News Release

2016 年 9 月 29 日

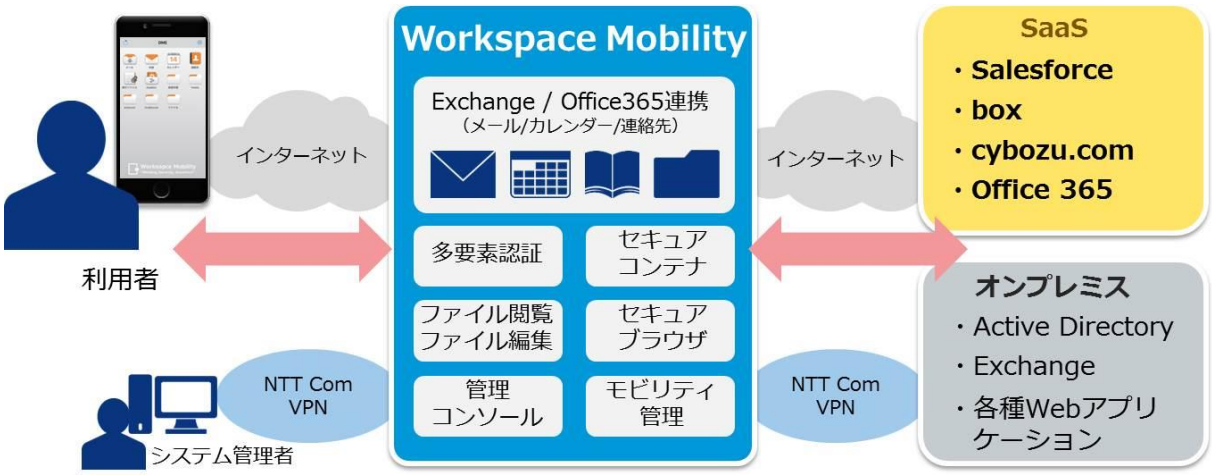
スマートフォンやタブレット端末からのセキュアな業務を実現する SaaS 「Workspace Mobility」の提供を開始

～セキュアコンテナ[*1]により、オフラインでも Office 365 などのメールの閲覧や Office ファイルの編集が可能～

NTT コミュニケーションズ(略称:NTT Com)は、スマートフォンやタブレット端末から、業務で利用する Web アプリケーションへのセキュアな接続やファイル編集を可能にする「Workspace Mobility」の提供を、2016 年 9 月 30 日より開始します。

本サービスの利用により、普段業務で利用している Microsoft 社の「Microsoft Exchange」や「Office365 Exchange Online」などのグループウェア、あるいは SaaS やオンプレミスの Web アプリケーションなどを[*2]、「Workspace Mobility」のアプリ(セキュアコンテナ)上から利用することが可能になります。「Workspace Mobility」アプリ内のデータは強固な認証でガードできるほか、スマートフォンなどの紛失時には外部からアプリ内の情報のみを削除することが可能なため、出先での業務や在宅勤務においてもセキュアな作業環境を実現できます。

【構成イメージ】



1．背景

スマートフォンやタブレット端末の業務における利用拡大や、時間や場所にとらわれない「働き方改革」への取り組みの進展などを背景に、BYOD[*3]や COPE[*4]によるモバイルワークの本格化が想定されます。NTT Com は、これらの動向を踏まえ、強固な認証機能や情報漏洩対策など、モバイルワークに求められるセキュリティをまとめて実現できるサービスとして「Workspace Mobility」の提供を開始します。

NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation　Public Relations Office
〒100-8019　東京都千代田区内幸町 1-1-6
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

２．特長

(1) 多要素認証とセキュアコンテナによる強固なセキュリティ

「Workspace Mobility」アプリへのログイン時には、お客さまの AD（Active Directory）を利用したユーザー認証と、利用する端末固有の ID による機体認証を組み合わせた多要素認証によって不正ログインを抑止します。

また、ログインした「Workspace Mobility」のアプリ内は、利用端末内の他のアプリやデータと隔離された状態のセキュアコンテナとして機能するため、会社と個人のデータ領域を完全に分離することが可能です。セキュアコンテナ内のデータは暗号化[*5]され、外部へのコピーも禁止されます。

なお、端末紛失時には会社領域（セキュアコンテナ）のみをリモートワイプすることが可能なため、個人領域を消去することがありません。

【セキュアコンテナのイメージ】

(2) セキュリティと使い勝手の良さを両立

各種 Web アプリケーションの利用は、セキュアコンテナ内のセキュアブラウザを利用して行います。データをダウンロードせずに利用するため情報漏洩対策となるほか、HTML5 ベースの最新ユーザーインターフェイスに対応しており、快適な操作性も実現しています。

また、セキュアコンテナ内の専用ビューア／エディターではメールの添付ファイルも閲覧でき、さらに暗号化保存したデータはオフラインでも編集することが可能なため、電波の状況によらずストレスなく作業ができます。

(3) SaaS 型のためスピーディーで安価な導入が可能

SI 型のサービスと異なり、構築期間と初期費用を抑えた導入が可能です。また、24 時間 365 日

での監視保守体制を含めた安価な月額料金で提供します。

初期費用		100,000 円/企業
月額料金	基本利用料	50,000 円/企業
	ライセンス利用料	1,100 円/1ID

・「Workspace Mobility」のシステム基盤と、お客さまがご用意される Web アプリケーションシステムを閉域網でセキュアに接続する仕様のため、別途 NTT Com の企業向けネットワークサービス「Arcstar Universal One」サービスの契約が必要です。
・価格はすべて税抜です。

3. 提供開始日

2016 年 9 月 30 日(金)

4. その他

企業内で利用するスマートフォンやタブレット端末、パソコンを一元的に管理する NTT Com の「Workspace MDM [*6]」と合わせてご利用いただくことで、「Workspace Mobility」で利用する端末から、業務アプリケーションに至るまでを統合管理できる EMM(Enterprise Mobile Management)ソリューションの実現が可能です。

*1: スマートフォンやタブレット端末の中に、仮想的に構築された会社(業務)用のデータ領域のこと。セキュアコンテナ内のデータは暗号化され、個人(プライベート)用のデータ領域と隔離されるため、業務情報の流出リスクを抑えることができます。
*2: 構成イメージ図内にある「Office 365」など、本サービスと接続する Web アプリケーションサービスは、別途お客さまにご用意いただく必要があります。
*3: Bring Your Own Device の略で、社員の私有端末を業務に有効活用すること。
*4: Corporate Owned Personally Enabled の略。会社支給端末を利用者に私的利用を許容する端末のこと。
*5: AES（Advanced Encryption Standard) 128bit。はアメリカ合衆国の新暗号規格として 2001 年に規格化された共通鍵暗号方式。米軍主導のネットワーク秘匿化オープンソースプロジェクトである Tor などに採用され、欧州の暗号規格 NESSIE や日本の暗号規格 CRYPTREC でも採用されています。
*6: iOS、Android、Windows、Mac のマルチ OS に対応したモバイルデバイス管理ツールサービス。端末資産管理／セキュリティ管理／会社指定アプリケーションの配信／インターネット接続管理／情報漏洩対策などの多彩な機能をブラウザ上から簡単に設定・管理できる SaaS 型の MDM サービス。

※本文に記載されている社名、商品名、サービス名は各社の商標または登録商標です。