのユーザーの抵抗を軽減し、Windows の古いバージョンのサポートを続ける必要がなくなります。

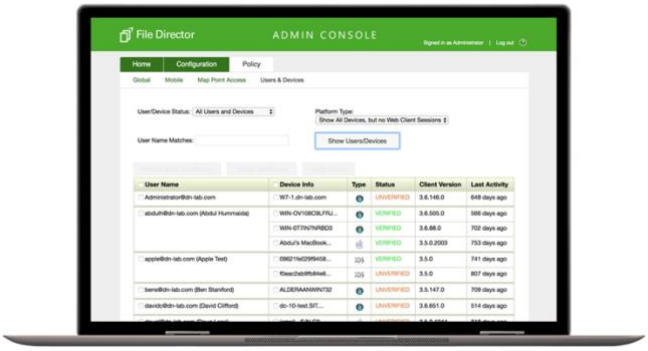
移行後ユーザー設定を維持するため、根底にあるオペレーティングシステムとアプリケーションから個別にユーザーのパーソナライゼーションを取得、管理する必要があります。これにより、ユーザーがログオンしているデバイスやプラットフォームに関わらずユーザー個人の設定が常に利用できるようになります。

役立つ情報 6：ユーザーに各自のデータへのアクセス権を付与する

新しい Windows 10 エンドポイントの提供にまつわる最大の課題のひとつが、ユーザーの古いデバイスのローカルに保存されているファイルとフォルダーの移行方法です。この場合、企業と個人のファイルが安全にバックアップされていることと、企業と個人のファイルが問題なく新しいデバイスに移行できることを IT 部門はどのような方法で確認すればいいのでしょうか？また、IT 部門にとっては、最善の移行方法を見極めるために、存在するローカルファイルの数を把握することもまた困難です。

ユーザーのファイルとフォルダーがデータセンターのファイル共有システムやホームドライブに保存されていることも、IT 部門とエンドユーザーにとっての課題となります。ユーザーがリモートもしくはオフラインで作業している場合、データセンターに保存されているファイルにはアクセスできません。オンプレミス環境のファイル共有システムにリモートでアクセスする場合、通常 VPN を使用する必要があります。これはユーザーを煩わせるだけでなく、セキュリティや複雑さのレイヤーを追加することになり、break/fix（**破損時補償**）、移行、アップグレードの点において、IT 部門の頭痛の種となります。

Ivanti® File Director（AppSense 提供）は、保存されている場所を問わず、ユーザーのデータの簡単な移行を可能にします。File Director を導入すれば、ユーザーのファイルとフォルダーの移行作業がシンプルかつストレスのない作業となります。一度起動すれば、IT 部門は瞬時に今後の移行プロジェクトに向け万全の体制を整えることができます。さらに、ユーザーに一切気付かれずにデータ移行プロセスを実行できます。



役立つ情報 7：Windows とアプリケーションにパッチが完全に適用されていることを確認する

ランサムウェアの攻撃とその他の種類の悪意ある攻撃の増加に伴い、新しいさらに高度な脅威からシステムを保護しつつ、コンプライアンス要件を満たすことは企業にとってますます難しくなっています。

ソーシャルエンジニアリングは、安全ではない操作を行わせる、もしくは機密情報を漏洩させるようユーザーを巧みに誘導するテクニックを使用します。これらの標的型攻撃の多くが、パッチが適用されていないオペレーティングシステムやアプリケーションによる OS とアプリケーションのコンテンツの脆弱性や弱点を探しています。

総合的なパッチ管理ソリューションは、Windows 10 のエンドポイントとインストールされているアプリケーション両方の脆弱性を検出することにより、事業継続を妨害することなく全社の Windows 10 環境を保護できます。

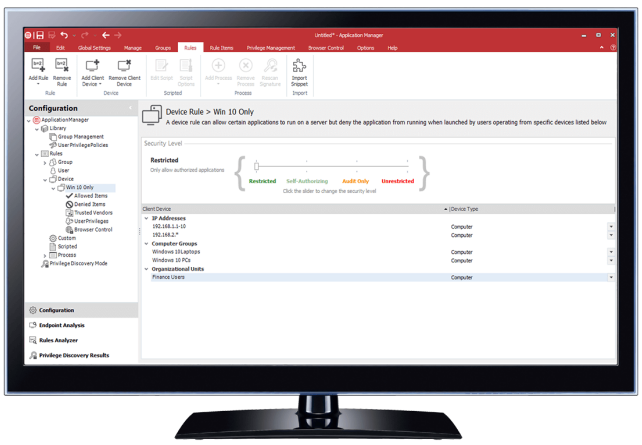
役立つ情報 8：悪意のある、もしくはライセンスが付与されていないアプリケーションを阻止する

ユーザーは Windows 10 Store アプリを使用する予定ですか？もし使用する場合、ユーザーがアクセス、インストール、実行できるアプリをどのような方法で管理しますか？何らかのアプリケーション管理を導入していなければ、おそらく生産性、コンプライアンス、セキュリティの問題に直面することになるでしょう。

ただし、管理しなければならないのは Windows Store アプリだけではありません。Windows の従来のアプリもまた管理する必要があります。様々なデバイスを仕事に導入しているユーザーが増えているため、ソフトウェアライセンスの利用状況を管理することは IT 部門にとってクリティカルな業務となっています。

さらに、ライセンスが付与されていないソフトウェアやランサムウェア、その他の悪意のある実行可能ファイルをユーザーがダウンロード/インストールできる場合、既存のデスクトップのセキュリティとコンプライアンスの低下につながる可能性があります。新しい初期状態の Windows 10 ワークスペースでこのような事態に陥ることは企業にとって望ましいことではありません。

従来のホワイトリストおよびブラックリストテクノロジーには、新しいサービスパックやアップグレードがリリースされた場合、もしくは不明なマルウェアが侵入した場合、一般的に継続的なメンテナンスが必要となります。これは IT のサポートコストの増加につながります。また、この種のソリューションは多くの場合、不明なアプリケーションやブラックリストのアプリケーションの名前をホワイトリストにあるアプリケーションの名前に変更することで簡単に潜り抜けられてしまいます。



Ivanti® Application Control（AppSense 提供）は、Trusted Ownership™ モデルを使用しています。このモデルでは、信頼されていない所有者、すなわち標準ユーザーによってインストールされたすべてのアプリケーションのインストールや実行が自動的に阻止されます。これにより、ゼロデイ攻撃から環境を保護し、アンチウィルスソフトウェアなど問題が発生してから対応する古いソリューション（更新の定義をダウンロードまたは適用する前に脅威について知る必要があるソリューション）の問題を排除できます。

Windows の従来のアプリケーションの管理について、Application Control は、強制的なデバイスベースのソフトウェアライセンス管理で Microsoft より評価されています。指定されたアプリケーションの実行権限を持つユーザーやデバイスを管理することで、アプリケーションインスタンスの数や、アプリケーションを実行できるデバイスやユーザー、ユーザーがプログラムを実行できるタイミングや実行できる時間の長さを制限できます。

役立つ情報 9：ユーザーから管理者権限を排除する

ユーザーに完全な管理者権限を付与することにより、エンドポイントが攻撃を受けやすくなります。これは、セキュリティや管理にかかるコストの増加、生産性の低下につながり、法的責任の問題に発展し、コンプライアンス遵守を難しくさせる可能性があります。クリティカルセキュリティコントロールに含まれる 20 項目のうち、米国インターネットセキュリティセンター（CIS）は「制限された管理者権限の利用」を 5 位にランク付けしています。

とは言っても、必要な機能やアプリケーションへの権限を付与せずに、一体どうやってユーザーの生産性を管理できるのでしょうか？

権限管理手法を導入することで、IT 部門はユーザーから速やかかつ簡単に完全な管理者権限をユーザーから排除し、代わりにユーザーが必要なアプリケーションやタスクのみに対する自己昇格権限を提供できます。これによりエンドポイントのセキュリティが単純化され、サポートへの問い合わせ電話を軽減し、TCO（総所有コスト）を削減できます。

役立つ情報 10：ハイブリッド環境向けの計画を立てる

IT チームは環境を単純化するため懸命に取り組んでいる一方、企業のコンピューター環境がかつてないほど複雑化しているのが現実です。ハイブリッドなコンピューター環境は新たな常識となっています。現代において企業の IT の成功と企業が使用しているテクノロジーはほとんど関係がなく、すべてはユーザーと IT 部門の両方にとって効率的な方法でまったく異なるテクノロジーを統合できるかにかかっています。

この新しい IT の枠組みに伴う最大の課題は、状況を予測し、それに対応できるかどうかです。Windows 10 には、PC、ノートパソコン、タブレットをはじめ、携帯デバイスやウェアラブルデバイスまで実に多くの種類のデバイスからアクセスできます。ユーザーは、異なる種類のエンドポイントを使用して様々な場所からワークスペースにログインしています。場所を問わずユーザーの生産性を向上するため、IT 部門にはユーザーがログオンしている状況を理解し、ワークスペースのエクスペリエンスをそれぞれの状況に合わせることが求められています。

例えば、一般的にユーザーがインターネットカフェにいる場合、そのユーザーは企業のリソースにアクセスするために安全が保証されている企業 LAN を使用している社員とは異なるレベルのアクセス権を必要とします。リソースに対する適切な権限を判断し、Windows 10 のエンドポイントを安全に保護するため、現在地やデバイス、接続の種類や時刻などユーザーの状況に関する情報を活用する必要があります。

http://www.ivanti.co.jp/

03-5226-5960

Contact-Japan@ivanti.com

Windows 10 の移行に関する詳細は、以下の URL にアクセスしてご確認ください。www.ivanti.co.jp/solutions/needs/migrate-my-users-to-win-10