豊富なMDM機能（ITポリシー）

ポリシー項目		設定項目	対象		対象		備考
			iOS	Android	コンテナ	端末	
セキュリティ	リモート制御	リモートワイプ	○	○	○	○	
		リモートロック	○	○	○	○	
	パスワード	パスワードの強制	○	○	○	○	
		文字列のルール	○	○	○	○	
		パスワードの長さ	○	○	○	○	
		有効期限の設定	○	○	○	○	
	アプリケーション	コンテナ内⇒外へのコピー&ペーストの禁止	○	○	○	－	
メール	添付ファイル	送受信許可	○	○	○	－	
		容量制限	○	○	○	－	
		拡張子制限	○	○	○	－	
	同期設定	受信トレイ　ヘッダのみ、ヘッダ・ボディ両方	○	○	○	－	
		送信トレイ	○	○	○	－	
ブラウザ	セキュアブラウザ(コンテナ内ブラウ	アクセス許可	○	○	○	－	
		ホワイトリスト指定	○	○	○	－	
アドレス帳	社内アドレス帳	アクセス許可	○	○	○	－	
その他、コンテナ外アプリ	AppStore	利用禁止	○	×	－	○	アプリインストールの禁止はできるが、AppStoreのアイコンは残り閲覧もできる状態。
	Siri	利用禁止	○	×	－	○	
	カメラ	利用禁止	○	○	－	○	
制限	ハードウェアモデル	制限	△ (一部可)	△ (一部可)	△	－	違反している端末に対して、コンテナをロックするか、コンテナ内のデータをワイプするか、いずれか選択可能。 ※iOS/Android→将来的な新端末に対応するには、サーバ側のアップグレードが必要。 ※Android→一部の端末にのみ対応。
	OSバージョン	制限	○	○	○	－	違反している端末に対して、コンテナをロックするか、コンテナ内のデータをワイプするか、いずれか選択可能。 ※将来的なバージョンについては、「Unknown」で設定可能。
	コンテナバージョン	制限	○	○	○	－	違反している端末に対して、コンテナをロックするか、コンテナ内のデータをワイプするか、いずれか選択可能。 ※将来的なバージョンについては、「Newer」で設定可能。
監視	Jailbreak/Root化の検知	検知	○	○	○	－	検知された端末に対して、コンテナをロックするか、コンテナ内のデータをワイプするか、いずれか選択可能。
	接続確認	接続確認	○	○	○	×	一定期間、NOCへの通信が発生していない端末に対して、コンテナをロックするか、コンテナ内のデータをワイプするか、いずれか選択可能。
	アプリの例外	アプリの例外	○	○	○	－	ブラックリスト等に指定されているアプリケーションをインストールした端末に対して、コンテナをロックするか、コンテナ内のデータをワイプするか、いずれか選択可能。