STAR-MDM

Lookout連携機能

スターネット株式会社

第1.0版

版	日 付	内 容	備 考
1.0	2021/05/12	初版	

目　次

※　掲載している WEB 画面キャプチャは、Lookout 社のもの・又は開発中のものであるため、予告なく変更される場合がございます。また、本資料に掲載している WEB 画面キャプチャは、Chrome での表示のため、他ブラウザでは一部表示が異なる場合がございます。予めご了承ください。

Lookout連携機能の概要

本機能を利用することで、Lookout 社のモバイルセキュリティサービス「Lookout」と連携が可能です。
連携機能を利用することで、以下の機能を STAR-MDM 管理画面上で利用することができます。
※本機能はフル機能パック（拡張機能パック）でのみご利用いただけます
※Lookout のご利用には、別途お客様にて Lookout のご契約を行う必要があります。なお、本製品は
弊社ではお取り扱いしておりません。提供元ならびに各販売代理店へお申し込みいただく必要があります。

イベントごとの連携動作	アラート表示 （管理画面 TOP）	ログ記録 （ログ管理）	一覧表示 （端末管理画面）	詳細表示 （端末情報画面）	メール通知 （管理者/端末利用者宛）
脅威の検知時	○	○	○	○	○
脅威の解決・無視時	－	○	○	○	－
稼働状況の変化時	－	○	○	－	－

各動作の詳細については、各連携機能の詳細 をご確認ください。

【動作環境について】

≪Android≫

以下の OS バージョンの端末にてご利用いただけます。

Android OS v6.0.1～8.x

なお、ご利用には Android Enterprise でのキッティングが必須です。

Android Enterprise (Work Managed Device)の対応機種は以下のページをご確認ください

https://www.sppm.jp/対応機種

※ Work Managed Device または Comp の Work Managed Device 領域でのみご利用いただけます。
Work Profile 領域ではご利用いただけません。

※ ガラホ端末ではご利用いただけません

≪iOS≫

以下の OS バージョンの端末にてご利用いただけます。

iOS v11.x/ v12.x

【サポート範囲について】

Lookout 自体の機能については弊社にてサポートいたしかねます。Lookout 管理画面の操作（アカウント作成方法等）や脅威の詳細等につきましては Lookout 側のヘルプやマニュアルをご確認ください。

各連携機能の詳細

【アラート表示】

「脅威の検知時」に、STAR-MDM 管理画面の「TOP」にアラートログを表示します。

また、アラートが確認済みになるまで、端末管理画面のアラートステータスが「赤」で表示されます。

【ログ記録】

「脅威の検知時」「脅威の解決・無視時」「稼働状況の変化時」、ログ管理にログを記録します。

【一覧表示】

端末管理画面の一覧表示に、Lookout のアイコンと端末のステータスが表示されます。

ステータス表示は「脅威の検知時」「脅威の解決・無視時」「稼働状況の変化時」に更新されます。

一覧表示を利用するためには、端末管理画面の「一覧表示設定」で設定が必要です。

【詳細表示】

「脅威の検知時」「脅威の解決・無視時」、「端末詳細情報」画面に検知情報が時系列で表示されます。

【Lookout検知情報】　　詳細はLookoutの管理画面でご確認ください

検知日時	タイプ	重要度	脅威の分類	脅威への対応
2019-07-24 14:33:50	アプリケーション	低	アドウェア	検出
2019-07-24 14:33:24	アプリケーション	低	アドウェア	解決
2019-07-24 14:27:30	アプリケーション	低	アドウェア	検出
2019-07-24 13:17:00	アプリケーション	低	アドウェア	解決
2019-07-24 13:16:56	アプリケーション	中	リスクウェア	解決
2019-07-24 13:16:56	アプリケーション	高	スパイウェア	解決
2019-07-24 13:13:45	アプリケーション	高	スパイウェア	検出
2019-07-24 13:11:36	アプリケーション	中	リスクウェア	検出
2019-07-24 13:09:15	アプリケーション	低	アドウェア	検出
2019-07-24 13:00:40	アプリケーション	低	アドウェア	解決

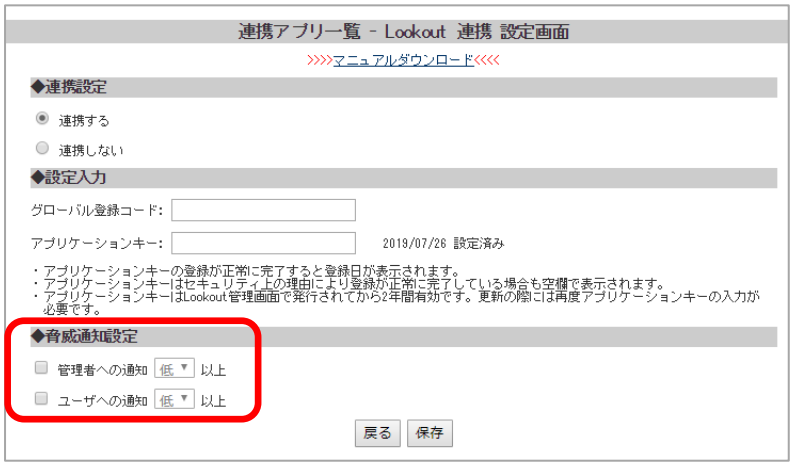
【メール通知】

「脅威の検知時」に STAR-MDM の管理者とユーザにメールで通知することができます。

通知する基準（脅威のレベル）については「連携アプリ」＞「Lookout 連携」設定画面で設定できます。

なお、Lookout の管理画面でメール通知設定を行っている場合は、二重で通知が行われます。

Lookout 側のメール設定は「ユーザー名 ＞ ユーザー設定 ＞ メール通知」より変更可能です。



【脅威別詳細設定】

「脅威通知設定」を設定している場合「脅威別詳細設定」が表示され、

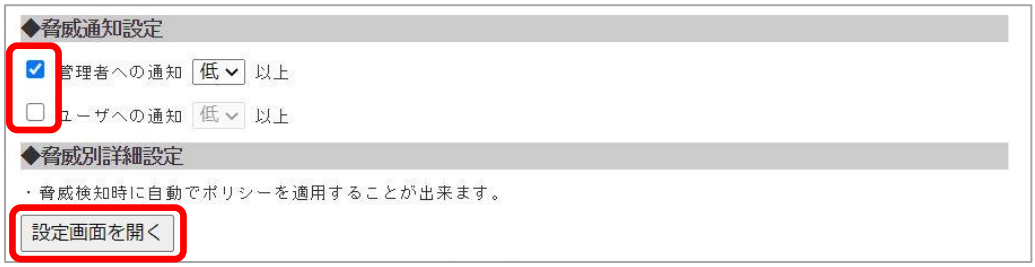
「脅威の検知時」に自動でポリシーを設定することができます。

「設定画面を開く」をクリックすると、脅威別に選択できる端末制御設定画面が開きます。

脅威を検知した際に自動で実行される制御を、端末制御内容から選択してください。

※「デバイス制御」、「Wi-Fi 接続先制限」、「利用アプリ制限」はポリシー名も選択する必要があります。

※「Wi-Fi 接続先制限」と「利用アプリ制限」は iOS 非対応です。



連携設定手順

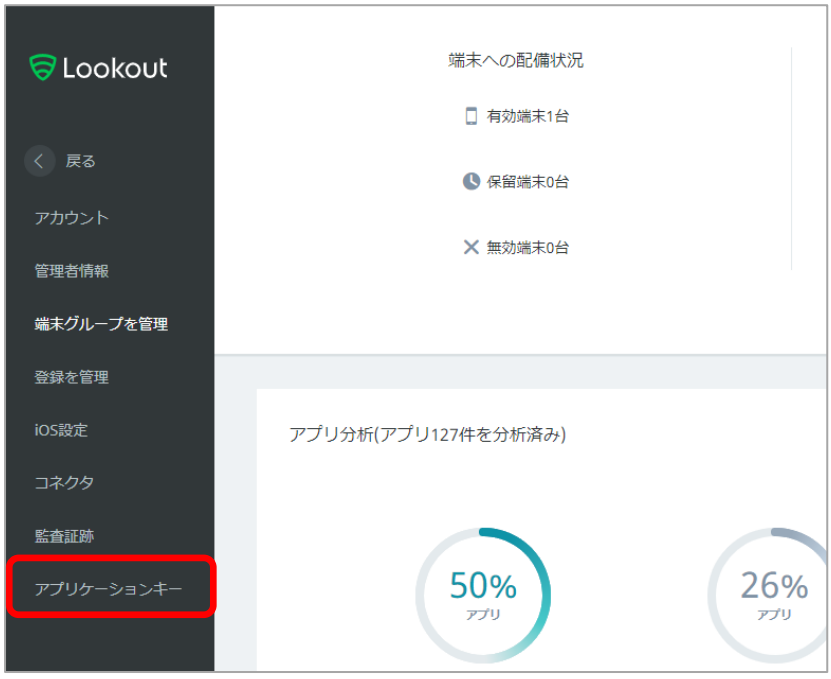
「Lookout 連携」機能を利用するために、まず初めに以下の設定を行ってください

※　以下の手順はすでに Lookout の利用契約があり、各ユーザ分のアカウントが発行されている状態を前提としています。Lookout 側の操作については Lookout 側のヘルプやマニュアルをご確認ください。

【Lookout 管理者画面側】

① Lookout 管理画面にログインし、メニューから「システム」を選択します

② 「アプリケーションキー」を選択します



③ 「キーを生成」を押します

④ 任意の名前（KeyName）を入力します

⑤ 画面表示に従って「アプリケーションキー」をコピーします

※「OK」押下後、アプリケーションキーの再表示はできませんのでご注意ください

次のページへ続きます。

【STAR-MDM 管理者画面側 / 「連携アプリ」設定】

① STAR-MDM 管理画面にログインし、「連携アプリ」の項目から「Lookout 連携」を選択します

② 「◆連携設定」を「連携する」に変更します

③ 「グローバル登録コード」と前の手順で生成した「アプリケーションキー」を入力して「保存」を押します

※「グローバル登録コード」は Lookout 管理画面の「システム」>「アカウント」から確認できます

設定手順は以上です。

アプリのインストール手順（Android）

Android 端末にて Lookout 連携を行うためには、Android Enterprise 機能を利用して「アプリ設定」および「サイレントインストール」を行う必要があります。各手順は以下をご確認ください。

※以下の手順はすでに Lookout の利用契約があり、各ユーザ分のアカウントが発行されている状態を前提としています。Lookout 側の操作については Lookout 側のヘルプやマニュアルをご確認ください。

【1】アプリの承認

「その他」＞Android Enterprise 「承認アプリ管理」にて Lookout for Work アプリを承認してください。
詳細な手順については「Android Enterprise マニュアル」をご確認ください。

【2】アプリ設定

① STAR-MDM 管理画面＞「その他」＞Android Enterprise「アプリ設定」を開く
② Lookout for Work のラジオボタンにチェックを入れて「アプリ設定」を押下
③ 「◆個別 CSV 登録」にて「登録用フォーマット」をダウンロードします。
④ 以下を参考に CSV に情報を入力し、上書き保存します

項目名	入力値
device_id	端末のIMEI
MDMName	（空欄でよい）
androidId	（空欄でよい）
deviceId	端末のIMEI
activationCode	Lookout のグローバル登録コード※
email	Lookoutで利用するユーザ名（メールアドレス形式）
dualEnrollmentRequired	（空欄でよい）
DeviceUniqueIdentifier	端末のIMEI

※「グローバル登録コード」は Lookout 管理画面の「システム」＞「アカウント」から確認できます

⑤ 対象端末分の入力が完了した CSV データを「登録用ファイル選択」で選択し、登録します

【3】サイレントインストール

アプリ設定後に、Android Enterprise「サイレントインストール」機能にて Lookout for Work アプリを端末にインストールします。 詳細な手順については「Android Enterprise マニュアル」をご確認ください。

アプリのインストール手順（iOS）

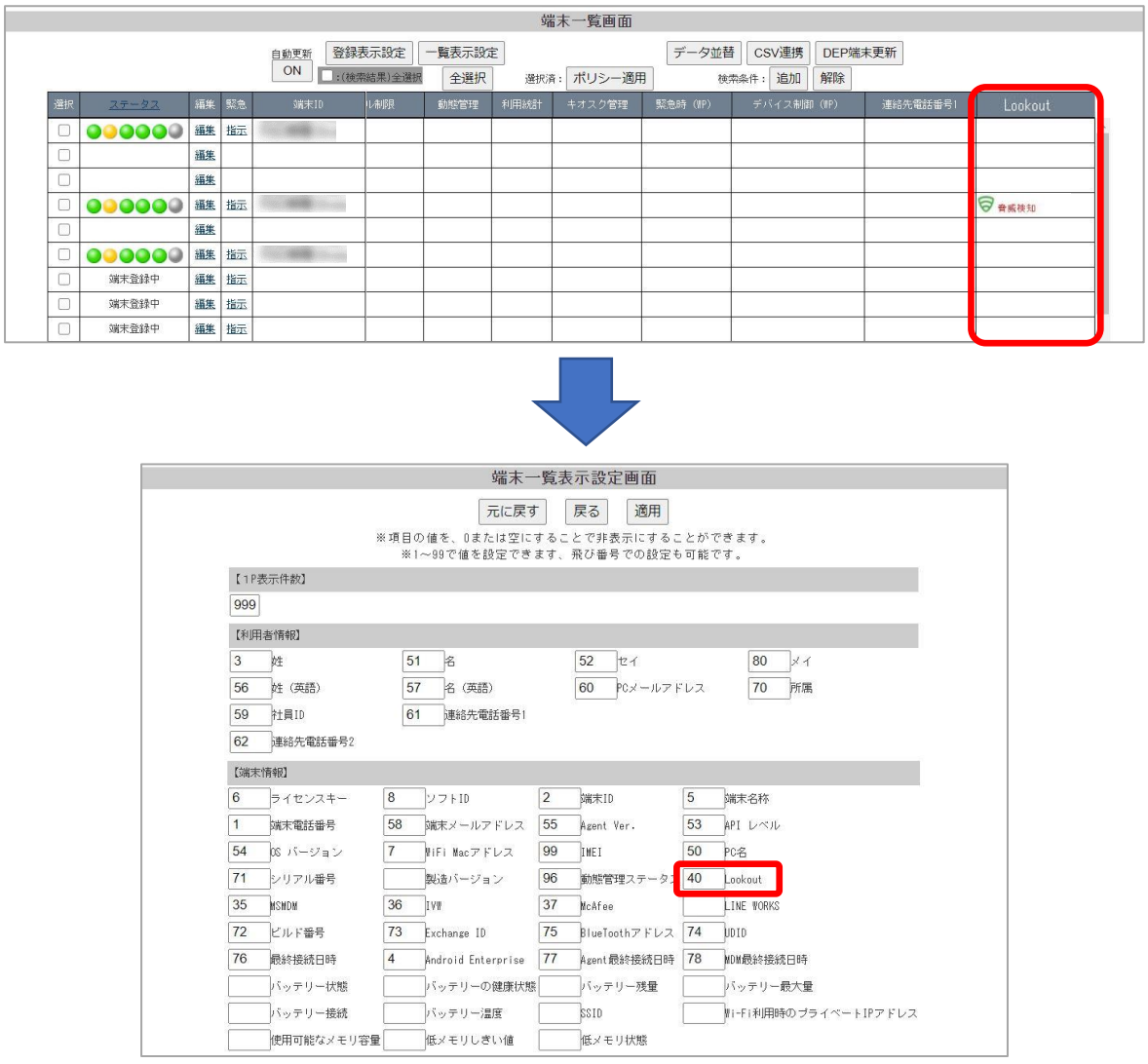
iOS 端末にて Lookout 連携を行うためには、Lookout 連携設定を行った後に、Lookout for Work アプリを「アプリ管理」ポリシーにてインストールする必要があります。「アプリ管理」ポリシーについては「iOS 管理者マニュアル」をご確認ください。 ※VPP ライセンスの利用は必須ではありません

管理画面表示

端末の連携登録が完了した端末は、STAR-MDM 管理画面＞端末管理＞端末一覧画面＞端末一覧表示設定から変更をすると、端末一覧画面と端末情報画面に Lookout の項目が表示されるようになり、現在のステータスを確認することができます。

※端末一覧画面に表示させるには、端末一覧画面＞端末一覧表示設定から変更する必要があります。
詳しくは Android 管理者マニュアルの「一覧表示設定」をご確認ください。

■端末一覧画面



■ステータス一覧

表示される文言	状態
空欄	端末に Lookout がインストールされていない状態や、Lookout の管理画面から削除された状態
正常	端末で Lookout が正常に動作し、脅威が発生していない状態
脅威検知	端末側で脅威が検出された状態
無効	Lookout 管理画面側で「無効」と指示された状態
切断	一定期間端末との通信がない状態
保留中	Looout 管理画面から招待メールが送信されたがユーザーがまだ登録していない端末の場合

■端末情報画面

【Lookout 検知情報】　詳細はLookoutの管理画面でご確認ください

検知日時	タイプ	重要度	脅威の分類	脅威への対応
2020-12-03 14:08:52	設定	低	パスコードが未設定です	解決
2020-12-03 13:45:25	設定	低	パスコードが未設定です	検出
2020-12-03 12:24:55	設定	低	パスコードが未設定です	解決
2020-12-03 12:19:33	設定	低	パスコードが未設定です	検出
2020-12-03 12:05:47	設定	低	パスコードが未設定です	解決
2020-12-03 11:46:09	設定	低	パスコードが未設定です	検出
2020-12-03 11:42:42	設定	低	パスコードが未設定です	解決
2020-12-03 11:31:34	設定	低	パスコードが未設定です	検出
2020-12-03 11:27:35	設定	低	パスコードが未設定です	解決
2020-12-03 11:22:18	設定	低	パスコードが未設定です	検出

注意事項

・Lookout 連携設定を行う前に、Lookout for Work アプリがすでに端末にインストールされている場合は、一度 Lookout for Work アプリをアンインストールした上で、「アプリ管理」ポリシーや「サイレントインストール」機能でのアプリ配信が必要です。

・Android 端末にて、Lookout for Work アプリの再インストールが必要な場合は、都度「アプリ設定」を実施してください。「アプリ設定」を再設定せずに Lookout for Work アプリを再インストールすると、グローバル登録コード・メールアドレスが設定されない場合があります。

・アプリアンインストールや端末初期化により、Lookout に端末を再登録する必要がある場合、Lookout 管理画面上で該当端末のデータを削除してから行ってください。上記を行わない場合、STAR-MDM の端末一覧画面上 Lookout 列が空欄で表示される場合があります。