ユニファイドエンドポイント管理：デジタルワークスペースに対応したセキュリティと生産性の実現

ワークプレースの在り方に変化が見られます。IT 部門から配布された Windows のデスクトップやラップトップを一箇所で使用する形態から、個人所有のラップトップやタブレット、スマートフォンなどのモバイルデバイスを場所を選ばず利用するスタイルへと変化しています。10 年前に、IT 部門が展開する数百、数千規模に上る多数の Windows システムを管理する場合、企業が利用できるソリューションとして、Microsoft SCCM や LANDESK などの CMT（クライアント管理ツール）がありました。しかし、モビリティ、BYOD（個人所有デバイスの業務利用）、IoT（モノのインターネット）の時代となった今、CMT では、この状況に対処するには十分ではありません。

その代わりとして今、IT 組織のあいだで期待が高まりつつあるソリューションがあります。それが、UEM（ユニファイドエンドポイント管理）です。このソリューションでは、CMT と EMM（エンタープライズモビリティ管理）を統合し、あらゆるデバイスとオペレーティングシステムを対象に、それらの管理とセキュリティの維持を、単一の画面で可能にします。デスクトップ、ラップトップ、スマートフォン、タブレット、IoT デバイスのいずれにも対応します。また、UEM では、個々のデバイスよりもユーザーを中心とした管理にいっそう重点が置かれるようになっています。一方、UEM は、ユーザーにとってもメリットがあります。単一の統合ワークスペースが実現するので、デバイスを問わずに同じレベルで容易に、コラボレーションや情報の利用が可能になります。

Forrester 社によれば、現在、15%の組織が UEM ソリューションを導入しているといいます。そして同社は、この比率が 2020 年までに 54%になると予想しています。モバイル化とグローバル化が進む今、CMT と EMM のプラットフォームを別々に運用する形態から、Citrix Workspace が提供する UEM のような単一のツールを利用する環境へと、移行するのが自社にとって望ましいのではないのか、組織は本腰を入れて検討する必要があります。

センサーやビーコンその他の類似デバイスを含め、企業内における IoT の利用が進んでいます。今後数年のうちに組織は、この状況に対応するうえで、統合管理ソリューションを拡張する必要に迫られることになります。Citrix Workspace の UEM は進化を続けており、これら IoT デバイスにも完全に対応します。

デジタルワークスペースに UEM を選択する理由

多くの組織にとって、デジタルワークスペースの UEM が賢明な選択肢といえますが、それには理由が多数あります。

シンプルな管理を実現：CMT ツールと EMM ツールは機能が大きく異なるため、多くの組織ではそれぞれのツールごとに、スタッフを用意したり、トレーニングを実施したりする必要があります。一方で、すべてのデバイスを単一の画面で管理できれば、そのほうが当然、業務効率が高いことは明らかです。また、複数の管理ツールに投資するよりも単一のツールに投資したほうが、ツール自体のコストがかからないばかりでなく、運用スタッフの数やトレーニングの回数も減らすことができるため、運用コストが大幅に削減され、より戦略的な目標の達成に向けてスタッフを活用できます。

一貫性のあるソリューション：従業員の生産性を高め、情報のセキュリティを維持するには、管理、セキュリティ、ユーザービリティにおいて、一貫性を確保することが求められます。複数のデバイスやアプリケーション、情報間で、セキュリティポリシーや管理ポリシーにわずかでも意図しない差異があるだけで、セキュリティインフラストラクチャにセキュリティホールが生じ、ハッカーやマルウェアの侵入を許す危険があります。また、従業員の生産性を確保するためには、モバイルでのアプリケーションや情報の利用で一貫性を維持することも重要になります。UEM では、以下のようにして一貫性を確保しています。

- 本来、あらゆるデバイスとユーザーを対象として、企業の管理・セキュリティポリシーを実装する場合、それが単一のセットであったとしても、異なる 2 つのツールを組み合わせて作業するより、単一の UEM ソリューションのほうが作業が簡単です。
- ユーザー向けにヘルプデスクサービスを提供する場合やシステムのトラブルシューティングを行う際に、単一の管理プラットフォームのほうが一貫した対応ができます。さらに、Windows 10 のようなオペレーティングシステムを使えば、デバイスの種類が異なっていても、より一貫性のあるインターフェイスを利用することが可能です。
- 単一のプラットフォームを使用する場合のほうが、包括的かつ容易にレポーティングの処理ができるのは間違いありません。ハードウェアとソフトウェアのアップグレードや更新について、プランニングやコストの計算をする際に有用です。
- Windows 10 では、デスクトップ、モバイルデバイスで共通のオペレーティングシステム、アプリケーション開発ツール、API セットを使用し、独自に一貫性を確保しています。デバイスのアプリケーションはすべて、企業が承認したセキュアな単一のアプリケーションストアから入手できるほか、個人所有のデバイスと社内ネットワークの両方を使い、きわめて一貫性の高い環境で業務アプリケーションや業務情報にアクセスすることが可能です。
- レガシーの Win 32 アプリケーションも、アプリケーションの展開、構成、アンインストールなど、ライフサイクル全体にわたり、必要に応じて、Citrix Workspace の UEM ソリューションで管理できます。

モバイル環境に対応した管理：CMT ツールが考案された当時、デバイスは企業が支給するもので、一箇所から移動することがなく、ほとんどの場合、社内の LAN と接続されていました。このような状況から、デスクトップやラップトップの初期構成とその後の管理を CMT ツールで行う場合、対象のデスクトップやラップトップを LAN に接続し、グループポリシーオブジェクトのセットを有する企業ドメインに参加させる必要がありました。また、一般にユーザーは、個人所有のデバイスをネットワークに接続したり、構成したり、アップグレードしたりすることはできませんでした。このような作業は、究極のスーパーユーザーである IT 部門の仕事だったのです。

旧来の CMT ソリューションでは、IT 部門がカスタムのシステムイメージのセットを 1 つ以上作成し、ネットワークに接続された数台、あるいは数百台規模のデスクトップやラップトップに、LAN を介して配布していましたが、これには非常に時間がかかりました。また、イメージの展開サービスを利用するケースでは、システムあたり最大で 25 ドルのコストがかかりました。このような手法では、新たにデバイスを導入したり、紛失や盗難時に代わりのデバイスを導入したりする際に、必要なアプリケーションの設定を完了するうえで多大なリソースと作業時間を要し、ユーザーの生産性にも影響が生じます。同様に、CMT のアプリケーションを配付する場合も、IT 部門を中心に作業が行われ、複雑な配布パッケージが必要でした。

これとは対照的に、UEM の API やツールでは、その開発の当初より、ワイヤレス接続と自身で選択したデバイスを利用するモバイルユーザーのサポートを想定していました。ユーザーは、ベンダーがオペレーティングシステムやアプリケー

ションを構成したデバイスを取得し、社内の UEM ポータルや構成アプリケーションを利用して、社内で定められた設定やポリシーに従い、ワイヤレスネットワークを通じて自分でデバイスの登録や構成ができます。IT 部門による作業やサポートはほとんど、あるいはまったく必要ありません。

また、ユーザーは、社内のアプリケーションストアポータルから、IT 部門が事前承認したアプリケーションをダウンロードしてインストールすることもできます。ただし、現在では従来とくらべ、クラウドの SaaS や仮想アプリケーションがかなり企業に浸透しているので、多くの場合、アプリケーションをダウンロードする必要はまったくありません。それでも、必要に応じて IT 部門は、数百台規模のモバイルデバイスを対象に、グローバルレベルでアプリケーションやアップデートをプッシュすることが可能です。

数年前までは、OS やアプリケーションのアップデート頻度は今よりもずっと少なくアップデートの作業は LAN の性能に依存し、非常に多くの時間とリソースをかけていました。今日のモバイルオペレーティングシステムは、クラウドサービスモデル上で動作する傾向があり、アップデートは規模が小さいながら、その頻度が高くなっており、これらは、モバイルユーザーにとって特に、重要な意味を持つ要素となっています。

コンテナ化

UEM やモバイル OS の API で BYOD や COPE（業務端末の私的利用）のワークスタイルを実現する方法の 1 つにコンテナ化があります。この手法では、アプリケーションのラッピングや暗号化、あるいはほかの類似の手法を用いて、業務アプリケーションおよび業務データを個人のアプリケーションおよびデータとデバイス上で分離します。これにより、企業のセキュリティポリシーに合わせて、相互のやり取りを無効化したり、制限したりできます。

コンテナ化は、マルウェア対策や DLP（データ漏洩対策）の役割も果たします。業務用のアプリケーションおよびデータと個人のアプリケーションおよびデータは、デバイス上でお互いに分離されているため、個人所有のアプリケーションの利用や私的なインターネットの閲覧でマルウェアに感染した場合でも、それがコンテナ化された業務アプリケーションに影響を及ぼすことはありません。また、デバイスが業務用のネットワークに接続していても、ネットワークに感染が広がることもありません。ほとんどの UEM ソリューションでは、このような分離を適用しているほか、特定の業務アプリケーションが社内の LAN に接続したときに、アプリケーションごとに VPN（仮想プライベートネットワーク）接続が自動的に起動されます。この VPN 接続では、単一のアプリケーションだけと接続し、デバイス全体とネットワークを確立するわけではないため、個人所有のアプリケーションの利用で感染したマルウェアを遮断できます。

同様にほとんどのオペレーティングシステムの API や UEM システムでは、ユーザーの操作を制限するポリシーを多数、構成および適用できます。業務用アプリケーションから個人所有のアプリケーションへデータをカット&ペーストしたり、業務用のデータやファイルを個人のメールメッセージにペーストまたは添付したり、機密性の高いデータを含むファイルを印刷したりするといった操作に制限を加えることが可能です。

Windows 10 のラップトップやデスクトップ、UEM では、デジタル著作権管理の機能を通じてコンテナ化の処理が行われます。すべての業務アプリケーション、業務データに Windows 情報保護による暗号化を適用されます。このあとに IT 部門は、ユーザーが、個人のメールクライアントソフトウェアなど、Windows 情報保護による暗号化を使用しない管理対象外のアプリケーションに暗号化されたコンテンツをカット&ペーストをしないよう、ポリシーで制限をかけることができます。SharePoint や共有ネットワークなどのサービスからダウンロードされたデータもすべて暗号化されます。

Windows 10 には、このほかにも、複数の種類のデバイスを対象とした管理で IT 部門が必要とする重要なエンタープライズ管理機能が数多く用意されています。多数のポリシーや設定のプッシュダウンと適用、パスワードと暗号化の適用、

Azure Active Directory やサードパーティの UEM ソリューションを通じた新規デバイスの自動登録ができるようになるほか、ユーザーがインストールしたアプリケーションと企業がプロビジョニングしたアプリケーションを区別した管理もできます。また、msi パッケージを通じた Windows 32 アプリケーションの配布や、アップデートの適用と展開、危険な Web サイトへのアクセスの防止も可能です。そしてこれらすべてが、デバイスが企業の LAN に接続されていない状態で実現されます。また、Windows 10 の機能を通じて利用できない Win32 のアプリケーションについても、Citrix Workspace のデスクトップ仮想化ソリューションを通じてモバイルデバイスに展開することができます。CMT と完全に同一の管理機能が提供されるわけではないものの、重要性の高い広く利用されている管理機能が利用可能となっており、利用できる機能の範囲は今後も拡大していく予定です。

Mac OS X Lion から、アップルはデスクトップオペレーティングシステムに、iOS とほぼ同等となるポリシーベースの自動登録管理 API を導入し始めました。macOS Sierra の場合、その度合いがさらに増しています。

シトリックスの UEM ソリューション

Citrix XenMobile は、デスクトップ、ノートブック、Chromebook を含め、iOS、Android、Windows 10、MacOS のデバイスなど、複数のプラットフォームを管理できる包括的な統合 UEM ソリューションです。Citrix Workspace の一部として機能し、アプリケーションとデスクトップの仮想化、ファイルの同期と共有、セキュアなネットワークゲートウェイサービス、Office 365 に関するセキュリティと生産性の強化機能を、UEM と連携させます。一方、Citrix mVPN は、マルウェアに感染したアプリケーションがファイアウォールの内側にあるリソースにアクセスするのを防ぐほか、デバイスレベルでなくアプリケーションレベルで一意のモバイルデバイス ID を割り当てて、個々のコネクションやデバイスの監視、フィルタリング、ブロックを行います。このよう機能の連携により、Office の生産性アプリケーションはもとより、レガシーの Windows アプリケーションや SaaS、Web アプリケーション、モバイルアプリケーションなど、ユーザーが必要とするあらゆるアプリケーションが、デジタルワークスペースのかたちで提供され、統合アプリケーションストアを通じて利用できます。

Citrix Workspace の XenMobile では、あらゆるオペレーティングシステムのエンタープライズ管理 API をサポートしています。デバイスのオペレーティングシステムをまたがり管理の一貫性を実現する独自の機能が API に追加され続け、API 自体の数も増加しているなかで、XenMobile がサポートする API もその数を増しています。FIPS 140-2 完全互換の AES 256 ビット暗号化や、オペレーティングシステムの API が提供するコンテナ化機能をベースとした独自の MDX コンテナ化機能に対応するほか、関連する機密情報を保護するためのポリシーやコンテナ化手法を用いて個々のアプリケーションをラッピングする独自のツールキットや SDK もサポートしています。

Citrix Workspace は、シームレスかつ生産性の高い作業環境を可能にする一方、企業にとって必要な一貫性のあるセキュリティも実現しており、この点は非常に重要です。

Citrix Workspace では、Citrix Secure Mail や Citrix Secure Web など、エンタープライズレベルのセキュリティ機能を備えた独自のモバイルアプリケーションも提供されます。これらは、iOS や Android のデバイスで利用できます。

Citrix Secure Mail は、企業ユース向けのメールクライアント兼個人情報マネージャーです。デバイス標準のメールクライアントソリューションのそれと非常に似かよった、ユーザーフレンドリーなインターフェイスを持ち、それに加え、企業環境での利用を想定した強固なセキュリティと高いユーザービリティを実現する豊富な機能を備えています。

Secure Mail では、業務で使用するメール、連絡先、予定表のアイテムはすべて、デバイス上において、個人の用途のものと完全に分離して保存されます。Secure Hub にログインした後、ユーザーは、シングルサインオンで Secure Mail にアクセスできます。また、Secure Mail では、

多要素認証やリモートワイプが利用可能のほか、保存時と移動時のデータの暗号化にも対応しています。また、IT 部門は、メールの添付ファイルについて制約を設けることができ、メールの情報をほかのアプリケーションで印刷したり、カット&ペーストしたりするような操作に制限を加えることも可能です。

Secure Mail は、組織にある既存の DLP（データ漏洩対策）ツールと連携できるので企業において送信されるメールのコンテンツを監視したり、制限したりすることができます。また、Secure Mail では、非常に便利な機能が多数用意されており、たとえば、ミーティング参加者の出席の可否を確認したり、新規ミーティングへの参加依頼にオンラインミーティングや電話会議のリンクを埋め込んだり、オンラインミーティングに参加したりするといったことがワンクリックで可能です。

Secure Mail は Secure Web モバイルアプリケーションと緊密に連携するので、メールに記載された Web リンクのオープンはすべて、セキュアなサンドボックス化された Web ブラウザ環境で実行されます。また、あとで述べるように、シトリックス独自のファイル同期共有アプリケーション、ShareFile とも緊密に連携するため、コンテンツをメールで共有する際は、コンテンツのファイルそれ自体ではなく ShareFile のリンクをメールに埋め込むことで、共有するコンテンツの操作権限を厳密に管理することができます。

Citrix Secure Web はセキュアなブラウザソリューションの 1 つです。特に企業ネットワークやイントラネットへのアクセスにおいて、Web ブラウジングにポリシーや制限を適用するうえで役立ちます。ポリシーを適用して、ユーザーのアクセスを許可または禁止する Web サイトを指定したり、アクセスに使用する社内のファイアウォールプロキシを制御したりできるほか、URL を分析、フィルタリングして、URL の安全性を確保することも可能です。

Citrix ShareFile はエンタープライズグレードのセキュアなモバイルファイル同期共有アプリケーションです。コンシューマーユーザーになじみの Box や DropBox と同等またはそれ以上に機能豊富で使い勝手が良く、しかも、エンタープライズレベルのセキュリティと管理性を実現しています。ShareFile の場合、必ずしも情報をすべてクラウド上に置く必要はありません。ファイアウォールで保護されたオンプレミス環境、Citrix ShareFile のクラウドサービス、その他のパブリッククラウドストレージのいずれにも、ShareFile Storage Zones を通じて自由に共有ファイルを保存できます。また、ShareFile では、CIF ベースの内部ネットワークストレージシステムにファイルを保存できるほか、Windows ネットワーク共有や Microsoft SharePoint 用のコネクターも提供されます。このため、別のサービスとの共有にあたり、そのサービスへファイルを移行する必要がありません。完全な機能を備えていながらドラッグ&ドロップで簡単に操作できるソリューションであるため、さまざまなデバイス上で動作するフォームベースのモバイルアプリケーションを初心者でも開発、実装、保存することができます。ShareFile を利用すれば、手動のワークフローやプロセスのデジタル化、自動化を短期間で実現できるようになり、現場では、データの二重登録がなくなり、ペーパーワークが不要になります。そしておそらくこれが最も重要な点ですが、ShareFile では、Citrix XenMobile の強力なセキュリティ機能と管理機能をすべて利用できます。これにより、企業データのセキュリティが確保されるほか、XenMobile の他の機能や生産性アプリケーションとのシームレスな連携が可能になります。

Citrix Secure Hub は、シトリックスのアプリケーションストアです。組織はここで、単一のアプリケーションストアを運用し、セキュリティアプリケーションやモバイルアプリケーション（サードパーティが開発した商用アプリケーションや社内開発のアプリケーション）、Web/SaaS サービス、さらには、Active Directory のグループポリシーをベースとした Windows のデスクトップとアプリケーションを提供することができます。

Podio（この製品は日本語化されていません）は、クラウドベースで無償の強力な企業向けモバイルコラボレーションプラットフォームを実現し、チームのコ

ミュニケーションやプロセスの連携、コンテンツの共有を促進するほか、Citrix XenMobile のセキュリティ機能や管理機能と密接に連携します。数万ドル規模の投資を必要とするエンタープライズソリューションと同等もしくはそれ以上のコラボレーション機能を備えています。

現在、新たに、IoT 対応のワークプレースという概念が登場していますが、このワークプレースでは、コンテキストに対応した環境を通じ、異なる数多くのソースからデータを取得して統合し、ユーザーのさまざまニーズに応えるとともに、ワークプレースの効率と生産性を高めます。Citrix Workspace のモビリティ管理は、このワークプレースにも対応できるようになっています。ワークプレースの自動化サービスの構築では、Octoblu ソフトウェアを使用します。ユーザーが近づいたときに起動するようデスクトップをカスタマイズしたり、会議室に人が入室したのと同時に空調や照明を制御したり、GoToMeeting や Skype for Business Meetings を起動したりできます。IoT の可能性は無限です。

まとめ

Windows 10 や macOS Sierra では、あらゆるエンドポイントやデバイス、アプリケーションに対応する単一のユニファイドエンドポイント管理機能を実現することができます。モバイルワークプレースの管理コストや、そのセキュリティの確保と簡素化のコストを効率化および削減する方法として、さらには、IoT の時代に対応できるモバイルエンタープライズ環境を実現する手段として、企業は UEM のソリューションを十分に検討する必要があります。

Citrix Workspace の提供するソリューションをユニファイドエンドポイント管理に活用すれば、あらゆるアプリケーションを対象とした ID の管理や連携の機能を通じ、ハイブリッドクラウドサービスのオンボーディングや統合、運用に関する管理作業を簡素化することができます。

Citrix Workspace では、エンドポイントの管理とアクセスの管理を統合できるほか、パフォーマンスについての詳細な情報が得られます。シトリックス独自の完全なワークスペースであり、コンテキスト対応のセキュリティに対応でき、インフラストラクチャ、アプリケーション、ネットワーク、デバイスを横断した包括的なアナリティクスを提供して、他に類のない監視機能を実現します。一方、エンドユーザーは、生産性高め、コラボレーションを実現するうえで必要なアプリケーションやデータを 1 箇所から利用できるようになります。しかも、エンドポイントの制約はありません。シトリックスの UEM ソリューションは、統合管理機能やセキュリティ機能を提供でき、アプリケーションとデスクトップの仮想化やモバイルコラボレーションにも対応するほか、エンタープライズ IoT を実現することも可能です。このような完全な UEM ソリューションを提供できるのは、シトリックスのみです。

Citrix Workspace では、ワークスペースがサービスとして提供されるため、IT 管理の一元化とアップグレードの効率化、設備投資コストの削減が可能となり、ビジネスの効率を高めることができます。クラウドのテクノロジーを利用するだけで、ビジネスのニーズに合わせて柔軟にインフラストラクチャを拡大、縮小でき、たとえば、新たに従業員を雇用したときにはインスタンスを追加し、退職者が出たときにはインスタンスを削除するだけです。Citrix Workspace をサービスとして提供することで、時間をかけず、最もシンプルかつ柔軟に、デジタルワークスペーステクノロジーをセキュアに利用することが可能になります。