▶KASPERSKY SECURITY FOR MOBILE

モバイル端末の安全な業務利用に必要なセキュリティを提供

企業においてもモバイル端末の利用が広がり、モバイル端末を狙う攻撃対策や、紛失・盗難時における情報漏洩対策の必要性が高まっています。Kaspersky Security for Mobileは、企業におけるモバイル端末のセキュリティ対策を効率よく実現し、危険サイトやフィッシングの脅威から保護します。また、Android端末のマルウェア感染も防ぎます。モバイル端末の紛失・盗難の対策としてリモートロックやリモートワイプ機能などを搭載し、システムの運用管理を容易にするため、セキュリティプログラムの設定展開やモバイル端末のイベント情報取得による一元管理を実現します。

- **アンチマルウェア**
- **アンチフィッシングとアンチスパム**
- **危険サイトのブロック**
- **モバイルアプリケーション管理（MAM）**
- **コンテナー**
- **モバイルデバイス管理（MDM）**
- **盗難対策（リモートロックなど）**
- **一元管理**
- **コンプライアンスコントロール**
- **root化／jailbreak（脱獄）の検知**
- **セルフサービスポータル**
- **サポート端末**
  - Android端末
  - iOS端末

製品の特長

モバイルセキュリティ
さまざま防御テクノロジーを組み合わせた多層防御の仕組みで、モバイル端末を標的にした脅威から保護します。

モバイルアプリケーション管理（MAM）
業務アプリとデータ用の専用領域であるコンテナーを設け、セキュリティを一層強化してアプリ利用を制御できます。BYODにおけるセキュリティリスクの低減にも有効です。

モバイルデバイス管理（MDM）
リモートロックやリモートワイプなどの盗難対策機能により、データ漏洩リスクを低減します。また、カメラやWi-Fiの使用を制限します。

一元管理
システムの運用管理を容易にするため、モバイル端末へのセキュリティプログラムの設定展開や、モバイル端末のイベント情報取得による一元管理を実現します。

主な機能

アンチマルウェア
ウイルス定義データベース、クラウドプロテクション（Kaspersky Security Network）といったテクノロジーで、モバイル端末を狙う既知のマルウェアだけでなく、未知のマルウェアからも防御します。また、管理者が指定したスケジュールでモバイル端末を定期的にスキャンできます。

アンチフィッシングとアンチスパム
アンチフィッシングテクノロジーとアンチスパムテクノロジーでフィッシング攻撃から保護し、迷惑な電話やテキストメッセージをブロックします。

危険なWEBサイトをブロック
マルウェアに感染させる、個人情報を盗む、など危険なWebサイトへのアクセスをブロックします。また、アダルトやギャンブルなど、管理者が予め指定したコンテンツを含むサイトへのアクセスを制限できます。レピュテーション分析を用いて、安全なモバイルブラウジング環境を提供します。

アプリの起動コントロール
ホワイトリストに登録されたアプリのみ起動を許可するポリシーや、ブラックリストに登録されたアプリのみ起動をブロックするポリシーを展開できます。また、指定したカテゴリーに該当するアプリの起動を制限することも可能です。禁止されたアプリを実行しようとすると、管理者向けレポートに記録されます。アプリの起動を実際にはブロックせずに報告のみ行うことも可能です。

コンテナー
業務アプリとデータ用の専用領域であるコンテナーを設けることで、業務領域と個人領域と分離します。分離することで、業務領域のアプリやデータの消去が必要な場合、個人データに影響を及ぼすことなく削除できます。また、アプリをコンテナー内に配置することで以下のことが可能となり、セキュリティが確保された環境で業務アプリを使用できます。

- アプリ起動時におけるユーザー認証の設定
- アプリのデータを暗号化
- 他のモバイルアプリへのデータ転送の制御
- アプリのインターネットへのアクセス制限
- アプリにより送信されたSMSの監視
- アプリが発信する通話の監視

Root化／Jailbreak（脱獄）の検知
端末のroot化やJailbreakを検知すると管理者に通知します。そして、その端末のコンテナー上にある業務アプリやデータへのアクセスをブロックしたり、リモートよりデータを削除することができます。

盗難対策
端末の紛失・盗難時には、リモート操作による端末のロックや、GPS追跡機能で端末の位置を特定できます。また、リモートから全てのデータまたは業務データ（コンテナー上のデータや、Wi-FiおよびVPNへの接続設定など）の削除や、SIMが差し替えられた場合に新しい電話番号を管理者に通知したり端末をロックするSIM監視が可能です。Google Cloud メッセージング（GCM）を通じて、Android端末へコマンドをプッシュ通知し、モバイル端末と素早く同期を可能とします。

管理コンソールで一元管理
システム管理者が設定したポリシー（セキュリティ設定）をモバイル端末に反映したり、ウイルス検知などのイベント通知やレポートで、端末のセキュリティ状況を把握できます。また、ポリシーに準拠しているかを確認し、必要に応じて端末の動作を制限します。例えば、リアルタイム保護が有効か、ウイルス定義データベースが最新か、管理サーバーと定期的に同期しているかをチェックします。そして基準を満たさず、指定した時間を経過しても修正されていない場合、アプリの起動ブロック、端末ロック、データ消去といった処理を実施します。

Android for Workとの連携
Googleが提供するAndroid for Workの仕事用プロファイルを作成し、管理端末に反映してセキュリティを強化できます。例えば、仕事用プロファイル内で提供元不明のアプリのインストールを禁止したり、仕事用プロファイルから個人用プロファイルへのデータ転送を禁止することができます。

セルフサービスポータル
定型的なセキュリティ管理を従業員に委譲し、承認されたデバイスを自分で登録できるようにします。新しい端末を有効にする際、必要な証明書がポータル経由で配信されます（管理者が作業する必要なし）。端末の紛失時には、従業員はポータルを通じて端末ロックやデータ消去といった盗難対策のアクションを実行できます。

購入のご案内

Kaspersky Security for Mobileは以下のライセンスで使用可能です。

- Kaspersky Endpoint Security for Business – Advanced
- Kaspersky Endpoint Security for Business – Select

オフィシャルサイト　www.kaspersky.co.jp/
ご購入相談窓口　jp-sales@kaspersky.com

Kaspersky Security for Mobile / Ver. 1.0 / APR 2016 / Japan