



# スマートフォンおよびタブレットの透過的なデータ保護

## Dell Data Protection | Mobile Edition

現在は、従業員、パートナー、ベンダーが、それぞれ時間や場所を問わず、さまざまなデバイスを使用してファイルをダウンロードし、共有しています。デスクトップやノートパソコンと同様、個人所有のスマートフォンやタブレットも、業務用のツールとして広く使用されるようになりました。それに伴い、BYOD（私物デバイスの業務利用）が機器関連コストの削減と生産性の向上に役立つことが分かり、ほとんどの組織でBYODが認められるようになりました。

しかし、モバイルデバイス上のデータは、暗号化とパスワードが適切に適用されていないければ、社内のサーバであってもパブリッククラウドであっても、アクセスした際の保護は行われません。デバイスの紛失や盗難が発生したり、オープンなワイヤレスホットスポットからデータへのアクセスが行われれば、データがハイジャックされたり、企業がセキュリティ侵害やコンプライアンス違反の危険にさらされることもあります。IT部門は、データ保護と、データアクセスの制限による従業員の生産性低下とのバランスを取ることに苦慮しています。

Dell Data Protection | Mobile Editionを導入すると、iOSまたはAndroidオペレーティングシステムを実行するスマートフォンやタブレット上でアクセスされるデータの保護が可能になり、データセキュリティをIT部門自らコントロールできるようになります。エージェント不要で導入が簡単なこのソリューションは、Dell Data Protection | Enterprise Editionプラットフォームに完全に統合されています。Dell Data Protection | Mobile Editionを使用することによって、IT部門はプロファイルの検査、インストール、および削除、パスワードの削除、および機器のリモート完全削除を、すべて1つのプラットフォームから簡単に実行できます。

## エンドユーザーの生産性を向上させる包括的な保護

Dell Data Protection | Mobile Editionでは、iOSおよびAndroidプラットフォームで提供されるネイティブなセキュリティ機能を使用することによって、デバイスに追加搭載する必要のあるセキュリティソフトウェアが削減されます。そのためサポートがシンプルになり、エンドユーザーエクスペリエンスへの影響を少なくして、簡単にセキュリティ機能を使用できます。また、デバイスとユーザーとの関連付けも自動的に実行されるため、ワークフローの中断を最小限に抑えることができます。

## iOSデバイスのセキュリティ保護

Dell Data Protection | Mobile Editionにより、管理者はポリシーをユーザーレベルで、また、コマンドをデバイスレベルで適用できます。デバイス管理コマンドは、Apple Push Notification Service (APNS) を介して管理対象のiPhoneおよびiPadデバイスに送信されます。ポリシー、制限、およびコマンドは設定プロファイルとしてiOSに実装され、ワイヤレスで配信されます。

## Androidデバイスのセキュリティ保護

Androidモバイルデバイスの保護はMicrosoft Exchange ActiveSync (EAS) プロトコルによって管理されます。ポリシーはユーザーレベルで、また、コマンドはデバイスレベルで設定および適用できます。デバイス管理コマンドはExchange ActiveSyncを介してAndroidデバイスに送信され、適用されます。許可、ブロック、およびリモート削除のコマンドは、ワイヤレスで配信されます。

## iOS専用ポリシー

デバイスロックまでの猶予期間	iTunesパスワードの強制
パスワードのリセット	信頼されていないSSLサーバ証明書
リモートロック	iCloudバックアップの許可
削除用パスワードの許可	iCloud文書同期の許可
ユーザーによる設定用プロファイルの削除	iCloudキー値同期の許可
YouTubeの許可	iCloudフォトストリームの許可
iTunesの許可	Webペイロード - WebクリップのURL
アプリのインストールの許可	Webペイロード - Webクリップのラベル
明示的なコンテンツの許可	Webペイロード - Webクリップのアイコン
画面キャプチャの許可	Webペイロード - Webクリップの削除の許可
アシスタント (Siri) の許可	

## iOSおよびEAS共通ポリシー

パスワードの要求	カメラを無効にする
単純なパスワードの許可	ブラウザの許可
複雑な文字数	パスワードの最小文字数
パスワードの最長存続期間	英数字パスワードの要求
固有のパスワードが再利用できるようになるまでの変更回数	デバイスロックまでの非アクティブ経過時間
デバイス上のデータが消去されるまでのパスワード入力試行回数	

## EAS専用ポリシー

ストレージカードの暗号化
デバイス暗号化の要求



## シンプルな管理とコンプライアンス

Dell Data Protection | Mobile Editionは1つのコンソールを使用して一元管理されるため、ITの状況把握やコントロールがしやすくなり、コンプライアンス業務の負荷やデータ侵害のリスクを大幅に低減できます。全社規模のポリシーの設定や制限の適用を簡単に実行でき、リモート削除などのコマンドを即座に適用できるため、データ漏洩にも迅速に対応して漏洩の範囲を抑えることが可能になります。また、未登録デバイスの自動検出と一元管理およびレポート作成機能により、企業データのセキュリティを維持しながら、ユーザーが中断なく業務を行える環境を実現します。

Dell Data Protection | Mobile Editionには、次のような機能が  
あります。

- ポリシーと制限の設定 - PINの要求やバックアップを無効にするなどのポリシーを全社規模で設定
- コマンドの実行 - リモート削除やパスコードのリセットなどのコマンドを即座に発行
- デバイスの検出 - 未登録デバイスを自動的に検出
- デバイスのブロック - 紛失や盗難が発生したりサービス停止が必要となったデバイスからExchangeサーバへのアクセスを排除
- コンプライアンスレポートの作成 - コンプライアンスレポートを作成して監査要件に対応

## クラウドストレージデータの保護

パブリッククラウドでのファイル共有が普及し、エンドユーザーがスマートフォンやタブレットからクラウド上のファイルにアクセスすることが一般的となっているため、モバイルデバイスの保護も不可欠になっています。Dell Data Protection | Mobile Editionは、Dell Data Protection | Cloud Editionと連携するように設計されています。Dell Data Protection | Cloud Editionはパブリッククラウドストレージの内外へ移動するデータを透過的に暗号化します。この2つのソリューションは、併用することでシームレスに機能します。エンドユーザーはパブリッククラウドが常に自分の手元にあるかのように中断なく使用できる一方、企業は機密データのセキュリティとコンプライアンスを確実に維持できます。

## Dell Data Protection | Enterprise Edition

Dell Data Protection | Mobile Editionは、統合プラットフォームDell Data Protection | Enterprise Editionの一部です。以下を含むすべての物理および仮想エンドポイントのデータのセキュリティを保護します。

- デスクトップ、ノートパソコン
- スマートフォン、タブレット
- リムーバブルメディア
- パブリッククラウド、プライベートクラウド
- 自動暗号化ドライブ
- BitLocker

インストールが簡単で管理しやすいDell Data Protection | Enterprise Editionにより、データの移動先を問わずにデータを保護できます。

## 仕様詳細

### サポート対象のオペレーティングシステム:

- iOS 4.x, iOS 5.x, iOS 6以降
- Android 2.2、2.3以降、3.x、4.0以降

### サポート対象のデバイス:

- iPhone、iPad
- Androidスマートフォン、Androidタブレット

### サポート対象のExchange ActiveSync Server:

- Exchange ActiveSync 12.0 – Exchange Server 2007のコンポーネント
- Exchange ActiveSync 12.1 – Exchange Server 2007 SP1のコンポーネント
- Exchange ActiveSync 14.0 – Exchange Server 2010のコンポーネント
- Exchange ActiveSync 14.1 – Exchange Server 2010 SP1のコンポーネント

[www.Dell.com/DataProtection](http://www.Dell.com/DataProtection)でもっと詳しく