

STAR-MDM 管理者マニュアル（Android版）



スターネット株式会社

第4.5版

版	日 付	内 容	備 考
1.0	2015/07/16	初版	
1.1	2015/12/09	AndroidOS5.0 対応 (緊急時、デバイス制御、SIM 監視、利用アプリ制限、メッセージ配信) E-API のアプリ配信ポリシーでのサイレントインストールに対応 対応端末に iOS9.1 を追加 機能追加 (SIM 監視、位置情報取得、デバイス制御、利用アプリ制限)	
1.2	2016/06/24	AndroidOS6.0 対応 利用アプリ制限-OS5.1.1 以上対応 利用アプリ制限-アプリ排除機能追加 E-SDK,E-API セーフモード制御追加 CSV 書出しデータ[シリアル番号]対応 E-API スモールアプリ制限機能追加 メッセージ配信にメール送信機能追加 コールピックアップ 0 番対応追加	
1.3	2016/07/28	対応端末に iOS9.3.3 を追加	
1.4	2016/09/06	E-SDK アクティブキー制限機能追加 E-API デバイス制御 新機能追加 対応端末に iOS9.3.5 を追加	
1.5	2016/09/27	E-API スクリーンショット制限機能追加 対応端末に iOS10.0.1 を追加	
1.6	2016/10/24	E-API デバイス制御 新機能追加 管理画面更新による各機能追加	
1.7	2017/5/18	AndroidOS7.0 対応 アプリアンインストール制限ポリシー追加 マルチユーザー検知機能追加 稼働環境に iOS10.3.1 までの環境を追加 E-API デバイス制御 から AutoBoot を削除	
1.8	2017/06/05	アプリポータル機能追加	
1.9	2017/08/24	Android Enterprise 対応	
2.0	2017/09/06	SHARP モジュール対応 利用アプリ制限 CSV 対応	
2.1	2017/10/31	接続日時の項目に「MDM 接続情報」「Agent 接続情報」を追加	

2.2	2018/01/24	Android OS 8.0 対応 パスワード初期化値指定機能追加 SmartLock 制限機能追加	
2.3	2018/4/19	電話帳配信データー括削除機能追加 利用アプリ制限 suspend 制御対応	
3.0	2018/7/23	Comp 対応	
3.1	2019/2/7	電話帳配信ポリシーCSV 書出機能追加 ログイン IP アドレス制限機能追加 機能追加 SHARP モジュール OS8.0 に対応 FCM 対応追加 Agent v3.41 以降の発着信番号履歴ポリシー・発着信番号制限ポリシー・指定番号着信による緊急指示機能の提供終了 Android OS 9.0 対応	
3.2	2019/5/21	SHARP 製のガラホ端末をご利用時の注意点を追加	
3.3	2019/8/1	管理画面の IP 制限機能追加	
3.4	2020/3/12	発着信番号履歴・発着信番号制限ポリシー、電話着信による緊急指示機能の提供再開 Lookout 連携機能追加 Agent 管理機能の仕様変更に伴う修正 Android 10 対応 アプリ配信機能の提供内容変更 SHARP モジュール機能追加 アプリ配信機能の仕様変更	
3.5	2020/8/28	ファイル配布機能の提供内容の一部変更に伴う修正 SHARP モジュール機能追加に伴う修正 端末再起動機能の追加に伴う修正 デバッグログ取得機能の追加に伴う修正 端末詳細情報の定期取得並びに CSV 出力機能追加に伴う修正 キオスク管理機能追加に伴う修正	
3.6	2020/11/26	CSV 連携の新機能追加に伴う修正	

3.7	2022/2/13	電話帳配信の対応 Agent 変更に伴う修正 グループポリシー管理機能追加 ロック画面のセキュリティ強化に伴う修正 CSV 連携の新機能追加に伴う修正 IVW の対応 OS バージョン変更に伴う修正 Android 11 対応に伴う修正 管理モード: WorkProfile[企業所有]追加 ライセンスキーリセット時の表示文言変更に伴う修正 個人情報利用の許諾追加に伴う修正 発着信番号制限の対応 Agent 変更に伴う修正 管理者一覧画面の表示変更に伴う修正	
3.8	2022/9/25	Android 12 対応に伴う修正 ファイル配布機能の提供内容の一部変更に伴う修正 端末ロック時の新機能追加に伴う修正 IVW の新機能追加に伴う修正 アプリポータル機能変更に伴う修正	
3.9	2022/11/2	IVW の対応 OS 変更に伴う修正	
4.0	2022/12/16	管理画面の Microsoft Edge 対応に伴う修正	
4.1	2023/3/24	Android13 対応に伴う修正	
4.2	2023/11/10	URL の削除	
4.3	2024/2/21	URL の削除	
4.4	2024/4/25	Android14 対応に伴う修正	
4.5	2024/8/6	発着信番号制限の機能変更に伴う修正 Work Profile、Work Profile[企業所有]の Android14 対応に伴う修正	

1章	はじめに	10
1.	概要	10
2.	ご注意	10
2章	STAR-MDMの特徴と機能	11
3章	システム構成と稼働環境	12
1.	STAR-MDMのシステム構成	12
2.	SPPM Agent(端末アプリ)	12
3.	稼働環境	13
4章	機能ラインナップ	14
1.	STAR-MDM機能ラインナップ	14
5章	クイックスタートガイド	16
1.	端末のセットアップ	16
	Android端末のセットアップ	16
2.	STAR-MDM管理サーバで端末の登録を確認	24
2-1.	STAR-MDM管理サーバへのログイン	24
2-2.	端末情報の確認・編集	24
3.	操作例:端末のリモートロック	28
3-1.	端末ロック指示の操作	28
3-2.	端末ロック指示解除の操作	30
4.	SPPM Agentの操作	31
4-1.	SPPM Agentの起動	31
4-2.	SPPM Agentの機能	31
5.	クイックSPPMの操作	34
6章	STAR-MDM管理画面	36
1.	ログイン画面	36
2.	STAR-MDM TOP画面	37
7章	ログ管理	39

8章 端末管理	41
1. 端末一覧画面	41
2. 端末状態シグナル	42
3. 端末情報編集	43
4. 緊急時指示	45
4-1. 端末ロック	45
4-2. 位置情報取得	46
4-3. データ消去	47
4-4. ハードリセット	48
4-5. ポリシー即時適用	49
4-6. パスワード初期化指示	49
4-7. ライセンスキーリセット	50
4-8. アンインストール有効化	51
4-9. 端末再起動	52
4-10. デバッグログ取得	53
5. 端末情報	54
6. 登録表示設定	64
7. 一覧表示設定	65
8. 端末並び替え	66
9. 端末検索	67
10. ポリシー 一括設定	68
11. CSV連携	70
12. その他	75
9章 ポリシー管理(概要)	76
1. ポリシー管理画面	76
2. ポリシーの作成／編集／削除	79
2-1. ポリシー 一覧画面	79
2-2. ポリシー作成画面	80
10章 ポリシー管理(基本機能パック)	82
1. サーバ端末間通信	82
2. 緊急時	85
Android Enterprise端末向け設定	91
3. 異常検知・通報	93

4. Agent管理	95
SPPM Agentのバージョンアップ実行手順	95
11章 ポリシー管理(フル機能パック)	99
1. パスワード管理	99
Android Enterprise端末向け設定	104
2. デバイス制御	105
3. 発着信番号履歴	113
4. 発着信番号制限	114
5. 位置情報取得	117
Android Enterprise端末向け設定	121
6. アプリ配信	122
7. 利用アプリ制限	129
8. アプリ一覧	143
9. APN固定化	145
10. Wi-Fi接続先制限	147
11. 接続先URL制限	148
11-1. 本機能の利用条件	149
11-2. 設定手順	149
11-3. SecBrowserの操作	153
12. ファイル配布	156
12-1. OS10以降におけるファイル配布の仕様	158
12-2. OS11以降かつv3.60.5以降におけるファイル配布の仕様	160
13. Wi-Fi設定	162
13-1. Wi-Fiアクセスポイントの登録手順	163
13-2. Wi-Fi設定ポリシーの作成手順	166
13-3. Wi-Fiアクセスポイントの削除手順	169
14. 端末暗号義務化	171
14-1. 本機能の利用条件	171
14-2. 事前準備	171
14-3. 暗号化の義務化から暗号化実行までの手順	172
15. SIM監視	175
16. メッセージ配信	176
17. 電話帳配信	184
18. アプリアンインストール制限	188

19. 動態管理	190
20. 利用統計	196
21. キオスク管理	197
12章 動態管理.....	198
1. 概要	198
2. 申し込み方法	198
3. 設定方法	199
4. 動態管理画面	200
13章 利用統計.....	204
1. 概要	204
2. 申し込み方法	204
3. 設定方法	205
4. 利用統計画面	206
4-1. アプリ利用時間	208
4-2. 通信量	210
14章 その他.....	212
1. その他画面	212
2. 管理者管理	213
3. レポート管理	218
4. グループ管理	221
グループ新規登録	221
グループポリシー管理	223
5. 動態管理 / 利用統計 利用設定	224
6. SIM情報自動更新	226
8. Crashlytics設定	227
9. 言語表示設定	228
10. デバッグロガー一覧	229
15章 連携アプリ	230
1. 連携アプリ画面	230
2. Mon(SPPM監視ソフト)	230

3. AV連携アプリ.....	231
Internet VirusWall(IVW).....	233
4. E-SDK専用モジュールアプリ.....	236
5. Sony Xperia E-API.....	240
6. SHARP モジュールアプリ.....	242
7. コールピックアップ	244
8. アプリポータル.....	248
16章 注意事項と機種依存情報	250
1. 他の端末管理システムとの併用.....	250
2. 端末の識別方法	250
3. SIM未装着の場合の機能制限.....	250
4. 機種依存.....	250

1. 概要

本書は、STAR-MDMの設定方法、利用方法を記載した管理者用のマニュアルです。

STAR-MDMは、Google Android OS及びApple iOSをベースとするスマートフォンやタブレットなどのモバイル端末に対して、端末管理(MDM: Mobile Device Management)やセキュリティ・ポリシーを集中管理するためのセキュリティ統合管理システムです。

モバイル端末をセキュリティ・ポリシー管理下に置くことで、小型・軽量・多機能なモバイル端末の紛失、盗難、悪用によるリスクを低減し、業務活用のための管理基盤を提供します。

《SPPMについて》

「Smart Phone Policy Manager」の頭文字をとった造語であり、株式会社STARNETの登録商標です。

2. ご注意

STAR-MDMは、端末のハード、ソフトの基本部分の設定変更や制御を行います。非対応端末に適用するとAndroid端末が制御不能になるなど甚大な影響を与える場合がありますので、非対応機種でのご利用はご遠慮くださいますようお願いいたします。

端末アプリ「SPPM Agent」は非対応端末でも動作しますが、正常動作は保証されません。非対応機種でのご利用はユーザー様の責任において行ってください。

対応機種でもまれに端末初期化を余儀なくされる可能性があります。STAR-MDMのご利用により直接的または間接的によらず、いかなる障害、損害が発生いたしましても、スターネット株式会社は責任を負いかねますことをご理解の上ご利用ください。

他のMDM製品、Exchangeサーバ、一部のウイルス対策ソフトなどのMDM(パスワード管理や端末初期化等の端末管理)機能を試用または利用したことのある端末は、管理サーバ側でのMDM設定を解除した後、端末初期化を実施した上で、SPPM Agentをインストールするようにしてください。

STAR-MDMは、ユーザーが利用するモバイル端末に常駐し、セキュリティ・ポリシーを維持するための端末アプリ「SPPM Agent」と、管理者がセキュリティ・ポリシーを設定・管理するための「STAR-MDM管理サーバ」からなる、エージェント・サーバ型のシステムです。

STAR-MDMの最大の特長は、STAR-MDM管理サーバにより、多数のモバイル端末のセキュリティ・ポリシーをリモートから一元管理できることです。STAR-MDMの端末管理画面には、Android、iOS、通信キャリア、端末機種の違いなく一覧表示することができます。

Android端末では、端末の配布に先立ち、SPPM Agent(端末アプリ)をインストールする手間が必要となりますが、端末にて常駐稼働するSPPM Agentと管理サーバとの連携により、モバイル端末を各ユーザーに配布した後も端末を回収することなく、ポリシー設定、カメラやSDカードといったデバイス機能の利用制限、アプリ(apkファイル)の配布からインストール、バージョンアップの一斉実施、利用状況の継続的な把握などが可能です。

例えば、

- ・セキュリティ・ポリシーを遵守し、スマートフォンを適正に利用しているか？
- ・カメラなどの禁止デバイスを利用しようとしていないか？
- ・端末をパスワードロックし、安全に利用しているか？
- ・仕事以外の電話に利用していないか？

といったことを、STAR-MDM管理サーバの管理画面にて、閲覧・管理できます。

STAR-MDM管理サーバによる利用ログの集中管理により、ポリシー違反の試みや異常をSTAR-MDM管理サーバが自動的に検知し、管理者への通知メールや問題のあるユーザーへの警告メールを自動的に送信します。従って、管理者はログ情報の目視チェックによる異常端末の検出や問題のあるユーザーへの対処に労力・時間を費やす必要がなく、管理工数を大幅に軽減することができます。

このほか、モバイル端末自体やアプリの管理、紛失時のリモート端末ロック指示やリモートデータ消去、端末初期化など、モバイル端末の安全性を高め、業務活用を推進するための機能を実現しています。

iOSの場合には、iOS自体にApple社が用意した端末管理機能(MDM機能)が搭載されているため、

- ・iOSに準備された機能は当然ながらOSとして保証されている

というメリットがあります。

その一方で、

- ・Apple IDの事前取得が必須
- ・自社アプリの配信・インストールには iDEPアカウント(有償)が必須
- ・iOSのMDM機能を用いるための証明書の準備とインストールが必須
- ・iOSのMDM機能以外の実装が困難
- ・Apple社のプッシュサーバを経由してのIPプッシュ指示でしか制御できないなどの制限があります。

1. STAR-MDMのシステム構成

STAR-MDMは、モバイル端末にて常駐稼動する端末アプリ「SPPM Agent」と「STAR-MDM管理サーバ」で構成され、管理サーバ⇄エージェント間の情報交換によって各種機能を実現しています。

※iOS端末の場合、iOS自体の端末管理機能を利用します。

2. SPPM Agent (端末アプリ)

Android端末用の「SPPM Agent」(端末アプリ)は、STAR-MDMのご利用お申し込み時にダウンロードURLをお知らせしますので、端末のブラウザからアクセスして、インストールしてください。

Google Playが利用できない場合は、STAR-MDMのご利用お申し込み時にダウンロードURLをお知らせしますので、端末のブラウザからアクセスして、インストールしてください。

Google Play Storeからのアプリインストールではないため、予め端末の[設定]-[アプリケーション]-[不明なアプリケーション](端末によっては「不明な提供元」、「提供元不明のアプリ」と表示されます)にチェックを入れておく必要があります。

SPPM Agentは、管理者がSTAR-MDM管理サーバに設定したポリシーや指示を取得し、Android端末を制御します。

3. 稼働環境

【対応端末】

■ 対応OS

Android OS v2.3～v14.x

※SPPM Agent v3.25以降では Android OS 4.0 未満は非対応です。

※SPPM Agent v3.45以降では Android OS 4.2 未満は非対応です。

※SPPM Agent v3.59.4以降では Android OS 4.4 未満は非対応です。

※SPPM Agent v3.59.6以降では Android OS 5.0 未満は非対応です。

※Android10以降ではAndroidEnterpriseの利用が必須です。通常キットティングでの利用は非対応です。

■ 対応機種

対応機種は適時更新されますので、弊社にお問い合わせください。



マルチユーザ機能との併用は動作保証対象外です。

【管理者用ブラウザ】

Google Chrome(最新版に対応)

Microsoft Edge(最新版に対応)

1. STAR-MDM機能ラインナップ

端末管理、ポリシーの設定・リモート適用、利用状況把握(ログ収集・管理)といった標準機能に加え、ポリシー設定機能は「基本機能パック」「フル機能パック」の2種類からニーズに合わせて選択できます。また、ウイルス対策、データ暗号化、URLフィルタリング、アプリフィルタリングなどの機能を各々オプションで利用可能です。

機能項目	Android	iOS	基本機能パック	フル機能パック
<標準機能>				
端末管理	○	○	✓	✓
ポリシー設定・リモート適用	○	○	✓	✓
利用状況把握(ログ収集・管理)	○	○	✓	✓
コールピックアップ	○	-	✓	✓
<ポリシー管理機能>				
サーバ端末間通信	○	○	✓	✓
緊急時処置 (端末ロック指示/データ消去/ハードリセット)	○	○*1	✓	✓
異常検知・通報	○	○	✓	✓
Agent管理 (SPPM Agentリモートバージョンアップ)	○	-	✓	✓
パスワード管理 (パスワード利用の義務化等)	○	○		✓
デバイス制御 (カメラ、SDカード、Wi-Fi、Bluetooth等)	○	○*2		✓
発着信番号履歴取得	○	-		✓
位置情報取得	○	○*3		✓
アプリ一覧取得・変更通知	○	○		✓
アプリ配信・インストール	○	-		✓
アプリ管理	-	○		✓
ファイル配布	○	-		✓
利用アプリ制限	○	*4		✓
APN設定固定化	○	-		✓
発着信番号制限	○	-		✓
Wi-Fi接続先制限	○	-		✓
接続先URL制限	○	-		✓
Wi-Fi設定	○	-		✓
端末暗号義務化	○	-		✓
構成プロファイル配信	-	○		✓
構成プロファイル削除	-	○		✓
SIM監視	○	-		✓
メッセージ配信	○	○		✓
利用アプリ検知	-	○		✓
電話帳配信	○	○		✓
VPP管理配布(iOS9以降対応)	○	○		✓
アプリアンインストール制限	○	-	-	✓
動態管理	○	-	-	✓
利用統計	○	-	-	✓
キオスク管理	○	-	-	✓
<連携オプション機能>				
ウイルス/マルウェア対策システム連携 オプション	○	-	✓	✓

データ暗号化オプション	○	-	✓	✓
URLフィルタリングオプション	○	-	✓	✓
アプリフィルタリングオプション	○	-	-	✓

*1: iOSはパスワードロックとハードリセットのみ可能。

*2: iOSはカメラ、スクリーンショット、YouTube、iTunes Store、App Store、iCloud、Safariの利用制限のみ可能。

*3: iOSはSPPM Agentをインストールすると自動取得。

*4: iOSはデバイス制御ポリシー内アプリの利用制限のみ可能。

1. 端末のセットアップ

モバイル端末をリモートで一元管理するために、対象の端末をセットアップし、STAR-MDM 管理サーバに登録します。

Android端末のセットアップ

管理対象のAndroid端末にSPPM Agent (端末アプリ) をインストールします。インストールが完了すると端末がSTAR-MDM管理サーバに自動的に登録されます。

- ① 管理対象の端末にSTAR-MDMが対応している必要があります。
対応機種については弊社にお問い合わせください。
- ② **Android OS 10以降では Android Enterprise の利用が必須**です。(通常キッティングでの利用は非対応)
キッティング手順等は Android Enterprise マニュアルをご確認ください。
- ③ 既に該当の端末でSPPM Agentをご利用いただいている場合、もしくはセットアップ中になにかしらの不具合が発生した場合、再度セットアップを行う前に、端末からSPPM Agentをアンインストール、管理画面からライセンスキーをリセットする必要があります。
関連情報 [「ライセンスキーリセット」](#)

【事前準備】

①SPPM Agent (端末アプリ) のインストールには、次の情報が必要です。

- ・グループキー (ご契約法人ID)
- ・SPPM Agent URL (SPPM Agentのインストール用URL)

上記を参照できるようお手元にご準備ください*1。

*1: ご利用開始時にメールでお知らせします。

②端末の設定メニューで[セキュリティ]→[提供元不明のアプリ]にチェックを入れます。

【Android OS 8.0 未満】

[設定]→[セキュリティ]→[提供元不明のアプリ]にチェック。

【Android OS 8.0 以降】

[設定]→[アプリと通知]→[詳細設定]→[特別なアクセス]→[不明なアプリのインストール]→[SPPM]→[この提供元のアプリを信頼する]にチェック



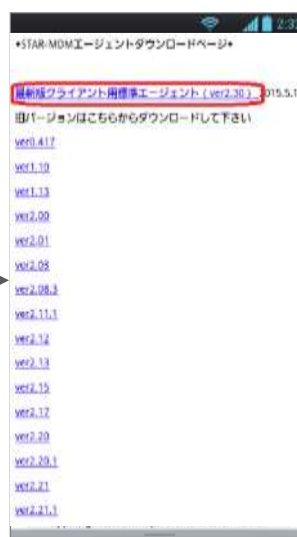
【SPPM Agent(端末アプリ)のインストール ～ 端末の登録】

※端末により画面表記が異なる場合があります。



① 端末のブラウザを起動して、URL 欄に「SPPM Agent URL」を入力します。

*1: ご利用開始時にメールでお知らせします。



② 「SPPM Agent」のダウンロードサイトにアクセスしたら、[最新版クライアント用標準エージェント (verX.XX)] をタップします。



③ダウンロードが完了したら、画面上部のステータスバーを下にスライドし、[SppmAgent_vX-XX.apk]をタップします。

◎ダウンロード完了の通知が消えていたら？

アプリトレイから「ダウンロード」を起動し、[SppmAgent_vX-XX.apk]をタップします。

◎「アプリケーションを選択」の画面が表示されたら？

[パッケージインストーラー]をタップします。



④[インストール]をタップします。



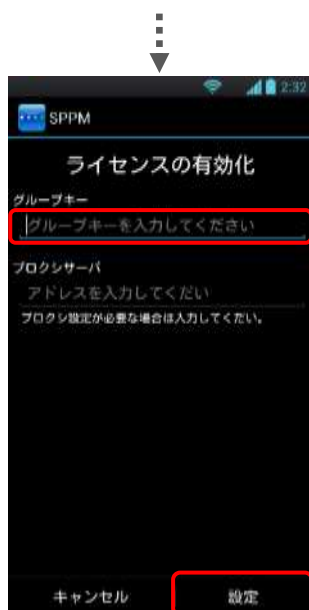
⑤インストールが完了したら、[開く]をタップします。

インストール完了

インストールが完了すると、アプリトレイにSPPM Agentのアイコンが追加されます。



※[完了]をタップしてインストーラー画面を終了させてしまった場合は、このSPPMアイコンをタップしてください。



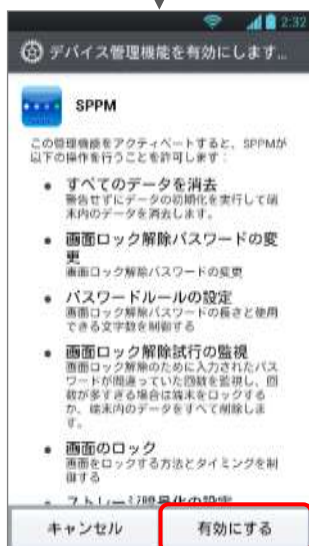
⑥「ライセンスの有効化」の画面になりますので、12桁のグループキーを正しく入力し、[設定]をタップします。

※SPPM Agent v3.40以降では「WorkProfileを利用する」のチェックボックスが表示されますが、AndroidEnterpriseのWorkProfile利用時以外はチェック不要です。

★ワンポイント:専用インストーラについて

専用インストーラ(有償オプション)を利用すると、この画面は省略され、グループキーの入力が不要になります。

大量の端末に SPPM Agent アプリをインストールする場合には、大変便利です。

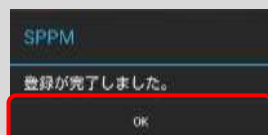


⑦「デバイス管理機能を有効にしますか?」の画面で[有効にする]をタップします。

※SPPMが実行する機能が表示されます。

端末の登録完了

STAR-MDMサーバと通信が行われ、端末に基本ポリシーが適用されます。



◎「初期パスワードの設定を行ってください」の画面が出たら

STAR-MDMをフル機能パックでご利用の場合、STAR-MDM管理サーバの基本ポリシーのデフォルト設定で、パスワード利用が義務化されています。SPPMから初期パスワードの設定を求められた場合は[OK]をタップし、「ロック解除方法の選択」画面にてロック解除の方法を指定して設定を行ってください。



こんなときは

■端末からSPPM Agentをアンインストールしたい:

☞「[アンインストール有効化](#)」

☞「[ライセンスキーリセット](#)」

◎権限催促画面(OS6.0 以降)

OS6.0 以降の端末の場合、SPPM アプリをインストール後、権限催促画面が表示されます。

以下の手順で権限を許可してください。その後ライセンス有効化画面が表示されます。

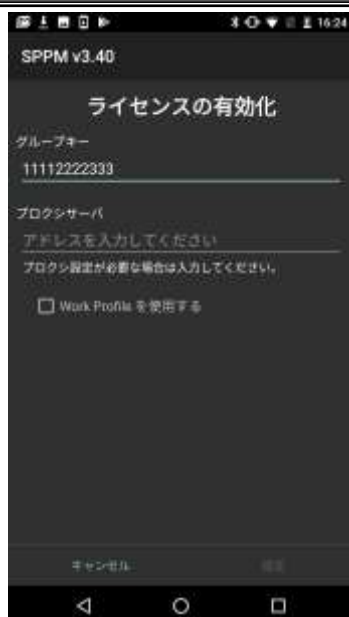


「許可する」をタップしてください。

項目ごとに許可画面が表示されるので全て許可してください。

別画面が表示される権限については手動で ON にしてからバックキーをタップしてください。
予めチェックが ON の場合は一度 OFF にしてから ON にしてください。

◎ライセンス有効化画面(OS8.0 以降)



SPPM Agent v3.40 以降ではライセンスキー有効化画面に「WorkProfile を利用する」と表示されますが、Android Enterprise の Work Profile 利用時以外はチェック不要です。

【端末ロック時の発信機能の制御について】

Android OS 10 以降、端末ロック指示時において音声通話の発信がデフォルトで許可されています。
 端末ロック指示時の音声通話の発信を禁止する場合、端末側にて設定を行ってください。

- ❗ 「電話転送アプリ」を SPPM Agent に指定した場合、
 SPPM Agent 以外の電話転送アプリが利用できません。

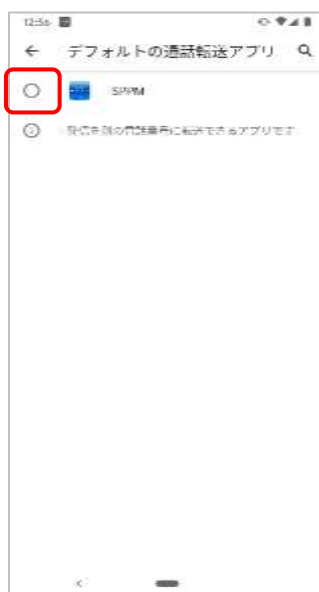
※端末により画面表記が異なる場合があります。



① 端末設定を開き、
「アプリと通知」をタップします。

②「デフォルトのアプリ」を
タップします。

③「電話転送アプリ」を
タップします。



④SPPM にチェックを入れ、
設定は完了です。

【GalaxyシリーズでのSPPM Agent(端末アプリ)のインストール】

GalaxyシリーズE-SDK『4』以降の端末にSPPM Agent v2.29以降で端末登録が完了すると、独自機能である『KNOX』のライセンス有効化が求められるので、有効化設定をしてください。

規約に同意の上、有効化を実行するとE-SDK*1による制限機能がE-SDK専用モジュールアプリをインストールせずに利用ができます。

*1 「E-SDK専用モジュールアプリ」

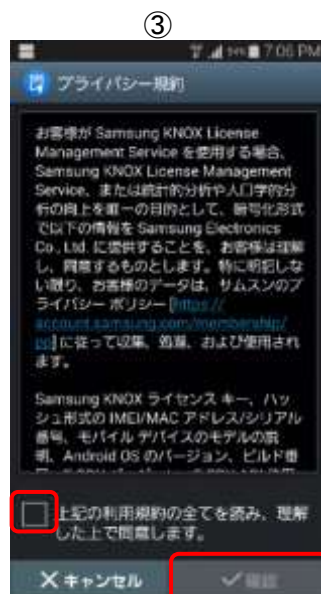
【KNOXライセンス有効化画面と確認】



SPPM のデバイス管理有効化後、端末の通知バーに KNOX ライセンス有効化が表示されたら選択してください。



『有効にする』を選択してください。



規約画面でチェックをして、『確認』をタップしてください。



KNOX ライセンス有効化が完了すると SPPM Agent 起動時に E-SDK バージョンが白く表示されます。

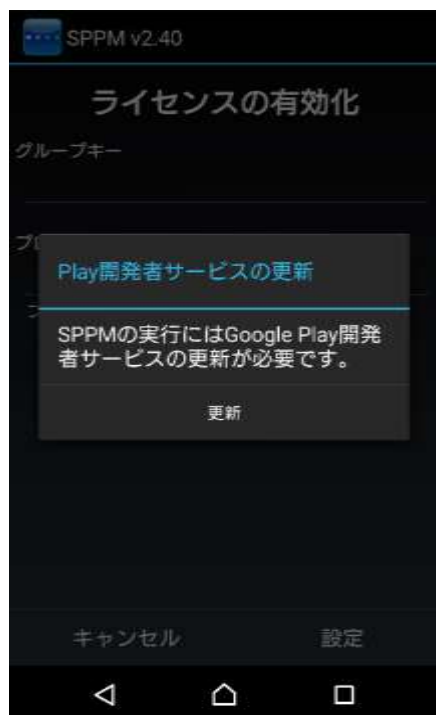
◎ライセンス有効化を行わなかった場合

ライセンス有効化を行わなかった場合は、通知バーの表示とパスワード解除毎にKNOXライセンスの有効化画面のポップアップが表示されます。



◎Play開発者サービスの更新

ご利用中の端末が以下3点の条件を満たし、該当のいずれかの操作を行った際に「SPPMの実行にはGoogle Play開発者サービスの更新が必要です。」というダイアログが表示されます。Google Play開発者サービスの更新を行うまで、該当端末でGCM/FCMをご利用いただけません。※GCMは2019年4月11日に廃止となります。FCM対応版のSPPM Agent v3.40以降をご利用ください。



【条件】

1. SPPM ver 2.31以降のバージョンを利用している。
2. サーバ端末間通信ポリシーにて、「GCM/C2DM/FCMを利用する」にチェックを入れたポリシーが適用されている。または、適用しようとしている。
3. Google Play開発者サービスがGCM/FCM利用登録を行えないバージョンである。

【操作】

1. 端末にSPPM Agentをインストール、キッティングする。
2. 端末情報設定ボタンを押下する。
3. GCM/FCMを利用していなかった端末にてGCM/FCMを利用する。

該当端末でGCM/FCMをご利用いただくためには、Google Play開発者サービスを最新版に更新してください。

※ E-API / E-SDK をご利用中の場合、Google Play開発者サービスの更新のために、利用アプリ制限でのGoogle Playの許可が必要です。

※ Google Playをご利用いただくためには、Googleアカウントの登録が必要です。

☞「[サーバ端末間通信](#)」

☞「[利用アプリ制限](#)」

◎管理サーバへの登録画面



v3.04 からは登録が完了できていない状態では「管理サーバへの登録画面」が表示され、その画面から正常に登録し直すことができます。

※仕様により v3.04 以降へのバージョンアップ直後に「管理サーバへの登録画面」が表示されることがあります

2. STAR-MDM管理サーバで端末の登録を確認

STAR-MDM管理サーバにログインし、端末の登録を確認します。また、管理に必要な端末情報を編集します。

2-1. STAR-MDM管理サーバへのログイン

①ログイン情報の確認

STAR-MDM管理サーバへのログインには、次の情報が必要です。

- ・STAR-MDM管理サーバURL
- ・アカウント
- ・パスワード

上記を参照できるようお手元にご準備ください*1。

*1: ご利用開始時にメールでお知らせします。

②ログイン

管理者用のPCにてブラウザを起動し、「STAR-MDM管理サーバURL」にアクセスしてログイン画面を表示します。IDには「アカウント」、PASSには「パスワード」を正しく入力して、[Login]をクリックしてください。



2-2. 端末情報の確認・編集

① STAR-MDM管理画面が表示されたら、メニューバーの[端末管理]をクリックします。



② 「端末一覧画面」が表示されます。

この画面では、STAR-MDM管理サーバに登録されたすべての端末の情報を一覧で確認することができます。



《端末情報について》

・ライセンスキー:

ライセンスキーはご契約の端末数に応じて事前に登録されています。

・端末電話番号、端末名称、ソフトID、端末ID:

端末のセットアップ時に自動収集されて登録されます。

関連情報 [「端末一覧画面」](#)

③ 対象端末の[編集]をクリックします。



④「端末情報編集画面」が表示されますので、「利用者情報」を編集します。

端末の管理に必要な情報を入力して[上書保存]をクリックしてください。

関連情報 ➡ [「端末情報編集」](#)

★ワンポイント

Android端末では、「利用者情報」を各端末側で入力してSTAR-MDM管理サーバに登録することもできます。
※STAR-MDM管理サーバ上で「利用者情報」が未登録状態の項目に限ります。STAR-MDM管理サーバに登録済みの情報を端末側から上書き更新することはできません。

所属については事前に「グループ登録」で登録が必要です。

➡「SPPM Agentの操作」> [「端末情報設定」](#)

➡ [「グループ登録」](#)

《ポリシー情報について》

端末情報編集画面の「ポリシー情報」では、各ポリシー管理項目で現在選択されているポリシーが表示されており、プルダウンメニューで変更することができます。

いくつかのポリシー管理項目では既に「基本ポリシー」が選択されています。「基本ポリシー」とは、STAR-MDM管理サーバがデフォルトで選択するポリシーです。「基本ポリシー」は、新規登録の端末に対して自動的に適用されます。

以下のポリシー管理項目において、それぞれの「基本ポリシー」がデフォルトで選択されます。

また、その他のポリシーは別途ポリシー作成画面で「基本ポリシー」を作成できます。

■サーバ端末間通信(Android, iOS)

■緊急時(Android, iOS)

■異常検知・通報(Android, iOS)

■パスワード管理*1(Android, iOS)

■デバイス制御*1(Android, iOS)

*1: STAR-MDMのご利用形態が基本機能パックの場合、ポリシー管理項目には含まれません。フル機能パックにてご利用いただけます。

関連情報➡「[ポリシー管理\(概要\)](#)」

◎基本ポリシーの編集

「基本ポリシー」は編集可能です。既に「基本ポリシー」を適用済みの端末への反映はもちろん、新規登録の端末に自動適用される設定内容を最適化することができます。

◎ポリシーを新規作成

STAR-MDMの利用を開始した時点で選択できるポリシーは「基本ポリシー」しかありません。「基本ポリシー」以外の各種ポリシーは、管理者が設定して登録します。

こんなときは

■多数の端末情報を効率的に編集したい:

・CSVデータを利用して「端末情報」の一括更新が可能です。➡「[CSV連携](#)」

・複数の端末に同一ポリシーの一斉割り当てが可能です。➡「[ポリシー 一括設定](#)」

■端末の登録を解除したい:

➡「[不要となったAndroid端末の解除手順](#)」

3. 操作例: 端末のリモートロック

緊急時の操作例として、端末のリモートロックを行う方法をご紹介します。端末の紛失・盗難時に、管理者は管理画面から簡単な操作で端末をロックし、第三者による端末の不正使用を防ぐことができます。

3-1. 端末ロック指示の操作

- ① STAR-MDM管理画面でメニューバーの[端末管理]をクリックします。



- ②「端末一覧画面」が表示されますので、対象端末の[指示]をクリックします。



- ③「緊急時指示画面」が表示されますので、[端末ロック指示]をクリックします。

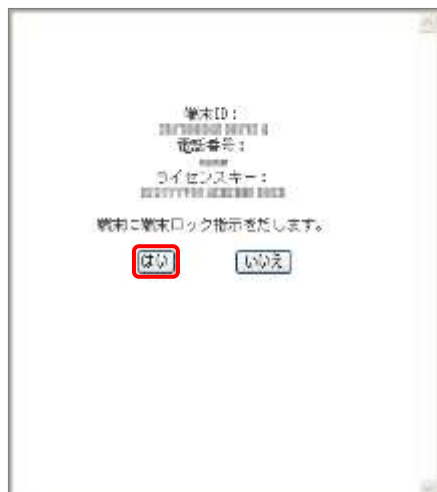


◎ 表示されるボタンがスクリーンショットと異なるのは？

「緊急時指示画面」におけるボタン表示の有無は、当該端末に適用されているポリシーに依存します。また、STAR-MDMのご利用形態が基本機能パック、フル機能パックのどちらか、当該の端末がAndroid端末かiOS端末かによっても差異があります。

⇒「[緊急時指示](#)」

- ④ 当該端末の「端末ID、電話番号、ライセンスキー」が表示されますので、確認の上[はい]をクリックします。



★ワンポイント

以下の端末では、即時に端末ロック指示が実施されます。

- ・Googleプッシュが利用可能なAndroid端末*1

*1 : STAR-MDM 管理サーバの設定で Google プッシュ (GCM/C2DM/FCM) にチェックが必要です。(デフォルト設定ではチェック済みです) ⇨「[サーバ端末間通信](#)」

★ワンポイント

Android端末では、特定の電話番号からの「電話着信」のみで即時に端末ロック指示を実施することも可能です。

※SPPM Agent v3.41～v3.43では、電話着信による端末ロック指示は非対応です

⇨「[緊急時指示](#)」

Android「端末ロック指示」

■STAR-MDM管理サーバ「端末一覧画面」



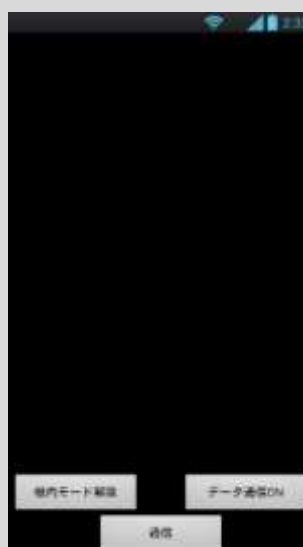
端末に指示が届き、「端末ロック指示」が実施されると、端末状態シグナルの中央の表示が青色に変わります。



■Android端末 (SPPM Agent v2.10以上)



■Android端末 (SPPM Agent v2.09.3以下)

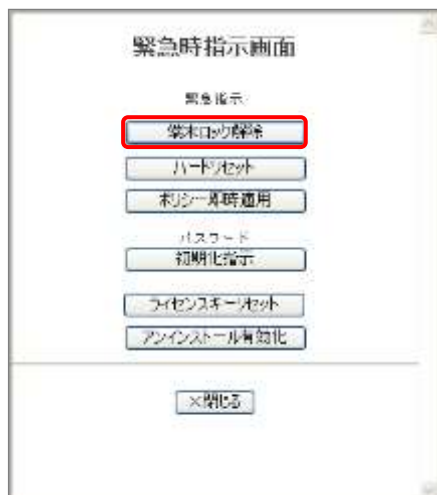


Android端末では、STAR-MDM専用のロック画面になり、表示されているボタン以外の操作はできなくなります。

3-2. 端末ロック指示解除の操作

① 端末ロック指示の操作①～②と同様、STAR-MDM管理画面でメニューバーの[端末管理]をクリックし、「端末一覧画面」で、対象端末の[指示]をクリックします。

② 「緊急時指示画面」が表示されますので、[端末ロック指示解除]をクリックします。

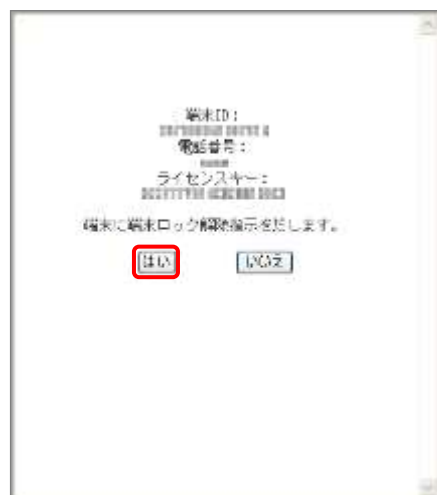


◎ 表示されるボタンがスクリーンショットと異なるのは？

「緊急時指示画面」におけるボタン表示の有無は、当該端末に適用されているポリシーに依存します。また、STAR-MDMのご利用形態が基本機能パック、フル機能パックのどちらか、当該の端末がAndroid端末かiOS端末かによっても差異があります。

☞ 「[緊急時指示](#)」

③ 当該端末の「端末ID、電話番号、ライセンスキー」が表示されますので、確認の上[はい]をクリックします。



★ワンポイント

以下の端末では、即時に端末ロック指示解除が実施されます。

・Googleプッシュが利用可能なAndroid端末*

※STAR-MDM管理画面の設定でGoogleプッシュ(GCM/C2DM/FCM)にチェックが必要です。(デフォルト設定ではチェック済みです)

☞ 「[サーバ端末間通信](#)」

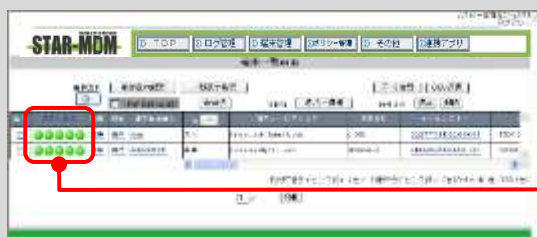
★ワンポイント

Android端末では、特定の電話番号からの「電話着信」のみで即時に端末ロック指示解除を実施することも可能です。(SPPMAgent v3.41～v3.43では非対応)

☞ 「[緊急時指示](#)」

「端末ロック指示解除」完了

■STAR-MDM管理サーバ「端末一覧画面」



端末に指示が届き、「端末ロック指示解除」が実施されると、端末状態シグナルの中央の表示が緑色に戻ります。



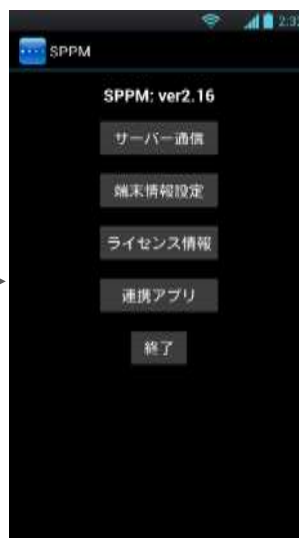
4. SPPM Agentの操作

端末では、SPPM Agent(端末アプリ)が端末の制御を行います。基本的には自動でSTAR-MDM管理サーバと通信を行い、管理者が設定したポリシーや指示を取得して実行しますが、ユーザーが直接起動して操作する場合もあります。ここでは、SPPM Agentの操作について解説します。

4-1. SPPM Agentの起動



①インストール後アプリ一覧に追加されたSPPMアイコンをタップします。



②SPPM Agentが起動し、メニュー画面が表示されます。

関連情報 ➡ [「端末のセットアップ」](#)

4-2. SPPM Agentの機能

【サーバ通信】



[サーバー通信]をタップすると、SPPM AgentがSTAR-MDM管理サーバと通信を行い、反映待ちのポリシーや指示を取得して実行します。

【端末情報設定】

[端末情報設定]をタップすると、端末の利用者情報を入力することができます。入力後[設定]をタップすると端末に情報が保存されます。

☆ワンポイント: 端末情報を STAR-MDM 管理サーバに反映させる

STAR-MDM 管理サーバにおける当該端末の「利用者情報」の内、未登録状態の項目に対しては、端末で入力した内容が反映されます。

端末セットアップの際に必要な情報の入力をユーザーに委ねることも可能です。

※STAR-MDM 管理サーバ上で登録が済んでいない項目に限ります。既に情報が登録済みの項目については、端末側から上書き更新されません。

※STAR-MDM 管理サーバ上で登録・更新した内容は、端末には反映されません。

関連情報 ➡ [「端末情報編集」](#)

◎Play開発者サービスの更新

ご利用中の端末が以下3点の条件を満たし、該当のいずれかの操作を行った際に「SPPMの実行にはGoogle Play開発者サービスの更新が必要です。」というダイアログが表示されます。

Google Play開発者サービスの更新を行うまで、該当端末でGCMをご利用いただけません。

【条件】

1. SPPM ver 2.31以降のバージョンを利用している。
2. サーバ端末間通信ポリシーにて、「GCM/C2DM/FCMを利用する」にチェックを入れたポリシーが適用されている。
または、適用しようとしている。
3. Google Play開発者サービスがGCM/FCM利用登録を行えないバージョンである。

【操作】

1. 端末にSPPM Agentをインストール、キッティングする。
2. 端末情報設定ボタンを押下する。
3. GCM/FCMを利用していなかった端末にてGCM/FCMを利用する。

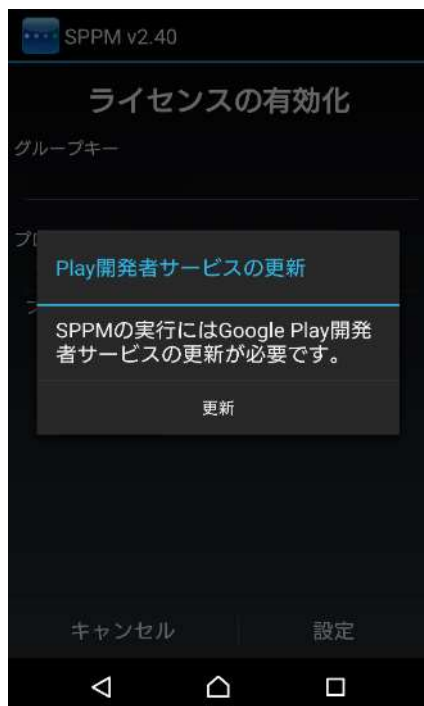
該当端末でGCMをご利用いただくためには、Google Play開発者サービスを最新版に更新してください。

※ E-API / E-SDK をご利用中の場合、Google Play開発者サービスの更新のために、利用アプリ制限でのGoogle Playの許可が必要です。

※ Google Playをご利用いただくためには、Googleアカウントの登録が必要です。

➡ [「サーバ端末間通信」](#)

➡ [「利用アプリ制限」](#)



【ライセンス情報】

[ライセンス情報]をタップすると、端末に割り当てられたライセンスキーとソフトIDが表示されます。

【メッセージ】

[メッセージ]をタップすると、端末に配信されたメッセージを見る事ができます。

関連情報➡「[メッセージ配信](#)」

【ファイル】

[ファイル]をタップすると、端末に配信されたファイルが表示されます。

関連情報➡「[ファイル配布](#)」

【連携アプリ】



STAR-MDMの連携アプリに関連するアイコンが、それぞれの仕様に依じて表示されます。

※アイコン表示の有無は、連携アプリの仕様によります。

※スクリーンショットに表示されているのは、「コールピックアップ」の機能に関連するアイコンです。

関連情報➡「[連携アプリ](#)」

こんなときは (..)φ

■ 端末を管理サーバからライセンスキーリセットしたい:

➡「[\[不要となったAndroid端末の解除手順\]](#)」

5. クイックSPPMの操作

【クイックSPPMの設定】

クイック設定パネルに機能の一部を利用できる「クイック SPPM」が設置可能です。

クイック SPPM では「サーバー通信」「コールピックアップ」「端末ロック指示中のメッセージ確認/緊急時連絡先への発信」が利用可能です。また、端末のパスワード認証を行わない状態でも起動できます。

※Android 14.0 以降では、端末のパスワード認証前はクイック SPPM を起動できません。

※Android 8.0 以降の機種のみ利用可能です。

※Work Profile, Work Profile[企業所有]は非対応です。

■設定手順



① ステータスバーを開きます。



② クイック設定パネルの編集ボタンをタップします。



③ 画面をスクロールします。



④ 「SPPM」を画面上部へ



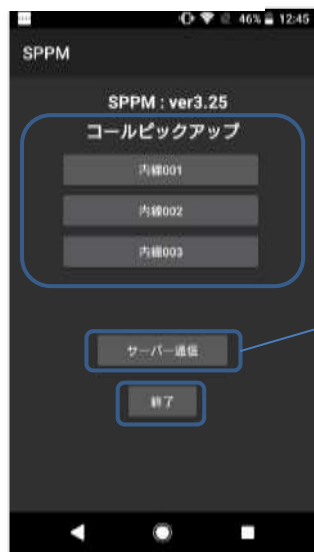
⑤ 任意の場所に「SPPM」を設置します。



⑥ クイック設定パネルに「SPPM」が表示されます。タップすると「クイック SPPM」が起動します。

■クイック SPPM 画面

【通常時画面】



・コールピックアップ

コールピックアップ設定で追加したボタンが表示されます。
ボタンを押下すると設定した番号へ発信します。
※コールピックアップが設定されていない場合は表示されません。
※Android 8.0 以降ではボタンの高さ・位置・色は指定できません。

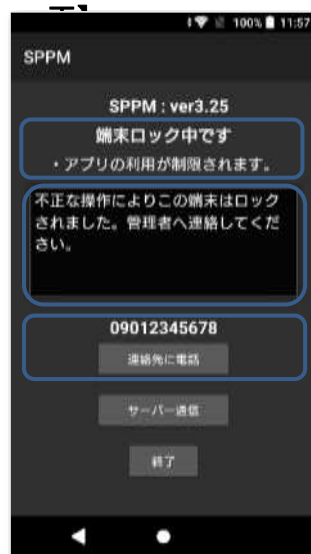
・サーバー通信

SPPM Agent が STAR-MDM 管理サーバと通信を行い、
反映待ちのポリシーや指示を取得して実行します。

・終了

クイック SPPM の画面を閉じます。

【端末ロック指示中画



※端末ロック指示中は「コールピックアップ」が非表示となります。

・端末ロック指示中メッセージ

固定メッセージが表示されます。

緊急時ポリシー設定項目

・メッセージ

緊急時ポリシーに設定されたメッセージが表示されます。
※設定がない場合は非表示になります。

・緊急時連絡先/連絡先に電話ボタン

緊急時ポリシーに設定された緊急時連絡先番号が表示され、
「連絡先に電話」ボタンを押下すると緊急時連絡先に発信します。
※設定がない場合は非表示になります。

1. ログイン画面

ブラウザにて所定のURLにアクセスすると、下記のようなログイン画面が表示されます。



初期の管理者ID、及びパスワードは、事前にご連絡します。

ログイン後、メニューバーの[その他]>[管理者管理]をクリックし、直ちに管理者パスワードを変更してください。

関連情報⇒「[管理者管理](#)」

- ・7回連続でログインに失敗すると警告メッセージが表示されます。
 - ・10回連続でログインに失敗するとアカウントが停止(30分間ログイン不可)されます。
 - ・アカウントが停止された後、さらに5回失敗すると凍結(ログイン不可)されます。
 - ※ログインが成功した時点で、失敗回数はクリアされます。
 - ・アカウントが停止または凍結された場合、マスター管理者による指示で解除可能です。
- 関連情報⇒「[アカウント停止・凍結解除](#)」

sppm エラー

IDまたはパスワードが間違っています。ご確認ください。
あと3回ログインに失敗するとアカウントが30分間ロックされます。

ログイン画面

パスワードを忘れた場合は「パスワードを忘れた方はこちら」のリンクをクリックしてください。

管理者IDとグループキーの入力をして送信すると、パスワードが再発行されます。

パスワード再発行のご案内

登録情報

ご登録情報を入力の上、送信ボタンを押してください。
パスワード再設定用URLをご登録のメールアドレスにお送りします。

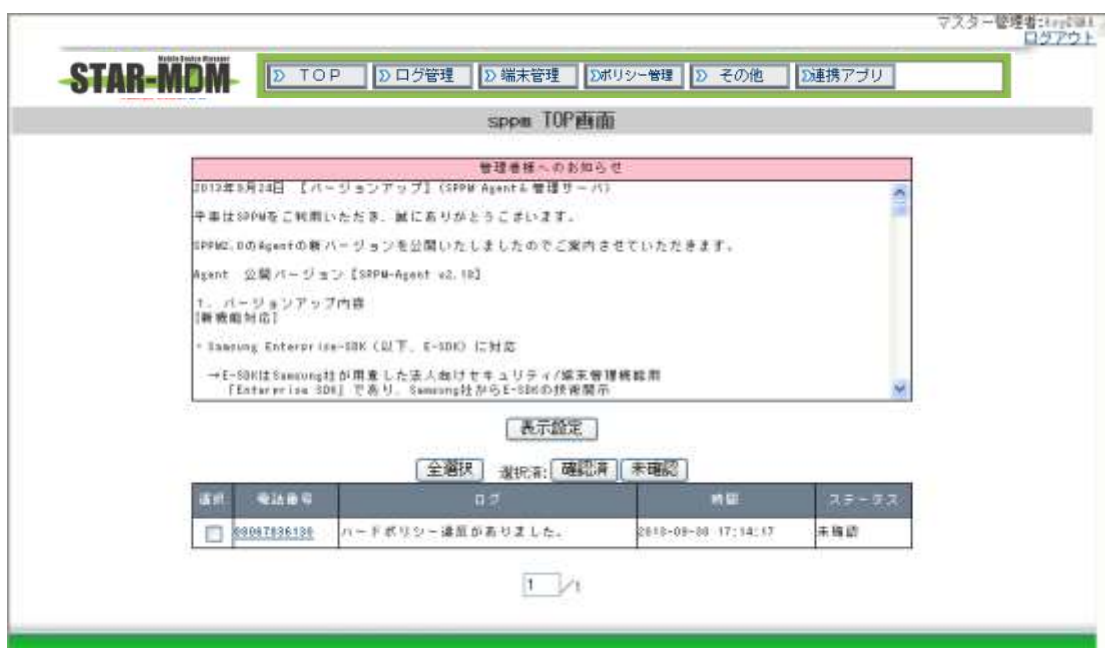
管理者ID:

グループキー:

送信

2. STAR-MDM TOP画面

ログインに成功すると、下記のようなTOP画面が表示されます。



■メニューバー

STAR-MDM管理サーバの各画面の上部には、メインメニューに相当するメニューバーが表示されており、メニューバーの各ボタンをクリックすることで各画面に遷移します。

■管理者様へのお知らせ

バージョンアップのお知らせやシステムメンテナンスなど、管理者向けのお知らせが表示されます。直近3か月以前のお知らせは「過去のお知らせを確認」から、「過去の管理者様へのお知らせ」画面でご確認いただけます。

■アラート一覧

ポリシー違反等がある場合に、どの端末でどのようなアラートが発生したか、一覧で表示されます。一覧の中の[端末]では電話番号を持たない端末は「端末ID」が表示されます。表示されるアラートの内容は、「異常検知・通報」ポリシーの設定内容に依存します。表示されているアラートのチェックボックスにチェックを入れて選択し、[確認済]をクリックすると、選択したアラートは一覧から消えます*1。[全選択]をクリックすると、表示されているアラートすべてのチェックボックスにチェックが入ります。また、条件指定による絞り込みとCSVファイルでの書出しが可能です。

*1: 表示設定にて「未確認のみ表示」を選択している場合。

■表示設定

[表示設定]をクリックすると、アラート一覧の表示内容を設定することができます。1ページに表示するアラートの数、確認済みのアラートも表示するか否かなどを設定できます。

《一旦、確認済みとしたアラートを、再度、未確認化させる必要がある場合》

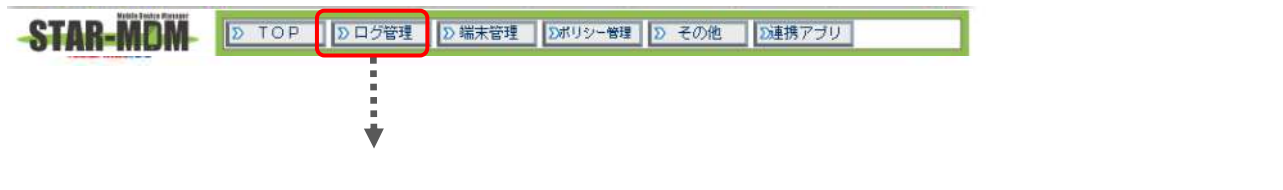
まず、「表示設定」画面の「表示対象ステータス選択」にて、[未確認、確認済み両方表示]を選択し、[適用]をクリックします。次に、アラート一覧にて当該アラートのチェックボックスにチェックを入れて、[未確認]をクリックしてください。これにより、確認済みの状態から、未確認状態に戻ります。

☆ワンポイント: ユーザーに正しい端末利用を促すために

頻繁にアラートが表示される端末については、当該端末の利用者に利用状況を確認し、正しい利用を促すことで情報漏洩リスクを低減してください。アラート一覧に表示される内容については、STAR-MDM管理サーバから管理者宛に通知メールが送信されます。また、「異常検知・通報」ポリシーの設定にて「ユーザー警告メール」にチェックを入れておくことで、問題のあるユーザーへも通知メールを送信することができます。当該端末の利用者情報として端末のメールアドレスと共にPCのメールアドレスも登録されていれば、両方に自動送信されます。通知メールのタイトルや本文も設定可能です。

関連情報 [「異常感知・通報」](#)

メニューバーの[ログ管理]をクリックすると、「ログ管理 - Log 管理」画面が表示されます。



ログ管理 - Log 管理

絞り込み 絞り込み解除 前々日のログ

イベント時刻	電話番号	ログソフト	ログメッセージ	ステータス	受付時間
2015-10-16 16:16:39.088	09000000000	server	Connect From device	INFO	2015-10-16 16:16:39.088
2015-10-16 16:10:23.899	09000000000	sppmda	Pollingでポリシーチェックを実施しました。	INFO	2015-10-16 16:10:24.9
2015-10-16 16:10:23.649	09000000000	server	Connect From device	INFO	2015-10-16 16:10:23.649
2015-10-16 15:37:53.808	09000000000	server	Connect From device	INFO	2015-10-16 15:37:53.808
2015-10-16 15:37:53.474	09000000000	sppmda	Pollingでポリシーチェックを実施しました。	INFO	2015-10-16 15:37:54.474
2015-10-16 15:08:54.473	09000000000	sppmda		INFO	2015-10-16 15:37:54.473
2015-10-16 15:07:56.385	09000000000	server	Connect From device	INFO	2015-10-16 15:07:56.385
2015-10-16 15:07:53.655	09000000000	sppmda	Pollingでポリシーチェックを実施しました。	INFO	2015-10-16 15:07:57.655
2015-10-16 15:02:13.642	09000000000	sppmda		INFO	2015-10-16 15:07:57.642
2015-10-16 15:01:40.641	09000000000	sppmda	認証に成功しました。	INFO	2015-10-16 15:07:57.641
2015-10-16 15:01:31.641	09000000000	sppmda	端末のルート化は検知されませんでした。	INFO	2015-10-16 15:07:57.641
2015-10-16 15:01:31.64	09000000000	sppmda		INFO	2015-10-16 15:07:57.64
2015-10-16 14:58:25.64	09000000000	sppmda		INFO	2015-10-16 15:07:57.64
2015-10-16 14:57:02.639	09000000000	sppmda		INFO	2015-10-16 15:07:57.639
2015-10-16 14:56:13.638	09000000000	sppmda	認証に成功しました。	INFO	2015-10-16 15:07:57.638
2015-10-16 14:55:39.638	09000000000	sppmda	端末のルート化は検知されませんでした。	INFO	2015-10-16 15:07:57.638
2015-10-16 14:55:39.637	09000000000	sppmda		INFO	2015-10-16 15:07:57.637
2015-10-16 14:54:14.636	09000000000	sppmda		INFO	2015-10-16 15:07:57.636
2015-10-16 14:53:35.651	09000000000	server	Connect From device	INFO	2015-10-16 14:53:35.651
2015-10-16 14:53:35.315	09000000000	sppmda	パスワード管理ポリシーを取得し反映しました。	INFO	2015-10-16 14:53:40.315

<<最新へ/newest <前へ/newer 次へ/older> 最後へ/oldest>>

CSV書出し

「ログ管理 - Log管理」画面には、前日分までのログが表示されます。

それより前のログは、「前々日のログ」をクリックし、「絞り込み画面」で日時など検索条件を指定することで、絞り込んで表示することができます。

※[絞り込み]をクリックすることでも同様に「絞り込み画面」が表示されます。

「前々日のログ」で確認できるのは90日前までのログです。

Log管理 - 絞り込み画面

表示対象期間 年 月 日 時 分 - 年 月 日 時 分

絞り込み条件

電話番号

ステータス ☐ ERROR ☐ WARN ☐ INFO

ログメッセージキーワード
※ログメッセージの黒字の部分

ログメッセージキーワード
※ログメッセージの青色の部分

個々のログメッセージについては、管理画面の「各種資料」にあります「Logメッセージ一覧」を参照ください。

※ 管理者にグループ権限が設定されている場合、ログ管理画面に表示されるログは、そのグループに属す端末のもののみになります。

1. 端末一覧画面

「端末一覧画面」では、STAR-MDMに登録されているすべてのモバイル端末を一元的に管理できます。端末情報の確認・編集、ライセンス管理をはじめ、端末の状態確認や端末へのポリシー割り当て、緊急時指示も、この画面から実施します。

メニューバーの「端末管理」をクリックすると、「端末一覧画面」が表示されます。

The screenshot shows the STAR-MDM interface with the following callouts:

- 1. 自動更新 (Automatic Update)
- 2. 端末状態シグナル (Device Status Signal)
- 3. 端末情報編集 (Edit Device Information)
- 4. 緊急時指示 (Emergency Instruction)
- 5. 端末情報 (Device Information)
- 6. 登録表示設定 (Registration Display Settings)
- 7. 一覧表示設定 (List Display Settings)
- 8. 端末並び替え (Sort Devices)
- 9. 端末検索 (Search Devices)
- 10. ポリシー一括設定 (Batch Policy Settings)
- 11. CSV連携 (CSV Integration)

The interface includes a menu bar with 'TOP', 'ログ管理', '端末管理' (highlighted), 'ポリシー管理', 'その他', and '連携アプリ'. Below the menu is the '端末一覧画面' title and a table of devices. The table has columns for '選択' (Select), 'ステータス' (Status), '種別' (Type), '指示' (Instruction), '端末識別番号' (Device ID), '機種' (Model), '端末メールアドレス' (Device Email Address), '端末名称' (Device Name), and 'ライセンスキー' (License Key). A '全選択' (Select All) button is located below the table. A search bar with '検索条件' (Search Conditions) and '追加' (Add) / '削除' (Delete) buttons is also present.

端末一覧の下には、横方向のスクロールバーがあります。個々の端末情報をスクロールして確認できます。各機能の詳細については、それぞれの参照先ページにてご確認ください。

こんなときは (..)φ

■端末一覧の表示内容を変更したい:

項目の選択や順番(列順)を変更するには⇒「[一覧表示設定](#)」

端末の並び順(行順)や行数を変更するには⇒「[端末並び替え](#)」

2. 端末状態シグナル

表示方法 >>> 「端末一覧画面」でステータス欄の最上部の[ステータス]にマウスオーバー

端末を登録すると、「端末一覧画面」のステータスに欄には端末の状態がシグナルで表示されます。これにより、アラートやポリシー反映状況など、現在の端末の状態を把握することができます。

端末状態シグナル

- メッセージ配信シグナル: ▲ Agent非対応 ● ポリシー未設定 ● メッセージ未確認 ● ● メッセージ確認済
- 端末初期化シグナル: ● 平常時 ● 初期化指示発令中 ● 初期化済み
- データ消去シグナル: ● 平常時 ● 消去指示発令中 ● 消去済み
- 端末ロック・シグナル: ● 平常時 ▲ ロック指示発令中 ▼ アンロック指示発令中 ● 端末ロック中
- ポリシー変更シグナル: ● ポリシー反映済み ● ポリシー反映待ち
- アラート・シグナル: ● アラート無 ● アラート有

ステータス欄の最上部にある、[ステータス]の文字列にマウスオーバーすると、シグナルの意味を説明する上記の画面がポップアップします。また、表示中の各シグナルにマウスオーバーすることでも、それぞれの説明が表示されます。

<シグナル一覧>

アラート・シグナル	ポリシー変更シグナル	端末ロック指示・シグナル	データ消去シグナル	端末初期化シグナル	メッセージ配信シグナル
● アラート無	● ポリシー反映済	● 平常時	● 平常時	● 平常時	▲ Agent非対応
● アラート有	● ポリシー反映待	▲ ロック指示発令	● 消去指示発令	● 初期化指示発	● ポリシー未設定
		▼ アンロック指示発令中	● 消去済み	● 初期化済み	● メッセージ未確認
		● 端末ロック指示			■ メッセージ確認済

※Android Enterprise (Comp) 端末では端末一台にWork Managed Device / Work Profile 両方のシグナルが存在しますが、端末一覧ではどちらか片方が平常時外(「アラート有」や「ポリシー反映待ち」)だった場合、平常時外のシグナル状態が優先して表示されます。

3. 端末情報編集

表示方法 >>> 「端末一覧画面」で[編集]をクリック

端末情報の入力・編集やポリシー割り当ての設定を行うことができます。

<端末情報編集画面>

端末管理 - 端末情報編集画面

元に戻す 戻る 上書き保存

【利用者情報】

姓

名

端末メールアドレス

PCメールアドレス

所属 登録情報が1件も登録されていません。

社員ID

連絡先電話番号

【端末情報】

ライセンスキー 00000000-00000000-0000

ソフトウェアID 00000000-00000000-0000

端末ID 00000000-00000000-0000

端末名称 L-010

端末電話番号

【ポリシー情報】

サーバー端末間通信	基本ポリシー	ポリシー編集
緊急時	基本ポリシー	ポリシー編集
異常検知・通報	基本ポリシー	ポリシー編集
ログ管理	<未設定>	ポリシー編集
パスワード管理	基本ポリシー	ポリシー編集
デバイス制御	基本ポリシー	ポリシー編集
電話番号管理	<未設定>	ポリシー編集
位置情報取得	<未設定>	ポリシー編集
アプリ配信	<未設定>	ポリシー編集
利用アプリ制御	<未設定>	ポリシー編集
APK固定化	<未設定>	ポリシー編集
アプリ一覧	<未設定>	ポリシー編集
ファイル配布	<未設定>	ポリシー編集
接続先URL制御	<未設定>	ポリシー編集
電話番号制御	<未設定>	ポリシー編集
WiFi接続先制御	<未設定>	ポリシー編集

元に戻す 戻る 上書き保存

本画面にて編集できる項目は、「登録表示設定」でチェックが入っている項目です。目的の項目が見つからない場合は、「登録表示設定画面」にて項目にチェックが入っているかを確認してください。

関連情報 [「登録表示設定」](#)

■利用者情報

運用スタイルに合わせて必要な情報を入力できます。「端末検索」で端末を絞り込みする際のキーワードとしても有効です。

※端末によっては端末メールアドレスが自動収集されて登録されます。

■端末情報

・ライセンスキー:

ライセンスキーはご契約の端末数に応じて事前に登録されています。

・ソフトID、端末ID、端末名称、端末電話番号:

端末のセットアップ時に自動収集されて登録されます。

■ポリシー情報

基本ポリシー及び作成済みのポリシーをプルダウンメニューから選択できます。

※Android/iOSごとにOS対応ポリシーのみ表示されます。

関連情報➡「[ポリシー管理\(概要\)](#)」

■ポリシー情報(Comp_Work Profile)

Android Enterprise (Comp) 端末のWork Profileへの基本ポリシー及び作成済みのポリシーをプルダウンメニューから選択できます。

※Android Enterprise (Comp) 端末以外では表示されません。

関連情報➡「[ポリシー管理\(概要\)](#)」

☆ワンポイント

Android端末では、「利用者情報」を各端末側で入力してSTAR-MDM管理サーバに登録することもできます。
 ※STAR-MDM管理サーバ上で「利用者情報」が未登録状態の項目に限ります。STAR-MDM管理サーバに登録済みの情報を端末側から上書き更新することはできません。
 ➡「SPPM Agentの操作」>「[端末情報設定](#)」

こんなときは (..)φ

■多数の端末情報を効率的に編集したい:

- ・CSVデータを利用して「端末情報」の一括更新が可能です。➡「[CSV連携](#)」
- ・複数の端末に同一ポリシーの一斉割り当てが可能です。➡「[ポリシー一括設定](#)ポリシー一括設定」

■項目の表示／非表示選択や追加をしたい:

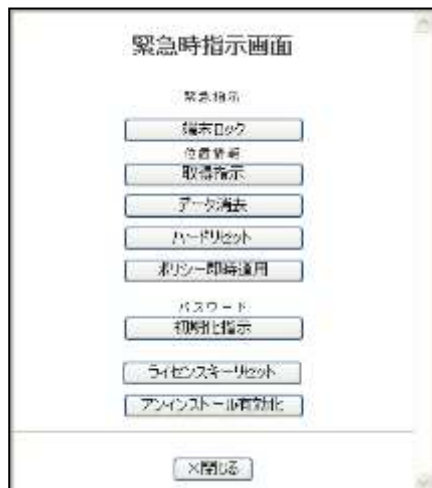
➡「[登録表示設定](#)」

4. 緊急時指示

表示方法 >>> 「端末一覧画面」で[指示]をクリック

端末への緊急指示やライセンスキーリセットを実施することができます。

<緊急時指示画面>



「端末一覧画面」で[指示]をクリックしても、ブラウザの状態によっては本画面が「端末一覧画面」など他の画面の奥に隠れていて表示されないことがあります。その場合は、本画面をアクティブにして手前に表示させてください。

4-1. 端末ロック指示

Android OS 8.0 未満: 端末にSTAR-MDM専用のロック画面を表示させることができます。

Android OS 8.0 以降: 端末の一部を除く全てのアプリを制限することができます。

[端末ロック指示]ボタンの表示の有無は、「緊急時」ポリシーの設定内容に依存します。端末ロック指示の発動条件として「SPPMサーバ指示」にチェックが入っている場合、[端末ロック指示]ボタンが表示されます。

関連情報⇒「[緊急時](#)」

端末ロック指示

端末ロック指示の指示を出すには、[端末ロック指示]ボタンをクリックします。確認画面で[はい]をクリックすると、サーバからのプッシュ通信*1により、即時に端末ロック指示を実施します。

端末ロック指示取消

端末ロック指示の指示を出した直後*2、及び端末へ反映待ち（ロック指示発令中）の間*3は、ボタンが[端末ロック指示取消]になります。端末ロック指示の指示を取り消す場合は、このボタンをクリックし、確認画面で[はい]をクリックします。

端末ロック解除指示

端末ロック指示が実施されている間は、ボタンが[端末ロック指示解除]になります。端末ロック指示を解除するには、このボタンをクリックします。確認画面で[はい]をクリックすると、サーバからのプッシュ通信*1により、即時に端末ロック指示を解除します。

端末ロック解除指示取消

端末ロック指示解除の指示を出した直後*2、及び端末への反映待ち（アンロック指示発令中）の間*3は、ボタンが[ロック解除指示取消]になります。端末ロック指示解除の指示を取り消す場合は、このボタンをクリックし、確認画面で[はい]をクリックします。

*1: Android端末の場合、「サーバ端末間通信」のポリシー設定で、Googleプッシュ（GCM/C2DM/FCM）にチェックが入っている必要があります。

*2: 端末ロック指示解除の指示を出した直後は、端末に指示が反映された場合でも、一旦このボタンになります。

*3: 端末と通信できない状況も含みます。（プッシュサーバの問題、通信状況の問題、端末稼働状況の問題等）

4-2. 位置情報取得指示

端末の位置情報を連続して取得することができます。[取得指示]ボタンは、「位置情報取得」ポリシーが適用されている場合に表示されます。

関連情報➡「[位置情報取得](#)」

位置情報

取得指示

位置情報取得の指示を出すには、[取得指示]ボタンをクリックします。サーバからのプッシュ通信*1により、即時に位置情報の取得を実施します。

※SPPM Agent v2.13以下では、[位置情報取得指示]のクリック後、端末からの定期ポーリング待ちとなります。すぐに位置情報の取得を開始するには、続けて「緊急時指示画面」で[ポリシー即時適用]をクリックしてください。

位置情報

取得指示中

位置情報取得の指示を出した直後*2、及び端末への反映待ちの間*3は、ボタンが[取得指示中]になります。位置情報取得の指示を取り消す場合は、このボタンをクリックします。

位置情報

取得解除指示

位置情報取得が実施されている間は、ボタンが[取得解除指示]になります。位置情報取得を解除するには、このボタンをクリックします。サーバからのプッシュ通信*1により、即時に位置情報取得を解除します。

位置情報

取得解除指示中

位置情報取得解除の指示を出した直後*2、及び端末への反映待ち（ポリシー反映待ち）の間*3は、ボタンが[取得解除指示中]になります。位置情報取得解除の指示を取り消す場合は、このボタンをクリックします。

- *1:「サーバ端末間通信」のポリシー設定で、Googleプッシュ(GCM/C2DM/FCM)にチェックが入っている必要があります。
 *2: 位置情報取得解除の指示を出した直後は、端末に指示が反映された場合でも、一旦このボタンになります。
 *3: 端末と通信できない状況も含みます。(プッシュサーバの問題、通信状況の問題、端末稼働状況の問題等)

◎取得した位置情報を確認するには？

取得した位置情報は、「端末情報画面」の項目にある「位置情報」で確認します。

☞「[端末情報](#)」

4-3. データ消去

端末のデータを消去することができます。[データ消去指示]ボタンの表示の有無は、「緊急時」ポリシーの設定内容に依存します。データ消去の発動条件として「SPPMサーバ指示」にチェックが入っている場合、[データ消去]ボタンが表示されます。

※消去対象データの種類の、「緊急時」ポリシーの設定内容に依存します。

関連情報☞「[緊急時](#)」

データ消去指示

データ消去の指示を出すには、[データ消去]ボタンをクリックします。確認画面で[はい]をクリックすると、サーバからのプッシュ通信*1により、即時にデータ消去を実施します。

データ消去指示取消

データ消去の指示を出した直後*2、及び端末への反映待ち(消去指示発令中)の間*3は、ボタンが[データ消去指示取消]になります。

＜データ消去指示の取り消しが可能な場合＞

このボタンをクリックすると「個人データ消去指示を取り消します。」のメッセージが表示されますので、[はい]をクリックします。

＜データ消去指示の取り消しが不可能な場合＞

このボタンをクリックしても上記のメッセージは表示されません(端末ID、電話番号、ライセンスキーのみが表示されます)。この場合、データ消去は実施されています。[戻る]をクリックしてください。

データ消去済み [リセット](#)

データ消去が実施されると、データ消去済みの表示と併せて、ボタンが[リセット]になります。クリックするとボタンが[データ消去]にリセットされます。

- *1:「サーバ端末間通信」のポリシー設定で、Googleプッシュ(GCM/C2DM/FCM)にチェックが入っている必要があります。
 *2: データ消去指示解除の指示を出した直後は、端末に指示が反映された場合でも、一旦このボタンになります。
 *3: 端末と通信できない状況も含みます。(プッシュサーバの問題、通信状況の問題、端末稼働状況の問題等)

4-4. ハードリセット

端末の初期化と外部メモリのフォーマットを行うことができます。[ハードリセット指示]ボタンの表示の有無は、「緊急時」ポリシーの設定内容に依存します。ハードリセット(端末初期化)の発動条件として「STAR-MDMサーバ指示」にチェックが入っている場合、[ハードリセット]ボタンが表示されます。

関連情報 [「緊急時」](#)

ハードリセット指示

ハードリセットの指示を出すには、[ハードリセット指示]ボタンをクリックします。確認画面で[はい]をクリックすると、サーバからのプッシュ通信*1により、即時にハードリセットを実施します。

ハードリセット指示取消

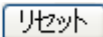
ハードリセットの指示を出した直後*2、及び端末への反映待ち(初期化指示発令中)の間*3は、ボタンが[ハードリセット指示取消]になります。

＜ハードリセット指示の取り消しが可能な場合＞

このボタンをクリックすると「端末にハードリセット指示を取り消します。」のメッセージが表示されますので、[はい]をクリックします。

＜ハードリセット指示の取り消しが不可能な場合＞

このボタンをクリックしても上記のメッセージは表示されません(端末ID、電話番号、ライセンスキーのみが表示されます)。この場合、ハードリセットは実施されています。[戻る]をクリックしてください。

ハードリセット済み 

ハードリセットが実施されると、ハードリセット済みの表示と併せて、ボタンが[リセット]になります。クリックするとボタンが[ハードリセット]に戻ります。

*1: Android端末の場合、「サーバ端末間通信」のポリシー設定で、Googleプッシュ(GCM/C2DM/FCM)にチェックが入っている必要があります。

*2: ハードリセット解除の指示を出した直後は、端末に指示が反映された場合でも、一旦このボタンになります。

*3: 端末と通信できない状況も含みます。(プッシュサーバの問題、通信状況の問題、端末稼働状況の問題等)



Comp端末へのハードリセットについての詳細はAndroid Enterpriseマニュアルをご覧ください。

4-5. ポリシー即時適用

端末に適用待ちのポリシー設定を、サーバからのプッシュ通信で即時に適用することができます。Android端末では、「サーバ端末間通信」のポリシー設定でGoogleプッシュ（GCM/C2DM/FCM）にチェックが入っている場合、[ポリシー即時適用]ボタンが表示されます。

関連情報 [「サーバ端末間通信」](#)

ポリシー即時適用指示

ポリシー即時適用の指示を出すには、[ポリシー即時適用指示]ボタンをクリックします。確認画面で[はい]をクリックすると、サーバからのプッシュ通信*1により、即時にポリシーを適用します。

*1: Android端末の場合、「サーバ端末間通信」のポリシー設定で、Googleプッシュ（GCM/C2DM/FCM）にチェックが入っている必要があります。

4-6. パスワード初期化指示

端末に設定済みのパスワードを、強制的に変更もしくは初期化することができます。[初期化指示]のボタンは標準で表示されます。

-  本機能は、Androidの場合はSPPM Agent v2.04以上で有効です。SPPM Agentがv2.04未満の端末では、緊急時指示画面に[初期化指示]ボタンは表示されませんのでご注意ください。
-  本機能はパスワード管理ポリシーを端末に適用する事が必須となります（フル機能パック）
-  パスワード初期化指示を行った際に「起動時の保護」が有効であった場合、起動時の保護のパスワードは初期化されない場合がありますのでご注意ください。
 ※Android Enterprise・Android OS 8.0以降・Agent v.3.41以降の条件を満たす場合、「起動時の保護」のパスワードは消去されます。なお、一度「起動時の保護」が消去された端末では、以降初期化するまでは「起動時の保護」を端末に設定できなくなります。

パスワード 初期化指示

パスワード初期化の指示を出すには、[初期化指示]ボタンをクリックします。確認画面で[はい]をクリックすると、サーバからのプッシュ通信*1により、即時にパスワードの初期化を実施します。

※Android版SPPM Agent v2.04～v2.13では、[初期化指示]のクリック後、端末からの定期ポーリング待ちとなります。すぐにパスワードの初期化を実施するには、続けて「緊急時指示画面」で[ポリシー即時適用]をクリックしてください。

パスワード指定

※半角英数字4-16桁のみ
※指定なしでは[abcd1234]に変更

パスワード初期化指示により変更されるパスワードを半角英数字4-16桁で指定できます。

指定がない場合の指示では[abcd1234]に変更されます。

また、指示を発令した指定値は端末毎の緊急指示画面に保存されます。

パスワード
初期化指示取消

パスワード初期化の指示を出した直後*2、及び端末への反映待ちの間*3は、ボタンが[初期化指示取消]になります。パスワード初期化の指示を取り消す場合は、このボタンをクリックします。

*1: Android端末では「サーバ端末間通信」のポリシー設定で、Googleプッシュ(GCM/C2DM/FCM)にチェックが入っている必要があります。

*2: パスワード初期化指示解除の指示を出した直後は、端末に指示が反映された場合でも、一旦このボタンになります。

*3: 端末と通信できない状況も含みます。(プッシュサーバの問題、通信状況の問題、端末稼働状況の問題等)

4-7. ライセンスキーリセット

端末とライセンスキーの紐付けを解除することができます。端末が故障し代替機に交換する場合などには、[ライセンスキーリセット]ボタンをクリックすることでライセンスキーが当該の端末から解放され、他の端末に割り当てることができるようになります。[ライセンスキーリセット]ボタンは標準で表示されます。

ライセンスキーリセット

ライセンスキーのリセットを実施するには、[ライセンスキーリセット]ボタンをクリックします。確認画面で[はい]をクリックすると、即時にライセンスキーリセットを実施します。

*1: Android端末の場合、「サーバ端末間通信」のポリシー設定で、Googleプッシュ(GCM/C2DM/FCM)にチェックが入っている必要があります。



Android11以降 かつ Agent v3.58以降の端末の場合、工場出荷状態に初期化されます。



ライセンスキーリセットが実施されると、端末と通信ができない状況でも、STAR-MDM管理サーバ側では当該端末の登録情報を即時に消去します。これにより、STAR-MDM管理サーバから当該端末への制御は一切行えなくなりますので、ご注意ください。

【不要となったAndroid端末の解除手順】

STAR-MDMによる管理が不要になったAndroid端末のSPPM Agentをアンインストールせずに放置しますと、ライセンスキーリセットを行っても、ライセンスキーを他の端末に適用できないなどの悪影響が出る可能性があります。不要になったAndroid端末には、必ず以下の手順を適用してください。

①STAR-MDM管理サーバの「緊急時指示画面」で[アンインストール有効化指示]をクリック

②端末の「設定」メニューからSPPM Agentをアンインストール

③STAR-MDM管理サーバの「緊急時指示画面」で[ライセンスキーリセット]をクリック



ライセンスキーリセット後に再度SPPM Agentをお使いになる場合は、再度端末をセットアップしてください。

☞「[端末のセットアップ](#)」

4-8. アンインストール有効化

端末に対してSPPM Agentのアンインストールを許可します。このボタンは標準で表示されます。

※Android Enterprise端末では「アンインストール有効化指示」ボタンは表示されません。

アンインストール有効化

アンインストール有効化の指示を出すには、[アンインストール有効化指示]ボタンをクリックします。確認画面で[はい]をクリックすると、サーバからのプッシュ通信^{*1}により、即時にアンインストール機能を有効化します。



アンインストールが有効化になった状態でも、利用アプリ制限ポリシーによってSppmHomeが
端末に設定された状態ではAndroid OS 5.0 以上ではSTAR-MDMをアンインストールできません。
利用アプリ制限ポリシーを未設定に変更し、アンインストールを行ってください。

アンインストール機能有効化指示発令中

キャンセル

アンインストール有効化の指示を出した直後^{*2}、及び端末へ反映待ちの間^{*3}は、ボタンが[キャンセル]になります。アンインストール有効化の指示を取り消す場合は、このボタンをクリックし、確認画面で[はい]をクリックします。

SPPM Agent

アンインストール無効化指示

SPPM Agentがアンインストール可能な状態の場合、ボタンが[アンインストール無効化指示]になります。SPPM Agentをアンインストールできないようにするには、このボタンをクリックします。確認画面で[はい]をクリックすると、サーバからのプッシュ通信^{*1}により、即時にアンインストール機能を無効化します。

アンインストール機能無効化指示発令中

キャンセル

アンインストール無効化の指示を出した直後^{*2}、及び端末へ反映待ちの間^{*3}はボタンが[キャンセル]になります。アンインストール無効化の指示を取り消す場合は、このボタンをクリックし、確認画面で[はい]をクリックします。

*1:「サーバ端末間通信」のポリシー設定で、Googleプッシュ(GCM/C2DM/FCM)にチェックが入っている必要があります。

*2:アンインストール無効化の指示を出した直後は、端末に指示が反映された場合でも、一旦このボタンになります。

*3:端末と通信できない状況も含みます。(プッシュサーバの問題、通信状況の問題、端末稼働状況の問題等)

4-9. 端末再起動

端末の再起動を管理画面から指示することができます。端末再起動の発動条件として「SPPMサーバ指示」にチェックが必要です。

なお、本機能は **Android OS 7.0以降**の **Work Managed Device** モード端末にて、Agent **v3.53以降**を利用して
いる場合、利用できます。

利用条件を満たさない端末では「端末再起動指示」ボタンは表示されません。

関連情報➡[「緊急時」](#)

端末再起動指示

端末再起動の指示を出すには、[端末再起動指示]ボタンをクリックします。確認画面で[はい]をクリックすると、サーバからのプッシュ通信*1により、即時に端末再起動を実施します。

※CSVファイルを利用し、複数の端末に一括で再起動指示を実施する事ができます。

関連情報➡[「CSV連携」](#)

端末再起動指示取消

端末再起動の指示を出した直後*2、及び端末への反映待ちの間*3は、ボタンが[端末再起動指示取消]になります。端末再起動の指示を取り消す場合は、このボタンをクリックします。

*1: Android端末では「サーバ端末間通信」のポリシー設定で、Googleプッシュ(GCM/C2DM/FCM)にチェックが入っている必要があります。

*2: 端末再起動指示解除の指示を出した直後は、端末に指示が反映された場合でも、一旦このボタンになります。

*3: 端末と通信できない状況も含みます。(プッシュサーバの問題、通信状況の問題、端末稼働状況の問題等)

《管理アカウント設定》

既に作成済みの管理者アカウントにて端末再起動指示機能を利用するためには、管理者アカウントのグループ権限設定で「端末再起動」の項目をそれぞれ ON にする必要があります。

※管理者アカウントを新規作成する場合、該当の項目はデフォルトで ON に設定されます。

権限を設定されていない管理アカウントでは、緊急時指示画面にて指示ボタンが表示されません。

関連情報➡[「管理者管理」](#)

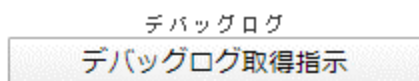
4-10. デバッグログ取得

端末のバグレポートを取得し、STAR-MDMサーバに送信することができます。デバッグログ取得の発動条件として「SPPMサーバ指示」にチェックが必要です。

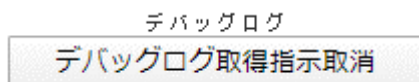
なお、本機能は **Android OS 7.0以降**の **Work Managed Device** モード端末にて、Agent **v3.53以降**を利用して
いる場合、利用できます。

利用条件を満たさない端末では「デバッグログ取得指示」ボタンは表示されません。

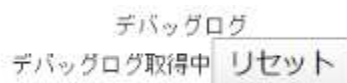
関連情報 [「緊急時」](#)



デバッグログ取得の指示を出すには、[デバッグログ取得指示]ボタンをクリックします。確認画面で[はい]をクリックすると、サーバからのプッシュ通信*1により、即時にデバッグログ取得を実施します。



デバッグログ取得の指示を出した直後*2、及び端末への反映待ちの間*3は、ボタンが[デバッグログ取得指示取消]になります。デバッグログ取得の指示を取り消す場合は、このボタンをクリックします。



デバッグログ取得指示が端末に到達し、端末にてデバッグログが作成中のタイミングでは、デバッグログ取得中の表示と併せて、ボタンが[リセット]になります。クリックするとボタンが[デバッグログ取得指示]に戻ります。

*1: Android端末では「サーバ端末間通信」のポリシー設定で、Googleプッシュ(GCM/C2DM/FCM)にチェックが入っている必要があります。

*2: 端末再起動指示解除の指示を出した直後は、端末に指示が反映された場合でも、一旦このボタンになります。

*3: 端末と通信できない状況も含みます。(プッシュサーバの問題、通信状況の問題、端末稼働状況の問題等)

《管理アカウント設定》

既に作成済みの管理者アカウントにてデバッグログ取得指示機能を利用するためには、管理者アカウントのグループ権限設定で「デバッグログ取得」の項目をそれぞれ ON にする必要があります。

※管理者アカウントを新規作成する場合、該当の項目はデフォルトで ON に設定されます。

権限を設定されていない管理アカウントでは、緊急時指示画面にて指示ボタンが表示されません。

関連情報 [「管理者管理」](#)

5. 端末情報

表示方法 >>> 「端末一覧画面」で[端末電話番号]または[ライセンスキー]をクリック

端末の詳細な情報を網羅的に閲覧することができます。端末情報として、「端末状態シグナル」「個別情報」「ポリシー反映状況」「ファイル配布状況」「接続情報」「認証情報」「通話情報」「位置情報」「インストールアプリ一覧」「変更履歴」を確認できます。

【端末情報画面：端末情報シグナル／個別情報／ポリシー反映状況】 ※表示例

《端末情報画面》

端末管理 - 端末情報画面

[戻る](#)

【端末状態シグナル】				
アラート	ポリシー変更	端末ロック	データ消去	端末初動化
● アラート無	● ポリシー反映待ち	● 正常時	● 正常時	● 正常時

【個別情報】 選択			
端末ID	2013-09-09 00:22:29		
APIレベル	15	OSバージョン	4.0.4
端末電話番号		Agent Ver.	v2.16
姓	山田	名	田中
セイ		メイ	
端末メールアドレス	2013-09-09 00:22:29	PCメールアドレス	
所属			
写真ID			

【ポリシー反映状況】			
ポリシー名		反映状態	処理日時
（サーバー-端末接続）	端末ポリシー	反映済	2013-09-09 00:22:29
（緊急時）	端末ポリシー	反映待ち	2013-09-09 11:06:00
（異常検知・通報）	端末ポリシー	反映済	2013-09-09 12:58:09
（Agent管理）	v2.16	反映待ち	2013-09-09 11:06:00
（パスワード）	端末ポリシー	反映待ち	2013-09-09 11:06:00
（デバイス制御）	端末ポリシー	反映済	2013-09-09 12:58:09
（端末位置登録）	端末位置登録の取得を行う。	反映待ち	2013-09-09 11:07:15
（位置情報取得）	社内標準	反映済	2013-09-09 10:05:22
（アプリ配布）	<未設定>	反映待ち	2013-09-09 11:06:00
（利用アプリ制御）	L-012	反映待ち	2013-09-09 11:07:15
（アプリ一覧）	アプリ一覧	反映済	2013-09-09 17:20:41
（APN固定化）	<未設定>	未設定	---
（ファイル配布）	<未設定>	反映済	2013-09-09 12:58:09
（接続先URL制御）	企業型標準	反映待ち	2013-09-09 11:15:08
（緊急通報制御）	<未設定>	未設定	---
（Wi-Fi接続制御）	<未設定>	未設定	---
（Wi-Fi設定）	<未設定>	反映済	2013-09-09 07:22:29
（端末番号簡略化）	<未設定>	未設定	---
最終ポリシー確認日時			2013-09-09 10:41:20

《Android Enterprise (Comp) 端末の端末情報画面》

Comp端末の場合は画面上部に「Work Managed Device」と「Work Profile」ボタンが表示され、Work Managed DeviceとWork Profileの端末情報画面を切り替えることができます。

※Work Profileの端末情報画面では表示される情報は限られます。

端末管理 - 端末情報画面

戻る

Work Managed Device

Work Profile

【端末状態シグナル】					
アラート	ポリシー変更	端末ロック	データ消去	端末初期化	メッセージ配信
● アラート無	● ポリシー反映済み	▲ 非対応	▲ 非対応	● 平常時	▲ 非対応

【個人情報】 [編集](#)

Work Managed Device 端末情報画面

[illegible]

Work Profile 端末情報画面

[illegible]

■ 端末状態シグナル

「端末一覧画面」のステータス欄に表示されているシグナルと同じものが表示されます。アラートやポリシー反映状況など、現在の端末の状態を把握することができます。

■ 個体情報

以下の情報が表示されます。

- ・端末ID ・APIレベル ・OSバージョン ・端末電話番号 ・Agent Ver. ・姓 ・名 ・端末メールアドレス
・PCメールアドレス ・所属 ・社員ID ・Android Enterprise (Android Enterprise端末のみ表示)

※[編集]をクリックすると「端末情報編集画面」に移動できます。

■ポリシー反映状況

ポリシー管理項目ごとに、割り当てられているポリシー名、反映状態、処理日時が表示されます。

※Android/iOSごとにOS対応ポリシーのみ表示されます。

【端末情報画面：ファイル配布状況／接続情報／認証情報／通話情報】 ※表示例

【ファイル配布状況】			
ファイル名		配布状態	処理日時
FILE-01	手順書.txt	済	2013-09-20 20:10:45
FILE-02	会社ロゴ.png	済	2013-09-20 20:10:45

【接続情報】	
最終接続日時	2013-09-14 16:04:09.27

【認証情報】	
最終認証日時	2013-09-14 16:04:09.01

【通話情報】		
種別	電話番号	発信日時
着信通話	000000000001	2013-09-19 09:48:27
着信通話	000000000001	2013-09-19 09:34:42
着信通話	000000000001	2013-09-17 17:53:03
発信	0000 00000000	2013-09-17 12:57:51
不在着信	0000 00000000	2013-09-17 12:40:38
着信通話	000000000001	2013-09-15 15:43:10
発信	000000000001	2013-09-15 15:41:14

■ファイル配布状況

「ファイル配布」*1のポリシーが適用されている場合、直近の配布ファイルに対して、状態と処理日時が表示されます。

*1: STAR-MDMのご利用形態が基本機能パックの場合、ポリシー管理項目には含まれません。フル機能パックにてご利用いただけます。

関連情報👉「[ファイル配布](#)」

■接続情報

STAR-MDM管理サーバへの直近の接続日時が表示されます。

■認証情報

端末で設定されたパスワードの最終認証日時が表示されます*1。

*1: 端末に「パスワードを義務化する」に設定されたパスワード管理ポリシーが適用されている必要があります。

■通話情報

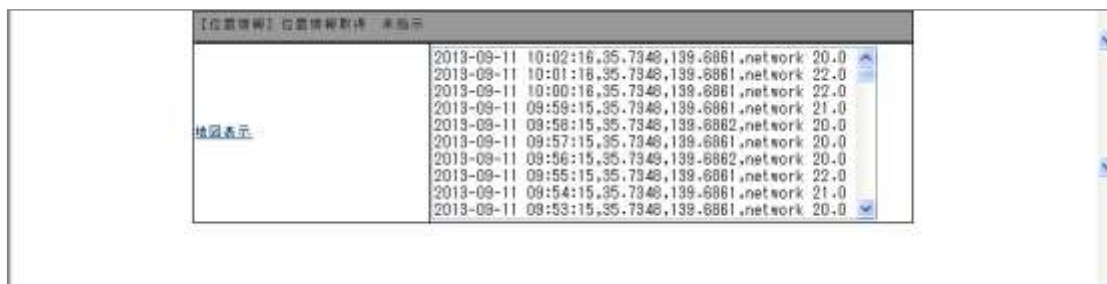
「発着信番号履歴」*1ポリシーで“発着信履歴を取得する”が適用されている場合、通話種別、電話番号、発着信日時が表示されます。

*1: STAR-MDMのご利用形態が基本機能パックの場合、ポリシー管理項目には含まれません。フル機能パックにてご利用いただけます。

※「発着信番号履歴」の取得はSPPM Agent v3.41～v3.43 / v3.59.1.2～では非対応です

関連情報➡「[発着信番号履歴](#)」

【端末情報画面: 位置情報】 ※表示例



【位置情報】位置情報取得結果表示				
2013-09-11	10:02:16.35	73.48	139.6881	network 20.0
2013-09-11	10:01:16.35	73.48	139.6881	network 22.0
2013-09-11	10:00:16.35	73.48	139.6881	network 22.0
2013-09-11	09:59:15.35	73.48	139.6881	network 21.0
2013-09-11	09:58:15.35	73.48	139.6882	network 20.0
2013-09-11	09:57:15.35	73.48	139.6881	network 20.0
2013-09-11	09:56:15.35	73.48	139.6882	network 20.0
2013-09-11	09:55:15.35	73.48	139.6881	network 22.0
2013-09-11	09:54:15.35	73.48	139.6881	network 21.0
2013-09-11	09:53:15.35	73.48	139.6881	network 20.0

■位置情報

「位置情報取得」*1ポリシーが適用されている場合、日時、緯度、経度などの位置情報取得結果がデータで表示されます。このデータを用いて、位置情報取得開始から終了までの端末の位置を地図上に表示することができます。「位置情報」の表示件数は上限100件です。

また、過去90日間の取得位置情報をCSVファイルでの書出しができます。

*1: STAR-MDMのご利用形態が基本機能パックの場合、ポリシー管理項目には含まれません。フル機能パックにてご利用いただけます。

関連情報➡「[位置情報取得](#)」

■位置情報データについて

緯度 精度(プロバイダ)
 2013-11-14 12:51:37, 35.6587, 139.7076, gps 35.599
 取得日時 経度 精度(半径)

○取得日時

該当位置情報の取得日時

○緯度・経度

実際の緯度経度情報

○精度 (プロバイダ)

位置情報取得した時の取得方法

GPS : GPS で取得

network : ネットワークデータで取得

fused : GPS もしくはネットワークデータで取得

bs : ドコモ基地局による取得*1

ERROR : 位置情報の取得に失敗

*1 : ドコモ基地局による位置情報取得はドコモ端末、事前に SP モードによる位置情報設定などが必要です。

☞「[ドコモ基地局による位置情報取得](#)」

○位置情報の精度 (単位/メートル)

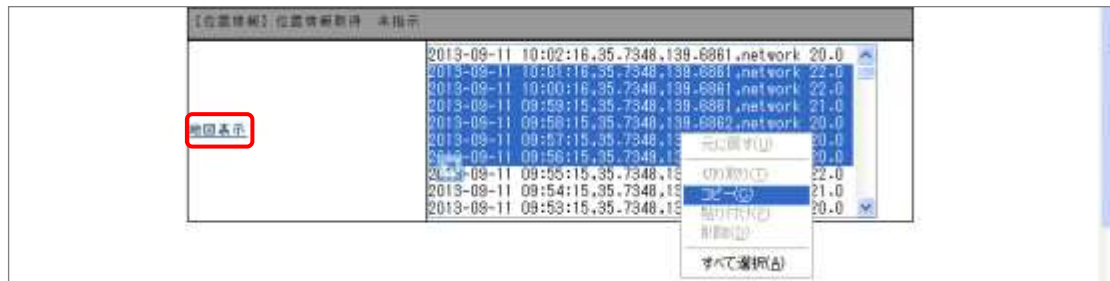
緯度・経度を中心として、おおよそ数字を半径とする円が位置情報のズレの範囲となります。値が小さいほど、位置情報の確度が高くなります。

※0.0の場合は位置情報取得に失敗しています。(ドコモ基地局による位置情報は、必ず0.0になります)

<位置情報取得結果の地図表示手順>

①表示させたい位置情報のデータをマウスのドラッグ等で範囲指定してコピーします。続けて、[地図表示]をクリックしてください。

※経度以降の文字列も一緒にコピーして構いません。貼り付け時に自動的に無視されます。



- ②Google Mapが別ウィンドウで開きます。地図の左下にある入力エリアに、①でコピーした位置情報を貼り付け、[表示]をクリックしてください。



- ③ 位置情報が地図上に表示されます。「START」の旗、「END」の旗、及びその間の青丸が、取得された位置情報です。それぞれをクリックすると、日時等を確認することができます。



◎位置情報の取得を開始するには？

位置情報の取得を開始するには、「緊急時指示画面」で[位置情報取得指示]をクリックします。

※SPPM Agent v2.14以上では、[位置情報取得指示]のクリックと同時にGoogleプッシュによるサーバ指示が発動します*1。

*1: Googleプッシュ(GCM/C2DM/FCM)の設定にチェックが入っている必要があります。

※SPPM Agent v2.13以下では、[位置情報取得指示]のクリック後、端末からの定期ポーリング待ちとなります。すぐに位置情報の取得を開始するには、続けて「緊急時指示画面」で[ポリシー即時適用指示]をクリックしてください。

☞「緊急時指示」>「[位置情報取得指示](#)」

【端末情報画面：インストールアプリ一覧】 ※表示例

インストールアプリ一覧		利用アプリ制限設定作成		リスト取得日: 2015-04-19 10:14:42
アプリ名	バージョン	パッケージ名	更新日時	
(ウィジェット)Content: Headline	2.01	jp.co.nttdocom.contentheadline		
(ウィジェット)Gmail	3.0.5	com.google.android.gm		
(ウィジェット)Google Playストア	4.2.11	com.android.vending		
(ウィジェット)Google+ プッシュジェー	2.0.0.10606255	com.google.android.apps.plus		
(ウィジェット)Google検索	1.4.1.538851	com.google.android.googlequicksearch		
(ウィジェット)World Clock widget	0.4.5	com.ige.sizeshangbia.worldclock		
(ウィジェット)YouTube	2.5.5	com.google.android.youtube		
(ウィジェット)チャンネル	200.0	jp.co.nttdocom.ichannel		
(ウィジェット)カレンダーウィジェット	0.1.0	com.ige.sizeshangbia.calendar		
(ウィジェット)スケジュール&メモ	02.040.0617	com.nttdocom.android.schedulmemo		

■インストールアプリ一覧

「アプリ一覧」*1ポリシーで“アプリ一覧を取得する”が適用されている場合、端末にインストールされているアプリを一覧表示します。

また、「アプリ一覧」*1ポリシーが適用されている場合には、[アプリ制限ポリシーを作成]ボタンが表示されます。

[アプリ制限ポリシーを作成](#)

このボタンをクリックすることで当該の端末を参照端末とした「利用アプリ制限」のポリシー作成を行うことができます。

*1: STAR-MDMのご利用形態が基本機能パックの場合、ポリシー管理項目には含まれません。フル機能パックにてご利用いただけます。

関連情報☞「[アプリ一覧](#)」

関連情報☞「[利用アプリ制限](#)」

【端末情報画面: 変更履歴】 ※表示例

【変更履歴】 変更履歴			
状態	アプリ名	パッケージ名	記録日時
変更	Google設定	com.google.android.gm	2013-09-19 10:14:
削除	SpeedZone	jp.co.knspeed.sppm_setup	2013-09-19 10:14:
追加	SpeedZone	jp.co.knspeed.browsers	2013-09-19 12:59:
追加	ダウンロード	jp.co.knspeed.browsers	2013-09-19 12:59:
削除	イベントプラス	jp.gr.java_conf.matchama.EventPlus	2013-09-19 08:53:
削除	(ウィジェット)イベントプラス	jp.gr.java_conf.matchama.EventPlus	2013-09-19 08:53:
追加	イベントプラス	jp.gr.java_conf.matchama.EventPlus	2013-09-19 08:53:
追加	(ウィジェット)イベントプラス	jp.gr.java_conf.matchama.EventPlus	2013-09-19 08:53:
追加	SpeedZone	jp.co.knspeed.sppm_setup	2013-09-19 08:53:
削除	SpeedZone	jp.co.knspeed.sppm_setup	2013-09-11 12:28:
削除	SpeedZone	jp.co.knspeed.sppm_setup	2013-09-09 17:01:

■変更履歴

前項インストールアプリ一覧にあるアプリに関する、追加、変更、削除の記録を日時と共に表示します。

※「アプリ一覧」*1ポリシーで“アプリ一覧を取得する”が適用された以降のデータになります。

*1: STAR-MDMのご利用形態が基本機能パックの場合、ポリシー管理項目には含まれません。フル機能パックにてご利用いただけます。

【端末情報画面: 端末詳細情報(インベントリ情報)】

【端末詳細情報】		リスト取得日: 2013-12-11 10:39:57
コード	状態	
ビルド番号	KRT16M	
ブランド名	google	
バッテリー状態	フル充電	
バッテリーの健康状態	良い	
バッテリー残量	95 [%]	
バッテリー最大量	100 [%]	
バッテリー接続	0	
バッテリー電圧	4205 [mV]	
バッテリー温度	24 [度]	
バッテリー原理	Li-ion	
バッテリー	"..."	

■端末詳細情報 表示例

バッテリーをはじめとした端末の各種情報を取得し端末詳細画面に表示いたします*1。

*1: 取得できる端末情報(インベントリ)情報は機種・OS に依存致します。

《端末詳細情報の取得タイミングと条件》

※v3.51 以降の SPPM Agent を利用している場合、端末詳細情報はサーバ端末間通信時に更新されます。
(定期通信 / 即時適用時 等)

※v3.51以降にもかかわらず更新されない場合は、ポリシー(アプリ配信 / Agent管理以外)を変更するか適用し直しをしてください。

■取得情報サンプル

Android 取得項目			
CPU-ABI	シリアル番号	OS 識別子	ビルドタイプ
ブランド名	ブートローダーバージョン	ビルド時間	CPU-ABI2
ビルドのタグ名	ビルド ID	ホスト名	OS 製造者
デバイス名	ハードウェア名	製品名	OS ユーザー
モデル名	バッテリー状態	バッテリー残量	バッテリーの健康状態
バッテリー最大量	バッテリー接続	バッテリー電圧	バッテリー温度
バッテリー原理	SSID	BSSID	Wi-Fi 利用時のプライベート IP アドレス
接続速度	ネットワーク ID	使用可能なメモリ容量	低メモリしきい値
低メモリ状態	キャリア名称	現在起動しているアプリ	タスクのアクティビティ数
稼働中のアクティビティ数	トップのアプリ	現在起動しているアプリ	マナーモード設定
有効な位置情報機能	ストレージ暗号化状態	呼び出し音量	通知音量
アラーム音量	音楽再生音量	システム音量	CPU 使用率

《端末詳細画面のCSV出力について》

端末詳細情報の一部項目は、CSVにて出力することができます。

関連情報  [「CSV連携」](#)

■メッセージ配信履歴

過去に配信したメッセージの履歴が 20 件まで表示されます*。

履歴にはメッセージの配信日時・設定やメッセージ内容、メッセージの確認状況などが表示されます。

詳細表示をクリックするとWindowにメッセージの詳細が表示されます

【メッセージ配信履歴】					
詳細表示	ポリシー名	メッセージ	配信日時	確認日時	状態
詳細表示	業務連絡	営業部の皆様、資料を更新しま	2014-09-08 17:21:13.73	2014-09-08 17:21:22.741	確認済
詳細表示	業務連絡	営業部の皆様、資料を更新しま	2014-09-08 17:20:42.8	2014-09-08 17:21:00.41	確認済
詳細表示	業務連絡	営業部の皆様、資料を更新しま	2014-09-08 10:44:35.845	2014-09-08 10:44:55.738	未確認

戻る



6. 登録表示設定

表示方法 >>> 「端末一覧画面」で「登録表示設定」をクリック

「端末情報編集画面」に表示する項目を設定することができます。表示する項目にはチェックを入れ、非表示にする項目からはチェックを外します。

※新機能(ポリシー)追加時は自動でチェックされませんので、手動でチェックを入れて下さい。

<登録表示設定画面>

登録表示設定画面			
元に戻す 戻る 適用			
【利用者情報】		全選択 全解除	
☒ 姓	☒ 名	☒ セイ	☒ メイ
☒ 姓(英語)	☒ 名(英語)	☒ PCメールアドレス	☒ 所属
☒ 社員ID	☒ 連絡先電話番号1		
☒ 連絡先電話番号2			
【端末情報】		全選択 全解除	
☒ ライセンスキー	☒ ソフトID	☒ 端末ID	☒ 端末名称
☒ 端末電話番号	☒ 端末メールアドレス		
【ポリシー情報】		全選択 全解除	
☒ サー/端末間通信	☒ 緊急時	☒ 異常検知・通報	☒ Agent管理
☒ パスワード管理	☒ デバイス制御	☒ 宛着信番号履歴	☒ 位置情報取得
☒ アプリ配信	☒ アプリ一覧	☒ ファイル配布	☒ 宛着信番号制限
☒ SIM監視	☒ 接続先URL制限	☒ 端末暗号義務化	☒ Wi-Fi接続先制限
☒ 構成プロファイル制限(iOS)	☒ 利用アプリ制限	☒ APN固定化	☒ 構成プロファイル配信(iOS)
☒ 利用アプリ検知(iOS)	☒ Wi-Fi設定	☒ アプリ管理(iOS)	☒ DEP設定(iOS)
☒ メッセージ配信	☒ Knox管理	☒ 電話帳配信	☒ 利用統計
☒ VPP管理配布(iOS9)	☒ アプリアンインストール制限	☒ 動態管理	
☒ キオスク管理			
【ポリシー情報(Comp_WorkProfile)】		全選択 全解除	
☒ 緊急時	☒ デバイス制御		
【自由項目】		全選択 全解除	
☒ じゆうこうもく	☐ 自由枠2	☐ 自由枠3	☐ 自由枠4
☐ 自由枠5	☐ 自由枠6	☐ 自由枠7	☐ 自由枠8
☐ 自由枠9	☐ 自由枠10	☐ 自由枠11	☐ 自由枠12
☐ 自由枠13	☐ 自由枠14	☐ 自由枠15	☐ 自由枠16
☐ 自由枠17	☐ 自由枠18	☐ 自由枠19	☐ 自由枠20
☐ 自由枠21	☐ 自由枠22	☐ 自由枠23	☐ 自由枠24
☐ 自由枠25	☐ 自由枠26	☐ 自由枠27	☐ 自由枠28
☐ 自由枠29	☐ 自由枠30		
元に戻す 戻る 適用			

7. 一覧表示設定

表示方法 >>> 「端末一覧画面」で「一覧表示設定」をクリック

端末一覧に表示する項目の設定を行うことができます。項目ごとに、端末一覧に表示する順番(列順)を数字入力で指定します(端末一覧で非表示にする場合は、「空白」または「0」を入力します)。また、1ページあたりの表示件数(行数)、自由項目の項目名も設定することができます。

<一覧表示設定画面>

端末一覧表示設定画面

※項目の値を、0または空にすることで非表示にすることができます。

【1件表示件数】

【利用情報】

2 姓 名

3 姓(英語) 名(英語)

4 会社ID 連絡先電話番号1

5 連絡先電話番号2

【端末情報】

6 ライセンスキー

7 ソフトID

8 端末ID

9 端末名称

10 端末電話番号

11 端末メールアドレス

12 Agent Ver.

13 API レベル

14 OS バージョン

15 WiFi Macアドレス

16 IMEI

17 PC名

18 シリアル番号

19 製造バージョン

20 初期設定ステータス

21 ビルド番号

22 Enterprise ID

23 Bluetoothアドレス

24 UUID

25 最終接続日時

26 Android Enterprise

27 Agent最終接続日時

28 Agent最終接続日時

29 バッテリー残量

30 バッテリー最大量

31 バッテリー接続

32 バッテリー温度

33 SSID

34 Wi-Fi利用時のプライベートIPアドレス

35 使用可能なメモリ容量

36 低メモリしきい値

37 低メモリ状態

【ポリシー情報】

38 サーマロゲングレージ

39 緊急時

40 異常検知・通知

41 Agent管理

42 パスワード管理

43 デバイス制御

44 異常は番号履歴

45 位置情報取得

46 アプリ配信

47 アプリ一覧

48 ファイル配布

49 異常は番号制限

50 SD監視

51 電話帳配信

52 接続拒否制限

53 端末番号露出

54 構成プロファイル制限(100)

55 利用アプリ制限

56 APK固定化

57 Wi-Fi接続先制限

58 利用アプリ制限(100)

59 Wi-Fi 設定

60 アプリ管理(100)

61 構成プロファイル配信(100)

62 オペレーティング

63 低メモリ

64 DEP固定(100)

65 APP管理配布(100)

66 アプリアンインストール制限

67 APP管理

68 利用拒否

69 キオスク管理

【ポリシー情報(Cong. Work Prof. Info)】

70 製造時

71 APIバージョン

【自由項目】

8. 端末並び替え

表示方法 >>> 「端末一覧画面」で[データ並替]をクリック

端末一覧に表示する端末の順番(行順)を設定することができます。

端末ごとに行順を数字入力で指定します。

※端末登録前のレコード(ライセンスキーのみの行)も設定対象となります。

<端末並び替え操作画面>

端末管理 - 端末並び替え操作画面

順番は少数指定も可能です。[確定]ボタンを押すと結果が反映されます。

確定 一覧へ

順番	端末電話番号	姓	端末メールアドレス	端末名称	ライセンスキー	ソフトウェア	
1	03-XXXX-XXXX	鈴木	03-XXXX-XXXX@xxx.co.jp	エーエス	XXXXXXXXXXXXXXXXXXXX	XXXXXXXXXXXXXXXXXXXX	
2	03-XXXX-XXXX	高橋	03-XXXX-XXXX@xxx.co.jp	エーエス	XXXXXXXXXXXXXXXXXXXX	XXXXXXXXXXXXXXXXXXXX	
3					XXXXXXXXXXXXXXXXXXXX		
4					XXXXXXXXXXXXXXXXXXXX		
5					XXXXXXXXXXXXXXXXXXXX		

1 移動

9. 端末検索

表示方法 >>> 「端末一覧画面」で「検索条件:追加」をクリック

端末一覧に表示する端末の絞り込み検索を行うことができます。

※[解除]をクリックで絞り込み条件を解除します。

※「端末登録中ライセンス検索」はiOSのみに対応している検索ツールです。

※「空きライセンス検索」は端末が登録されていないライセンスを絞り込み検索できます。

※フリー検索からAndroid Enterprise端末を絞り込み検索できます。

<端末検索画面>

端末管理 - 端末検索画面

元に戻す

戻る

絞り込み

※検索項目は一覧表示設定に進じます。

フリー検索

端末ID

姓

所属

ライセンスキー

ソフトID

端末名称

端末電話番号

WiFi Macアドレス

元に戻す

戻る

絞り込み

端末登録中ライセンス検索

※「端末登録中」「詳細情報待ち」とステータスに表示されたiOS端末の登録処理中ライセンスを検索します。

空きライセンス検索

※端末が登録されていないライセンスを検索します。

10. ポリシー一括設定

表示方法 >>> 「端末一覧画面」で「選択済:ポリシー適用」をクリック

選択状態にある複数の端末に対して、同一のポリシーを一斉に割り当てることができます。例えば、選択した端末群に対して、「アプリ配信」ポリシーのみを統一、あるいは「パスワード管理」ポリシーの統一と「デバイス制御」ポリシーの統一をそれぞれ同時に一括して行うということが可能です。

<「ポリシー 一括設定画面」>

端末管理 - ポリシー一括設定画面

サービスのインストール	<変更しない>	▼	ポリシー編集
電源 切	<変更しない>	▼	ポリシー編集
背景画像・通知	<変更しない>	▼	ポリシー編集
Agent管理 (Host - red)	<変更しない>	▼	ポリシー編集
Agent管理 (Windows)	<変更しない>	▼	ポリシー編集
パスワード管理	<変更しない>	▼	ポリシー編集
デバイス制御	<変更しない>	▼	ポリシー編集
無通信番号制限	<変更しない>	▼	ポリシー編集
無通信番号制限	<変更しない>	▼	ポリシー編集
位置情報取得	<変更しない>	▼	ポリシー編集
アプリ制御	<変更しない>	▼	ポリシー編集
利用アプリ制御 (Android)	<変更しない>	▼	ポリシー編集
利用アプリ制御 (Windows)	<変更しない>	▼	ポリシー編集
アプリ一覧	<変更しない>	▼	ポリシー編集
#000000	<変更しない>	▼	ポリシー編集
Wi-Fi (接続先制御)	<変更しない>	▼	ポリシー編集
Wi-Fi 設定	<変更しない>	▼	ポリシー編集
接続先Wi-Fi制御	<変更しない>	▼	ポリシー編集
端末番号の表示	<変更しない>	▼	ポリシー編集
Bluetooth 設定	<変更しない>	▼	ポリシー編集
アプリ管理 (iOS)	<変更しない>	▼	ポリシー編集
権限プロファイル (設定) (iOS)	<変更しない>	▼	ポリシー編集
iOS 権限	<変更しない>	▼	ポリシー編集
メッセージ管理	<変更しない>	▼	ポリシー編集
権限プロファイル (権限) (iOS)	<変更しない>	▼	ポリシー編集
iOS 権限	<変更しない>	▼	ポリシー編集
利用アプリ制御 (iOS)	<変更しない>	▼	ポリシー編集
通知許可	<変更しない>	▼	ポリシー編集
通知許可 (iOS)	<変更しない>	▼	ポリシー編集
通知許可 (Android)	<変更しない>	▼	ポリシー編集
アプリインストール制御	<変更しない>	▼	ポリシー編集
通知管理	<変更しない>	▼	ポリシー編集
利用アプリ	<変更しない>	▼	ポリシー編集

Windows Enterprise (Long-Run Only)

電源 切	<変更しない>	▼	ポリシー編集
デバイス制御	<変更しない>	▼	ポリシー編集

【番号登録なし】
【番号登録なし】

(1) 右の画面にポリシーの適用を行ってもよろしいですか?

はい いいえ

＜端末検索との併用例＞

端末情報として部署名を登録している場合を例にします。同じ部署の端末に共通のポリシーを適用するために、部署名をキーワードに端末を絞り込み検索し、抽出された端末群に対して特定のポリシーを一括して割り当てます。以下は操作手順です。

- ①「端末一覧画面」で[検索条件:追加]をクリックします。
- ②「端末検索画面」が表示されますので、部署名をキーワードとして入力し、[絞り込み]をクリックします。
- ③「端末一覧画面」には当該部署の端末のみが絞り込み抽出されて表示されます。
[全選択]をクリックすることで、参照中の1ページに表示されている端末のみをすべて選択することができます*1。絞り込み抽出後の端末一覧が複数ページに渡る場合には、[(検索結果)全選択]にチェックを入れることで、絞り込み抽出されたすべての端末を選択できます*2。
- ④[ポリシー適用]をクリックすると、「ポリシー一括設定画面」が表示されます。画面下部には、選択済み端末の簡易情報が表示されますので、間違いが無いかを確認します。
問題がなければ、各種ポリシー管理項目のプルダウンメニューからポリシーを選択します。(変更をしないポリシー管理項目については、＜変更しない＞を選択したままにしておきます)
- ⑤設定が完了したら、最後に[はい]をクリックします。選択済み端末へのポリシーの割り当てが完了します。

*1: 選択可能なのは参照中の1ページにある端末のみです。現在参照中ではない他のページのチェックボックスは選択されません。

*2: [(検索結果)全選択]にチェックを入れると、端末ごとのチェックボックスにチェックが入ってなくても(あるいはチェックが入っていた場合にチェックを外しても)、「端末一覧に表示中のすべての端末」が選択されているものとして処理されます。ご注意ください。

関連情報⇒「[その他](#)」

11. CSV連携

表示方法 >>> 「端末一覧画面」で[CSV連携]をクリック

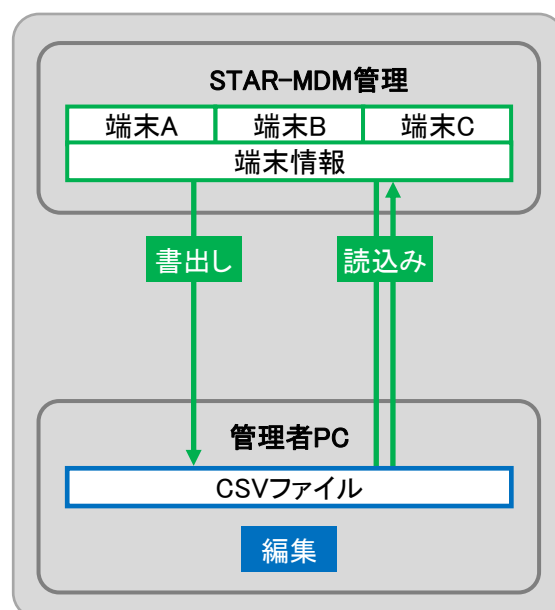
「端末情報」をCSVファイルで書き出すことができます。また、管理者のPCで編集したCSVファイルを読み込むことで、「端末情報」を一括して更新できます。

※「端末情報」の更新では、ポリシーの割り当ては変更できません。一括更新を実行後も、ポリシーの割り当ては既存のままの状態となります。

<CSV操作画面>

<操作手順>

- ①[CSV書き出し]をクリックすると、ダイアログが表示されますので、CSVファイルを管理者のPC上に保存してください。
- ②保存されたCSVファイルを管理者のPC上で編集して保存します。
- ③[参照]をクリックして、編集後のCSVファイルを指定し、[更新方法]を選択のうえ、[一括更新]をクリックしてください。CSVデータに問題がなければ、STAR-MDM管理サーバのデータが更新され、端末情報に反映されます。
※編集後のCSVデータに問題がある場合、更新は実行されず、エラーが発生した行の内容が表示されます。CSVデータを修正の上、再度[一括更新]をクリックしてください。



《CSV更新方法について》

■すべての端末情報を更新

全ての端末情報の更新や、端末一覧の並び順をアップロードしたCSVの並び順に更新できます。

■アップロードしたファイル内の端末のみ更新

アップロードした端末情報のみ更新できます。管理画面に表示される端末の並び順は変更されません。



CSVファイルで一部の端末のみをデータ内に残して更新する場合は「アップロードしたファイル内の端末のみ更新」を選択して、アップロードをしてください。

《CSVデータの見出し語とフォーマットについて》

■[CSV書出し]で保存したCSVファイルの1行目のデータは、項目を表す見出し語です。見出し語の種類は以下の通りです。

姓	名	セイ	メイ
姓(英語)	名(英語)	端末メールアドレス	PCメールアドレス
所属	社員ID	連絡先電話番号1	連絡先電話番号2
ライセンスキー	ソフトID	端末ID	端末名称
端末電話番号	API レベル	OS バージョン	Agent Ver.
サーバ端末間通信	緊急時	異常検知・通報	Agent管理
パスワード管理	デバイス制御	発着信番号履歴	発着信番号制限
位置情報取得	アプリ配信	利用アプリ制限	アプリ一覧
APN固定化	Wifi接続先制限	接続先URL制限	データ暗号化ファイル配布
WiFi Macアドレス	IMEI	ビルド番号	PC名
シリアル番号	Exchange ID	UDID	BlueToothアドレス
最終接続日時	Agent最終接続日時	MDM最終接続日時	Android Enterprise
バッテリー状態	バッテリーの健康状態	バッテリー残量	バッテリー最大量
バッテリー接続	バッテリー温度	SSID	Wi-Fi利用時のプライベートIPアドレス
使用可能なメモリ容量	低メモリしきい値	低メモリ状態	監視対象端末
自由枠1	自由枠2	自由枠3	自由枠4
自由枠5	自由枠6	自由枠7	自由枠8
自由枠9	自由枠10	自由枠11	自由枠12
自由枠13	自由枠14	自由枠15	自由枠16
自由枠17	自由枠18	自由枠19	自由枠20
自由枠21	自由枠22	自由枠23	自由枠24
自由枠25	自由枠26	自由枠27	自由枠29
自由枠29	自由枠30		

※見出し語が間違っているとエラーになり、一括更新は実行されません。カタカナや数字、英字の全角／半角違いなども許容されません。「CSV操作画面」からCSVファイルを書き出すことで、正確な見出し語を得てください。



「CSV書出し」で保存したCSVファイルの1行目は、データを書き込む際の見出し行となっていますので、変更しないようご注意ください。



「シリアル番号」の欄に表示される情報は下記の通りです。

iOS: 端末ID Android、Windows: シリアル番号

■「CSV連携」でSTAR-MDM管理サーバに読み込むCSVファイルは、「CSV操作画面」で書き出したCSVファイルをベースに編集を行なってください。また、見出し語の順序と値の順序は正確に対応付けしてください。

書き出したCSVファイルのライセンスキー、ソフトID、端末ID、電話番号の項目は、Microsoft Excel等で読み込んだ際に数値として認識されないよう、先頭に“#”が付いています。



・ライセンスキー、ソフトID、端末ID、端末名称のデータ欄(列)は、絶対に編集しないでください。データを更新する際のキー情報となっております。これらの情報に変更があると正しく更新が行われません。

・見出し語の順序と値の順序の対応付けが不正確な場合、一括更新が実行できたとしても、誤った端末情報に更新されることになり、正常な管理ができませんのでご注意ください。

■「CSV連携」による「端末情報」の更新では、ポリシーの割り当ては変更できません。一括更新を実行後も、ポリシーの割り当ては既存のままの状態となります。

《インストールアプリ一覧CSVファイル出力について》

インストールアプリ一覧CSVファイル出力
CSV書出し

CSV書出しをクリックすると、クリック時点での各端末にインストールされているアプリ情報をCSVファイルで書き出せます*1

書き出される情報は、「電話番号」「端末ID」「アプリ名」「バージョン」「ビルド番号」「パッケージ名」「更新日時」です。

※電話番号の頭には#が表示されます。

※電話番号の登録がない場合は空欄になります。

*1:本機能では事前に「アプリ一覧」ポリシーを端末に適用し、アプリ情報の取得が必要です。

《iOSアプリ管理ポリシー配信結果CSV出力》

iOSアプリ管理ポリシー配信結果CSV出力
CSV書出し

CSV書出しをクリックすると、クリックした時点のiOS端末のアプリ管理ポリシーの配信結果をCSVファイルで書き出せます。

書き出される情報は「電話番号」「端末ID」「ポリシー名」「アプリ名」「配信ステータス」「インストールステータス」「更新日時」です。

※電話番号の頭には#が表示されます。

※電話番号の登録がない場合は空欄になります。

《VPPライセンス付与・回収結果CSV出力》

VPPライセンス付与・回収結果CSV出力
CSV書出し

CSV書出しをクリックすると、クリックした時点のVPPライセンス付与・回収結果をCSVファイルで書き出せます。書き出される情報は「電話番号」「端末ID」「Store ID」「アプリ名」「ライセンス処理内容」「結果」「失敗原因」「実施日」です。

※電話番号、端末ID、Store IDの頭には#が表示されます。

※電話番号の登録がない場合は空欄になります。

※付与・回収が正常に行われた場合、失敗原因は空欄になります。

《証明書配布状況CSV出力》

証明書配布状況CSV出力
CSV書出し

CSV書出しをクリックすると、クリックした時点の証明書配布状況をCSVファイルで書き出せます。

書き出される情報は「電話番号」「端末ID」「証明書名」「エイリアス」「配布状況」「証明書種別」「Wi-Fi設定」「利用アプリのパッケージ名」「更新日時」です。

《構成プロファイルインストール状況CSV出力》

構成プロファイルインストール状況CSV出力
CSV書出し

CSV書出しをクリックすると、クリックした時点の構成プロファイルインストール状況をCSVファイルで書き出せます。

書き出される情報は「電話番号」「端末ID」「構成プロファイル名」「構成プロファイル識別子」です。

※電話番号と端末IDの頭には#が表示されます。

※電話番号の登録がない場合は空欄になります。

《一括端末再起動指示CSV読み込みについて》

一括端末再起動指示CSV読み込み

<端末再起動指示用CSVダウンロード>

登録用フォーマット

端末再起動指示用フォーマットがCSVでダウンロードされます。

<端末再起動指示用ファイル選択>

※Agent v3.53以降のWork Managed Deviceのみ有効です。

※再起動は指示後のサーバ通信時（定期通信等）に実行されます。

ファイルを選択

選択されていません

一括再起動指示

「登録用フォーマット」をクリックすると、端末再起動指示用のCSVファイルがダウンロードされるのでPCに保存してください。保存したCSVファイルに「端末ID」を入力し、再度保存します。

「ファイルを選択」をクリックして、編集後のCSVファイルを指定し、「一括再起動指示」をクリックしてください。

CSVデータに問題が無ければ、指定した端末に対し再起動の指示が実施されます。（サーバ通信時）

※編集後のCSVデータに問題がある場合、指示は実施されず、エラー内容が表示されます。

12. その他

自動更新

[ON]にしておくことで、1分ごとに端末一覧がリフレッシュされます。

※クリックで[ON]／[OFF]が切り替わります。

全選択

端末一覧で参照中の1ページのみを対象に、すべてのチェックボックスにチェックを入れることができます。現在参照中ではない他のページのチェックボックスは選択されません。

※クリックで[全選択]／[全解除]が切り替わります。

※端末登録前のレコード(ライセンスキーのみの行)も対象となります。

(検索結果)全選択

チェックボックスへのチェックの有無に関わらず、端末一覧に表示中のすべての端末を選択することができます。現在参照中ではない他のページの端末もすべて選択されます。

※端末登録前のレコード(ライセンスキーのみの行)も対象となります。



- ・[(検索結果)全選択]でのチェックと端末ごとのチェックボックスは連動しません。
- ・[(検索結果)全選択]にチェックを入れると、端末ごとのチェックボックスにチェックが入っていても(あるいはチェックが入っていた場合にチェックを外しても)、「端末一覧に表示中のすべての端末」が選択されているものとして処理されます。充分にご注意ください。
- ・「端末検索」を行った場合は、検索結果として端末一覧に残った端末のみがすべて選択されます。
- ・「端末検索」を行っていない場合は、すべての登録端末が対象になります。

1. ポリシー管理画面

「ポリシー管理」画面では、端末管理のポリシーを設定します。表示されるポリシー管理項目は、STAR-MDMのご利用形態（基本機能パック／フル機能パック）によって変わります。各ポリシー管理項目においてポリシーはいくつでも作成することができ、端末ごとに自由に割り当てることができます。

メニューバーの[ポリシー管理]をクリックすると、「ポリシー管理」画面が表示されます。

基本機能パックでご利用の場合

- 基本機能
 - サーバと端末間通信 (Android, iOS)
 - 緊急時 (Android, iOS)
 - 異常検知・通報 (Android, iOS)
 - Agent管理

フル機能パックでご利用の場合

- オプション機能
 - パスワード管理 (Android, iOS)
 - デバイス制御 (Android, iOS)
 - 発信番号履歴
 - 発信番号制限
 - 位置情報取得
 - アプリ配信
 - 利用アプリ制限
 - アプリ一覧 (Android, iOS)
 - APN固定化
 - Wi-Fi接続先制限
 - 接続先URL制限
 - 端末暗号義務化
 - ファイル配布
 - Wi-Fi 設定
 - アプリ管理 (iOS)
 - 構成プロファイル配信 (iOS)
 - SIM監視
 - メッセージ配信

戻る

設定を行うポリシー管理項目名をクリックすると、ポリシーの「一覧」画面が表示されます。

【基本機能】

STAR-MDMのご利用形態が「基本機能パック」の場合、ポリシー管理項目は以下の基本機能のみがアクティブ表示されます。

※フル機能パックで対応する項目はグレーアウト表示となります。

	Android対応	iOS対応	基本ポリシー有無
サーバ端末間通信	○	○	○
緊急時	○	○	○
異常検知・通報	○	○	○
Agent管理	○		
コールピックアップ	○		○
パスワード管理			○
DEP設定 (iOS)		○	

関連情報  「[ポリシー管理\(基本機能パック\)](#)」

【フル機能】

STAR-MDMのご利用形態が「フル機能パック」の場合、基本機能を含むすべてのポリシー管理項目がアクティブ表示されます。

基本機能に加え			
	Android	iOS	基本ポリシー
パスワード管理	○	○	○
デバイス制御	○	○	○
発着信番号履歴	○		○
発着信番号制限	○		○
位置情報取得	○	○	○
アプリ管理・配信	○	○	○
利用アプリ制限	○		
アプリ一覧	○	○	○
APN固定化	○		○
Wi-Fi接続先制限	○		○
接続先URL制限	○		○
ファイル配布	○		○
Wi-Fi設定	○		○
端末暗号義務化	○		○
アプリ管理		○	
構成プロファイル配信		○	○
構成プロファイル削除		○	

SIM監視	○		○
メッセージ配信	○	○	
利用アプリ検知		○	○
電話帳配信	○	○	○
VPP管理配布(iOS9)		○	
アプリアンインストール制限	○		
動態管理	○		
利用統計	○		
キオスク管理	○		

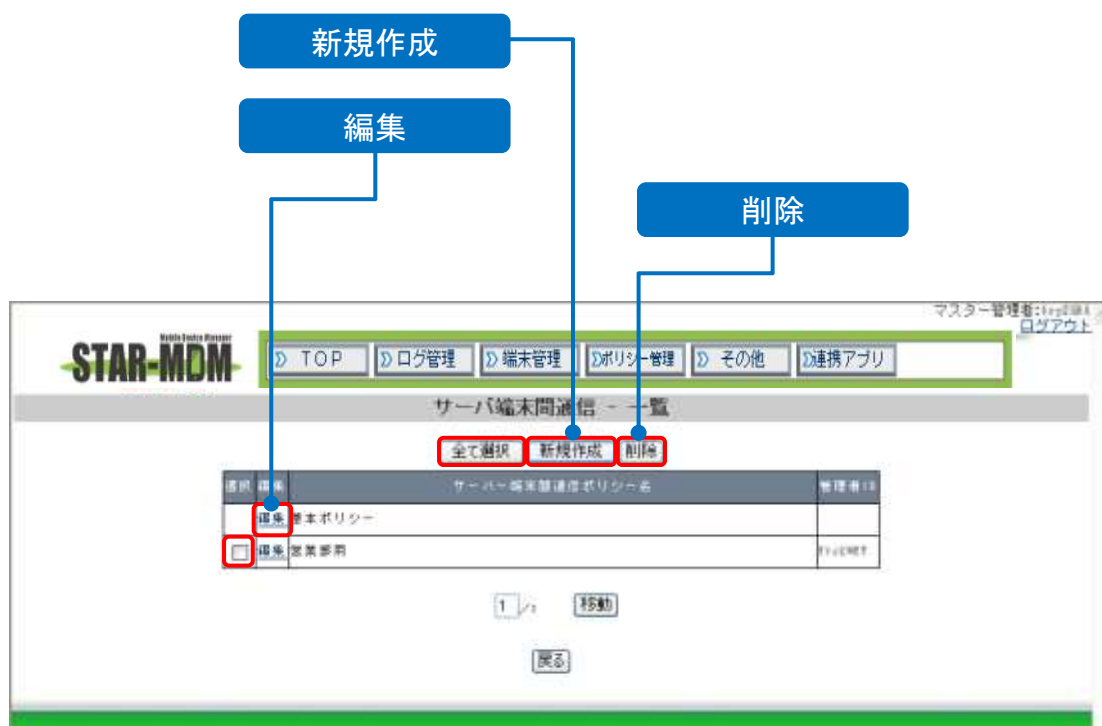
関連情報  「[ポリシー管理\(フル機能パック\)](#)」

2. ポリシーの作成／編集／削除

ポリシーの作成／編集／削除の操作について説明します。ここでは、「サーバ端末間通信」の画面を例として使用します。

2-1. ポリシー 一覧画面

「ポリシー管理」の画面で、設定対象の管理項目名をクリックすると、「ポリシー 一覧」画面が表示されます。



■新規作成

新規にポリシーを作成する場合は、[新規作成]をクリックして「ポリシー更新画面」を表示します。

※基本ポリシーがないものは、新規で基本ポリシーを1つ作成できます。

■編集

既存のポリシーを編集する場合や内容の参照を行う場合は、[編集]をクリックして「ポリシー更新画面」を表示します。

※基本ポリシーも編集可能です。

■削除

ポリシーを削除する場合は、対象ポリシー名のチェックボックスにチェックを入れ、[削除]をクリックします。確認画面が表示されますので、問題がなければ[はい]をクリックします。[全て選択]をクリックすることで、一度にすべてのポリシーを選択することができます。

※基本ポリシーは削除することができません。

◎基本ポリシーとは？

いくつかのポリシー管理項目ではあらかじめ「基本ポリシー」が設定されています。「基本ポリシー」とは、STAR-MDM管理サーバがデフォルトで選択するポリシーです。「基本ポリシー」は、新規登録の端末に対して自動的に適用されます。

以下のポリシー管理項目において、それぞれの「基本ポリシー」がデフォルトで選択されます。

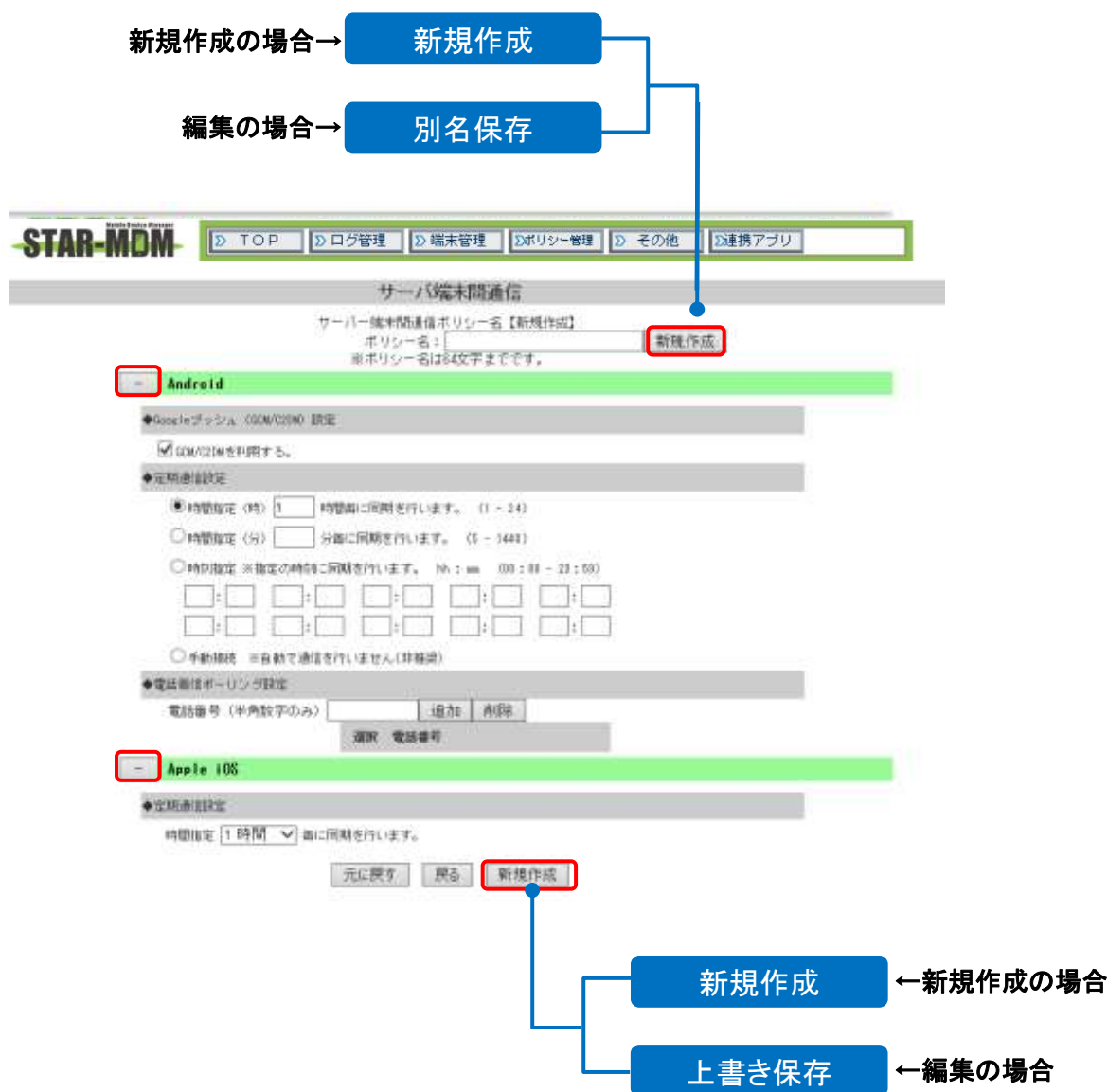
- サーバ端末間通信(Android, iOS)
- 緊急時(Android, iOS)
- 異常検知・通報(Android, iOS)
- パスワード管理^{*1}(Android, iOS)
- デバイス制御^{*1}(Android, iOS)

「基本ポリシー」は編集可能です。既に「基本ポリシー」を適用済みの端末への反映はもちろん、新規登録の端末に自動適用する設定内容を最適化することができます。

その他基本ポリシーが作成可能なポリシーについては基本ポリシー作成後に空きライセンスへ一括設定してください。登録先の空きライセンスに設定されたポリシーが自動的に適用されます。

2-2. ポリシー作成画面

「ポリシー 一覧」画面で、[新規作成]または[編集]をクリックすると、「ポリシー更新画面」が表示されます。Android端末用、iOS端末用、両方の設定が可能なポリシーでは、それぞれのOS名の横にある[+]をクリックすると、折りたたまれていた状態の設定項目が展開されます。ポリシーはいくつでも作成することができ、端末ごとに自由に割り当てることができます。また、共通のポリシーを複数の端末に割り当てすることも可能です。



■新規作成の場合

新規に設定したポリシーを保存する場合は、ポリシー名を入力して[新規作成]をクリックします。「ポリシー一覧」画面にポリシー名が追加されます。

■編集の場合

[別名保存]: 既存のポリシー設定を基に編集し、別のポリシーとして保存する場合は、新たなポリシー名を入力の上、[別名保存]をクリックします。「ポリシー一覧」画面にポリシー名が追加されます。

[上書き保存]: 既存のポリシー設定を編集後、同じポリシー名で保存する場合は、[上書き保存]をクリックします。

1. サーバ端末間通信

STAR-MDM管理サーバと端末間の通信ポリシーを設定します。

【Googleプッシュ(GCM/C2DM/FCM)設定】

■GCM/C2DM/FCMを利用する。

上記にチェックを入れると、GoogleのプッシュサービスであるGCM(Google Cloud Messaging for Android)／C2DM(Cloud to Device Messaging)／FCM(Firebase Cloud Messaging)を利用できるようになります。



携帯キャリアの閉域網サービスやWi-FiでのGCM／FCMの利用には、閉域網内から外部への通信(5228,5229,5230ポート)、C2DMの利用には閉域網内から外部への通信(5228ポート)を許可する必要があります。



GCMは2019年4月11日にサービス終了となります。SPPM Agentをv3.40以下のバージョンでご使用される場合、Google社がGCMを廃止する2019年4月11日までは従来通りGCMでご利用いただくことが可能です。
(予めGCM対応版へのバージョンアップをお勧めします)
また、GCM/C2DMが使えない場合に備えて、電話着信ポーリング設定を強くお勧めします。

◎GoogleプッシュによるSTAR-MDMサーバ指示

GoogleプッシュによるSTAR-MDMサーバ指示は「緊急時指示画面」から行います。

☞「[緊急時指示](#)」

【定期通信設定】

端末からSTAR-MDM管理サーバへの定期ポーリングの設定を行います。定期ポーリングをさせない「手動接続」を指定することも可能です。

- 時間指定(時)(n時間毎に同期を行います)
- 時間指定(分)(n分毎に同期を行います)
- 時刻指定 ※指定の時刻に同期を行います。(n時n分 × 10パターン)
- 手動接続 ※自動で通信を行いません(非推奨)

端末側のスペック等の影響により、SPPM の定期通信が停止した際には、以下のアラートが管理画面上に表示されます。



・Agent の定期通信が停止している可能性があります。端末を再起動してください。

【定期更新】

定期通信されるタイミングで、更新される端末情報画面の項目があります。取得される項目は以下になります。

- ・バッテリー状態
- ・バッテリーの健康状態
- ・バッテリー残量
- ・バッテリー最大量
- ・バッテリー接続
- ・バッテリー温度
- ・SSID
- ・Wi-Fi 利用時のプライベート IP アドレス
- ・使用可能なメモリ容量
- ・低メモリしきい値
- ・低メモリ状態

【電話着信ポーリング設定】

■電話番号(半角英数のみ)

GCM/G2DM/FCMが使えない場合に即時ポーリングを実現するための手段として、電話着信指示機能を用意しています。着信指示用の電話番号は、最大10台分まで登録できます。

登録したいずれかの電話番号から発番通知(186)にて、即時ポーリングさせたい端末に電話をかけると、着信を検知したSPPM Agentが即座にSTAR-MDM管理サーバへ通信し、ポリシー変更や指示を取得して実行します。

※本機能はSPPM Agent v3.41～v3.43では非対応です。



- ・着信指示用の電話番号からの着信を検知すると直ちに切断するため、通話はできません。
- ・着信指示用の電話番号の桁数は4桁～30桁、記号は「*」「+」が指定できます。

・本機能の利用は端末が着信番号情報を保持できることが条件となり、機種によって対応できる番号桁数が異なります。指定した桁数の情報が端末で保持できない場合は、電話着信指示が機能しない場合があります。



STAR-MDMでは端末の死活監視目的として、Push指示可能なAndroid端末に対して、1日に1度Push通信を実施し、端末の死活監視を行います。
こちらは定期通信が『手動接続』に適用されていても、実行されます。

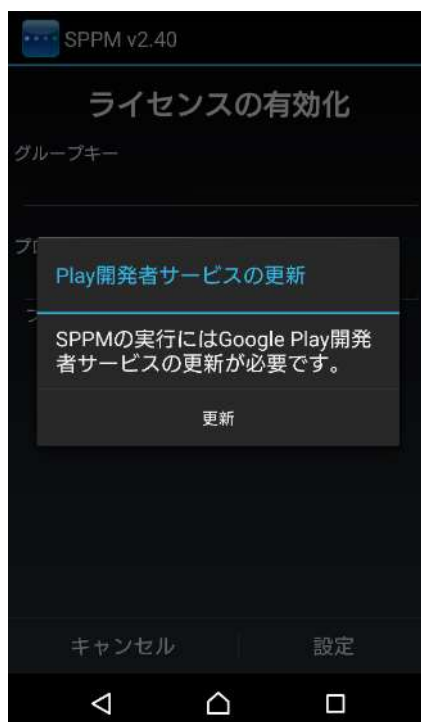
Play開発者サービスの更新

ご利用中の端末が以下3点の条件を満たし、該当のいずれかの操作を行った際に「SPPMの実行にはGoogle Play開発者サービスの更新が必要です。」というダイアログが表示されます。

Google Play開発者サービスの更新を行うまで、該当端末でGCM/FCMをご利用いただけません。

※v3.40以降はFCMのみの対応となるため、GCMは非対応となります。

V3.40へのバージョンアップをお願いします。



【条件】

1. SPPM ver 2.31以降のバージョンを利用している。
2. サーバ端末間通信ポリシーにて、「GCM/C2DM/FCMを利用する」にチェックを入れたポリシーが適用されている。
または、適用しようとしている。
3. Google Play開発者サービスがGCM/FCM利用登録を行えないバージョンである。

【操作】

1. 端末にSPPM Agentをインストール、キッティングする。
2. 端末情報設定ボタンを押下する。
3. GCM/FCMを利用していなかった端末にてGCM/FCMを利用する。

該当端末でGCM/FCMをご利用いただくためには、Google Play開発者サービスを最新版に更新してください。

※ E-API / E-SDK をご利用中の場合、Google Play開発者サービスの更新のために、利用アプリ制限でのGoogle Playの許可が必要です。

※ Google Playをご利用いただくためには、Googleアカウントの登録が必要です。

関連情報 ➡ [「サーバ端末間通信」](#)

関連情報 ➡ [「利用アプリ制限」](#)

2. 緊急時

端末の紛失、盗難等における緊急処置のポリシーを設定します。

※「個人領域も合わせてロックする」と、「個人領域も合わせてハードリセットする」は、Work Profile[企業所有]でキットングした端末のみ利用できます。

Android端末向け設定

緊急時 - ポリシー更新画面

緊急時ポリシー名【新規作成】

ポリシー名: 新規作成

※ポリシー名は64文字までです。

Android

端末ロック

発動条件

☐ SPMサーバー指示

☐ ユーザー連続認証失敗回数 回 (2 ~ 50: Android 6.0以降のみ有効)

<注1> パスワード管理オプション利用時のみ有効です

<注2> パスワード難易度を必ず行なってください。

<注3> PIN, 英数字パスワードにおける4桁未満の認証は、Android 10.0の新約により失敗とカウントされません。

☐ 管理サーバーへの接続断期間 時間 (6 ~ 720 時間の間で設定してください)

☐ 端末の認証成功なし期間 時間 (6 ~ 720 時間の間で設定してください)

☐ 電話番号(半角数字のみ)

☐ ロック ☐ 解除 追加

注1: 電話番号 削除

端末側のロック画面に表示するメッセージ

ロック時の緊急時連絡先
(指定することでロック状態の端末から指定先に電話することが可能になります。)

データ消去

発動条件

☐ SPMサーバー指示

☐ ユーザー連続認証失敗回数 回 (2 ~ 50: Android 6.0以降のみ有効)

<注1> パスワード管理オプション利用時のみ有効です

<注2> パスワード難易度を必ず行なってください。

<注3> PIN, 英数字パスワードにおける4桁未満の認証は、Android 10.0の新約により失敗とカウントされません。

☐ 管理サーバーへの接続断期間 時間 (6 ~ 720 時間の間で設定してください)

☐ 端末の認証成功なし期間 時間 (6 ~ 720 時間の間で設定してください)

☐ 電話番号(半角数字のみ)

追加

注1: 電話番号

消去対象

☐ SMS ☐ 連絡先 ☐ GIF画像 ☐ ブラウザ(ブックマーク、履歴)

☐ 外部メモリ ☐ 内部記憶メモリ ☐ 連絡先 ☐ 予定表

ハードリセット(ワイプ)※ハードリセットはAndroid 6.0以降の機種でのみ有効です。

発動条件

☐ SPMサーバー指示

☐ ユーザー連続認証失敗回数 回 (2 ~ 50: Android 6.0以降のみ有効)

<注1> パスワード管理オプション利用時のみ有効です

<注2> パスワード難易度を必ず行なってください。

<注3> PIN, 英数字パスワードにおける4桁未満の認証は、Android 10.0の新約により失敗とカウントされません。

☐ 管理サーバーへの接続断期間 時間 (6 ~ 720 時間の間で設定してください)

☐ 端末の認証成功なし期間 時間 (6 ~ 720 時間の間で設定してください)

☐ 電話番号(半角数字のみ)

追加

注1: 電話番号

Apple iOS

元に戻す
戻る
新規作成

【端末ロック指示】

※Android OSバージョンにより端末ロック指示時の動作が異なります。

Android OS 8.0 未満

発動条件に従って、端末にSTAR-MDM専用のロック画面を表示させることができます。端末ロック指示が実施されると、端末は表示されているボタン以外の操作ができなくなります。

※SPPMのデバイス管理者権限を外した場合、端末ロック指示は実施されません。

＜端末に表示されるSTAR-MDM専用のロック画面＞



SPPM Agent v2.09以降では、端末側の操作でSTAR-MDMもしくはMonのデバイス管理者権限を端末の設定メニューから外した場合にも端末ロック指示を実施します。

※v3.09.2以降ではSTAR-MDMのデバイス管理者権限を外しても端末ロック指示は実施されません。

AndroidOS5.0以上では、ロック画面に関して以下のことができません



- ・ロック画面上で着信に応答すること
- ・ロック画面上で着信を切断すること
- ・モバイルデータ通信OFFのとき、ロック画面上でサーバ通信ボタンを押下してモバイルデータ通信をONにすること

◎ 端末ロック指示の解除方法

端末ロック指示を解除するには、「緊急時指示画面」で[端末ロック指示解除]をクリックします。

※使用SIMがPINロックされている場合、STAR-MDM端末ロック指示状態では端末起動後にSIMロック解除の画面を表示できないため、SIMによる通信ができなくなる場合がありますのでご注意ください。

☞「[緊急時指示](#)」

Android OS 8.0 以降

※Android OS 8.0 以降では専用ロック画面が廃止されます。

- ① 一部のアプリを除く全てのアプリが利用制限されます。
- ② 端末の画面を点灯、またはパスワード認証すると「端末ロック指示中メッセージ」が表示されます。
- ③ 端末ロック指示解除時に「端末ロック指示解除メッセージ」が表示されます。
- ④ SPPM の通知メッセージが変更されます。
- ⑤ 緊急時連絡先に設定された番号以外へは発信できなくなります。
- ⑥ SPPM Agent/クイック SPPM 画面が端末ロック指示中画面になります。
- ⑦ [ロック時に例外的に制限の対象となるアプリ]を設定した場合、設定をしたアプリは無効化されます。

※端末ロック時に制御対象外のアプリには、適用されません。

■詳細

- ① 一部のアプリを除く全てのアプリが利用制限されます。

対象外アプリ：ホームアプリ / 電話 / アプリ制限非対応アプリ(各端末の機種依存をご確認ください)

※Android Enterprise、E-API、E-SDK 端末では アプリが無効化制限されます。

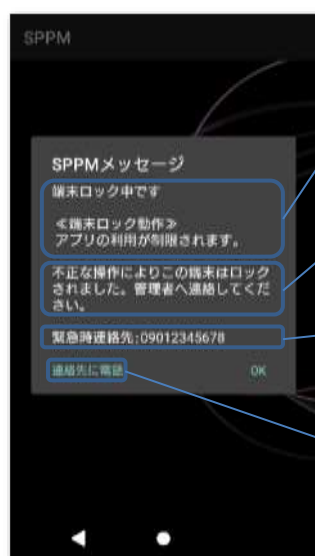
[Chrome]と[設定]はアイコンを押下するとブロック画面が表示されます。

※通常端末ではアプリを起動するとブロック画面が表示されます。

※[設定]が制限されるため USB の接続を「ファイルを送信する」に変更できず、ファイルの送受信は制限されます。

- ② 端末の画面を点灯、またはパスワード認証すると「端末ロック指示中メッセージ」が表示されます。

※1 回のみの表示ではなく操作の度に表示されます。



・**端末ロック指示中メッセージ**
固定メッセージが表示されます。

緊急時ポリシー設定項目

・**メッセージ**
緊急時ポリシーに設定されたメッセージが表示されます。
※設定がない場合は非表示になります。

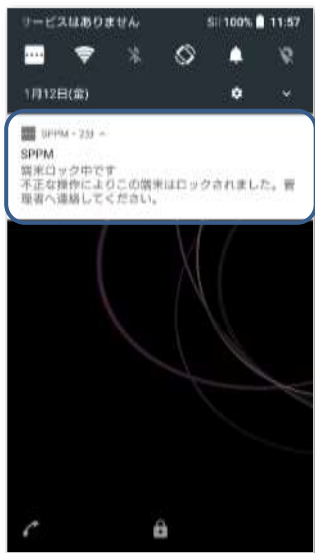
・**緊急時連絡先**
緊急時ポリシーに設定された緊急時連絡先番号が表示されます。
※設定がない場合は非表示になります。

・**連絡先に電話**
「連絡先に電話」ボタンを押下すると緊急時連絡先に発信します。
※設定がない場合は非表示になります。

- ③ 端末ロック指示解除時に「端末ロック指示解除メッセージ」が表示されます。



- ④ SPPM の通知メッセージが変更されます。



・通知メッセージ

通常時

「稼動しています」と表示されます。

端末ロック指示中

端末ロック指示中です(固定メッセージ)と緊急時ポリシーに設定されたメッセージが表示されます。
※設定がない場合は非表示になります。

- ⑤ 緊急時連絡先に設定された番号以外へは発信できなくなります。

※本機能は SPPM Agent v3.41～v3.43 では非対応です。

※Android 10 以降は、端末にて別途設定が必要です。詳しくは[こちら](#)

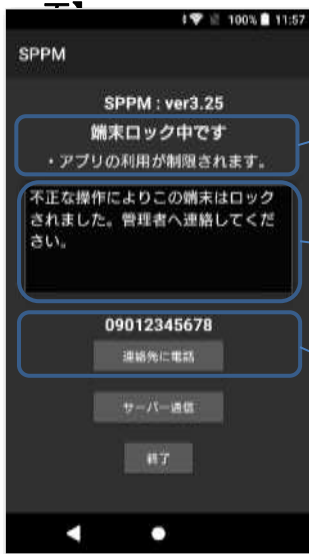


・発信制限メッセージ

緊急時連絡先以外への番号へ発信した際に、発信が制限され発信制限メッセージが表示されます。

- ⑥ SPPM Agent/クイック SPPM 画面が端末ロック指示中画面になります。

【端末ロック指示中画面】



※端末ロック指示中は「コールピックアップ」が非表示となります。

・**端末ロック指示中メッセージ**
固定メッセージが表示されます。

緊急時ポリシー設定項目

・**メッセージ**
緊急時ポリシーに設定されたメッセージが表示されます。
※設定がない場合は非表示になります。

・**緊急時連絡先/連絡先に電話ボタン**
緊急時ポリシーに設定された緊急時連絡先番号が表示され、「連絡先に電話」ボタンを押下すると緊急時連絡先に発信します。
※設定がない場合は非表示になります。

■注意点

端末ロック指示解除後にホームアプリによってはアプリアイコンが正しく表示されない場合があります
また、端末ロック指示解除した際はショートカット等の配置はリセットされるため再設定が必要です。



一部のアプリアイコンの表示が画像のようになりますが、再起動で元に戻ります。この状態のアイコンでもタップするとアプリが正常に起動します。

- ⑦ [ロック時に例外的に制限の対象となるアプリ]を設定した場合、アプリが非表示されます。

※電話アプリなど、ロック中に制御されないアプリに対しては非対応となります。



設定アプリを制限対象に追加し、再起動を実施すると予期せぬ事象が発生する為、制限をしないでください。

【データ消去指示】

発動条件に従い、端末のデータ種類を選択し消去することができます。

＜消去対象データ＞

- ・SMS ・通話履歴 ・Wi-Fi情報 ・ブラウザ(ブックマーク、履歴) ・外部メモリ ・内部拡張メモリ
- ・連絡先 ・予定表



SPPM Agent ver3.41～v3.43では、データ消去機能で通話履歴とSMSの指定削除が出来なくなりました。



「予定表」を消去した場合、同期されているGoogleカレンダー上のデータも削除される場合があります。

【ハードリセット指示(端末初期化)】

発動条件に従って、端末の初期化と外部メモリのフォーマットを行うことができます。

※「Work Profile 削除指示で表示するメッセージ」機能は、Android Enterprise 端末専用の機能です。



ハードリセットが実施されると、SPPM Agent自体も端末から消去されますので、他の緊急処置(端末ロック指示、データ消去)、およびSTAR-MDMのすべての機能が無効となります。



＜ユーザー連続認証失敗回数を発動条件に指定した場合の優先順位＞

設定回数の少ない緊急処置が先に実行されますが、ハードリセットにおける設定回数が他の緊急処置(端末ロック指示、データ消去)と同じ場合は、ハードリセットが優先されます。

《発動条件》 ※3種類の緊急処置共通

それぞれの緊急処置は、以下をトリガー(発動条件)にして実行させることが可能です。複数あるいはすべてのトリガーを有効にすることで、重要情報を多重防御できます。

■STAR-MDMサーバ指示

「緊急時指示画面」に発動用の指示ボタンを表示します。指示ボタンをクリックすると同時に、Googleプッシュ^{*1}によるサーバ指示が発動し、即時に緊急処置を実施することができます。

*1:「サーバ端末間通信」のポリシー設定でGoogleプッシュ(GCM/C2DM/FCM)にチェックが入っている必要があります。

関連情報➡「[緊急時指示](#)」

■ユーザー連続認証失敗回数(n回)

指定回数以上、連続して端末のパスワード認証に失敗した場合、緊急処置を実施します。



・「パスワード管理」^{*1}のポリシー設定でパスワード利用を義務化に設定してください。

*1: STAR-MDMのご利用形態が基本機能パックの場合、ポリシー管理項目には含まれません。フル機能パックにてご利用いただけます。

・PIN番号または英数字パスワードにおける4桁未満の認証は、Android OSの制約により失敗とカウントされません。

■管理サーバへの無接続期間(n時間)

指定期間以上、端末からSTAR-MDM管理サーバへの通信が無い場合、緊急処置を実施します。

■端末の認証成功なし期間(n時間)

指定期間以上、端末のパスワード認証成功が無い場合、緊急処置を実施します。

■電話着信

“緊急処置用に登録した電話番号*1”からの着信があった場合、STAR-MDM管理サーバと通信を行うことなく、電話着信のみで即座に緊急処置を実施します。電話番号は、最大10台分まで登録できます。

*1: 「端末ロック指示」用、「データ消去」用、「ハードリセット」用に別々の電話番号が必要です。

※電話着信による実施はSPPM Agent ver 3.41～v3.43では非対応です。



- ・着信指示用の電話番号からの着信を検知すると直ちに切断するため、通話はできません。
- ・着信指示用の電話番号の桁数は4桁～30桁、記号は「*」「+」が指定できます。
- ・本機能の利用は端末が着信番号情報を保持できることが条件となり、機種によって対応できる番号桁数が異なります。指定した桁数の情報が端末で保持できない場合は、電話着信指示が機能しない場合があります。



- ・サーバ端末間通信ポリシーの電話着信ポーリング、もしくは発着信制限ポリシーでの着信制限の番号は、電話着信端末ロック指示の番号と異なる番号に設定をしてください。同一のものとすると、電話着信端末ロック指示/解除が正常に動作しない場合があります。

Android Enterprise端末向け設定

【ハードリセット指示(端末初期化)】**■Work Profile 削除指示で表示するメッセージ**

仕事領域を削除する際に表示される、通知領域のメッセージ内容を設定することができます。メッセージを設定しない場合は、デフォルトのメッセージが表示されます。

※Work Profile 端末でのみ利用できます。

※400 文字まで作成できます。

【端末再起動】

発動条件に従って、端末の再起動を指示をすることができます。

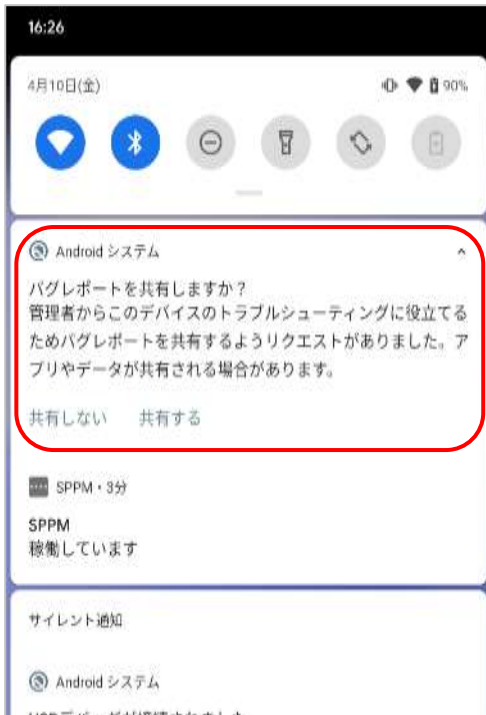
再起動指示の結果は、「ログ管理」画面にて確認できます。

対象端末の電源が未投入、または STAR-MDM サーバとの通信が停止しているタイミングで再起動を指示した場合、次の STAR-MDM サーバとの通信時に端末再起動が実施されます。

※再起動指示対象の端末が通話発着信中、または通話中の場合、再起動は実施されません。

【デバッグログ取得】

発動条件に従って、端末のバグレポートを取得し、STAR-MDM サーバに送信することができます。
 端末から送信されたデバッグログは、管理画面「その他」の「デバッグログ一覧」にて 30 日間保存されます。
 「デバッグログ一覧」機能についての詳細は、「その他」の[デバッグログ一覧](#)をご参照下さい。



《要求同意の通知》

デバッグログ取得指示が端末に到達すると、バグレポートを管理者へ共有する同意要求の通知が端末に表示されます。

この通知は、[共有する] [共有しない]のどちらかを選択するまで、表示され続けます。

※取得したデバッグログを STAR-MDM サーバに送信するためには、端末側に表示される通知にて[共有する]を選択する必要があります。端末利用者の承諾無しにデバッグログを送信することは出来ません。

【共有する】

「共有する」をタップすることで、取得したデバッグログを STAR-MDM サーバへ送信することが許可されます。

【共有しない】

「共有しない」をタップすることで、SPPM サーバへのデバッグログの送信が拒否されます。

「共有しない」を選択後はデバッグログ取得指示がリセットされるため、デバッグログを取得する場合は再度「デバッグログ取得指示」を実施する必要があります。

《発動条件》

端末再起動指示機能およびデバッグログ取得指示機能は、以下をトリガー(発動条件)にして実行させることが可能です。

■STAR-MDMサーバ指示

「緊急時指示画面」に発動用の指示ボタンを表示します。指示ボタンをクリックすると同時に、Googleプッシュ*1によるサーバ指示が発動し、即時に端末再起動を実施することができます。

*1:「サーバ端末間通信」のポリシー設定でGoogleプッシュ(GCM/C2DM/FCM)にチェックが入っている必要があります。

関連情報 [「緊急時指示」](#)

3. 異常検知・通報

蓄積されたログデータを解析して異常を検出し、STAR-MDM管理画面のTOP画面での通知表示のほか、管理者への通知メール、ユーザーへの警告メールを自動的に送信します。



本ポリシー項目でポリシーを作成する場合は、Android向け、iOS向け、それぞれに一項目はチェックを入れて有効にする必要があります。どちらか一方にだけチェックを入れてもポリシーは作成できません。

異常検知・通報

異常検知・通報ポリシー名【新規作成】
 ポリシー名: 新規作成
※ポリシー名は64文字までです。

- Android

異常検知ルール

	[管理者通知メール]	[ユーザー警告メール]
☐ デバイス制御ポリシー違反	☐	☐
☐ 無接続期間 日(1 - 99)	☐	☐
☐ 緊急時ポリシー実施通知	☐	☐
☐ 端末root化検知	☐	☐
☐ SIM交換検知(電話番号が変更された場合に通知)	☐	☐
ソフト制御ポリシー違反		
認証連続失敗(Android2.2以降のみ有効)		
認証成功なし期間(Android2.2以降のみ有効)		

【異常検知ルール】

下記の場合にアラート通知を実行します。必要な項目にチェックを入れてください。

※スクリーンショット中でグレイアウト表示されている項目は準備中の機能です。

■デバイス制御ポリシー違反

「デバイス制御」*1ポリシーの設定内容に反する操作を試みた形跡がある場合。

*1: STAR-MDMのご利用形態が基本機能パックの場合、ポリシー管理項目には含まれません。フル機能パックにてご利用いただけます。

「カメラ」「外部SDカード」については制限が実行されてもアラート通知がされません。

🔗関連情報「[デバイス制御](#)」

☆ワンポイント: USBを利用禁止にした際の通知について

SPPM Agent v2.13以上では、「デバイス制御」ポリシーの設定でUSBの利用を禁止に設定した場合、USBの利用制御ができない端末であっても、ポリシー違反として管理者への通知メール、ユーザーへの警告メールの送信が送信可能です。

※機種及びご利用の充電環境によっては、充電目的のAC接続がUSBの接続と検知される場合がありますので、ご注意ください。

■無接続期間(n日)

指定期間以上、端末からSTAR-MDM管理サーバへの通信が無い場合。

■緊急時ポリシー実施通知

端末ロック指示、データ消去、ハードリセット(端末初期化)、いずれかの緊急処置を実施した場合。

🔗 関連情報「[緊急時指示](#)」

■端末root化検知 ※SPPM Agent v2.16以上で有効です。

端末をroot化した場合。

■SIM交換検知通報 ※SPPM Agent v2.23以上で有効です。

SIMを交換して電話番号が変更された場合。

※端末管理一覧の電話番号欄が「none(電話番号なし)⇒電話番号(SIMを認識)」に変更された場合でもアラートメールは送信されます。

■マルチユーザーの追加や切り替え検知を通知

デバイス制御ポリシーにて「マルチユーザー」の追加や切り替えが検知された場合。

■マルチユーザーの追加や切り替え検知による端末ロック指示の実施を通知

デバイス制御ポリシーにて「マルチユーザー」検知による端末ロック指示が実施された場合。

■デバイス管理者が外された場合に通知 ※SPPM Agent v3.10.1以上で有効です。

デバイス管理者権限が手動で無効にされた場合。

■デバイス管理者が外された場合に端末をロックする ※SPPM Agent v3.10.1以上で有効です。

デバイス管理者権限が無効にされた場合に端末ロック指示を実施します。

その際、端末側のロック画面に表示するメッセージと緊急時連絡先を設定できます。

※SPPM Agent v3.09.2以降ではアンインストール時にデバイス管理者権限が手動で解除可能です。

※端末とSTAR-MDMサーバの通信が有効であることが必須です。

《管理者通知メール》

異常を検知した際、その端末の属するグループとその上層のグループの権限を持つ管理者全員のメールアドレスにメール通知を行うことができます。

通知メールの内容は、ポリシーの新規作成後に表示される[編集]をクリックすることで編集できます。

＜例＞

管理グループ「/東京本社/営業企画部」に所属する端末のアラートメールについて

「/」の管理権限を持つ管理者、

「/東京本社」の管理権限を持つ管理者、

「/東京本社/営業企画部」の管理権限を持つ管理者に送信。

※「/」「東京本社」が上層扱いとなります。

《ユーザー警告メール》

異常を検知した際、当該端末の利用者情報に登録されているメールアドレスにメール通知を行うことができます。通知メールの内容は、ポリシーの新規作成後に表示される[編集]をクリックすることで編集できます。

4. Agent管理

SPPM Agent(端末アプリ)のバージョンアップをリモートで実施します。

※本機能はAndroid Enterpriseと併用できません。

※本機能はSPPM Agent v3.48.1以降からガラホ端末専用の機能に変更となりました。

ガラホ端末以外のAndroid端末ではご利用いただけません。



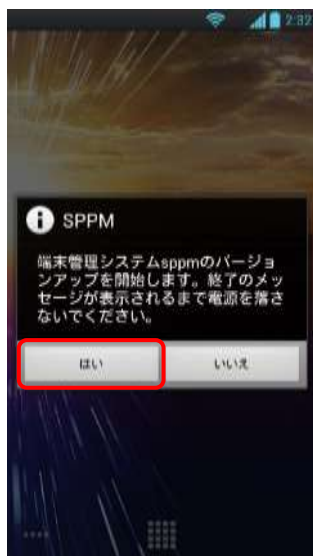
SPPM Agentのバージョンアップ実行手順

【STAR-MDM管理サーバの操作】

「ポリシー更新画面」の「バージョンの指定」の項目で、プルダウンメニューからSPPM Agentのバージョンを選択し、作成したポリシーを端末に適用します。指定したバージョンが既に端末にインストールされているバージョンより新しい場合にのみ、バージョンアップが実行されます。

※バージョンダウンは実行されません。

【端末側での操作】



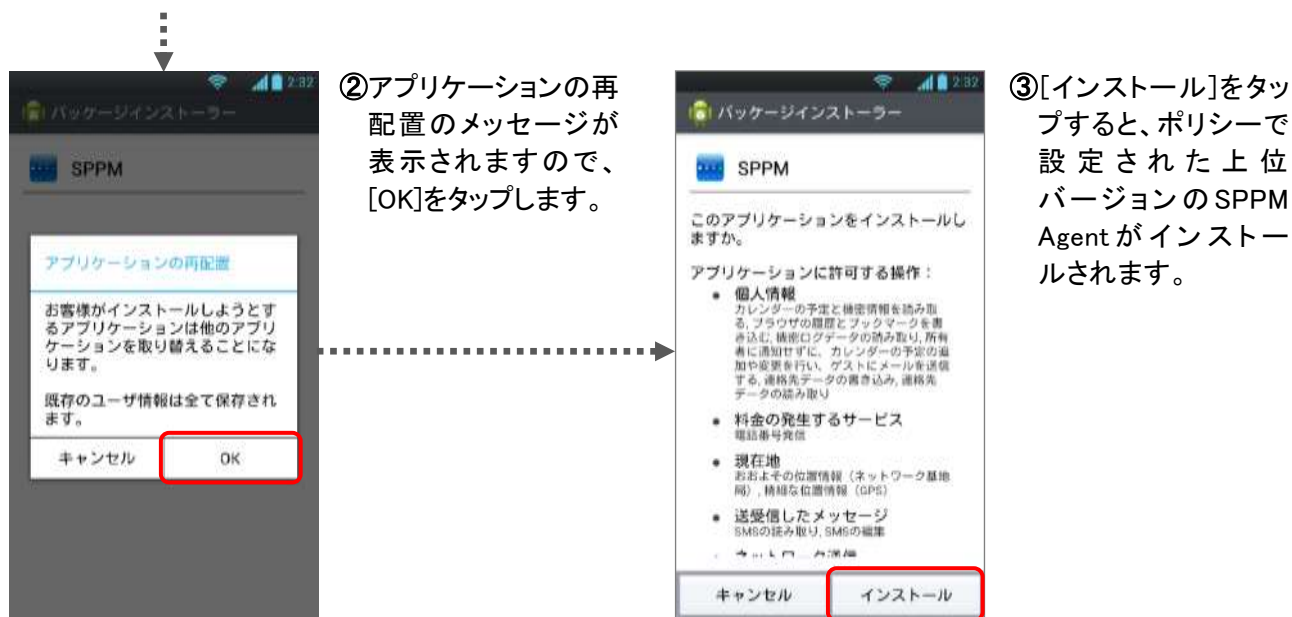
①バージョンアップのポリシーが適用されるとバージョンアップ開始の通知メッセージが表示されますので、[はい]をタップしてください。

※[いいえ]をタップした場合、約5分ごとに同じメッセージがポップアップ表示されます。

◎「アプリケーションを選択」の画面が表示されたら？

[パッケージインストーラー]をタップします。





◎「SppmHomeがデフォルト設定されていません。」のメッセージが出たら

「利用アプリ制限」機能のポリシー設定で「ホームアプリとしてSppmHomeを指定する」にチェックを入れている場合、ホームアプリのデフォルトをSppmHomeに指定する設定が再度必要となる場合があります。その場合は、以下のように設定操作を行ってください。



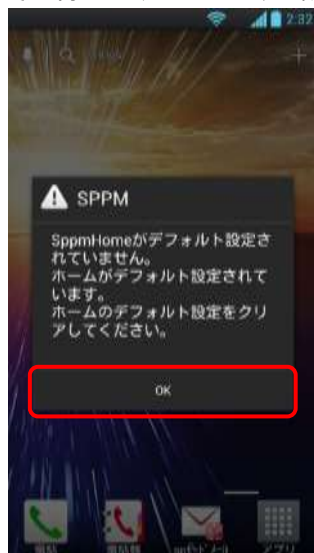
SppmHome以外のホームアプリをデフォルトに設定してしまった場合には、次の様なメッセージが表示されます。

「SppmHomeがデフォルト設定されていません。●●がデフォルト設定されています。●●のデフォルト設定をクリアしてください」

※E-APIによるデバイス制御の「設定」が制限されていると当メッセージは表示されません。デバイス制御ポリシーを解除するか、「設定」を有効化して下さい。

その際には、以下のように設定操作を行ってください。

[OK]をタップします。



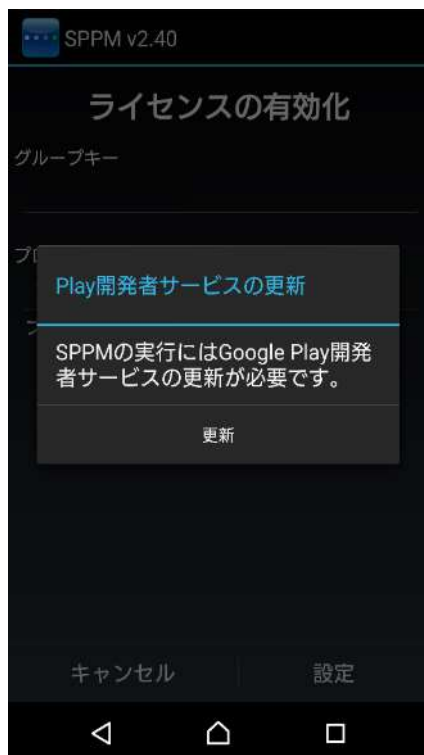
[設定の初期化]*1をタップして、ホームアプリのデフォルト設定を解除してください。

*1: 機種によっては[初期設定に戻す]や[デフォルトをクリア]等の表現です。

再度、「SppmHomeがデフォルト設定されていません。」のメッセージが表示されるようになりますので、前述の操作をやり直してください。

◎Play開発者サービスの更新

ご利用中の端末が以下3点の条件を満たし、該当のいずれかの操作を行った際に「SPPMの実行にはGoogle Play開発者サービスの更新が必要です。」というダイアログが表示されます。Google Play開発者サービスの更新を行うまで、該当端末でGCM/FCMをご利用いただけません。
※v3.40以降はFCMのみの対応となるため、GCMは非対応となります。
V3.40へのバージョンアップをお願いします。



【条件】

1. SPPM ver 2.31以降のバージョンを利用している。
2. サーバ端末間通信ポリシーにて、「GCM/C2DM/FCMを利用する」にチェックを入れたポリシーが適用されている。
または、適用しようとしている。
3. Google Play開発者サービスがGCM/FCM利用登録を行えないバージョンである。

【操作】

1. 端末にSPPM Agentをインストール、キッティングする。
2. 端末情報設定ボタンを押下する。
3. GCM/FCMを利用していなかった端末にてGCM/FCMを利用する。

該当端末でGCM/FCMをご利用いただくためには、Google Play開発者サービスを最新版に更新してください。

- ※ E-API / E-SDK をご利用中の場合、Google Play開発者サービスの更新のために、利用アプリ制限でのGoogle Playの許可が必要です。
- ※ Google Playをご利用いただくためには、Googleアカウントの登録が必要です。

関連情報☞「[サーバ端末間通信](#)」

関連情報☞「[利用アプリ制限](#)」

1. パスワード管理

パスワード利用の義務化や更新の義務化、パスワードの種類、アイドリングタイマーの設定を行います。

Android端末向け設定

パスワード管理

パスワードポリシー名【新規作成】

ポリシー名:

新規作成

※ポリシー名は40文字までです。

Android / Android Enterprise(Work Managed Device)

パスワード利用義務化

義務化する

※Android 6.0以下の端末ではパターンロックが義務化されます。Android 6.2以上の端末では下記より利用パターンについての指定が可能です。

パスワードの種類 (Android 6.0以降のみ有効)

パスワードの種類

利用者が自由に選択 (パターンロックを含む)

パスワードの桁数

パスワード全体の桁数

桁以上 (4 - 16)

カスタム設定 (全体で16桁以内に設定してください)

数字もしくは記号の必要最低数	桁以上
数字の必要最低数	桁以上
記号の必要最低数	桁以上
英字の必要最低数	桁以上
英字小文字の必要最低数	桁以上
英字大文字の必要最低数	桁以上

パターンロック: 8つの点を線で結ぶパターンを記録するパスワード
顔認証: フェイスアンロックやSmartLock内の「顔認証済みの顔」機能
数字PIN: 数字のみで構成されたパスワード
パスワード: 任意の英数字記号で構成されたパスワード
英数字パスワード: 英数字最低で構成されたパスワード
カスタム設定: 任意の文字種別の必要桁数を設定したパスワード
※Android 8.0未満ではカスタム設定利用時に数字/記号/英字がそれぞれ最低1桁必要です。

アイドリングタイマー (Android 6.0以降のみ有効)

画面表示が消えるまでの時間の上限を指定

2分

パスワード更新義務化 (Android 6.0以降のみ有効)

日間更新 (1 - 999)

月間更新 (1 - 60)

期間設定しない

世代チェック

(1 - 50)

パスワードの有効期限切れ5日前から端末に表示されるメッセージ #1

パスワードの有効期限切れ後に端末に表示されるメッセージ #1

※ 改行は無視されます。メッセージを設定しない場合はデフォルトメッセージが表示されます。

パスワード更新タイムアウトのロック (Android Enterpriseのみ)

パスワード更新画面表示からロックするまでの時間(分)の指定

(1 - 99)

Android Enterprise(Work Profile)

Apple iOS

Windows

元に戻す

戻る

新規作成

99

【パスワード利用義務化】

■義務化する

端末の本人認証を義務付けることができます。端末にパスワードロックが設定されていない場合、端末の電源オンならびにスリープからの復帰時に、パスワード設定を要求するポップアップを表示させます。

【パスワードの種類】

《パスワードの種類》

端末に設定できるパスワードタイプを指定できます。

※指紋認証を制限する機能はご用意しておりません。

ただし、端末によっては指紋認証の利用が意図せず制限される場合があります。

■利用者が自由に選択(パターンロックを含む)

パターンロック/PIN/パスワードからパスワードタイプを選択できます。

■利用者が自由に選択(パターンロック / 顔認証を含む) ※SPPM Agent v3.40以降対応

パターンロック/PIN/パスワードからパスワードタイプを選択できます。

また、端末内の顔認証機能が利用できます。

■数字PIN、パスワードのいずれかを利用

PIN/パスワードからパスワードタイプを選択できます。

■数字PIN、パスワードのいずれかを利用(数字PINは繰返しや単純値を禁止)

※SPPM Agent v3.40 / Android OS 5.0 以降対応

PIN/パスワードからパスワードタイプを選択できます。

また、「1111」や「1234」などの数字の繰返しや単純値を禁止します。

※Android OS9.0未満では、パスワードタイプが「パスワード」では数字の繰返しや単純値は制限されません。

※Android 11以降は、英字の繰返しや単純値(「abcd」や「aaaa」)も制限されます。

■パスワードを利用

任意の英数字記号で構成されたパスワードのみを選択できます。

※Android 11以降では、記号が入っていれば英字が含まれていなくてもパスワード設定が可能です。

■英数字パスワードを利用

任意の英数字混在で構成されたパスワードのみを選択できます。

※Android 11以降では、記号が入っていれば英字が含まれていなくてもパスワード設定が可能です。

■パスワードを利用(カスタム設定) ※SPPM Agent v3.40以降対応

任意の文字種別の必要桁数を設定したパスワードのみを選択できます。

※文字種別の必要最低数設定は「カスタム設定」欄から指定します。

※Android 6.0未満ではカスタム設定利用時に数字/記号/英字がそれぞれ最低1桁必要です。



例としてパスワード種別が「パスワードを利用」以上の場合、端末のパスワード設定画面は左図のように表示され、パスワード以外の設定は行えません。



パスワード義務化状態では左図のように顔認証は制限されます。
※「利用者が自由に選択(パターンロック / 顔認証を含む)」選択時のみ使用できます。

《パスワードの桁数》

■パスワード全体の桁数

パスワード全体の最低入力桁数を「4～16桁」で設定できます。

※「利用者が自由に選択(パターンロックを含む)」/「利用者が自由に選択(パターンロック/顔認証を含む)」以外を選択している場合はパスワードの桁数入力は必須となります。

※「カスタム設定」を選択している場合、カスタム設定で設定した合計桁数を下回る桁数は設定できません。

《カスタム設定》※SPPM Agent v3.40以降対応

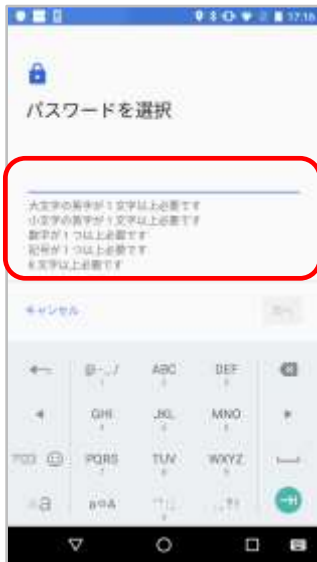
数字もしくは記号の必要最低数		桁以上
数字の必要最低数		桁以上
記号の必要最低数		桁以上
英字の必要最低数		桁以上
英字小文字の必要最低数		桁以上
英字大文字の必要最低数		桁以上

①数字もしくは記号の必要最低数: パスワードに含む数字、または記号の最低桁数を設定できます。

※②/③の合計桁数が上回っていた場合は無効となります。

②数字の必要最低数: パスワードに含む数字の最低桁数を設定できます。

- ③記号の必要最低数:パスワードに含む記号の最低桁数を設定できます。
- ④英字の必要最低数:パスワードに含む英字の最低桁数を設定できます。
- ※⑤/⑥の合計桁数が上回っていた場合は無効となります。
- ⑤英字小文字の必要最低数:パスワードに含む英字小文字の最低桁数を設定できます。
- ⑥英字大文字の必要最低数:パスワードに含む英字大文字の最低桁数を設定できます。



カスタム設定で文字種別の最低桁数を設定すると

左図のように設定条件が要求されます。

※画像はカスタム設定で全ての文字種の最低桁数を「1」とパスワード全体の桁数を「8」にした場合の画面です。

※画像は Nexus5X の設定画面です。

端末により仕様が異なる場合がございます。

【アイドリングタイマー】

■画面表示が消えるまでの時間の上限を指定(15秒／30秒／1分／2分／10分／30分)

端末の操作が指定時間以上無い場合、自動的にパスワードロックを実施することができます。(端末が無操作状態になってからスリープモードになるまでの時間の上限を設定します)

本設定はOS側の仕様(動作)として、端末の自動ロック上限値は画面非表示に設定した値により、設定できる時間が変動いたします。

例) STAR-MDMのポリシーでアイドリングタイマーを『2分』に設定

■ディスプレイ消灯時間を『1分』に設定

⇒自動ロックは1分までの間で設定が可能です。

■ディスプレイ消灯時間を『2分』に設定

⇒自動ロックは『今すぐロック』となります。

※ポリシーで設定した上限2分に、ディスプレイ消灯時間で達している為。

【パスワード更新義務化】

指定の日数または月数間隔で、端末のパスワード更新を義務付けることができます。以下のいずれか一つを選択する必要があります。

更新を義務化すると、更新期日の5日前から端末起動時に、パスワード更新を促すポップアップが端末に表示され、更新期日になると更新するまで数10秒ごとに表示されます。

※設定アプリを起動している間は警告が表示されない場合があります。

■(n)日間更新

前回のパスワード更新から指定日数が経過した日を更新期日に定めます。

■(n)ヶ月間更新

更新間隔の月の初日を更新期日に定めます。

■期間設定しない

パスワードの更新を義務化しません。

任意のタイミングでパスワードを変更することが可能です。

■世代チェック(パスワード世代管理機能)

ポリシー適用後に設定したパスワードの世代を覚えており、変更前と変更後の違いをチェックし、同一のパスワードを連続して設定できないように制限できます。1～50世代前までのチェックを行うことができます。

※世代チェックはAndroid OS 3.0以上で有効です。

※世代チェックはパターンロックには適用されません。

■パスワードの有効期限切れ5日前から端末に表示されるメッセージ

「(n)日間更新」「(n)ヵ月間更新」を設定された場合にパスワード有効期限切れ5日前から端末に表示されるメッセージを設定できます。メッセージは端末パスワード認証直後に表示されます。

※メッセージを設定しない場合はデフォルトメッセージが表示されます。

■パスワードの有効期限切れ後に端末に表示されるメッセージ

「(n)日間更新」「(n)ヵ月間更新」を設定された場合にパスワード有効期限切れ後に端末に表示されるメッセージを設定できます。メッセージは端末起動中に定期的に表示され続けます。

※メッセージを設定しない場合はデフォルトメッセージが表示されます。



Android OS標準のパターンロックの場合には、パターンを構成するグリッド数が同じだと、実際にパターンを変更しても変更と認識されません。その場合、パターンを変更したにもかかわらず、変更を求めるダイアログが表示され続けますので、パターンを変更する際には、パターンを構成するグリッド数を変えるようにしてください。(機種によってはメーカーの独自改良によりこの問題が解消されているものもあります)

Android Enterprise端末向け設定

【パスワード更新タイムアウトのロック(Android Enterpriseのみ)】

下記のポップアップを閉じてから指定の時間が過ぎると端末にロックがかかります。

- ・端末に設定されているパスワードより厳しいパスワードを要求するポリシーを適用した際に端末上に表示されるパスワード設定を要求するポップアップ
- ・パスワード更新義務化によるパスワード期限のポップアップ

本設定により端末ロック指示が実施されると「パスワード更新タイムアウトによる端末ロック指示を実施しました。」と

ログ管理画面に表示されます。



2. デバイス制御

端末に搭載されているカメラやスクリーンショット機能などの利用を制限します。

- **Android**

◆デバイス制御

☒ カメラ	☒ 無線LAN	☒ Bluetooth
☒ 外部SDカード	☒ USB *1	☒ Wi-Fiテザリング *2
☒ USBテザリング	☒ スクリーンショット	

以下はSAMSUNG Galaxyシリーズのみ有効です。 *3

☒ USB MediaPlayer	☒ MassStorage	☒ USB Debugging
☒ NFC	☒ Wall Paper Change	☒ Micro Phone
☒ Home Key	☒ VolumeUp Key	☒ VolumeDown Key
☒ Back Key	☒ Menu Key	☒ Power Key
☒ Mock Location	☒ Factory Reset	☒ Power OFF
☒ Status Bar	☒ Google Crash Report	☒ Google Backup
☒ TaskManager	☒ On the AirOS upgrade	

以下はSony Xperia シリーズのみ有効です。

☒ MassStorage	☒ USB Debugging	☒ On the AirOS upgrade
☒ Bluetooth HANDSFREE	☒ ADD Guest User	☒ "緊急時省電力モード"

【デバイス制御】

端末の「カメラ」「無線LAN」「Bluetooth」「外部SDカード」「スクリーンショット」「SmartLock」の利用許可／利用禁止をそれぞれ設定することができます。機種によっては、「USB」「Wi-Fiテザリング」「USBテザリング」の利用禁止も設定可能です。各項目のチェックボックスにチェックを入れると該当項目が利用許可に、**チェックを外すと利用禁止**に設定されます。

※USBの利用禁止は、SPMM Agent v1.14以上で有効です。

※Wi-Fiテザリングの利用禁止は、SPMM Agent v2.00以上で有効です。

※スクリーンショットの利用禁止は、SPMM Agent v2.13以上で有効です。

※マルチユーザーの利用禁止は、SPPM Agent v3.13以上で有効です。

※SmartLockの利用禁止は、Android OS 6.0以上/SPPM Agent v3.25以上で有効です。

《USBの利用禁止における機種依存について》

・GALAXY Tab 10.1 LTE SC-01D (Android OS v3.2)

USB利用を禁止した場合、設定メニューは使用できなくなります。ただし、PCと端末をUSBで接続している状態では設定メニューを使用することができます。

・ARROWS Tab LTE F-01D (Android OS v3.2)

USB利用を禁止した場合、設定メニューは使用できなくなります。

・SHARP機種 (Android OS v6.x～v8.x)

SPPM Agent v3.51 かつ SHARPモジュール v1.2 を利用している場合、PCとのUSB接続を制限する事ができます。

☆ワンポイント: USBを利用禁止にした際の通知について

SPPM Agent v2.13以上では、USBの利用制御ができない端末であっても、ポリシー違反として管理者への通知メール、ユーザーへの警告メールの送信が可能です。通知機能を利用するには、本ポリシー設定でUSBの利用を禁止にした上で、「異常検知・通報」のポリシー設定を行ってください。

※機種及びご利用の充電環境によっては、充電目的のAC接続がUSBの接続と検知される場合がありますので、ご注意ください。

☞「[異常検知・通報](#)」

《スクリーンショットの利用禁止について》

スクリーンショットを禁止した場合のSPPM Agentによる端末制御は下記の通りです。

■スクリーンショット利用禁止のポリシーが適用された時点でフォルダに保存されているデータをすべて削除します。

■スクリーンショット利用禁止の状態では、スクリーンショットの撮影が行われてフォルダに保存された時点でファイルが削除されます。また、スクリーンショットを削除した旨がログに出力されます。



SPPM Agent v3.10.1未満のAndroid OS 6.0端末ではスクリーンショットの撮影を検知できないため、保存された時点ではファイルは削除されません。定期通信等のサーバー通信時に削除されます。



E-API, E-SDK対応の端末ではスクリーンショット操作自体が制限されます。

《SDカードの利用禁止におけるOS依存について》

・Android OS 4.2 未満

SDカードを強制アンマウントします。(Android OS 4.1では検知ログ・アラートは表示されません。)

・Android OS 4.2 - 5.11

SDカードを挿入状態では端末ロック指示画面が表示され、操作不可となります。

・Android OS 6.0 以降

OS依存制限によりSDカードの制限は非対応です。

※Xperia / Galaxy 端末では、OS 4.2 以降や OS 6.0 以降でも、外部 SD カードを強制アンマウントします。

※SHARP 端末(Android OS v6.x～v8.x)では、SPPM Agent v3.51 かつ SHARPモジュール v1.2 以降を利用している場合、外部SDカードを強制的にアンマウントすることができます。(検知ログ・アラートは表示されません。)

《マルチユーザーの利用禁止について》

マルチユーザー機能でのユーザー追加と切り替えを検知し、ログとアラートを表示します。

また、切り替え後に再度SPPM Agentがインストールされたユーザーへ切り替えると端末ロック指示が実施され、端末ロック指示実施のログが表示されます。

※マルチユーザー機能自体の制限は行えませんのでご注意ください。

☆ワンポイント: マルチユーザーを利用禁止にした際の通知について

マルチユーザーを検知した際とそれによる端末ロック指示が実施された際に、ポリシー違反として管理者への通知メールとユーザーへの警告メールの送信が可能です。

通知機能を利用するには、本ポリシー設定で「マルチユーザー」の利用を禁止にした上で、「異常検知・通報」のポリシー設定を行ってください。

☞「[異常検知・通報](#)」

《カメラの利用禁止について》

「デバイス制御」ポリシーの「カメラ」を禁止設定にした場合、カメラ機能自体が制限されるため、カメラ機能を利用するアプリからのカメラの起動および、端末のパスワードロック画面からのカメラの起動が制限されます。

アプリ単位でカメラの制限を許可したい場合は、「利用アプリ制限」ポリシーでの制限をご検討ください。

例) 業務用アプリでのみカメラを利用したい場合の設定

- ・「デバイス制御」ポリシーの「カメラ」を「許可」に設定
- ・「利用アプリ制限」ポリシーにて業務用のアプリを「許可」に設定
- ・「利用アプリ制限」ポリシーにて業務用以外のカメラ機能を利用するアプリを制限

※上記の場合、パスワードロック画面からのカメラの起動は制限できませんのでご注意ください

《USBテザリングの利用禁止について》

- ・SHARP機種(Android OS v6.0～v8.x)

SPPM Agent v3.53 かつ SHARPモジュール v1.3 を利用している場合、USBテザリングを制限する事ができます。

《Galaxyシリーズについて》

SAMSUNG Galaxyシリーズの端末については、更に詳細に端末を制御することができます。

Galaxy端末毎に対応しているE-SDKバージョンが異なり、利用できる機能に違いがあります。各機種種のE-SDKバージョンは弊社にお問い合わせください。

設定項目	機能詳細	対応 E-SDK バージョン
On the AirOS upgrade	OS のバージョンアップを制限します。 設定メニューの「ソフトウェア更新」がグレーアウトします。	3.0 以上
Wi-Fi テザリング	従来の制限と異なり、有効にするボタンがグレーアウトします。	2.0 以上
USB テザリング	従来の制限と異なり、有効にするボタンがグレーアウトします。	2.0 以上
外部 SD カード	外部 SD カードを制限します。従来の制限方法と異なり、マウントするボタンがグレーアウトします。	2.0 以上
USB MediaPlayer	USB を接続した際の MTP モードを制限します。	2.0 以上
USB MassStorage	USB 接続時のマストストレージ接続を制限します。 ※SPPM Agent v3.45 以降ではご利用頂けません。	2.0 以上
USB Debugging	USB デバッグ機能を制限します。	2.0 以上
USB Host Storage	USB ストレージへの接続を制限します。	4.0 以上
NFC	NFC の利用を制限します。 ※SPPM Agent v3.45 以降ではご利用頂けません。	2.0 以上
Wall Paper Change	壁紙の変更を制限します。	3.0 以上
Micro Phone	マイク機能を制限します。	2.0 以上
Home Key	ホームボタン押下時のホームアプリ起動を制限します。	2.0 以上
TaskManager	ホームボタン長押しでのアプリ履歴表示を制限します。	2.0 以上
Hardware Key(VolumeUp)	ボリュームアップボタンを無効化します。	3.0 以上
Hardware Key(VolumeDown)	ボリュームダウンボタンを無効化します。	3.0 以上
Hardware Key(Back)	バックボタンを無効化します。	3.0 以上
Hardware Key(Menu)	メニューボタンを無効化します。	3.0 以上
Hardware Key(Power)	電源ボタンを無効化します。	3.0 以上
Mock Location	擬似ロケーション機能を制御します。	2.0 以上
Factory Reset	端末初期化操作を制限します。	2.0 以上
Status Bar	ステータスバーを非表示にします。	3.0 以上
Power OFF	電源ボタン長押し時の「電源を切る」を制限します。	3.0 以上
スクリーンキャプチャ	スクリーンキャプチャ操作を制限します。	2.0 以上
Google Crash Report	Google クラッシュレポートを無効にします。	3.0 以上
Google Backup	Google バックアップを制限します。	2.0 以上
App Switch Key	アプリ履歴ボタンを無効化します	3.0 以上
セーフモード	セーフモードでの端末の起動を制限します。	4.0 以上
アクティブキー	アクティブキーを無効化します。	3.0 以上

-  本機能は、Galaxy端末に「E-SDK用制御モジュールアプリ」をインストールする事で、利用可能です。E-SDKバージョン4以降の端末ではSPPM Agent v2.29以降をインストールすると、E-SDK用制御モジュールアプリをインストールせずにE-SDKの機能が利用できます。
-  Galaxy端末毎に対応しているE-SDKバージョンが異なり、利用できる機能に違いがあります。E-SDKの詳細は⇒「[連携アプリ](#)」
-  「E-SDK 用制御モジュールアプリ」をアンインストールする場合は、必ず全て「許可」に設定をしたデバイス制御ポリシーを端末に反映してからアンインストールしてください。
-  『MassStorage』『On the AirOS upgrade』『USB Debugging』『Power OFF』『Home Key』『Volume Key』『Back Key』『Status Bar』『アプリ履歴キー』のチェックボックスはE-API のチェックボックスと連動します。上記の 3 項目を E-API と E-SDK で分ける場合は別途ポリシーを作成して端末に適用をしてください。
-  SPPM Agent v3.45 未満の端末に 『USB MassStorage』と『NFC』の制限を行っている状態でSPPM Agent v3.45 以降にバージョンアップを行った場合、『USB MassStorage』と『NFC』の制限はバージョンアップ後も有効のままになります。
なお、制限を解除するためには SPPM Agent の再インストールが必要です。

《Xperiaシリーズについて》

Sony Xperiaシリーズの端末については、更に詳細に端末を制御することができます。

Xperia端末毎に対応しているE-APIバージョンが異なり、利用できる機能に違いがあります。各機種のE-APIバージョンは弊社にお問い合わせください。

設定項目	機能詳細	対応 E-API バージョン
MassStorage	USB 接続時のマストレージ接続を制限します。	5.0 以上
USB Debugging	USB デバッグ機能を制限します。 デバッグ機能は ON にすると、再起動して制限します。	5.0 以上
On the AirOS upgrade	端末での OS のバージョンアップを制限します。 PC 接続によるバージョンアップも制限する場合は PC_OS_UPGRADE と MassStorage を制限してください。	3.0 以上
Bluetooth HANDSFREE	Bluetooth を禁止していても Bluetooth HandsFree(ヘッドセット)の接続のみ個別許可をします。	3.0 以上
ADD Guest User	端末のユーザ追加を制限します。	6.0 以上
緊急時省電力モード	緊急時省電力モードの利用を制限します。 緊急時省電力モード ON にすると、再起動して制限します。	3.0 以上
外部 SD カード	OS4.4 以降でも、外部 SD カードをアンマウントします。	3.0 以上
スクリーンショット	スクリーンキャプチャ操作を制限します。	5.0 以上
設定	パスワード変更と暗号化を除く端末の設定を制限します	7.0 以上
セーフモード	セーフモードでの端末の起動を制限します	8.0 以上
スモールアプリ	スモールアプリの仕様を制限します	3.0 以上
Power OFF	電源オフ操作を制限します。	8.0 以上
AUTO_BOOT	充電時自動起動(オートブート)モードを有効にできます。	8.0 以上
PC_OS_UPGRADE	Xperia Companion によるソフトウェア修復時の OS アップグレードを制限します。	8.0 以上
SCREEN SLEEP	画面のスリープを制限します。	8.0 以上
FACTORY RESET BY USER	端末初期化操作を制限します。	9.0 以上
FACTORY RESET ALL	端末初期化操作を制限します。システムによるリセットや緊急時ポリシーによるリセットも制限します。	9.0 以上
トップに固定するパッケージ名	指定したアプリを開くとトップ画面に固定します。	8.0 以上
Home Key	ホームボタンを無効化します。	8.0 以上
Volume Key	ボリュームキーを無効化します。	9.0 以上
Back Key	バックボタンを無効化します。	8.0 以上
Status Bar	ステータスバーを非表示にします。 ※パスワード認証画面では有効です。	8.0 以上
アプリ履歴キー	アプリ履歴キーを無効化します。	8.0 以上

- PC 接続(Xperia Companion)を利用した OS バージョンアップを完全に制限する場合は、『PC_OS_UPGRADE』と『MassStorage』を制限してください。
- 『緊急時省電力モード』は、Agent v2.28 以降がインストールされている E-API バージョン対応機種の場合に、デバイス制御ポリシーが未設定でも制限がされます。
緊急時省電力モードを利用する場合は当機能を許可したデバイス制御ポリシーを端末に適用してください。
- 『MassStorage』、『On the AirOS upgrade』、『USB Debugging』、『Power OFF』のチェックボックスは E-SDK のチェックボックスと連動します。上記の 3 項目を E-API と E-SDK で分ける場合は別途ポリシーを作成して端末に適用をしてください。
- 『設定』の制限を行う際は、他機能との併用にご注意下さい。
- ・SppmHome 指定設定では他ホームアプリのデフォルト設定解除が催促されなくなります。
 - ・E-API7 の場合、外部メモリ暗号化が行われません。
- 『スモールアプリ』の制限を利用する際には、利用アプリ制限ポリシーも併せて適用してください。
利用アプリ制限未設定の状態では正しく制限されません。
また SPPM Agent バージョンによって動作が異なります。
- 【SPPM Agent v3.10.1 未満】**
- ＜ホワイトリストの場合＞
- スモールアプリの中で、プリインストールのブラウザと GooglePlay からインストールされたスモールアプリは制限対象外です。
そのため、手動でのスモールアプリアンインストールと、再インストールを防ぐため GooglePlay を禁止にする必要があります。
- ＜ブラックリストの場合＞
- スモールアプリは全て制限対象です。ただし、新規インストール直後のスモールアプリは一覧に表示されるため、GooglePlay を禁止にしてスモールアプリの追加を防ぐ必要があります。
- 【SPPM Agent v3.10.1 以降】**
- ホワイトリストでは全てのスモールアプリは制限されますが、
ブラックリストでは利用アプリ制限で設定されたアプリ一覧外のアプリは許可されます。
- 『ADD Guest User』の制限では、ユーザーの追加は制限できますが、
「ゲスト」の追加は制限出来ません。
「ゲスト」を完全制限するには『設定』を制限する必要があります。
- 『トップに固定するパッケージ名』によってアプリを画面固定化すると、アプリによっては正常に機能しなくなる場合があるため、運用前に固定化状態のアプリ動作をご確認下さい。
また、アプリによっては固定化指定をしていると、該当のアプリが起動できなくなる場合があります。
その場合は、アプリを起動した状態で固定化を設定したポリシーを適用することで、正常にアプリ起動状態での固定化が実行される可能性があるためお試しください。



SPPM Agent v3.42 以降では Android OS9.0 未満では『Volume Key』の制限ができなくなりました。

《SHARPシリーズについて》

SHARP AQUOS シリーズの端末については、更に詳細に端末を制御することができます。

※ 制御にはSHARPモジュールアプリのインストールが必要です。

※ SHARP モジュールは OS9 以降の端末は未対応です。

※ Android Enterprise 端末で SHARP モジュール機能は利用できません。

機能名	機能内容	OS	SHARP モジュール	SPPM Agent
On the AirOS upgrade	OS のバージョンアップを制限します。 (docomo 端末のみの機能です)	OS6～7	V1.0 以降	v3.22 以降
		OS8.x	V1.1 以降	
パスワードリセット機能	端末に設定されているパスワードをリセットします。	OS6～7	V1.0 以降	
		OS8.x	V1.1 以降	
USB 制限	USB 接続を制限します。	OS6～8.x	v1.2 以降	v3.51 以降
外部 SD カード制限	外部 SD カードを強制アンマウントします。			
USB テザリング	USB テザリングを制限します。		v1.3 以降	v3.53 以降

3. 発着番号履歴

端末の発着番号履歴をSTAR-MDM管理サーバが取得して保管します。

※本機能はSPPM Agent v3.41～v3.43 / v3.59.1.2～では非対応です。

【発着番号履歴取得】

■発着履歴の取得を行う

「発信先」「着信して通話した電話番号」「着信したが通話しなかった電話番号」を日時と共に記録します。取得した発着番号履歴は「端末情報画面」で閲覧することができます。

※履歴の保持期間は90日間です。

関連情報⇒「[端末情報](#)」

4. 発信番号制限

端末の発信通話および着信通話を制限します。

※本機能はSPPM Agent v3.41～v3.43では非対応です。

※AndroidOS 以降の場合、本機能の利用にあたり端末側の設定や制限事項があります。詳しくは[こちら](#)

発信番号制限 - ポリシー更新画面

発信番号制限【新規作成】

ポリシー名: 新規作成

※ポリシー名は40文字までです。

◆発信番号制限

☐ 発信許可 登録電話番号への発信通話を許可する

☐ 発信禁止 登録電話番号への発信通話を禁止する

ファイル指定: 参照 upload

電話番号リストを登録

未登録

<注意>

1. 許可/禁止電話番号リストの変更/編集は、CSVデータにて実施し、登録しておいてください。

2. 許可/禁止電話番号リストの電話番号は、99桁のみでも有効です。

◆着信番号制限

☐ 着信許可 登録電話番号からの着信通話を許可する

☐ 着信禁止 登録電話番号からの着信通話を禁止する

ファイル指定: 参照 upload

電話番号リストを登録

未登録

<注意>

1. 許可/禁止電話番号リストの変更/編集は、CSVデータにて実施し、登録しておいてください。

2. 許可/禁止電話番号リストの電話番号は、99桁のみでも有効です。

元に戻す 戻る 新規作成

【発信番号制限】

「発信番号制限」を実施するには、以下のいずれかを選択します。

- 発信許可 (登録電話番号への発信通話を許可する)
- 発信禁止 (登録電話番号への発信通話を禁止する)

【着信番号制限】

「着信番号制限」を実施するには、以下のいずれかを選択します。

- 着信許可 (登録電話番号からの着信通話を許可する)
- 着信禁止 (登録電話番号からの着信通話を禁止する)

《電話番号リストの登録》

「発信番号制限」「着信番号制限」共に、制限をかける電話番号のリストをCSVファイルでアップロードして登録します。

0323456789

09045678901

のように、ハイフンを含まない4～11桁の電話番号のみを記述したCSVファイルをご用意ください。[参照]をクリックしてファイルを指定後、[upload]をクリックすると、電話番号が一覧表示されます。

※最大設定可能数は「発信番号制限」「着信番号制限」とともに1,000件までです。

※制限の判定は登録された番号の後方一致です。

電話番号リストを編集する場合は、CSVデータにて実施の上、再度ファイルをアップロードし直してください。

《電話番号のワイルドカード指定》

SPPM Agent v3.70以降では、電話番号の一部に指定した番号が含まれる場合に、部分一致により発信通話、および着信通話を制限することができます。

部分一致で電話番号を制限する場合は、「%」を入力し、下記のように記載します。

032345%

%45678901

なお、番号の末尾に「%」を付けた場合は、「%」より前が一致している電話番号が対象となります。

(例)032345% を指定した場合

0323456789 ⇒ 制限対象

0322226789 ⇒ 制限対象外

番号の先頭に「%」を付けた場合は、%より後ろが一致している電話番号が対象となります。

(例)%45678901 を指定した場合

09045678901 ⇒ 制限対象

09000078901 ⇒ 制限対象外

◎「発信番号制限」か「着信番号制限」どちらか一方の機能だけを利用したい場合は？

使わない方の機能については、電話番号リストを未登録のままにしてください。これにより、未登録の方の制限機能は有効になりません。例えば、「着信番号制限」の機能は使わないとした場合、「着信番号制限」の着信許可／着信禁止いずれかのラジオボタンは選択しなければなりませんが、電話番号のリストが未登録であれば、制限機能は有効になりません。

【発着番号制限ポリシー適用時の端末の挙動】

Android OS 10 以降の端末にて本機能を利用する場合、端末内の「通話転送アプリ」を SPPM Agent に指定する必要があります。

- ❗ 「通話転送アプリ」を SPPM Agent に指定した場合、SPPM Agent 以外の通話転送アプリを利用できません。

本機能を端末に適用した場合、以下のポップアップが表示されますので、「SPPM Agent」を選択し、「デフォルトに設定」をタップしてください



5. 位置情報取得

端末の位置情報を連続して取得するための設定を行います。端末の紛失・盗難時にも有効です。

【位置情報設定有効義務化】

■無線ネットワーク

■GPS機能

位置情報を取得するために必要な端末側の機能の設定を義務化します。上記の項目のいずれか、または、両方にチェックを入れてください。該当の機能がオフに設定されている場合には、設定を要求するポップアップ画面が端末に表示されます。また、OSバージョンにより有効義務化時に要求される設定が異なります。

《OSバージョンによる有効義務化対象設定》

Android OS 8.1まで：位置情報機能の有効化と位置情報モードの選択を義務化します。

無線ネットワーク + GPS機能義務化ON ⇒ 「高精度」を選択

無線ネットワーク義務化のみON ⇒ 「高精度」または「バッテリー節約」を選択

GPS機能義務化のみON ⇒ 「高精度」または「端末のみ」を選択



Android OS 9.0以降：下記設定の有効化を義務化します。

「無線ネットワーク」+「GPS機能」義務化ON ⇒ 「Google位置情報の精度」「位置情報機能」の有効化

「無線ネットワーク」義務化のみON ⇒ 「Google位置情報の精度」の有効化

※ダイアログで有効化要求されるのは「Google位置情報の精度」ですが、「位置情報機能」自体がOFFの場合は「Google位置情報の精度」はONと認識されません。「位置情報機能」も合わせて有効にしてください。

「GPS機能」義務化のみON ⇒ 「位置情報機能」の有効化

＜「Google位置情報の精度」の設定方法＞

①義務化ダイアログで
「OK」をタップ



②位置情報設定画面で
「詳細設定」をタップ



③「Google 位置情報の精度」
をタップ



④「位置情報の精度を
改善」を ON にする



※画像はPixel 3の画面です。機種やAndroid OSバージョンによって画面表示が異なる場合がございます。

・ Android 11以降

「位置情報機能」がOFFの状態では有効義務化のポリシーを適用すると

「アプリに位置情報へのアクセスを許可しました」という通知が表示されます。

正常な動作となりますが、通知は自動では消えないため、必要に応じて手動で削除してください。



【位置情報取得条件】

■位置情報取得間隔(1分／2分／5分／10分)

■位置情報取得期間(n時間)

位置情報取得の頻度と期間を設定します。

※位置情報取得中にポリシーを変更しても、取得中の「取得間隔」と「取得期間」は変更されません。

■「位置情報取得終了後にGPS機能をOFFにする。」

チェックを付けると、位置情報取終了時、または位置情報取得解除時に、GPS機能が自動的にOFFになります。

※ ネットワークからの位置情報取得はOFFになりません。

※ E-SDK 3.0以上の機種にのみ対応しています。

◎位置情報の取得を開始するには？

位置情報の取得を開始するには、「緊急時指示画面」で[位置情報取得指示]をクリックします。サーバからのプッシュ通信*により、即時に位置情報の取得を実施します。

*1:「サーバ端末間通信」のポリシー設定で、Googleプッシュ(GCM/C2DM/FCM)にチェックが入っている必要があります。

※SPPM Agent v2.13以下では、[位置情報取得指示]のクリック後、端末からの定期ポーリング待ちとなります。すぐに位置情報の取得を開始するには、続けて「緊急時指示画面」で[ポリシー即時適用]をクリックしてください。

☞「緊急時指示」>「[位置情報取得指示](#)」

◎取得した位置情報を確認するには？

取得した位置情報は、「端末情報画面」の項目にある「位置情報」で確認します。

☞「[端末情報](#)」

【ドコモ基地局による位置情報取得】

SPPM Agent v2.29から、緊急時位置情報取得時に『ドコモ基地局による位置情報取得機能』が利用できます。

当機能を利用するには下記注意事項があります。

■ドコモ機種のみ対応。

■回線契約、端末APNの設定が『SPモード』時のみ機能します*1

■事前に『SPモード位置情報設定』が必要です。

■GPS・無線ネットワークで位置情報が取得できなかった場合に、当機能で取得した位置情報をSTAR-MDMサーバにアップロードします。

*1 端末がWi-Fi接続中、テザリング中は当機能による位置情報取得はできません。

【SPモード位置情報設定】



① SPPMアプリを起動し、設定メニューまたは端末のナビゲーションキーから『基地局位置情報設定』をタップ*1

② ブラウザを選択し設定ページに遷移

③ SPモード位置情報設定メニューで当機能による利用設定を実行*2

*1 『ドコモ以外の機種』『SPモード未契約』『APNがSPモード以外』『端末がWi-Fi・テザリン設定中』の場合は、『基地局位置情報設定』が表示されません。

*2 ドコモ社により、設定画面が変更される場合があります。

【位置情報の表示】

【位置情報】取得指示が端末に到達しました(1分間隔で1時間)	
地図表示	<pre> 2015-02-27 11:16:03.067, 35.6811, 139.7611, bs, 0.0 2015-02-27 11:15:02.066, 35.6811, 139.7611, bs, 0.0 2015-02-27 11:14:02.094, 35.6811, 139.7611, bs, 0.0 2015-02-27 11:13:02.204, 0.0, START 2015-02-24 14:44:53.503, 0.0, STOP 2015-02-24 14:44:51.889, 35.6811, 139.7611, gps, 150.0 2015-02-24 14:43:51.51, 35.6811, 139.7611, gps, 198.0 2015-02-24 14:42:51.51, 35.6811, 139.7611, network, 2253.0 2015-02-24 14:41:51.51, 35.6811, 139.7611, network </pre>

ドコモ基地局で取得した位置情報は、『bs』と表示されます。

また、精度情報は存在しない為、『0.0』と表示されます。

👉 [「位置情報表示について」](#)

Android Enterprise端末向け設定

【位置情報設定有効義務化】

Android Enterprise端末では位置情報設定の有効を義務化したポリシーを端末に適用すると端末上の位置情報モードがポリシーの設定値に自動設定されます。

※自動設定後手動で設定変更可能ですが、該当の機能がオフに設定されている場合には、通常端末と同様に設定を要求するポップアップ画面が端末に表示されます。

※画像はSO-03Jの画面です。機種やAndroid OSバージョンによって位置情報モードの項目が異なります。

■「無線ネットワーク/GPS機能」両方にチェック

位置情報モードが「高精度」に自動設定されます。

■「無線ネットワーク」のみにチェック

位置情報モードが「電池節約(ネットワークのみ)」に自動設定されます。

■「GPS機能」のみにチェック

位置情報モードが「GPSのみ」に自動設定されます。



6. アプリ配信

Androidアプリのインストール用ファイルである「apkファイル」を端末に配信し、アプリをインストールします。新規アプリのインストールやインストール済みアプリのバージョンアップを、端末を回収することなく実施できます。

Google 社の意向により、以下の条件を“**全て**”満たす端末では、「アプリ配信」ポリシー機能を利用できません。その他、機種やOSにより動作が異なる場合があります。詳細は[こちら](#)です。

- SPPM Agent v3.51 がインストールされている端末
- Android OS 7.0 以降の端末
- Android Enterprise を利用していない端末
- SONY Xperiaシリーズ / Samsung Galaxyシリーズ以外の端末
- ガラホ端末以外の端末

対象アプリのAPIレベル(targetSdkversion)がOSに対応していない場合、エラーが発生し、インストールが実施できません。

アプリ配信

アプリ配信【新規作成】

ポリシー名: 新規作成

※ポリシー名は36文字までです。
☐ 基本ポリシーとして保存する
 (ポリシー名は“基本ポリシー”となります。)

◆OS種別

☒ Android ☐ Windows

※・サーバ通信ボタン押下時のみ配信する。・処理開始日時指定・開始メッセージ再表示間隔はAndroidのみで有効です。※

◆処理実行時の条件指定

配信開始日時指定: yyyy mm dd hh : mm :

☐ サーバ通信ボタン押下時のみ配信する。

処理開始日時指定: yyyy mm dd hh : mm :

処理開始時にメッセージを表示する

☐

開始メッセージ再表示間隔: 秒間隔 (0の場合は再表示されません。)

処理終了後にメッセージを表示する

☐

◆配信ファイル指定 (Max.10)

ファイル指定:

※配信APKは半角英数字ファイル名でアップロードしてください。※
 ※「インストール前表示メッセージ」「配信先」はAndroidのみ有効です。※
 ※SPPM AgentのAPKは本機能で配布できません。Agent管理ポリシーで配信してください。※

【OS種別】

■Android

アプリ配信ポリシーのOS種別を選択します。

Android端末への配信では必ず「Android」を選択して下さい。

【処理実行時の条件指定】

■配信開始日時指定 (n年n月n日n時n分以降のサーバとの通信で配信を開始する)

指定した日時以降のサーバとの通信でアプリファイルをダウンロードします。

空欄の場合はポリシー適用時にアプリファイルをダウンロードします。

■サーバ通信ボタン押下時のみ配信する (SPPM Agent v2.29以降のみ対応)

SPPM Agentメニューの「サーバ通信」ボタン押下時のみ配信されるアプリファイルをダウンロードします。

SPPM Agentが2.29未満の場合は、本設定をしていてもポリシー適用時にアプリファイルをダウンロードします。

■処理開始日時指定 (n年n月n日n時n分以降にダウンロードが完了していた場合に展開処理を開始する)

apkファイルの「配信開始日時」とアプリの「インストール開始日時」をそれぞれ指定できます。これにより、あらかじめアプリの配布だけを済ませておいた上で、決まった日時にインストールを開始することが可能です。サーバと連携するアプリのインストールをサーバ側のバージョンアップ後に定めて実施することができます。

■処理(インストール)開始時にメッセージを表示する

配信アプリインストール開始時に、端末画面にメッセージを表示させることができます。

■開始メッセージ再表示間隔 (SPPM Agent v2.29以降のみ対応)

上記で設定したインストール開始時時のメッセージで、キャンセルを実行した場合の再表示するまでの時間を1秒～3600秒の間で指定できます (端末内部の処理状況で誤差が発生する場合があります)

SPPM Agentが2.29未満の場合は、本設定をしていても5分ごとに再表示がされます (変更できません)

■処理(インストール)終了後にメッセージを表示する

配信アプリインストール完了時に、端末画面にメッセージを表示させることができます。

Android OSの制約上、インストール時には端末に確認メッセージが表示され、ユーザーはインストールをキャンセルすることができますが、ユーザーによりインストールがキャンセルされた場合には、インストールが完了するまで5分ごとに繰り返しインストールを再開します。

【配信ファイル指定】

配信するapkファイルをアップロードして登録します。[ファイルを選択]をクリックしてファイルを指定後、[upload]をクリックするとファイル名が一覧表示されます。最大10個までのapkファイルを登録することができ、登録順にインストールが実施されます。1ファイルあたり最大30MBまでの容量に対応しています。

SPPM Agentのバージョンアップは当機能で行わないでください。必ず『Agent管理』ポリシーでバージョンアップを行ってください。

◆配信ファイル指定 (Max.10)

ファイル指定: 選択されていません

削除	ファイル名/インストール前表示メッセージ
☐	VirusWall.apk 社内開発アプリ

インストールアプリ情報の表示メッセージ(SPPM Agent 2.29以降のみ対応)

☐ 内にメッセージを入力すると、インストール実行前に『アプリ名』『ファイル名』が表示されるアプリ情報画面に表示されます。



配信アプリファイルの削除

☐ チェックをつけて、削除を実行するとアップロードしたアプリファイルを削除できます。



【ポリシー適用時の端末の挙動】

機種やOSバージョン、SPPM Agent バージョンによって、異なる3つの挙動が発生します。

	Android Enterprise	E-SDK、E-API 端末	OS7未満の端末	ガラホ端末	左記以外の端末
3.50未満	通常インストール	サイレントインストール	通常インストール	通常インストール	通常インストール
3.51	サイレントインストール	サイレントインストール	通常インストール	通常インストール	利用不可 ※
3.52以降	サイレントインストール	サイレントインストール	通常インストール	通常インストール	手動インストール

挙動についての詳細は、以下の各リンクよりご確認ください。

- ・[サイレントインストール](#)
- ・[通常インストール](#)
- ・[手動インストール](#)

【サイレントインストール】

アプリ配信を行う端末が「Android Enterprise」「Samsung Galaxy端末(E-SDK対応端末)」および「Sony Xperia端末(E-API対応端末)」の際、下記の場合においてアプリ配信でのアプリインストールをサイレントインストールで行うことができます。

・Android Enterprise の場合

- SPPM Agent v3.51 以降を利用している端末にて、サイレントインストールが可能です。

・Samsung Galaxy端末(E-SDK対応端末)の場合

- SPPM Agent v2.21 以降かつ、E-SDKモジュール v1.1.0 をインストールしている端末にて、サイレントインストールが可能です。
- E-SDK バージョン「4」以降の端末の場合、SPPM Agent v2.29 以降をインストールすることで、自動的にサイレントインストールになります。

☞「[E-SDK 専用モジュールアプリ](#)」

・Sony Xperia端末(E-API対応端末)の場合

- E-API バージョン「7」以降の端末では、SPPM Agent v2.4 以降を利用することでサイレントインストールが可能です。
- E-API バージョン「8」以降の端末では、SPPM Agent v3.06 以降を利用することでサイレントインストールが可能です。

☞「[Sony Xperia E-API](#)」

【通常インストール】

端末側に表示される、アプリのインストールを促すポップアップにて、ユーザが「インストール」を選択することでアプリのインストールが開始されます。

「あとで」を選択した場合は、時間経過ののち、インストールを促すポップアップが再度表示されます。

【手動インストール】

v3.52 以降の SPPM Agent を利用している一部端末の場合、apk ファイルのダウンロードは自動で実施されますが、インストールはユーザにて手動で実施する必要があります。

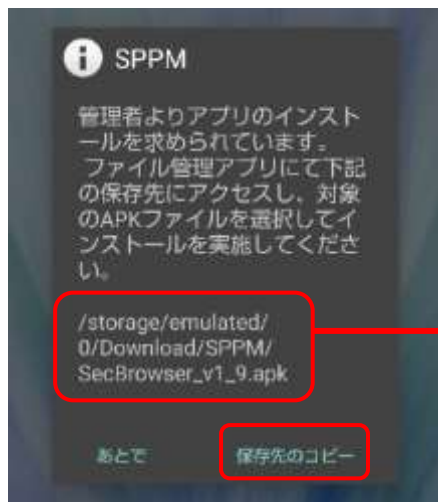
操作イメージは、以下をご確認ください。

※ご利用の端末やファイル管理アプリにより、画面表記が異なります。

※端末によっては、ファイル管理アプリのインストールが必要な場合があります。

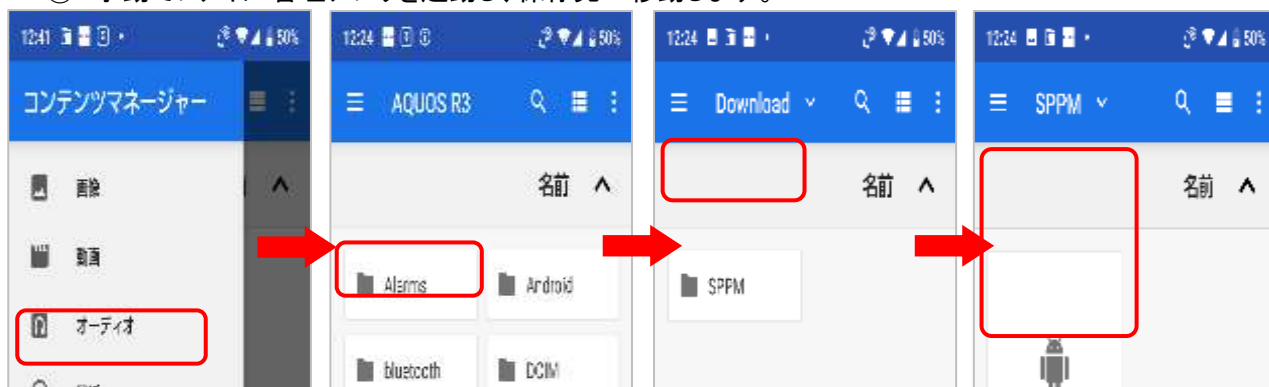
■手動インストールの操作イメージ

- ① 管理画面操作にて、端末にアプリ管理ポリシーを適用します。
- ② 端末に表示された以下のポップアップにて、apkファイルの保存先を確認します。
(「保存先のコピー」をタップすることで、クリップボードに保存先の情報がコピーできます。)



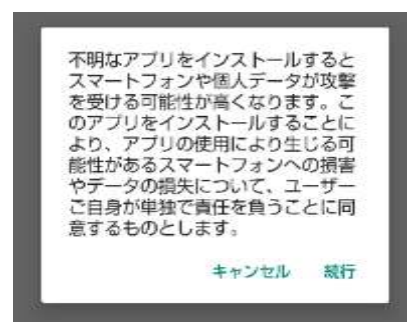
配信された apk ファイルの保存先(パス)が表示されます

- ③ 手動でファイル管理アプリを起動し、保存先へ移動します。



- ④ 提供元不明アプリのインストール許可が必要な場合があります。
許可を促すポップアップが表示された場合は、許可を行ってください。

- ⑤ インストール時、右のようなポップアップが表示される場合、
「続行」をタップしてください。



- ④ 対象の apk ファイルをタップし、インストールを実施します。
- ⑤ 端末側でのアプリインストール完了後、管理画面上でポリシーの反映状態が「反映済み」になります。

【配信アプリのインストールについて】

- ❗ 配信されたアプリインストール時にアプリケーション選択画面が表示された場合は、「パッケージインストーラ」を選択してください。

STAR-MDMでは配信設定されたアプリファイルのダウンロードが全て完了するまで、インストール処理には進みません。

- ❗ 複数アプリの配信時にダウンロード失敗をした場合は、次回サーバ通信時に全てのアプリを再ダウンロードします。

- ❗ インストール時には配信アプリの『アプリ名』『バージョンコード』『バージョン名』をチェックし、インストールすべきアプリを判定します。全て合致するアプリが端末にインストールされている場合は、既にインストールされているアプリと判断して、該当する配信アプリのインストールは行いません。

- ❗ ダウンロードしたアプリファイル(apk)は端末内の指定フォルダに保存されますが、直接apkファイル選択によるインストールや、削除は行わないでください。正常にアプリ配信の処理が完了しない場合があります。

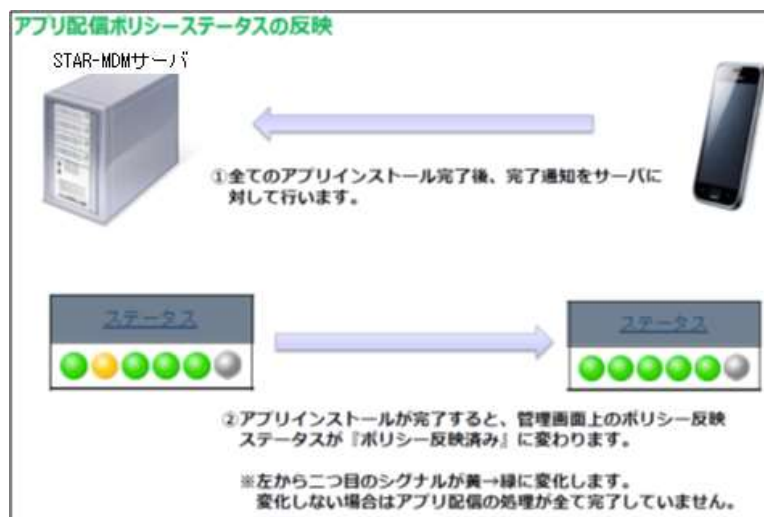
- ❗ 配信したアプリファイルが壊れているなど、問題があった場合はインストールは完了しません。他に配信アプリがある場合には次のアプリのインストールに進みますが、アプリ配信処理は完了しない為、アプリ配信ポリシーのステータスは反映待ち(黄)の状態のままとなります。
その場合は正しいアプリファイルをアップロードしたアプリ配信ポリシーを別途作成し、適用してください。

- ❗ アプリのインストール中は端末の電源を切らないでください。正常に配信が完了しない場合があります。

- ❗ v3.13以降のAgentではapkファイルがダウンロードされた後でも、ポリシーを「未設定」にすることでアプリ配信をキャンセルできます。

- ❗ アプリ配信ポリシーが**非対応の端末に当機能を適用した場合**、アプリの配信が実施されない他、下記の挙動が発生します。
 - ・アプリ配信ポリシーは「反映待ち」のままとなり、ポリシー変更シグナルは「黄色」の状態が継続します。
 - ・「ログ管理」画面にて、「ファイル[アプリ名]のdownloadが完了」「アプリ配信ポリシーが非対応の端末です。」および、「アプリ配信処理が完了しました。」のログが表示されます。
 - ・アプリ配信ポリシー内の「処理開始時にメッセージを表示する」および、「処理終了後にメッセージを表示する」機能にてメッセージを設定している場合、端末上に各メッセージが表示されます。

【配信アプリのステータス/ログ管理について】



アプリ配信ポリシーの反映ステータスは、配信設定をした全てのアプリのインストールが完了した際に、反映済み(緑)に更新されます。

一つでもアプリのインストールが完了していない場合は、反映待ちの状態のままとなります。

管理画面の『ログ管理』ではアプリ配信の処理状況を確認することができます。

ログ管理 - Log管理					
絞り込み 絞り込み解除 前々日のログ					
イベント時刻	電話番号	ログソフト	ログメッセージ	ステータス	受付時間
2015-03-17 18:07:12.240	08022785601	spoonka	アプリ配信処理が完了しました。	INFO	2015-03-17 18:35:44.240
2015-03-17 18:07:03.240	08022785601	spoonka	ファイル[test.apk]は、APKの形式に誤りがありインストールできませんでした。	INFO	2015-03-17 18:35:44.240
2015-03-17 18:00:41.240	08022785601	spoonka	ファイル[VirtualBox.exe]のインストールが完了しました。	INFO	2015-03-17 18:35:44.240
2015-03-17 18:00:39.913	08022785601	server	Internet_VirtualBox がインストールされました。	INFO	2015-03-17 18:00:39.913
2015-03-17 18:00:20.392	08022785601	spoonka	ファイル[VMware-11.0.0.997.Release.apk]は、インストール済みです。	INFO	2015-03-17 18:00:20.392
2015-03-17 18:00:18.392	08022785601	spoonka	ファイル[test.apk]のdownloadが完了。	INFO	2015-03-17 18:00:20.392
2015-03-17 18:00:16.391	08022785601	spoonka	ファイル[VirtualBox.exe]のdownloadが完了。	INFO	2015-03-17 18:00:20.391
2015-03-17 18:00:16.391	08022785601	spoonka	ファイル[VMware-11.0.0.997.Release.apk]のdownloadが完了。	INFO	2015-03-17 18:00:20.391
2015-03-17 18:00:13.39	08022785601	spoonka	SPM Connectでポリシーチェックを実施しました。	INFO	2015-03-17 18:00:20.39
2015-03-17 18:00:13.205	08022785601	server	Connect From device:	INFO	2015-03-17 18:00:13.205
最初へ 前へ 次へ 最後へ					
CSV書き出し					

ログメッセージ例

- ・〇〇のdownloadが完了
- ⇒ 配信設定をしたアプリファイルのダウンロードが完了
- ・〇〇はインストール済みです
- ⇒ 『アプリ名』『バージョンコード』『バージョン名』全てが同じアプリにおいてインストール済みである
- ・〇〇のインストールが完了しました
- ⇒ 配信設定をしたアプリのインストールが完了
- ・〇〇はAPKの形式に誤りがあり、インストールできませんでした
- ⇒ 配信設定をしたアプリファイルに問題がある為、インストールができなかった。

7. 利用アプリ制限

端末の設定メニュー、アプリ利用、アプリのインストールを制限します。

利用アプリ制限(Android) - ポリシー更新画面

利用アプリ制限ポリシー名【新規作成】

ポリシー名:

新規作成

※ポリシー名は64文字までです。

◆参照端末

端末ID

電話番号

機種名

API Level

選択

◆設定メニュー

◆アプリ設定

■SpmHome * AndroidEnterprise非対応

☒ デフォルト設定に指定する
 ☐ 使用しない

■apk展開 (提供元不明のアプリ)

*Android OS 5.0以降ではE-SDK, E-API7以上の機種のみ有効です。

*Android Enterprise非対応。デバイス制御ポリシーから制御できます。

☐ 許可
 ☒ 制限

☐ Google Play Store からのアプリインストールを禁止 *E-SDK機種のみ

■制限対象方式

☒ アプリ一覧にないアプリは全て制限 (ホワイトリスト制御)
 ☐ 許可アプリインストール禁止 *AndroidEnterpriseのみ
 ☐ アプリ一覧にないアプリは全て許可 (ブラックリスト制御)

■無効化/アンインストールを催促する対象を選択 *AndroidEnterprise非対応

☐ 全ての制限対象アプリ
 ☒ 制御チェックありのアプリ

◆制御対象アプリ一覧

許可

全て選択

制御

全て選択

選択アプリを削除

許可	制御	アプリ名	パッケージ名	削除

◆CSV連携

CSVファイルからアプリ一覧を取り込み

登録

【利用アプリ制御ポリシー項目一覧】

項目名	機能概要
7-1. 参照端末	端末の参照方法について
7-2. 設定メニュー	端末の設定メニューの制限について
7-3. アプリ設定	アプリを制限する際の詳細な設定について
7-4. 制御対象アプリ一覧	制限方法と制限方式について
7-5. アプリケーション追加	
7-6. CSV連携	

【参照端末】

端末に標準搭載されているアプリは、機種やOSのバージョンによって異なります。設定メニュー項目も機種により微妙に異なります。したがって、「利用アプリ制限」のポリシーは端末機種とOSごとに作成する必要があります。また、自社開発の業務アプリなど標準搭載以外のアプリを追加したい場合もあります。

そこで、必要なアプリをすべてインストールした参照用端末をまず用意し、STAR-MDM管理サーバに登録してください。

「参照端末」の項目で[選択]をクリックします。

◆参照端末

端末ID: 23456789012345

電話番号

選択 機種名: Nexus 5X

OS: 8.1.0

API Level: 27



「参照端末選択画面」になりますので、参照端末の電話番号または端末IDを入力して[検索]をクリックします。

ポリシー管理 - 利用アプリ制限(Android) - 参照端末選択画面

端末ID、または電話番号を入力してください

123456789012345

検索

選択	端末ID	電話番号	機種名	OS	API LV	備考
該当する端末がありません						



参照端末の「アプリ一覧」を事前に取得しておく必要があります。「アプリ一覧」を取得していないと、該当端末であっても検索結果に表示されません。「アプリ一覧」の操作手順については、該当ページをご参照ください。

👉 関連情報「[アプリ一覧](#)」



検索結果に該当端末が表示されたらラジオボタンで選択し、[設定]をクリックしてください。

ポリシー管理 - 利用アプリ制限(Android) - 参照端末選択画面

端末ID、または電話番号を入力してください

123456789012345

検索

選択	端末ID	電話番号	機種名	OS	API LV	備考
☒	23456789012345		Nexus 5X	8.1.0	27	

戻る 設定

※検索条件と完全一致ではない端末も検索することが可能です。その場合、候補が一覧で表示され、選択可能な端末にはラジオボタンが表示されます。



参照端末の設定メニュー情報とアプリ一覧を取得し、「ポリシー更新画面」に戻ります。

利用アプリ制限(Android) - ポリシー更新画面

利用アプリ制限ポリシー名【テスト】

ポリシー名: 別名保存

※ポリシー名は64文字までです。

◆参照端末

端末ID	123456789012345
電話番号	
機種名	AX-05E
API Level	24

◆設定メニュー

Android OSが3.0以上の場合、残念ながら本機能はご利用いただけません。
下記のアプリ制限にて『設定』アプリを利用不可にすることで、
端末ユーザによるすべての設定変更を禁止できます。

◆アプリ設定

■OpenHome *AndroidEnterprise非対応

☐ デフォルト設定に指定する

☒ 使用しない

■apk展開 (提供元不明のアプリ)

*Android OS 5.0以降ではE-SDK, E-API17以上の機種のみ有効です。
*Android Enterprise非対応。デバイス制約ポリシーから削除できます。

☐ 許可

☒ 制限 ☐ Google Play Store からのアプリインストールを禁止 *E-SDK機種のみ

■制限対象方式

☒ アプリ一覧にないアプリは全て制限 (ホワイトリスト制御)

☐ 許可アプリのみインストール禁止 *AndroidEnterpriseのみ

☐ アプリ一覧にないアプリは全て許可 (ブラックリスト制御)

■無効化/アンインストールを促進する対象を選択 *AndroidEnterprise非対応

☐ 全ての制限対象アプリ ☒ 制約チェックありのアプリ

◆制限対象アプリ一覧

許可 制約

許可	制約	アプリ名	パッケージ名	削除
☒	☐	(ウィジェット)Chrome	com.android.chrome	☐
☐	☒	Chrome	com.android.chrome	☐

★ワンポイント: 参照端末を検索せず、選択プロセスを省略する

「端末情報画面」の「インストールアプリ一覧」に表示された[利用アプリ制限設定作成]ボタンからポリシーを作成すると、参照端末の選択プロセスを省略することができます。

☞「端末情報画面」: [インストールアプリ一覧](#)

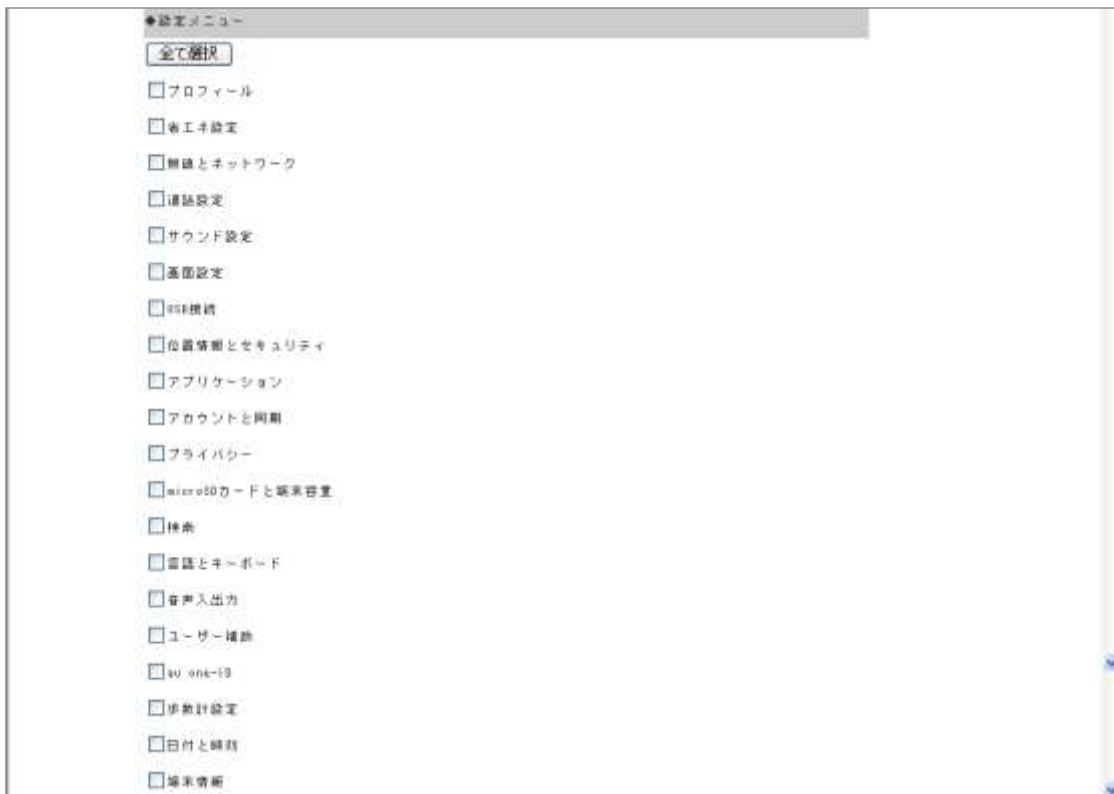
【設定メニュー】

端末の設定画面に表示されるメニュー項目を制限します。ユーザーに利用を許可する設定メニュー項目にはチェックを入れます。チェックを入れた設定メニュー項目は通常通りユーザーが使用できます。**利用を禁止する設定メニュー項目はチェックを外します。**チェックを外した設定メニュー項目は端末に表示されなくなり、ユーザーは利用できなくなります。



本機能は、Android OS v2.2～.2.3のみで有効です。また、「アプリ設定」の項目にて、ホームアプリとして SppmHomeを指定する必要があります。[しない]を選択した場合、端末の設定メニュー項目を制限することはできません。

<設定メニューの表示例>



◎Android OS v3.0以上で設定メニューを制限するには？

「リファレンス端末 アプリ一覧」の項目で「設定アプリ」を利用不可にすることで、端末上からのすべての設定変更を抑止することができます。

【アプリ設定】

◆アプリ設定

■ SppmHome * Android Enterprise非対応

- ☐ デフォルト設定に指定する
☒ 使用しない

■ apk展開 (提供元不明のアプリ)

- * Android OS 5.0以降ではE-SDK, E-API7以上の機種のみ有効です。
 * Android Enterprise非対応。デバイス制御ポリシーから制御できます。

- ☐ 許可
☒ 制限 ☒ Google Play Store からのアプリインストールを禁止 * E-SDK機種のみ

■ 制限対象方式

- ☐ アプリ一覧にないアプリは全て制限 (ホワイトリスト制御)
☐ 許可アプリインストール禁止 * Android Enterpriseのみ
☒ アプリ一覧にないアプリは全て許可 (ブラックリスト制御)

■ 無効化/アンインストールを催促する対象を選択 * Android Enterprise非対応

- ☐ 全ての制限対象アプリ ☒ 制御チェックありのアプリ

■ SppmHome ※Android Enterprise非対応

STAR-MDM専用のホームアプリSppmHomeをデフォルトに指定するよう設定することができ、禁止したアプリはアプリ一覧で非表示になります。

また、ウィジェットもSPPMで許可されたアプリのみ設置可能です。

ホーム画面



アプリ一覧



OS5.0以上では利用アプリ制限ポリシーによってSppmHomeが設定されていると、



アンインストール有効化後もSPPM Agentをアンインストールできません。

※端末設定内のアプリ管理からSppmHomeのデフォルト設定を解除後、アンインストールして下さい。

SppmHomeをデフォルト設定に指定する

ホームアプリのデフォルトをSppmHomeに指定する設定が必要となります。

以下のように設定操作を行ってください。



SppmHome以外のホームアプリをデフォルトに設定している場合には、次の様なメッセージが表示されます。

※E-APIによるデバイス制御の「設定」が制限されていると当メッセージは表示されません。デバイス制御ポリシーを解除するか、「設定」を有効化して下さい。

その際には、以下のように設定操作を行ってください。



■apk 展開(提供元不明のアプリ)

Androidアプリのインストール用ファイルである「apkファイル」の展開を許可するか制限するかを選択します。

* Android OS 5.0以降ではE-SDK, E-API7以上の機種のみ有効です。

* Android Enterprise非対応。デバイス制御ポリシーから制御できます。

許可 : 「apkファイル」の利用が許可されます。

制限 : 「apkファイル」の利用が制限されます。

【apk展開 制限動作】

Android OS 5.0未満

apkファイルを展開時にパッケージ
インストーラー画面がブロックされます。



Galaxy (E-SDK 2.0以上)、Xperia (E-API 7以上)

「提供元不明のアプリ」のインストール許可を
ON にできません。



Google Play Store からのアプリインストールを禁止

Google Play Storeからのアプリインストールを禁止できます。また、「提供元不明のアプリ」のインストール許可をONにできるようになりますが、apkファイル展開後のインストールが禁止されます。

※Galaxy (E-SDK 2.0以上)の端末のみ有効

※制限対象方式が「ブラックリスト制御」の場合は、アプリ一覧外のアプリインストールは許可されます。



■制限対象方式

ポリシー適用後の新規インストールアプリ等の制御対象アプリ一覧に表示されていないアプリを制限対象とするかを選択します。

・アプリ一覧にないアプリは全て制限(ホワイトリスト制御)

「◆制御対象アプリ一覧」に存在しないアプリは全て制限対象となります。

・許可アプリアンインストール禁止

ホワイトリスト制御を選択時にAndroid Enterprise端末のみオプションで選択できます。

上記のホワイトリスト制御に加えて、許可選択されたアプリは全てアンインストールが禁止されます。

通常端末で本項目を選択した場合は「アプリ一覧にないアプリは全部禁止」と同様の動作となります。

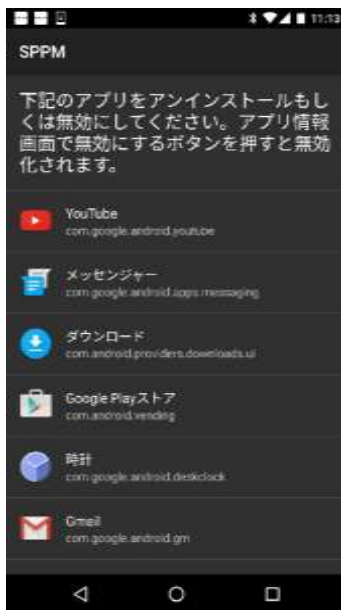
・アプリ一覧にないアプリは全て許可(ブラックリスト制御)

「◆制御対象アプリ一覧」に存在しないアプリは全て許可されます。

■無効化/アンインストールを催促する対象を選択 * Android Enterprise非対応

制限対象としたアプリの無効化/アンインストール催促画面が表示されます。

この催促画面は、表示された対象アプリをタップし、アンインストールまたはアプリ情報画面で無効化するまで、定期的に表示され続けます。



<対象設定>

全ての制限対象アプリ

全ての制限アプリを対象(許可アプリは対象外)

制御チェックありのアプリ

アプリ一覧の「無効」にチェックが入ったアプリと、
ホワイトリスト制御時のアプリ一覧にないアプリを対象



プリインアプリで無効化/アンインストールできないものは対象外となります。

また、無効化/アンインストールできないアプリがもし催促画面に表示された場合は、催促画面が表示されます。管理画面で該当アプリを対象外の設定とするか、弊社までアプリ名・パッケージ名を記載の上お問い合わせ下さい。

【制御対象アプリ一覧】

端末から取得したアプリ一覧が表示されます。チェックボックスにて、利用許可アプリを選択します。

◆制御対象アプリ一覧

許可
制御

許可	制御	アプリ名	パッケージ名	削除
☐	☐	(ウィジェット)Chrome Chrome	com.android.chrome	☐
☐	☐	(ウィジェット)Eメール Eメール	com.sonymobile.email	☐
☐	☐	(ウィジェット)Gmail Gmail	com.google.android.gm	☐
☐	☐	(ウィジェット)Google Google	com.google.android.googlequicksearchbox	☐
☐	☐	(ウィジェット)Google Play Music Play Music	com.google.android.music	☐
☐	☐	(ウィジェット)NFCサービス	com.android.nfc	☐
☐	☐	(ウィジェット)What's New What's New	com.sonymobile.entrance	☐
☐	☐	(ウィジェット)アシスト	com.sonymobile.assist	☐
☐	☐	(ウィジェット)カレンダー カレンダー	com.google.android.calendar	☐
☐	☐	(ウィジェット)スケジュール&メモ スケジュール メモ	com.nttdocomo.android.schedullememo	☐
☐	☐	(ウィジェット)ドコモメール ドコモメール	jp.co.nttdocomo.carriermail	☐
☐	☐	(ウィジェット)ドライブ ドライブ	com.google.android.apps.docs	☐
☐	☐	(ウィジェット)ミュージック ミュージック	com.sonyericsson.music	☐
☐	☐	(ウィジェット)時計ウィジェット	com.sonyericsson.advancedwidget.clock	☐
☐	☐	Facebook	com.facebook.katana	☐
☐	☐	File Commander	com.mobisystems.fileman	☐
☐	☐	Hangouts	com.google.android.talk	☐

■許可

許可するアプリをチェックボックスで選択します。

■制御

制御対象となったアプリに対する挙動を選択します。

通常端末とAndroid Enterprise端末では「制御」チェックボックスの動作が異なるため、各チェックボックスの組み合わせによる動作内容は次項以降を参照してください。

※「許可」にチェックが入っている場合、「制御」のチェックボックスはグレーアウトします。

グレーアウト状態でもチェックの値は保持されますが動作は行われません。

■削除

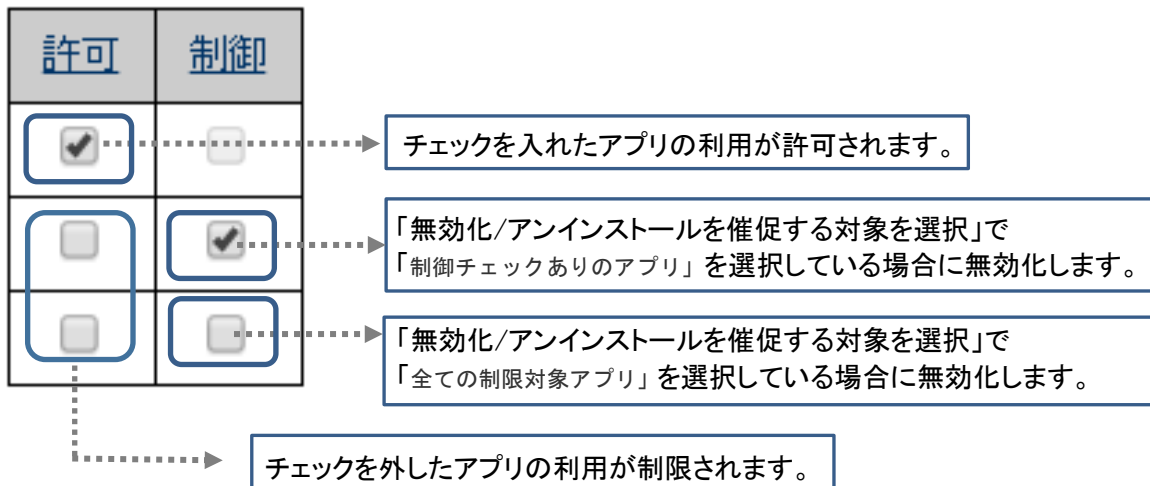
「削除」チェックボックスにチェックを入れて「選択アプリを削除」をクリックすることで、一覧からアプリを削除することができます。

【通常端末】

■制限方法（許可/制御チェック動作）

通常端末では、「許可」のチェックボックスでアプリの利用許可または制限を選択します。

また、「制御」のチェックボックスでは「無効化/アンインストールの催促対象」を選択します。



■制限の種類

《ブロック画面制限》

アプリを起動するとブロック画面が表示され、該当アプリの操作が不可になります。

※バックグラウンドの動作制御はできません。



Sumsung Galaxy シリーズ/ Sony Xperia シリーズの端末については、E-SDK/E-API 機能を利用して



禁止されたアプリを SPPM Home を利用せずに、端末上で非表示にできます。

※SPPM Agent v2.28.2以上でご利用いただけます。

※Xperiaシリーズでは『ドコモ電話帳』『電話』『dマーケット』など一部アプリは非表示対象外です。

◎Android OS5.1.1 以上の端末では、ポリシー適用後にアプリ情報への権限設定が必要です。

Android OS5.1.1以上の端末では、利用アプリ制限ポリシーを適用すると権限催促画面が表示されます。
以下の画面で操作を行い、SPPMの「使用履歴へのアクセス」権限をONにしてください。

※OS5.1.1未満の端末であってもソフトウェアバージョンアップによってこの操作が必要になる場合があります。



【Android Enterprise(Work Managed Device)端末】

■制限方法（許可/制御チェック動作）

Android Enterprise(Work Managed Device)端末では、「許可」のチェックを外し制限対象となったアプリの制限方法を「制御」のチェック有無により選択することができます。

※SPPM Agent v3.27.1未満では「制御」チェックに関わらずHidden制御方式となります。

許可	制御	
☒	☐	チェックを入れたアプリの利用が許可されます。
☐	☒	アプリの利用が「Suspend 制御方式」で制限されます。
☐	☐	アプリの利用が「Hidden 制御方式」で制限されます。

■制限の種類

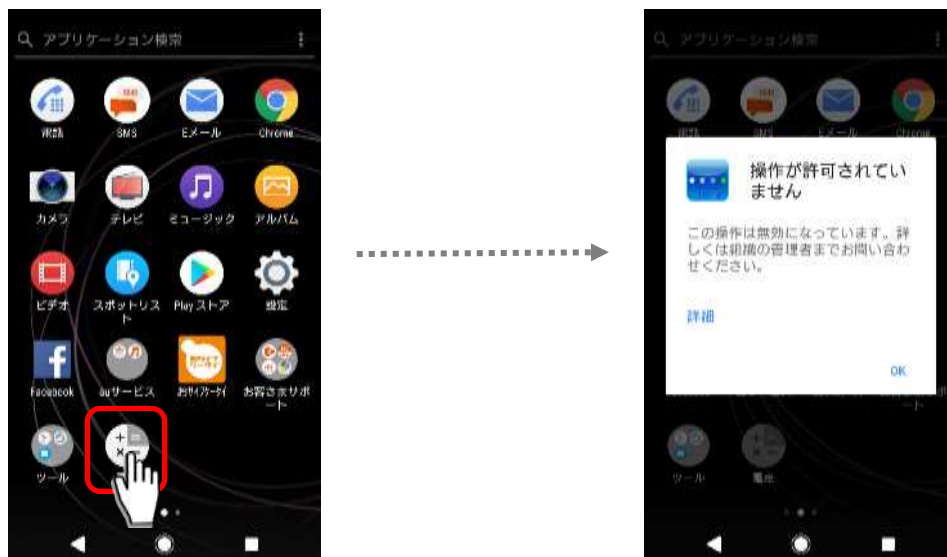
《Suspend 制御方式》

Suspend制御では、アプリをタップするとすると利用制限ポップアップが表示され、起動が制御されます。また、ウィジェットやバックグラウンドでの動作も制御されます。

※ホームアプリによってはSuspend制御時にアプリアイコンがグレーアウト表示になります。

※SPPM Agent v3.27.1以降/Android OS 7.0以降でご利用いただけます。

※Android OS 7.0未満の場合はSuspend制御方式指定時はブロック画面制限となります。



《Hidden 制御方式》

Hidden制御では、アプリアイコンが非表示になりアンインストール削除と同等の状態になります。

※Hidden制限ではアプリによって稀に削除と追加が繰り返される事象を確認しております。

電池消費過多に陥る可能性もあるため、事象発生時はSuspend制限への切り替えをお願いします。



《指定した制御方式と動作が異なるアプリについて》

一部のアプリではSuspend/Hidden制御方式が非対応のため「制御」チェックボックスにより指定した制御方式と異なる制御動作となります。

	制御チェックあり (Suspend指定)	制御チェックなし (Hidden指定)
設定	Suspend	Suspend
通話アプリ	ブロック画面	Hidden
Google Play	ブロック画面	ブロック画面
Chrome	Suspend	Android OS 7.0: Hidden Android OS 8.0: Suspend
ホームアプリ	Hidden/ブロック画面	Hidden/ブロック画面
ウィジェットのみ	Suspend	Suspend

※ SPPM Agent v3.27.1未満ではGooglePlayはHidden制御されます。

※ ホームアプリにより制限方式が異なります。

※ 「ウィジェットのみ」のアプリとはアプリランチャーにアプリアイコンが存在せず、ウィジェットのみ利用できるアプリを指します。

【アプリケーション追加】

アプリ名とパッケージ名を入力することで、任意のアプリケーションをリファレンス端末アプリ一覧に追加することができます。

- ① アプリケーション追加機能を利用するには、まず参照端末を選択してください。

参照端末が選択されていない場合、本機能はご利用になれません。

- ② アプリ名とパッケージ名を入力し、「追加」をクリックしてください。

字数について

アプリ名: 50 字以内で記入してください

パッケージ名: 250 字以内で記入してください

利用可能な文字種について

アプリ名: 「”(ダブルクォーテーション)”および機種依存文字は入力できません。

パッケージ名: 半角英数字および「.(ピリオド)」「_(アンダーバー)」のみで記入してください。

※追加されたアプリは、アプリ名でソートされてアプリ一覧内に表示されます。

※リファレンス端末を選択しなおすと、追加したアプリの情報はリセットされます。

【CSV連携】

「アプリ一覧と制限設定」を CSV ファイルで書き出すことができます。また、管理者が編集した CSV ファイルを読み込むことで、「アプリ一覧と制限設定」を一括して更新できます。

<操作手順>

- ①「アプリ一覧をCSVで書き出し」ボタン押下でCSVデータをダウンロードします。
- ②ダウンロードした CSV を編集し「CSV ファイルからアプリ一覧を取り込み」でファイルをアップロードし登録を押下します。

❗ 「制限」、「許可」の列は「0」または「1」のどちらかの値を入力してください。 1=選択 0=未選択

8. アプリ一覧

端末にインストールされているアプリの一覧を作成します。

アプリ一覧

アプリ一覧【新規作成】
 ポリシー名: 新規作成

※ポリシー名は64文字までです。

☐ 基本ポリシーとして保存する
 (ポリシー名は”基本ポリシー”となります。)

- Android

◆アプリ一覧取得設定

☐ アプリ一覧取得を行う（アプリ増減および更新時に再取得）

☐ アプリ一覧に変化があった場合に管理者にメールを送信する

☐ すべてのステータスをまとめて送信
☐ ステータス別に送信

☐ インストール
☐ アップデート
☐ アンインストール

☐ アプリ一覧に変化があった場合に利用者にメールを送信する

☐ すべてのステータスをまとめて送信
☐ ステータス別に送信

☐ インストール
☐ アップデート
☐ アンインストール

本ポリシーが端末に適用されると初期状態として、その時点のアプリ一覧を取得します。
 初期状態を取得した以降は、アプリ一覧に変化があった場合に一覧を取得します。

※Android Enterpriseをご利用の場合、アプリ一覧変化によるメール送信機能は非対応です。

【アプリ一覧取得設定】

■アプリ一覧取得を行う（アプリ増減および更新時に再取得）

端末にインストールされているアプリの一覧を取得します。ポリシー適用時点での取得以降は、アプリの追加、アプリの削除、アプリの更新をそれぞれ検知したタイミングで、アプリ一覧を再取得します。

■アプリ一覧に変化があった場合に管理者にメールを送信する

■アプリ一覧に変化があった場合に利用者にメールを送信する

アプリ一覧に変化があった場合には、管理者とユーザーそれぞれに通知メールを送信することができます。通知メールの内容は、ポリシーの新規作成後に表示される[編集]をクリックすることで編集できます。

「管理者にメールを送信」では、登録されている管理者全員のメールアドレスに、「利用者にメールを送信」では、当該端末の利用者情報に登録されているメールアドレスに、それぞれ通知メールを送信します。

143

■すべてのステータスをまとめて送信

アプリの追加、アプリの削除、アプリの更新が行われた場合に通知メールが送信されます。

■ステータス別に送信

アプリの追加、アプリの削除、アプリの更新が行われた場合にチェックされたステータスのみ通知メールが送信されます。

例) インストールのみチェックを入れている場合はインストール時のみ通知メールが送信されます。

◎取得したアプリ一覧を閲覧するには？

取得したアプリ一覧は、「端末情報画面」に「インストールアプリ一覧」として表示されます。

☞「「端末情報画面」:[インストールアプリ一覧](#)」



Android Enterprise をご利用の場合、アプリ一覧変化によるメール送信機能は非対応です。

9. APN固定化

APN(Access Point Name)を固定し、本ポリシー適用時のAPN設定から変更できないようにします。



本機能は、Android OS v4.1以下で有効です。

【APN固定化】

■利用APNを固定する

APNの固定化を実施します。

※Android OSのバージョンにより制御が異なりますのでご注意ください。

＜Android OS v4.0未満の場合＞

端末にポリシーが適用された時点で端末が選択していたAPNに固定されます。(その後、端末が他のAPNを選択しても、固定化されたAPNに強制的に戻します)

＜Android OS v4.0以上の場合＞

端末にポリシーが適用された時点で端末が選択していたAPNを記録し、差異が発生した時点で端末に警告画面を表示して元のAPNに戻すよう促します。

＜Android OS v4.2以上の場合＞

APNの変更検知が出来ない為、Android OS v4.2以降では、端末のAPN設定が変更されたときに警告画面が表示されません。

【APN削除時の動作】

■ユーザーに作成を催促する

■警告画面を表示する

APNを削除した時の動作として、上記のいずれかを選択します。「ユーザーに作成を催促する」では、設定されていたAPN情報を警告画面で端末に表示します。「警告画面を表示する」を選択した場合は、入力欄が表示されますので、端末に表示させる任意の警告メッセージを入力してください。

【APN固定化失敗の検知】

■管理者への通知(利用する)

■ユーザーへの警告(利用する)

APN固定化の失敗を検知した場合の処理として、通知メールの送信を設定することができます。必要な項目にチェックを入れると、それぞれの通知メール用の件名・本文の入力欄が表示されます。

「管理者への通知」では、登録されている管理者全員のメールアドレスに、「ユーザーへの警告」では、当該端末の利用者情報に登録されているメールアドレスに、それぞれ通知メールを送信します。

◎端末でAPNを確認する方法

「メニュー」→「設定」→「無線とネットワーク」→「モバイルネットワーク」→「アクセスポイント名」で確認できます。
※端末の仕様によって異なります。

10. Wi-Fi接続先制限

許可したWi-Fiアクセスポイントにしか端末が接続できないよう設定します。

【Wi-Fi接続許可リスト】

接続を許可するWi-FiアクセスポイントのSSID、BSSIDのリストをCSVファイルでアップロードして登録します。[参照]をクリックしてファイルを指定後、[upload]をクリックすると、SSID、BSSIDが一覧表示されます。

※最大設定可能数は1,000件までです。

※SSIDは必須項目です。

※BSSIDの指定がない場合はSSIDが一致する接続先に接続可能です。

※BSSIDはWi-FiアクセスポイントのMACアドレスで省略可能です。

リスト作成時は下記のように、一行につき一つSSIDもしくはBSSIDを記載したファイルを作成してください。

【リスト作成例】

SSID-1 [改行]

SSID-2, BSSID-1 [改行] *1

*1 BSSID を登録する場合は、SSID の後ろにカンマで分けて 1 行で登録してください。

SSID、BSSIDリストを編集する場合は、CSVデータにて実施の上、再度ファイルをアップロードし直してください。

11. 接続先URL制限

STAR-MDM専用のブラウザ「SecBrowser」を利用して、ユーザーが閲覧できるWebサイトを制限します。

※「SecBrowser」はAndroid 11以降は、非対応となります。

Android Enterpriseの「ChromeアプリのURLアクセス制限」機能をご利用ください。

詳細は「Android Enterpriseマニュアル」をご確認ください。

ポリシー管理 - 接続先URL制限ポリシー - ポリシー作成画面

接続先URL制限ポリシー名【新規作成】 新規作成

※ポリシー名は64文字までです。

◆登録事項

■本機能は SecBrowser をインストールしている端末でのみ実効です。

※※ Blacklistを含む新しいポリシーは SPFM Agent v2.07 と SecBrowser v1.3以上の組み合わせで動作いたします。

■Whitelistの登録は下記形式のファイルで実施してください。

＜ファイル形式＞
"URL", "サイト名称"
例) "http://www.sxseed.co.jp/", "SXSEED"

■Blacklistの登録は下記形式のファイルで実施してください。

＜ファイル形式＞
"URL"
例) "http://www.sxseed.co.jp"

■ブックマークの登録は下記形式のファイルで実施してください。

＜ファイル形式＞
"URL", "サイト名称"
例) "http://www.sxseed.co.jp/", "SXSEED"

◆ホームページURL

◆Whitelist(最大500件)

参照 upload

Whitelist未登録

※※ Whitelist一覧 ※※

※長いURLは自動的に省略されます。

◆Blacklist(最大500件)

参照 upload

Blacklist未登録

※※ Blacklist一覧 ※※

11-1. 本機能の利用条件

■端末に「SecBrowser」をインストールしてください

本機能をご利用になるには、対象の端末にSTAR-MDM専用のブラウザアプリ「SecBrowser」をインストールする必要があります。

- ・SPPM Agentがv2.06以下の場合、SecBrowserはv1.2以下を利用してください。

※SecBrowser v1.2以下では、ホワイトリストのみが利用可能です。

- ・SPPM Agentがv2.07以上の場合、SecBrowserはv1.3以上を利用してください。

※SecBrowser v1.3以上では、ホワイトリスト、ブラックリスト、ブックマークリストのすべてが利用可能です。

＜SecBrowserのダウンロード及び配信＞

SecBrowserは「接続先URL制限ポリシー 一覧」画面（「ポリシー管理」画面から[接続先URL制限]をクリックした最初の画面）にてダウンロード可能です。管理者のPCに一旦保存の上、SecBrowserのapkファイルを「アプリ配信」機能を用いて対象端末にリモートインストールしてください。

※GooglePlayからのインストールも可能です。

関連項目 ➡ [「アプリ配信」](#)



SecBrowserはSPPM Agentとは別のアプリです。SPPM Agentが端末にインストール済みであっても、SecBrowserはインストールされていません。



SecBrowserではクライアント証明書が必要となるWEBサイトは非対応となります。

■ブラウザアプリの利用許可を「SecBrowser」のみにしてください

本機能は、ブラウザアプリにSecBrowserを利用することで閲覧URLの制限を実現します。「利用アプリ制限」ポリシーで他のブラウザアプリを利用禁止にし、ブラウザアプリはSecBrowserのみを利用許可に設定してください。

関連項目 ➡ [「利用アプリ制限」](#)

■URLリストを登録してください

URLリストを登録したポリシーを適用することでSecBrowserでのWebブラウズが可能になります。

11-2. 設定手順

【URLリストを用意】

《ホワイトリスト》

接続を許可するURLのリストを、CSV形式のテキストファイル(拡張子.txt)で用意します。

※最大設定可能数は500件までです。

- ・書式: “URL”, “サイト名称”

※文字列を” ”で括り、カンマで区切ってください。

- ・例: “http://www.starnet.ad.jp/”, “STARNET”

◎ホワイトリストは、登録したパス以下の階層への接続をすべて許可します

例1) ホワイトリストに `http://www.starnet.ad.jp/` を登録した場合、

接続を許可されるのは `http://www.starnet.ad.jp/` のサイト内すべてが対象となります。

<code>http://www.starnet.ad.jp/</code>	⇒ ○
<code>http://www.starnet.ad.jp/folder-A/folder-1/</code>	⇒ ○
<code>http://www.starnet.ad.jp/folder-A/folder-2/</code>	⇒ ○
<code>http://www.starnet.ad.jp/folder-B/folder-1/</code>	⇒ ○
<code>http://www.starnet.ad.jp/folder-B/folder-2/</code>	⇒ ○

例2) ホワイトリストに `http://www.starnet.ad.jp/folder-A/` を登録した場合、

接続を許可されるのは `http://www.starnet.ad.jp/folder-A/` 以下の階層のみが対象となります。

<code>http://www.starnet.ad.jp/</code>	⇒ ×
<code>http://www.starnet.ad.jp/folder-A/folder-1/</code>	⇒ ○
<code>http://www.starnet.ad.jp/folder-A/folder-2/</code>	⇒ ○
<code>http://www.starnet.ad.jp/folder-B/folder-1/</code>	⇒ ×
<code>http://www.starnet.ad.jp/folder-B/folder-2/</code>	⇒ ×

☆ワンポイント: GmailをSecBrowserで利用するには？

`https://mail.google.com/` のみならず、`https://www.google.co.jp/` `https://accounts.google.com/` の2つもホワイトリストに登録しておく必要があります。

《ブラックリスト》 ※SecBrowser v1.3以上で有効

接続を禁止するURLのリストをCSV形式のテキストファイル(拡張子.txt)で用意します。

※最大設定可能数は500件までです。

・書式: "URL"

※文字列を"で括ってください。

※ブラックリストに必要なのはURLのみです。

・例: "http://www.starnet.ad.jp/"

◎ブラックリストは、登録したパス以下の階層への接続をすべて禁止します

例1) ブラックリストに `http://www.starnet.ad.jp/` を登録した場合、

接続を禁止されるのは、`http://www.starnet.ad.jp/` のサイト内すべてが対象となります。

<code>http://www.starnet.ad.jp/</code>	⇒ ×
<code>http://www.starnet.ad.jp/folder-A/folder-1/</code>	⇒ ×
<code>http://www.starnet.ad.jp/folder-A/folder-2/</code>	⇒ ×
<code>http://www.starnet.ad.jp/folder-B/folder-1/</code>	⇒ ×
<code>http://www.starnet.ad.jp/folder-B/folder-2/</code>	⇒ ×

例2) ブラックリストに `http://www.starnet.ad.jp/folder-A/` を登録した場合、

接続を禁止されるのは `http://www.starnet.ad.jp/folder-A/` 以下の階層のみが対象となります。

<code>http://www.starnet.ad.jp/</code>	⇒ ○
<code>http://www.starnet.ad.jp/folder-A/folder-1/</code>	⇒ ×
<code>http://www.starnet.ad.jp/folder-A/folder-2/</code>	⇒ ×
<code>http://www.starnet.ad.jp/folder-B/folder-1/</code>	⇒ ○
<code>http://www.starnet.ad.jp/folder-B/folder-2/</code>	⇒ ○

☆ワンポイント:ホワイトリストでの運用にブラックリストを併用

ホワイトリストでの運用を基本としている中で、接続を許可しているWebサイトの特定階層のみを接続禁止にする必要性が発生したとします。その場合、ホワイトリストのURLはそのままに、接続を禁止したい特定階層のURLをブラックリストに追加します。

例) ホワイトリストの `http://www.starnet.ad.jp/` はそのままに、
接続を禁止したい `http://www.starnet.ad.jp/folder1/` をブラックリストに登録。

《ブックマークリスト》 ※SecBrowser v1.3以上で有効

ブックマークに登録するURLのリストをCSV形式のテキストファイル(拡張子:.txt)で用意します。

※最大設定可能数は500件までです。

・書式: "URL","サイト名称"

※文字列を" "で括り、カンマで区切ってください。

・例: "http://www.starnet.ad.jp/","STARNET"



ホワイトリストもしくはブラックリストのどちらも登録されていない場合、ブックマークを登録してもブックマーク先への接続はできません。また、ホワイトリストを登録して利用する場合には、ブックマークのURLもホワイトリストに含まれている必要があります。

【URLリストを登録】

■ホームページURL

SecBrowserの起動時に表示させるWebサイトのURLを登録することができます。空欄の場合、SecBrowserの起動時には空白のページが表示されます。

※ホワイトリストでの運用の場合、ここで設定するURLは接続許可の対象に入っている必要があります。

■White List(最大500件)

■Black List(最大500件)

■ブックマーク(最大500件)

それぞれのURLリスト(CSVテキストファイル)をアップロードして登録します。[参照]をクリックしてファイルを指定後、[upload]をクリックすると、URLが一覧表示されます。

URLリストを編集する場合は、CSVテキストデータにて実施の上、再度ファイルをアップロードし直してください。

◆Whitelist(最大500件)

URLホワイトリスト.txt

変更 uploaded 削除

※※ Whitelist一覧 ※※

URL	http://www.xxseed.co.jp/
サイト名称	ASSEED
URL	https://androider.jp/
サイト名称	アンドロイダー
URL	http://isora.jp/
サイト名称	ルクレ
URL	http://www.ad-fis.co.jp/

※長いURLは自動的に省略されます。

◆Blacklist(最大500件)

URLブラックリスト.txt

変更 uploaded 削除

※※ Blacklist一覧 ※※

サーバ名称	* https://www.xxseed.co.jp/form/contact/ *
サーバ名称	* http://www.ad-fis.co.jp/advertising/ *

※長いURLは自動的に省略されます。

◆ブックマーク(最大500件)

ブックマークURLリスト.txt

変更 uploaded 削除

※※ ブックマーカー一覧 ※※

URL	http://www.xxseed.co.jp/
サイト名称	ASSEED
URL	https://androider.jp/
サイト名称	アンドロイダー
URL	http://isora.jp/
サイト名称	ルクレ
URL	http://www.ad-fis.co.jp/

※長いURLは自動的に省略されます。

11-3. SecBrowserの操作

※SecBrowser v1.8を例に説明します。

■起動方法

- ①アプリ一覧にある「SecBrowser」アイコンをタップします。
- ②SecBrowserが起動し、ホームページURLが設定されている場合には当該のWebページが表示されます。
(スクリーンショットの例では株式会社STARNETのトップページを設定しています)

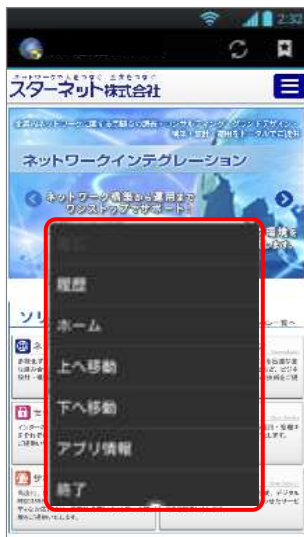
※ホームページURLが設定されていない場合は、空白のページが表示されます。

関連項目⇒「[ホームページURL](#)」



■メニュー表示

端末のメニューボタンをタップすると、SecBrowserのメニューが表示されます。

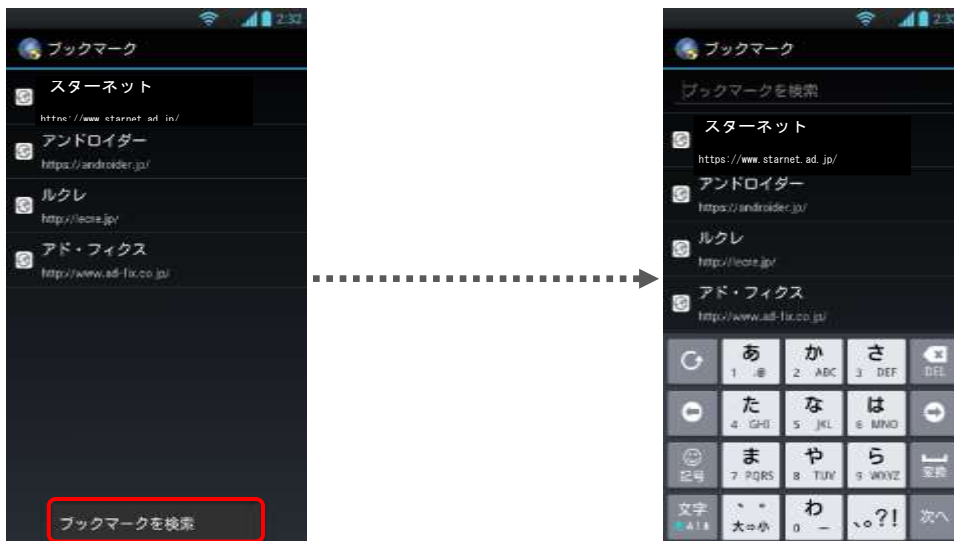


■ブックマーク

ブックマークのアイコンをタップすると、ブックマーカー一覧が表示されます。



ブックマーカー一覧が表示中に端末のメニューボタンをタップすると、[ブックマークを検索]が表示されます。[ブックマークを検索]をタップするとブックマークを検索することができます。



■ファイルダウンロード ※SecBrowser v1.4以上で有効

ダウンロードしたファイルは、アプリトレイにある「ダウンロード」アイコンをタップすると閲覧できます。

※SecBrowser専用のアイコンです。SecBrowserをインストールすると同時に作成されます。



12. ファイル配布

任意のファイルを端末の保存先フォルダを指定して配布します。

【同名ファイルが存在した場合の処理】

■無条件に上書き

■既存ファイル名を変更して保存

保存先フォルダに同名ファイルが存在する場合の処理方法として、上書き保存するか、既存ファイルに番号を付けてファイル名を変更してから保存するかを選択します。

【配布ファイル管理】

配布するファイルをアップロードして登録します。[参照]をクリックしてファイルを指定後、[追加]をクリックするとファイル名が一覧表示されます。最大20個までのファイルを登録することができ、1ファイルあたり最大30MBまでの容量に対応しています。

STAR-MDMで配信可能なファイル(拡張子)に制限はありません。

《保存先フォルダ(内部拡張メモリ搭載機種はSDカード指定はできません)》

端末の保存先フォルダを指定します。保存先フォルダをUNIX系のパス記述で入力してください。保存先フォルダは内部拡張メモリ(一部機種ではSDカード指定も可能)に限られます。

指定したフォルダが端末側に無い場合は、フォルダが自動で作成されます。

※OS10以降の場合、ファイルの保存およびフォルダの作成は SPPM Agent のローカルストレージ内にて実行されます。(「/ファイル配布テスト」を保存先フォルダに指定した場合、SPPM Agent のローカルストレージ内に「ファイル配布テスト」という名前のフォルダが、自動で作成されます。)

※OS11以降かつ v3.60.5以降の場合「ファイルへのアクセス」の権限を許可することによって、内部拡張メモリにファイルの保存およびフォルダが作成されます。権限を有効にしない場合は、従来の OS10以降の場合と同じ動作になります。

例)topの下 docs の中の man に配布ファイルを保存する場合。

/docs/man

※Windowsのパス記述 例)¥docs¥man は利用できません。

※保存ファイル名は登録ファイル名となり、変更することはできません。

【通知メール設定】

ユーザー(当該端末の利用者情報に登録されているメールアドレス)に通知メールを送信する場合は、件名と本文を入力します。

12-1. OS10以降におけるファイル配布の仕様

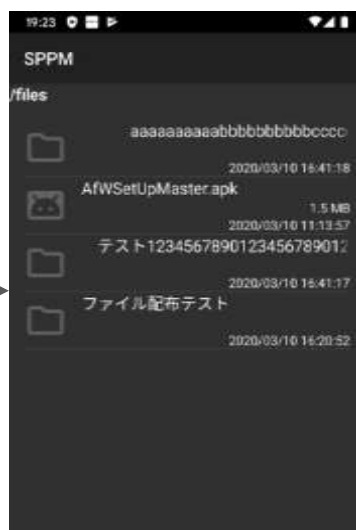
OS 側の仕様変更により、OS10 以降の端末では配布したファイルが SPPM Agent のローカルストレージに保存されます。※OS10 未満の端末では、指定した保存先フォルダにファイルを配布し保存します。

※OS11 以降かつ v3.60.5 以降の場合、「すべてのファイルへのアクセス」を許可することによって、内部拡張メモリにファイルの保存およびフォルダが作成されます。権限を有効にしない場合は、従来の OS10 以降の場合と同じ動作になります。

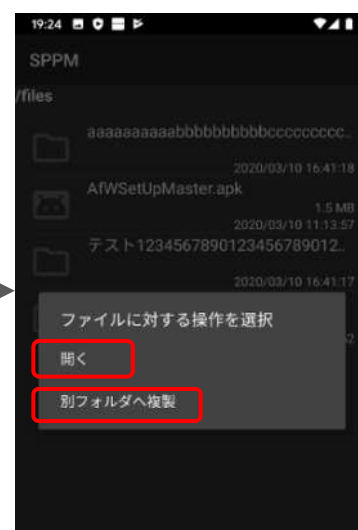
また、ローカルストレージに保存されたファイルは SPPM Agent の「ファイル」にて閲覧できます。



- ① 「ファイル」をタップします。
(OS10 以降の端末のみ表示されます。)



- ② 目的のファイル名または、
フォルダ名をタップします。
(ファイル名が長い場合は、
自動でスクロールします。)



- ③ 「開く」または「別フォルダへ複製」
をタップします。

■「開く」を選択時の端末の挙動

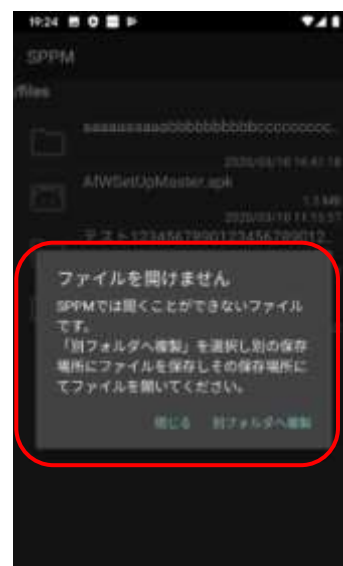
《開くことができるファイルの場合》

目的のファイルが SPPM Agent 経由にて
開く事が可能な場合、ビューワーが表示されます。



《開くことができないファイルの場合》

目的のファイルが SPPM Agent 経由にて開く事が
できない場合、以下のポップアップが表示されます。



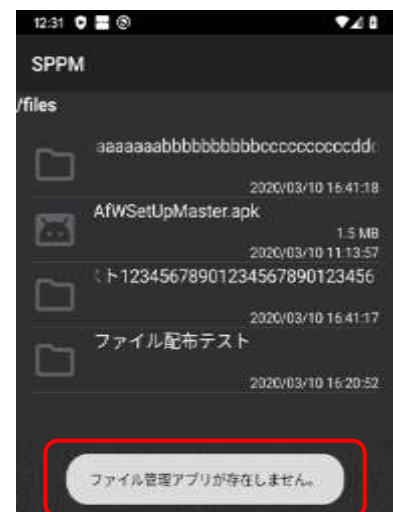
■「別フォルダへ複製」を選択時の端末の挙動

ファイル管理アプリに目的のアプリを複製します。複製時、ファイル名を変更もしくはフォルダを作成し、そのフォルダ内に目的のファイルを保存できます。

ダウンロードフォルダ以外にもファイルを保存する事ができます。



ファイル管理アプリが端末に無い、または「利用アプリ制限」ポリシーによって制限されている場合は、以下のメッセージが表示されます。

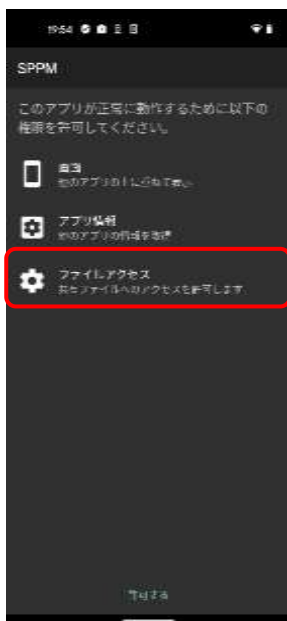


12-2. OS11以降かつv3.60.5以降におけるファイル配布の仕様

仕様変更により、OS11以降かつv3.60.5以降の端末は「すべてのファイルへのアクセス」を許可することによって、内部拡張メモリにファイルの保存およびフォルダが作成されます。権限を有効にしない場合は、従来のOS10以降の場合と同じ動作になります。

「すべてのファイルへのアクセス」は、初回キットング時または Agent のバージョンアップ時に求められます。

■初回キットング時の権限許可方法



初回キットング時、「ファイルアクセス」の権限を許可してください。

■Agent バージョンアップ時の権限許可方法



①「通知をタップして権限を許可してください。」をタップします。



②SPPM をタップします。



③「すべてのファイルへのアクセスを許可」の権限を ON にします。

■Agent バージョンアップ時の権限拒否方法

「すべてのファイルへのアクセス」の権限を拒否(許可しない)ことが可能です。



①「^」をタップすると「キャンセル」ボタンが表示されるため、タップします。

※端末によって操作方法が異なる場合があります。

②「通知を表示」を OFF にすると、権限の許可催促通知が非表示になります。

13. Wi-Fi設定

端末に対するWi-Fiアクセスポイントの接続設定を行います。



以下の場合、端末内の Wi-Fi AP 情報を一度削除のうえ、変更する必要があります。

- OS9で配信したWi-Fi AP の情報をOS10以降にバージョンアップし、変更する場合。
- OS10の端末に手動で登録した「デバイスMacアドレスを利用する」が有効となっている Wi-Fi AP情報を利用して変更する場合。

Wi-Fi 設定

Wi-Fi 設定名 : 新規作成

☐ 基本ポリシーとして保存する
(ポリシー名は”基本ポリシー”となります。)

本ポリシーで端末に設定したい Wi-Fi AP を登録します。

Wi-Fi AP 選択 Wi-Fi AP 作成

☒ 登録 ☐ 削除

Wi-Fi AP 解除	Wi-Fi AP 名
<現在登録されているWi-Fi AP はありません。>	

元に戻す 戻る 新規作成

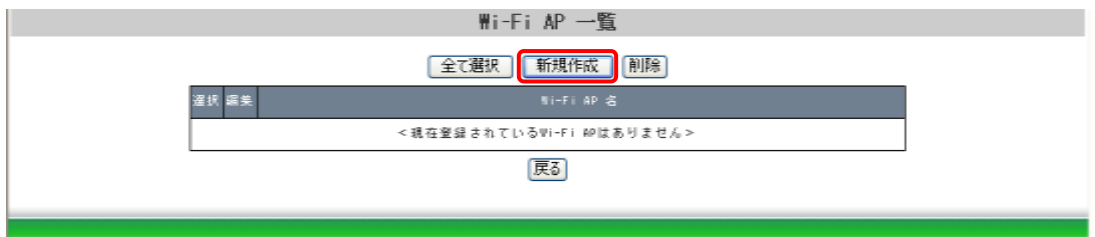
13-1. Wi-Fiアクセスポイントの登録手順

「Wi-Fi設定」のポリシーを作成する場合には、まずWi-Fiアクセスポイントの情報を登録する必要があります。

「Wi-Fi設定一覧」画面(「ポリシー管理」画面から[Wi-Fi設定]をクリックした最初の画面)にて、[Wi-Fi AP管理]をクリックします。



「Wi-Fi AP一覧」画面が表示されますので、[新規作成]をクリックします。





「Wi-Fi AP」画面が表示されますので、Wi-Fiアクセスポイント情報を設定します。入力が完了したら、[保存]をクリックしてください。

■Wi-Fi AP名

STAR-MDM管理サーバ上で管理するための名称を入力します。

■SSID(サービスセット識別子)

Wi-FiアクセスポイントのSSIDを入力します。

■自動接続

対象のWi-Fiアクセスポイントを端末が検知した際、自動接続させるにはチェックを入れます。

■非公開ネットワーク

対象のWi-Fiアクセスポイントが非公開アクセスポイントの場合、チェックを入れます。

■セキュリティの種類(なし／WEP／WPA/WPA2)

Wi-Fiアクセスポイントのセキュリティの種類を選択します。WEPまたはWPA/WPA2を選択した場合、パスワード欄が表示されますのでパスワードを設定してください。



「処理結果」画面にて「Wi-Fi APを追加しました」と表示されたら、[戻る]をクリックします。



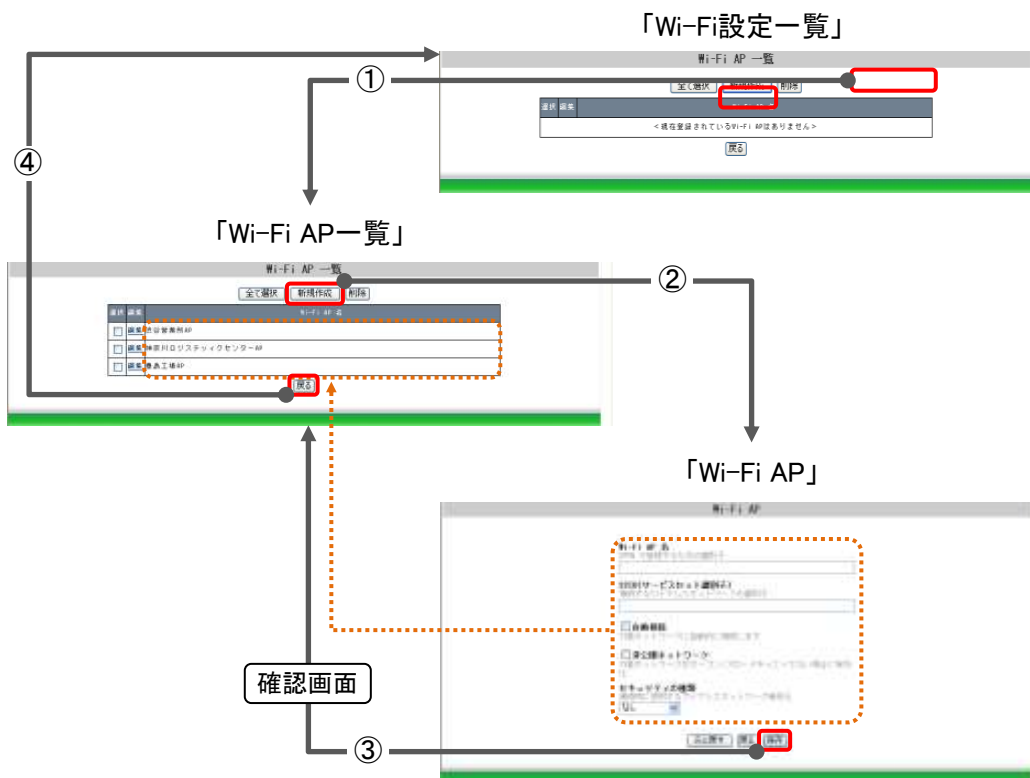


「Wi-Fi AP一覧」画面に戻ります。作成したWi-Fi AP名が一覧に追加されていれば完了です。問題が無ければ[戻る]をクリックして「Wi-Fi設定一覧」画面へ戻ります。



Wi-Fiアクセスポイント情報を修正するには、Wi-Fi AP名の横にある[編集]をクリックします。また、Wi-Fiアクセスポイント情報を削除する場合は、Wi-Fi AP名の横のチェックボックスにチェックを入れ、[削除]をクリックしてください。

【Wi-Fiアクセスポイントの登録手順:画面遷移概要】



13-2. Wi-Fi設定ポリシーの作成手順

「Wi-Fi設定一覧」画面(「ポリシー管理」画面から[Wi-Fi設定]をクリックして表示される最初の画面)にて [新規作成]をクリックします。



「Wi-Fi設定」画面が表示されますので、[Wi-Fi AP選択]をクリックします。

この画面から新規のWi-Fiアクセスポイント情報を設定することも可能です。

[Wi-Fi AP作成]をクリックすると[Wi-Fi AP]画面が表示されます。



「Wi-Fi AP選択」画面が表示されます。設定済みのWi-Fiアクセスポイント名の一覧から適用したいWi-Fiアクセスポイント名にチェックを入れて選択し、[設定]をクリックしてください。

※一つのポリシーで複数のWi-Fiアクセスポイントの設定を端末に適用することが可能です。

選択	Wi-Fi AP 名	SSID
☒	経営者専用AP	000B8A2E4E8202
☒	東川ロジスティクスセンターAP	000B8A2E4E8202
☐	東川工場AP	000B8A2E4E8202



「Wi-Fi設定」画面に戻ります。選択したWi-Fiアクセスポイント名が表示されますので、ラジオボタンで「登録」を選択して下さい。

問題が無ければポリシー名を入力して[新規作成]をクリックしてください。「Wi-Fi 設定一覧」画面にポリシーが追加されます。

Wi-Fi 設定

Wi-Fi 設定名 : 社内ap 新規作成

☐ 基本ポリシーとして保存する
(ポリシー名は”基本ポリシー”となります。)

本ポリシーで端末に設定したい Wi-Fi AP を登録します。

Wi-Fi AP 選択 Wi-Fi AP 作成

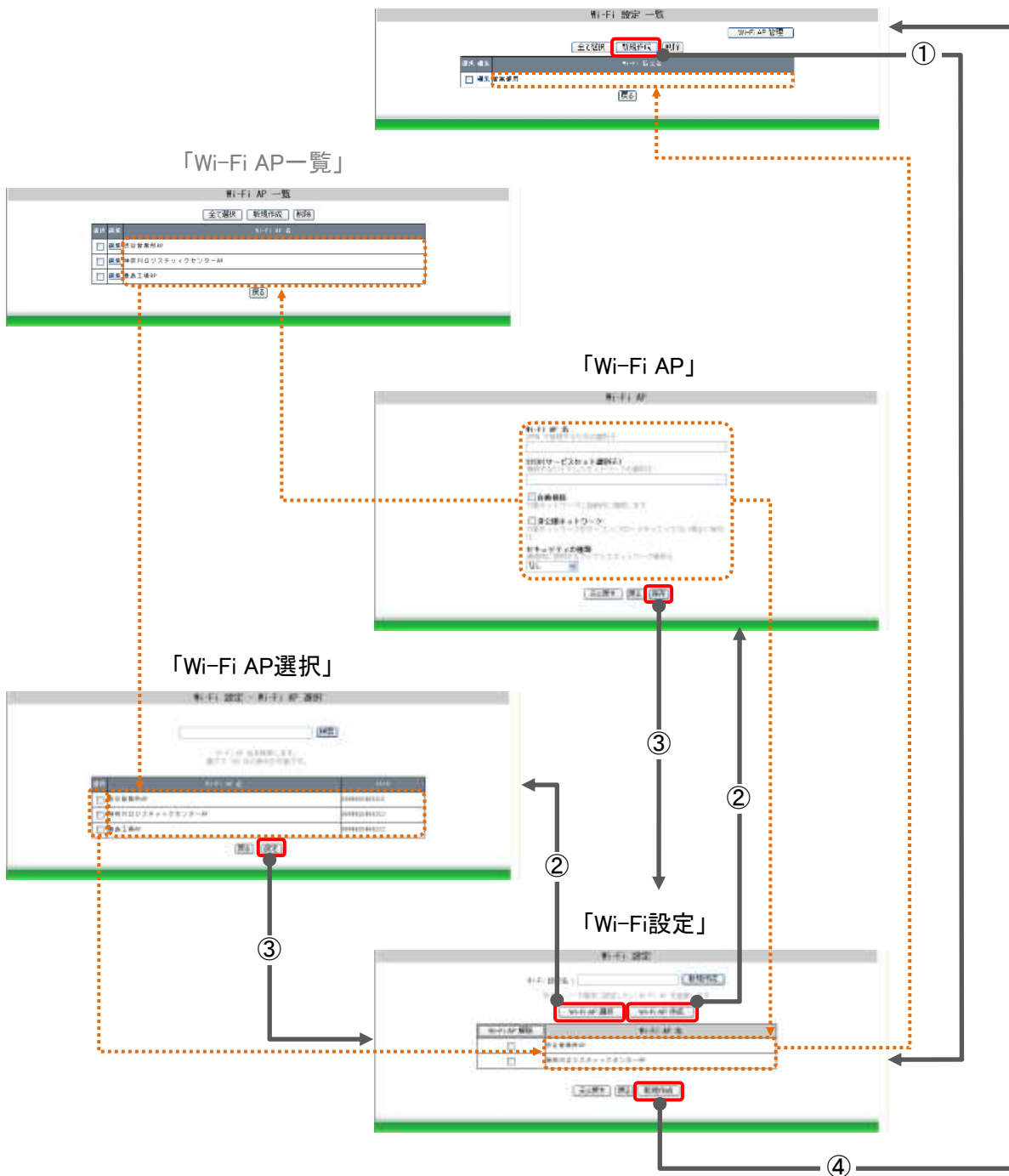
☒ 登録 ☐ 削除

Wi-Fi AP 解除	Wi-Fi AP 名
☐	ap
☐	ap2

元に戻す 戻る 新規作成

Wi-Fiアクセスポイントを選択から外す場合は、Wi-Fi AP名の横のチェックボックスにチェックを入れ、[Wi-Fi AP 解除]をクリックします。

【Wi-Fi設定ポリシーの作成手順:画面遷移概要】



13-3. Wi-Fiアクセスポイントの削除手順

「Wi-Fi設定一覧」画面(「ポリシー管理」画面から[Wi-Fi設定]をクリックして表示される最初の画面)にて [新規作成]をクリックします。

「Wi-Fi設定」画面が表示されますので、[Wi-Fi AP選択]をクリックします。

「Wi-Fi AP選択」画面が表示されます。設定済みのWi-Fiアクセスポイント名の一覧から適用したいWi-Fiアクセスポイント名にチェックを入れて選択し、[設定]をクリックしてください。

※一つのポリシーで複数のWi-Fiアクセスポイントの設定を端末に適用することが可能です。

選択	Wi-Fi AP 名	BSSID
☒	経営業務用AP	000B42E46820E
☒	堺川ロジスティクスセンターAP	000B42E46820E
☐	農工場用	000B42E46820E



「Wi-Fi設定」画面に戻ります。選択したWi-Fiアクセスポイント名が表示されますので、ラジオボタンで「削除」を選択して下さい。

問題が無ければポリシー名を入力して[新規作成]をクリックしてください。

「Wi-Fi 設定一覧」画面にポリシーが追加されます。

Wi-Fiアクセスポイントを選択から外す場合は、Wi-Fi AP名の横のチェックボックスにチェックを入れ、[Wi-Fi AP 解除]をクリックします。

《端末側での挙動》

ポリシーを適用すると、端末側で指定されたWiFiアクセスポイントが端末のWiFi一覧から削除されます。

※本ポリシーでの削除対象はWiFi設定ポリシーを利用して追加したアクセスポイントのみです。

手動で追加したアクセスポイントは削除されませんのでご注意ください。

14. 端末暗号義務化

Googleアカウントやアプリのデータ、取得した音楽・映像など、端末内データの暗号化を義務化します。

端末暗号義務化 - ポリシー作成画面

端末暗号義務化設定ポリシー名【新規作成】
 ポリシー名: 新規作成
※ポリシー名は64文字までです。

◆ 本体メモリの暗号義務化

☐ 義務化する ☐ 義務化しない

◆ 外部メモリの暗号義務化

☐ 義務化する ☐ 義務化しない

◆ 留意事項

端末暗号化は、Android OS 3.0(honeycomb)以上の端末にて使用できます。

- ・暗号化した端末は元に戻せません。
暗号化を解消するには初期化を行い、端末内のすべてのデータを削除する必要があります。
一部復号化できる端末もあります。各端末のマニュアルをご参照ください。
- ・暗号化には目安として一時間ほどの時間を要します。
この間、端末では一切の操作が行えませんがご注意ください。
- ・端末を暗号化するに当たり、事前に以下の準備が必要になります。
 - ロック画面のPIN番号、あるいはパスワードによるロック設定を行う
 - 端末を完全に充電された状態にする
 - 端末を外部電源と接続する
- ・Android OSの仕様により
端末を再起動した際には復号のためのパスワード入力完了までの間、
通話や通信ができない状態になります。
また、SPPMが起動されていないため、SPPMによる制御が行われません。
- ・外部メモリ暗号化はSAMSUNG GALAXYシリーズ、Sony Xperiaシリーズのみの機能です。

元に戻す
戻る
新規作成

14-1. 本機能の利用条件

- 「端末暗号化」機能は、Android OS v3.0以上で暗号化機能が搭載された機種で有効です。
- 暗号化した端末は基本的に元へ戻すことはできません^{*1}。暗号化を解消するには初期化を行い、端末内のすべてのデータを削除する必要があります。
- *1: 一部復号化できる端末もあります。各端末のマニュアルをご参照ください。
- 暗号化には目安として一時間ほどの時間を要します。この間、端末では一切の操作が行えませんがご注意ください。
- Android OSの仕様により、端末を再起動した際には復号のためのPIN番号あるいはパスワード入力完了までの間、通話や通信ができない状態になります。また、SPPM Agentが起動されていないため、STAR-DMによる制御が行われません。
- 外部メモリ暗号化はSAMSUNG GALAXYシリーズ、Sony Xperiaシリーズのみ利用可能です。
- E-APIによるデバイス制御の『設定』を制限状態では外部メモリ暗号化が行われません。(E-API7のみ)

14-2. 事前準備

- PIN番号またはパスワードによる画面ロック設定を行ってください
- 端末の画面ロック解除用に、PIN番号またはパスワードを設定しておく必要があります。
- ※暗号化に必要なロック設定の条件は、機種により異なる場合があります。暗号化設定画面にて条件が示されますので、それに従ってください。

■端末を完全に充電してください

端末の暗号化にはかなりの時間を要するため、途中で電源喪失といった事態に陥らないよう、端末は完全に充電しておく必要があります。

■端末を外部電源と接続してください

上記と同様、暗号化中の電源を確保するために、端末を外部電源と接続しておく必要があります。

14-3. 暗号化の義務化から暗号化実行までの手順

【STAR-MDM管理サーバの操作】

端末の暗号化を義務化する場合は、「ポリシー作成画面」の「端末暗号義務化」の項目で、[義務化する]にチェックを入れ、作成したポリシーを端末に適用します。

【端末側での操作】

①「端末暗号義務化」のポリシーが適用されると、暗号化の実行を要求するメッセージが表示されます。

■ダイアログ通知

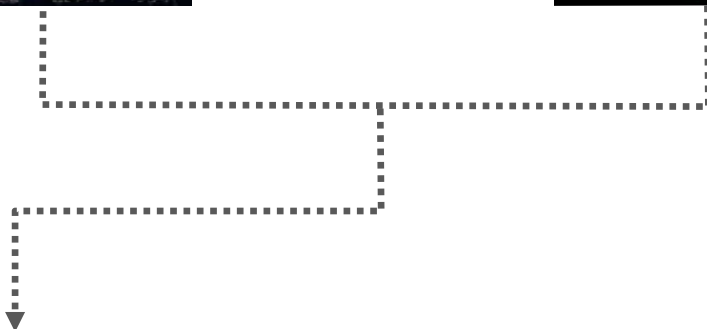
[暗号化する]をタップすると暗号化の実行画面が表示されます。

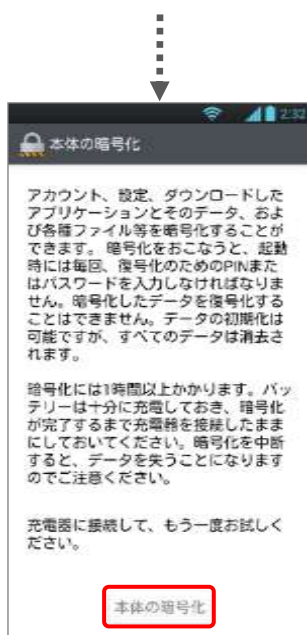


[あとで]をタップした場合は、暗号化の実行画面への遷移を保留し、以後は端末を起動するたびに暗号化を要求する画面が表示されます。

■ステータスバー通知

「SPPM 端末を暗号化してください」という通知をタップすると、暗号化の実行画面が表示されます。





②暗号化の実行画面が表示されたら、記載されている注意事項を充分に確認の上、[本体の暗号化]をタップします。



暗号化した端末は基本的に元へ戻すことはできません^{*1}。暗号化を解消するには初期化を行い、端末内のすべてのデータを削除する必要があります。

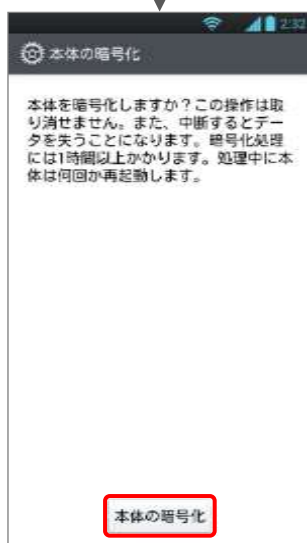
^{*1}: 一部復号化できる端末もあります。各端末のマニュアルをご参照ください。



暗号化処理の実行を中断するとデータが失われます。端末を完全に充電の上、外部電源に接続してください。また、暗号化には目安として一時間ほどの時間を要します。この間、端末では一切の操作が行えませんので、ご注意ください。



③端末に設定してあるPIN番号もしくはパスワードの入力を求められます。表示に従って操作してください。



④最終確認画面が表示されますので、記載されている注意事項を充分に確認の上、[本体の暗号化]をタップします。端末の暗号化処理が開始されます。

※暗号化の開始に先立ち、数回の再起動を行うことがあります。



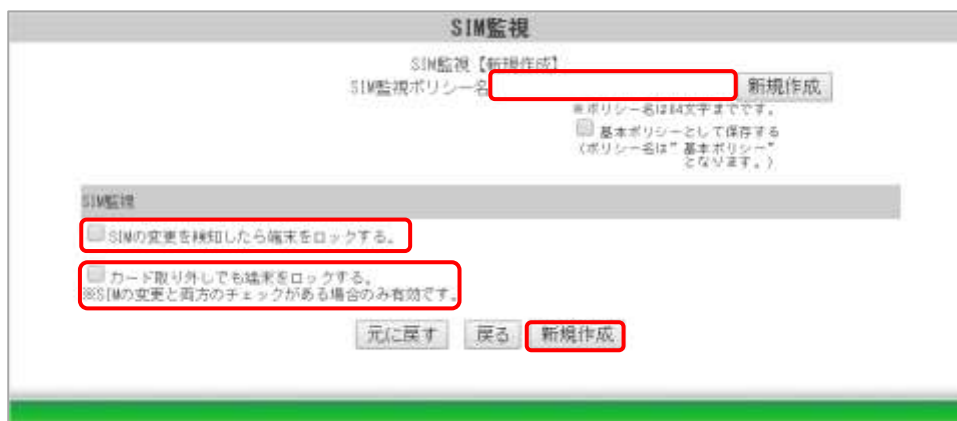
⑤暗号化を実行中の画面です。

15. SIM監視

■SIM 変更検知・ロック機能は、端末に挿入されている SIM を入れ替えて「電話番号」が変更された事を検知し、アラートメールの送信や端末ロック指示を行う機能になります。

【SIM 変更検知・ロック設定手順】

ポリシー管理から「SIM 監視」を選択し、ポリシーを作成します。



「SIM の変更を検知したら端末をロックする」にチェックをつけてポリシーを作成します。

「カード取り外しでも端末をロックする。」にもチェックを入れると、使用中の SIM カードが取り外された段階で端末がロックされます。

※「カード取り外しでも端末をロックする。」にチェックを入れる場合は、必ず「SIM の変更を検知したら端末をロックする」にもチェックを入れてください。

ポリシー作成完了後は通常のポリシー反映同様に端末にポリシーを反映してください。当ポリシー適用後に SIM を取り外したり、入れ替えたりすると、端末ロック指示が実行されます。

本機能で端末ロック指示が実行された場合は、SIM を元の電話番号のものに戻さないと解除がされません。

❗ 本機能でロックが実行された場合は、SPPM の管理画面上のロックステータスは緑のままとなる為、サーバ指示からの解除指示は行えません。
解除には SIM を元の電話番号のものに戻す事が必要です。

❗ 電話番号が取得できない SIM の場合は本機能でのロックは実行できません。

AndroidOS5.0以上では、ロック画面に関して以下のことができません

- ❗
- ・ロック画面上で着信に応答すること
- ・ロック画面上で着信を切断すること
- ・モバイルデータ通信OFFのとき、ロック画面上でサーバ通信ボタンを押下してモバイルデータ通信をONにすること

16. メッセージ配信

- メッセージ配信機能は、Android/iOS 端末に管理画面で設定をしたメッセージを配信する機能です。
- Agent のメッセージとして配信する方法と、端末利用者のアドレス宛てにメールを配信する方法があります。
- 管理画面ではメッセージの配信状況を確認できます。

【メッセージ配信/メール配信 設定手順】

ポリシー管理から「メッセージ配信」を選択し、ポリシーを作成します。

《メッセージ配信の場合》

■動作モード

「メッセージ（Agent のメッセージとして表示されます。）」を選択してください。

※メッセージ配信とメール配信の併用はできません。

◆ 動作モード

- ☒ メッセージ（Agent のメッセージとして表示されます。） ☐ メール（端末利用者のメールに配信されます。）

■メッセージ設定

配信したいメッセージをボックス内に入力をしてください。

◆ メッセージ

本文：

※入力可能な文字数は400文字までとなります。
※下記の内容は端末でリンクで表示されます。

- メールアドレス
- URL
- 電話番号

◆ 配信設定

☐ パスワード画面の上にメッセージを直接表示

☐ 強制的に通知音を鳴らす(Android)

※本文に「web サイトの URL」「メールアドレス」「電話番号」がある場合は、端末で各リンクを選択する事でブラウザアプリ、メールアプリ、電話アプリを起動する事ができます。

※配信できるメッセージの文字数は最大 400 字です。(バイト数には依存しません。)

■配信設定

・メッセージ表示設定

「パスワード画面の上にメッセージを直接表示」を選択すると、端末のパスワード入力画面上にメッセージが表示されます。

選択しない場合にはパスワード画面上に新着メッセージ通知が表示され、パスワード解除後にメッセージが表示されます。

・通知音設定

「強制的に通知音を鳴らす」を選択すると、端末でメッセージ受信時にマナーモードが設定されていても通知音が鳴ります（通知音は端末で設定した通知音になります）

また、通知音量・通知時間の設定ができます。

※v3.58.1 以降は「強制的に通知音を鳴らす」の設定は非対応です。（Work Profile）

・通知音設定値 小/中/大

・通知時間設定値 20 秒/40 秒/60 秒/80 秒/100 秒

※通知音設定は、Android 端末のみの対応となります。

※端末の設定で通知音をサイレントに設定した場合は、「強制的に通知音を鳴らす」を選択してもメッセージ通知音は鳴りません。

※「強制的に通知音を鳴らす」を選択しなかった場合は、端末の通知音・通知音量でメッセージ通知音が鳴ります（通知音がサイレント・通知音量がゼロの場合は鳴りません）

※AndroidOS5.0 以上では、強制通知音 ON のメッセージ配信ポリシーの適用により、サイレントモードが解除される場合があります。

《メール配信の場合》

■動作モード

「メール(端末利用者のメールに配信されます。)」を選択してください。

※メッセージ配信とメール配信の併用はできません。

◆ 動作モード

☐ メッセージ（Agentのメッセージとして表示されます。） ☒ メール（端末利用者のメールに配信されます。）

■メール設定

項目ごとに情報を入力してください。

タイトル:メールの件名として表示されます。

返信先:メールを受け取った端末が返信する際の宛先メールアドレスです。

本文:メールの本文として表示されます。

◆ メール

タイトル:

返信先:

本文:

※すべて入力必須項目です。

※返信先はメールアドレス形式以外だとポリシー作成ができません。

- ❗ ポリシーを適用済みの状態でポリシー編集した場合、「上書保存」ボタンを押したタイミングで端末にポリシー内容が適用されます。
- ❗ メール配信、メッセージ配信両方に入力があった場合、動作モードで選択された方の情報が適用され、選択されていない方の値は消えてしまいます。
- ❗ メール配信では端末一覧画面のシグナルの変化(未確認・確認済みなど)はありません。
- ❗ メール配信は「root@star-mdm.ne.jp」のアドレスから送信されます。
- ❗ メール配信は端末利用者情報に設定されたアドレスに送信されます。

端末管理 - 端末情報編集画面

元に戻す 戻る 上書保存

【利用者情報】

姓

名

セイ

メイ

姓(英語)

名(英語)

端末メールアドレス

PCメールアドレス

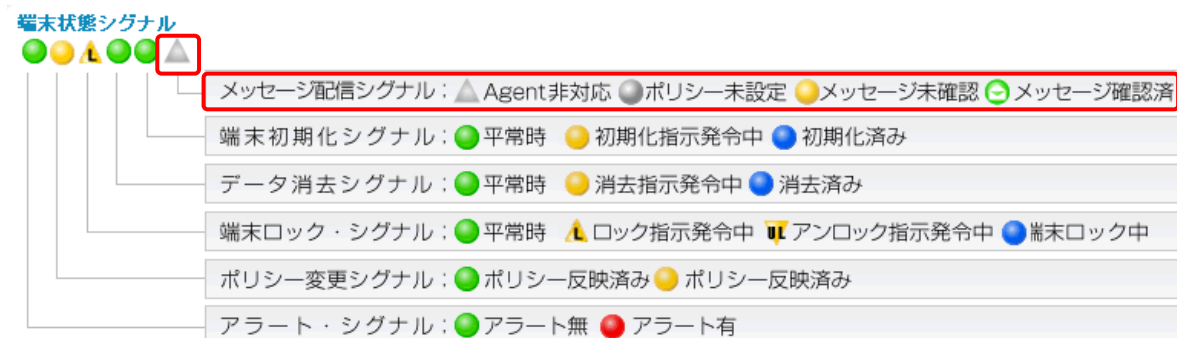
※入力されていない場合は送信されません。

※端末メールアドレスとPCアドレス、両方設定している場合は両方にメールが送信されます。

【メッセージ配信ステータス】

メッセージの配信状況を管理画面から確認できます。

メッセージ配信ステータスは4つのシグナルに分類されます。



■Agent 非対応

インストールされている SPPM Agent がメッセージ配信ポリシーに対応していないため、利用できません

- ・Android : v2.25 以降 対応
- ・iOS : v1.1.0 以降 対応

選択	ステータス	編集	緊急	端末電話番号	姓	メッセージ配信
☐	●●●●●▲	編集	指示	none	鈴木	

■ポリシー未設定

メッセージ配信ポリシーが未設定の状態です。

選択	ステータス	編集	緊急	端末電話番号	姓	メッセージ配信
☐	●●●●●●●●	編集	指示	1234567890	高橋	

■メッセージ未確認

メッセージ配信ポリシーが SPPM Agent に対して配信されていない状態、もしくはメッセージは配信されているが SPPM Agent で確認していない状態です。SPPM Agent では未確認のメッセージ一覧に表示されます。

- ・メッセージ配信ポリシーが SPPM Agent に配信されていない

選択	ステータス	編集	緊急	端末電話番号	姓	メッセージ配信
☐	●●●●●●●●	編集	指示	1234567890	高橋	社内通知 未確認

- ・メッセージ配信ポリシーが SPPM Agent に配信されているが、確認していない

選択	ステータス	編集	緊急	端末電話番号	姓	メッセージ配信
☐	●●●●●●●●	編集	指示	1234567890	高橋	社内通知 未確認

■メッセージ確認済み

メッセージ配信ポリシーが SPPM Agent に配信され、確認された(確認ボタンをタップした)状態です。

SPPM Agent では確認済みのメッセージ一覧に表示されます。

※メール配信の場合は、ポリシーを適用した時点でメッセージ確認済みシグナルに変更されます。

選択	ステータス	編集	緊急	端末電話番号	姓	メッセージ配信
☐	●●●●●●●●	編集	指示	1234567890	高橋	社内通知 確認済

【メッセージ配信履歴】

端末情報からは過去に配信したメッセージの履歴が 20 件まで表示されます*。

履歴にはメッセージの配信日時・設定やメッセージ内容、メッセージの確認状況などが表示されます。

関連項目 ➡ 「端末情報 [メッセージ配信履歴](#)」

詳細表示をクリックするとWindowにメッセージの詳細が表示されます

【メッセージ配信履歴】					
詳細表示	ポリシー名	メッセージ	配信日時	確認日時	状態
詳細表示	業務連絡	営業部の皆様、資料を更新しま	2014-09-08 17:21:13.73	2014-09-08 17:21:22.741	確認済
詳細表示	業務連絡	営業部の皆様、資料を更新しま	2014-09-08 17:20:42.8	2014-09-08 17:21:00.41	確認済
詳細表示	業務連絡	営業部の皆様、資料を更新しま	2014-09-08 10:44:35.845	2014-09-08 10:44:55.738	未確認

戻る



【配信されたメッセージの表示】

端末でメッセージを受信すると新着メッセージ通知、メッセージ本文が表示されます※1

メッセージが表示されるとメッセージを確認した事を管理サーバに通知する、確認ボタンが表示されます※2

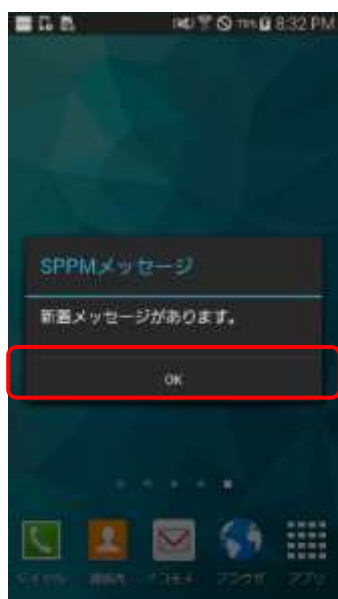
※1 メッセージ表示についてはポリシー作成時に設定できます

関連項目 ➡ 「[メッセージ配信設定](#)」

※2 確認ボタンを選択すると管理画面の配信ステータスが確認済みに変わります

関連項目 ➡ 「[メッセージ配信ステータス](#)」

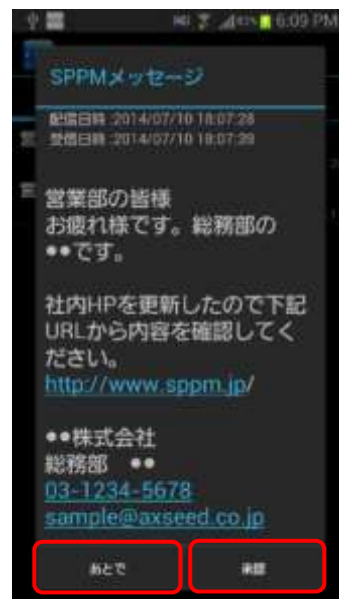
配信ポリシーで「パスワード画面の上にメッセージを直接表示」を設定していない場合



①



②



③

①パスワード画面の上にメッセージ通知画面が表示されます

②通知画面で OK や戻るボタンを選択するとパスワード入力画面になります

③パスワードを解除するとメッセージ本文と、「あとで」「確認」ボタンが表示されます※1

※1 「確認」を選択するとメッセージの「確認済」通知をサーバに送信します

※端末設定の「統一ロックを使用」が OFF の場合、OS10 以降の Work Profile では「新着メッセージがあります」の通知が表示されません。

※端末設定の「統一ロックを使用」が ON の場合、OS11 以降の Work Profile では「新着メッセージがあります」の通知が表示されません。

配信ポリシーで「パスワード画面の上にメッセージを直接表示」を設定している場合

①



②

①端末がパスワードロック画面の状態

②パスワード画面に上にメッセージ本文と、「あとで」「確認」ボタンが表示されます※1

※1 「確認」を選択するとメッセージの「確認済」通知をサーバに送信します

※端末設定の「統一ロックを使用」が OFF の場合、OS10 以降の Work Profile ではパスワード画面上にメッセージが直接表示されません。

※端末設定の「統一ロックを使用」が ON の場合、OS11 以降の Work Profile ではパスワード画面上にメッセージが直接表示されません。

【メッセージ確認】

配信されたメッセージは SPPM Agent 内で確認できます。



① SPPM Agent を起動

② SPPM Agent メニュー内のメッセージを選択(確認していないメッセージがある場合は件数が表示されます)

③ 「未確認」「確認済」タブ選択で、それぞれ受信したメッセージの件名・受信日時が表示されます

④ ③で未確認メッセージを選択すると「あとで」「確認」ボタンが表示されます※1

※1 メッセージ受信時に「あとで」を選択した場合でも、ここで「確認済」通知をサーバに送信します



SPPM Agent で保存されるメッセージは、「未確認」「確認済」合計 20 件までです。

以降は受信日が古いメッセージから順番に消去されます

17. 電話帳配信

CSV ファイルを用いて、端末に電話帳データを一括配信することができます。

また、配信した電話帳データの一括削除も可能です。



SPPM Agent v3.57 未満は電話帳配信ポリシーは非対応です。

電話帳配信

ポリシー名 【新規作成】

ポリシー名: 新規作成

※ポリシー名は64文字までです。

◆ 電話帳配信

☒ 電話帳配信 ☐ 電話帳全削除(SPPM配信データのみ)

ファイルを選択
選択されていません
upload

※ CSVファイル形式：電話番号,姓,名,セイ,メイ,所属,役職,メールアドレス
 例)
 09012345678,山田,太郎,ヤマダ,タロウ,営業部,部長,yamada@example.com
 09011112222,鈴木,花子,スズキ,ハナコ,,,suzuki@example.com

※ 項目を未入力にした場合はカンマの間に何も入力しないでください

※ 最大データ件数は1,000件です

元に戻す
戻る
新規作成

【CSV ファイル】

電話帳配信を行うには、まず配信したい電話番号等の情報を含む CSV ファイルを用意します。

CSV ファイルの形式は 1 行目の左端から『電話番号、姓、名、セイ、メイ、所属、役職、email アドレス』です。

自動保存 オフ 電話帳配信.csv 検索											
ファイル ホーム 挿入 ページレイアウト 数式 データ 校閲 表示 自動化 開発 ヘルプ											
L1											
	A	B	C	D	E	F	G	H	I	J	K
1	090-0000	安藤	一郎	アンドウ	イチロウ	スターネッ	部長	ando@starnet.ad.jp			
2	090-0001	伊藤	二郎	イトウ	ジロウ	スターネッ	課長	ito@starnet.ad.jp			
3	090-0002	宇藤	三郎	ウトウ	サブロウ	スターネッ	係長	uto@starnet.ad.jp			
4											
5											



電話番号に含まれるハイフンやスペースは配信時に削除されます。



Excel を用いて CSV ファイルを作成する場合、ハイフンやスペースを含まない電話番号は、csv 入力時および端末表示時に、1 文字目のゼロが省略されます。ゼロを省略したくない場合には、セルの書式設定で文字列を選択するか、電話番号の先頭に「' (シングルクォート)」を入力してください。

【登録方法】

電話帳配信

ポリシー名 【佐藤(千)】
 ポリシー名: 別名保存
 ※ポリシー名は64文字までです。

◆ 電話帳配信

ファイルを選択 電話帳配信.csv upload

ファイルのアップロードに成功しました

電話番号	姓	名	セイ	メイ	所属	役職	メールアドレス
090-0000-0000	安藤	一郎	アンドウ	イチロウ	スターネット	部長	ando@starnet.ad.jp
090-1111-1111	伊藤	二郎	イトウ	ジロウ	スターネット	課長	ito@starnet.ad.jp
090-2222-2222	宇藤	三郎	ウトウ	サブロウ	スターネット	係長	uto@starnet.ad.jp

元に戻す 戻る 上書保存

電話帳配信ポリシーの作成/編集画面を開き、「ファイルを選択」から用意した CSV ファイルを選択したのち、「upload」をクリックします。

CSV ファイルの情報が画面に反映されますので、内容確認後に保存をしてください。

【電話帳データの登録・上書き】

CSV ファイルで配信した電話帳データは、端末内に保存されます。(閲覧する電話帳アプリによっては配信データが表示されない場合があります。他電話帳アプリのインストール、または SPPM Agent のバージョンアップをお試し下さい。)

また、配信された電話帳は以下のルールに基づいて登録・上書きされます。

■ 電話番号をキーにして登録・上書きします

- 電話番号の比較は数値部分のみで比較します
(123-456、123456、123 456 は全て同じ番号と判断されます)
- 同じ電話番号を持つ連絡先が配信された場合、配信された情報が上書きされます。
- 配信先の電話帳に複数の電話番号を持つ登録があった場合、そのうちの 1 件の電話番号と合致すれば、配信された内容が上書きされます

■ 上書について

- CSV の項目が空欄だった場合は、空欄として登録・上書されます
- CSV 内に同一の電話番号があった場合は、より下の行にあるデータが優先されます

■ 電話番号、email は“勤務先”の電話番号、email として登録されます

- 更新したデータのメモ欄の末尾には“MDM_AddressBook”が追加されます
(すでに“MDM_AddressBook”がメモにあった場合はそのまま変わりません)
- 一部、CSV で配信しても端末に表示されない記号があります(端末から登録できない記号など)

【電話帳配信に関する注意事項】

- 配信件数の上限
一度に配信できる電話帳データは、1000 件を上限としています。
1000 件を超えて配信した場合、配信に時間がかかる、もしくは配信が終了しない場合があります。
- 配信できない記号について
端末側で登録できない文字や機種依存文字など、配信できない文字がございます。
機種依存文字、および“”はご利用になれません。配信した場合、端末側で非表示あるいは文字化け表示になります。(配信できない文字・配信時の表示は配信先の端末により異なります。)
- 文字数の上限
機種ごとに表示できる文字数に制限がありますので、利用する端末に合わせて文字数を調整してください。
- 配信した電話帳が消えてしまう件について
端末をセーフモードにすると配信した電話帳が消えてしまう場合があります。その場合は再度電話帳を配信してください。
- 同内容の電話帳データの配信について
同じ内容の電話帳データを再度配信する際は、同じ内容のポリシーを別に作成するか、既存のポリシー内で同じ内容の CSV ファイルを再度アップロードしてください。
- グループについて
更新した電話帳データのグループに“MDM_AddressBook”が追加されます。既にグループが登録されている連絡先のグループは更新されません。(SPPM Agent v3.00 以降の機能です。それ以前のバージョンで配信された電話帳データの場合、v3.00 へのバージョンアップ時にグループが追加されます。)
- 端末側で作成した連絡先について
端末側で作成した連絡先と同じ電話番号を持つ連絡先を配信した場合の動作は、SPPM Agent バージョンにより異なります。
v3.05.1 未満: 端末側で作成された連絡先は配信した連絡先に上書き更新されます。
v3.05.1 以降: 端末側で作成された連絡先は更新されず、新規の連絡先が作成されます。
- 「SPPM」アカウント連携について
電話帳配信ポリシーで配信された連絡先には「SPPM」アカウントが連携されます。
また、配信後は端末設定のアカウント項目に「SPPM」アカウントが登録されます。
既存の連絡先を「SPPM」アカウントに連携する場合は上書き配信が必要です。
※「SPPM」アカウントを削除すると、連携された連絡先も合わせて削除されるため予めご注意ください。
※「SPPM」アカウントに連携されていない連絡先は、その他アカウントの追加・削除動作等により Android OS により削除される可能性があります。
※「SPPM」アカウント連携は SPPM Agent v3.22 以降の機能です。

■ SPPM Agent アンインストール時の配信データについて

SPPM Agent アプリをアンインストールした場合、STAR-MDM の電話帳配信機能を利用して端末に配信した電話帳データはすべて削除されます。

【電話帳削除】

「電話帳全削除(STAR-MDM 配信データのみ)」を選択し、ポリシーを保存することで、電話帳削除のポリシーが作成されます。

ポリシーを適用に適用すると、STAR-MDM が配信した電話帳データを一括で削除することができます。

※SPPM Agent v3.26 以降対応。

※削除対象となる電話帳データは SPPM Agent v3.26 未満で配信したものも含まれます。



作成済みのポリシーは電話帳配信と電話帳削除を切り替えて上書保存できません。

【電話帳一覧を CSV で書き出し】

アップロードされた CSV ファイルをダウンロードできます。

ポリシーを開き、「電話帳一覧 CSV 書き出し」ボタンを押下すると CSV ファイルがダウンロードされます。

18. アプリインストール制限

管理画面で指定したアプリのアンインストールを制限します。

※本ポリシーは E-API 6 以上の Xperia 端末と E-SDK 1.0 以上の Galaxy 端末、および Android Enterprise 端末のみご利用いただけます。

アプリインストール制限

ポリシー名 【新規作成】
 ポリシー名: 新規作成
※ポリシー名は64文字までです。

◆ 参照端末から一覧に追加
 端末の電話番号または端末ID（シリアルNo）を入力してください

検索

アプリインストール制限はE-API6以上の機種のみ有効です。

◆ 自社アプリ情報を入力して一覧にアプリを追加

アプリ名

パッケージ名

アプリ一覧に追加

◆ アンインストール制限アプリ一覧

元に戻す
戻る
新規作成

【参照端末から一覧に追加】

端末の電話番号または端末 ID を入力検索することで該当の端末を表示します。

端末を選択し「アプリ一覧に追加」することで、その端末で取得されたアプリ一覧がアンインストール制限アプリ一覧に追加されます。

◆ 参照端末から一覧に追加

端末の電話番号または端末ID（シリアルNo）を入力してください

検索

選択	端末ID	電話番号	端末名	備考
☐	359835983598838		S0-03F	

アプリ一覧に追加
端末一覧を閉じる

【自社アプリ情報を入力して一覧にアプリを追加】

アプリ名とパッケージ名を入力することで、任意のアプリケーションをアンインストール制限アプリ一覧に追加することができます。

※字数について

アプリ名: 50 字以内で記入してください。

パッケージ名: 250 字以内で記入してください。

【アンインストール制限アプリ一覧】

参照端末から追加したアプリや、アプリ名とパッケージ名を指定し追加したが表示されます。

このアプリ一覧に表示されたアプリがアンインストール制限の対象となります。

「参照端末から一覧に追加」から追加された際は、参照端末の全てのアプリが最初に表示されるため、アンインストール制限を行いたいアプリ以外は全て削除してください。

◆ アンインストール制限アプリ一覧

全て選択

全て解除

選択されたアプリの削除

アプリ名	パッケージ名	削除
(ウィジェット)Chrome	com.android.chrome	☒
(ウィジェット)Eメール	com.android.email	☐
(ウィジェット)Gmail	com.google.android.gm	☐
(ウィジェット)Google Play ストア	com.android.vending	☐
(ウィジェット)Google Play ブックス	com.google.android.apps.books	☐

19. 動態管理

端末の位置情報を設定した間隔と取得時間帯で取得し、専用の管理画面により最新位置情報と移動経路をマップで確認できます。

※本機能のポリシー設定は SPPM Agent v3.28 以降でご利用いただけます。

※取得した位置情報は「動態管理」画面で管理できます。詳細は下記関連情報をご確認ください。

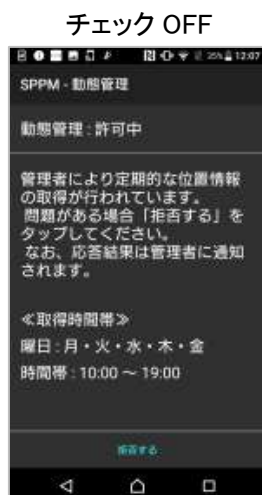
関連情報 [「動態管理」](#)

【取得中設定】

■Agent側での動態管理中の取得拒否を禁止する。

動態管理「許可」中はユーザーの Agent 操作により「拒否」への変更が可能です。

本項目のチェックボックスを ON にすることで、動態管理中の「拒否」操作が不可となります。



【取得間隔指定】

■位置情報取得間隔

動態管理中の位置情報の取得間隔を設定できます。

取得間隔は「5 分」「10 分」「20 分」「30 分」「60 分」から選択できます。

【取得時間帯指定】

位置情報を取得する時間帯を設定します。

■24 時間

「24 時間」取得されます。

■時間帯指定

取得開始時間 : 取得曜日に位置情報取得を開始する時間を設定します。

取得終了時間 : 取得曜日に位置情報取得を終了する時間を設定します。

※取得開始時間が取得終了時間以降に設定された場合は、翌日の取得終了時間まで取得されます。

【取得曜日指定】

位置情報を取得する曜日を設定します。

■毎日

「毎日」取得されます。

■曜日指定

取得する曜日を指定します。チェックのある曜日が取得対象となります。

※取得開始時間が取得終了時間以降に設定された場合は、取得開始時間が「曜日指定」の基準となり、翌日の曜日指定が OFF の場合でも、取得終了時間まで取得されます。

例) 取得時間帯指定 : 取得開始時間「22:00」、取得終了時間「07:00」

取得曜日指定 : 「月」のみ

上記設定では、月曜「22:00」に取得を開始し、火曜「07:00」に取得を終了します。

【Agent 動作】

■同意要求ダイアログ

動態管理ポリシーが適用されると端末に動態管理の同意要求ダイアログが表示されます。

このダイアログは「許可する」「拒否する」が回答されるまで、パスワード認証時に再表示されます。



<許可する>

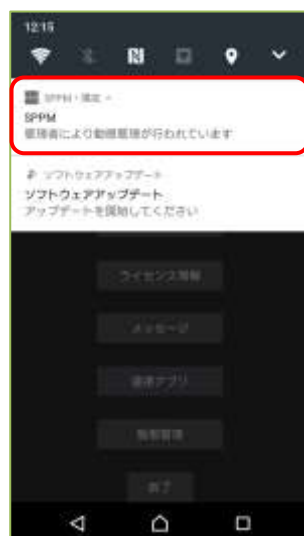
「許可する」をタップすることで動態管理が許可され、位置情報の取得が開始されます。

<拒否する>

「詳細」⇒「拒否する」をタップすることで動態管理が拒否されます。

■動態管理通知

動態管理の状況により SPPM Agent 通知内容が切り替わります。



<通知内容>

- 稼動しています

動態管理ポリシーが未設定の場合や、位置情報を取得していない時間帯に表示されます。

- 管理者により動態管理の同意が求められています

動態管理の同意要求ダイアログに回答していない場合や、動態管理を「拒否」中に表示されます。

- 管理者により動態管理が行われています

動態管理を「許可」中、位置情報の取得を行っている間に表示されます。

■Google 位置情報サービス使用の通知/ポップアップ

動態管理機能による位置情報の取得には Google の位置情報サービスを使用します。

動態管理が「許可」された端末の Google の位置情報サービスが ON になっていない場合に、使用するための「通知」「ポップアップ」が表示されます。表示された場合は「OK」をタップすることにより、Google の位置情報サービスを使用できるようになります。

※基本的に端末の位置情報の取得モードが「高精度」では表示されませんが、稀に「高精度」となっている場合 Google の位置情報サービスが ON にならず、ポップアップが表示される場合があります。

※本機能は SPPM Agent v3.31/ Android OS4.2 以降でご利用いただけます。

※Wi-Fi のスキャンがオフの場合に、位置情報が「高精度」であっても通知が出る場合があります。

位置情報設定内の「WiFi スキャン」OFF の状態で Wi-Fi を OFF にした場合、通知が表示されます。



- Google 位置情報サービスの許可を求めるポップアップで「OK」を押しても通知が表示される場合は、
 ① 端末設定内で「位置情報の使用」、もしくは「Google 位置情報の精度」を手動で一度 OFF にして再度 ON にしていただく必要がございます。

■SPPM Agent 画面

動態管理ポリシー適用中は「動態管理」ボタンが SPPM Agent トップ画面に表示されます。

また、動態管理による位置情報の取得が行われている間は「*動態管理中*」と表示されます。

動態管理画面では動態管理の「許可」「拒否」の状況とポリシーで設定した取得時間帯・曜日を確認でき、「拒否する」「許可する」ボタンからは動態管理の同意状況の変更が可能です。

※「Agent 側での動態管理中の取得拒否を禁止する。」設定が有効の場合、「拒否する」は表示されません。



【動態管理ステータス】

端末毎の動態管理同意状況等を端末一覧画面で「動態管理ステータス」として確認できます。

端末一覧画面の「一覧表示設定」から表示設定を行ってください。

※本機能は SPPM Agent v3.28 以降でご利用いただけます。v3.26～v3.27.2 では空欄となります。

関連情報  「[一覧表示設定](#)」

■動態管理ステータス一覧

表示文言	説明
Agent 非対応	動態管理ポリシーが適用されたが Agent が v3.26 未満である
回答待ち	同意要求ダイアログの回答が行われていない
許可	動態管理がユーザーの同意を得て「許可」されている
取得不可	動態管理を「許可」されているが、端末の位置情報機能がオフ
拒否	動態管理がユーザーの同意を得られず「拒否」されている

【ログ管理】

端末の操作により、動態管理が「許可」「拒否」操作をされた際に、該当するログがログ管理に表示されます。

■ロガー一覧

表示文言	説明
動態管理が開始されました	動態管理ポリシーの同意要求ダイアログで「許可」が選択された
動態管理が停止されました	動態管理ポリシーが「＜未設定＞」に適用された
動態管理の位置情報取得を許可されました	SPPM Agent の動態管理画面で「許可する」が選択された
動態管理の位置情報取得を拒否されました	動態管理ポリシーの同意要求ダイアログで「拒否」が選択された、または SPPM Agent の動態管理画面で「拒否する」が選択された

20. 利用統計

端末で利用されたアプリの時間を集計し、専用の管理画面で統計情報を確認できます。

※取得したアプリ利用情報は「利用統計」画面で管理できます。詳細は下記関連情報をご確認ください。

関連情報 [「利用統計」](#)

【Agent 動作】

■アプリ使用履歴のアクセス許可

利用統計ポリシーが適用されると端末に権限許可ダイアログが表示されます。

利用統計機能にはアプリ使用履歴へのアクセス権限が必要なため SPPM を許可してください。

【権限許可ダイアログ】



21. キオスク管理

【概要】

Work Managed Device モードの Android Enterprise 端末にキオスク管理ポリシーを適用することで、業務専用のアプリケーションのみを表示させ、そのほかの操作を禁止することが可能です。(以下、キオスクモードと記載) この機能を利用することで、端末を「単一業務のみに活用するデバイス」として管理することができます。

キオスク管理ポリシーの詳細については弊社までお問い合わせください。

【稼働環境】

・対応 OS

Android OS v7.x ~ v10.x

・対応 SPPM Agent

v3.54~

※Android OS9 の端末は、SPPM Agent v3.46 以降で利用可能です

1. 概要

端末の位置情報を設定した間隔で取得し続け、専用の管理画面により最新位置情報と移動経路をマップで確認できます。

※対応バージョン: SPPM Agent v3.26 以降 (ポリシー設定: SPPM Agent v3.28 以降)

※STAR-MDM フル機能パックまたは STAR-MDM 拡張プランをご契約いただいたお客様は、無償でご利用いただけます。

※動態管理機能をご利用いただくには GooglePlay 開発者サービスが必須となります。Google 非対応端末ではご利用いただけません。

※取得データの閲覧期間は 30 日間です。

【ご利用にあたっての注意】

- ・ 利用には端末側で動態管理の[許可]選択が必要です。端末利用者の許可無しで強制的に動態管理対象とすることは出来ません。また、位置情報は端末利用者のプライバシー情報となるため、あらかじめ必ず端末利用者の許諾を取ってください。
- ・ SPPM Agent v3.01 未満で端末登録した端末をバージョンアップした場合、動態管理での位置情報取得はできませんのでご注意ください。
ご利用するには一度 SPPM をアンインストールしてから最新版で再登録してください。

2. 申し込み方法

動態管理の申し込みは 2018 年 8 月 1 日を以って不要となりました。

管理画面の設定のみでご利用いただけます。

3. 設定方法

【動態管理 / 利用統計 利用設定】

その他>動態管理／利用統計 利用設定 で動態管理を「利用する」設定にします。

※マスター管理者でのみ設定が可能です。

※詳細情報は[「動態管理／利用統計 利用設定」](#)をご覧ください。

【所属グループ設定】

動態管理では所属設定がない端末は基本的に動態管理画面に表示されません。例外として、「/」（企業全体）のグループ管理権限を持つ管理者でのみ動態管理画面のグループ「全体」選択時に表示されます。

・グループ管理でグループを作成する。

その他>グループ管理から、端末利用者が所属するグループを作成してください。

・端末毎に所属先を設定する。

端末情報編集画面の【利用者情報】で所属先のグループを選択してください。

関連情報➡[「グループ管理」](#)

関連情報➡[「端末情報編集」](#)

【管理アカウント設定】

・管理者アカウントに管理グループを追加する。

その他>管理者管理から、各管理者アカウントに設定させる管理グループを追加してください。

・管理者アカウントの管理グループ権限で「動態管理」を ON にする。

管理者アカウントの管理グループの権限設定で「動態管理」を ON にしてください。

※権限を設定されていない管理アカウントではメニューの『動態管理』ボタンをクリック時に利用できない旨のメッセージが表示されます。

（一般管理者とマスター管理者では表示内容に差分がございますのでご注意ください。）

※動態管理 / 利用統計の利用設定前の状態では権限操作はできません。

関連情報➡[「グループ管理」](#)

関連情報➡[「管理者管理」](#)

【端末適用】

・ポリシーを作成する

ポリシー管理から動態管理ポリシーを作成してください。

・端末に「動態管理」機能を適用する。

端末編集画面から作成した動態管理ポリシーを選択し、上書保存します。

※端末情報編集画面に「動態管理」を表示するには「登録表示設定」の動態管理にチェックを付けます。

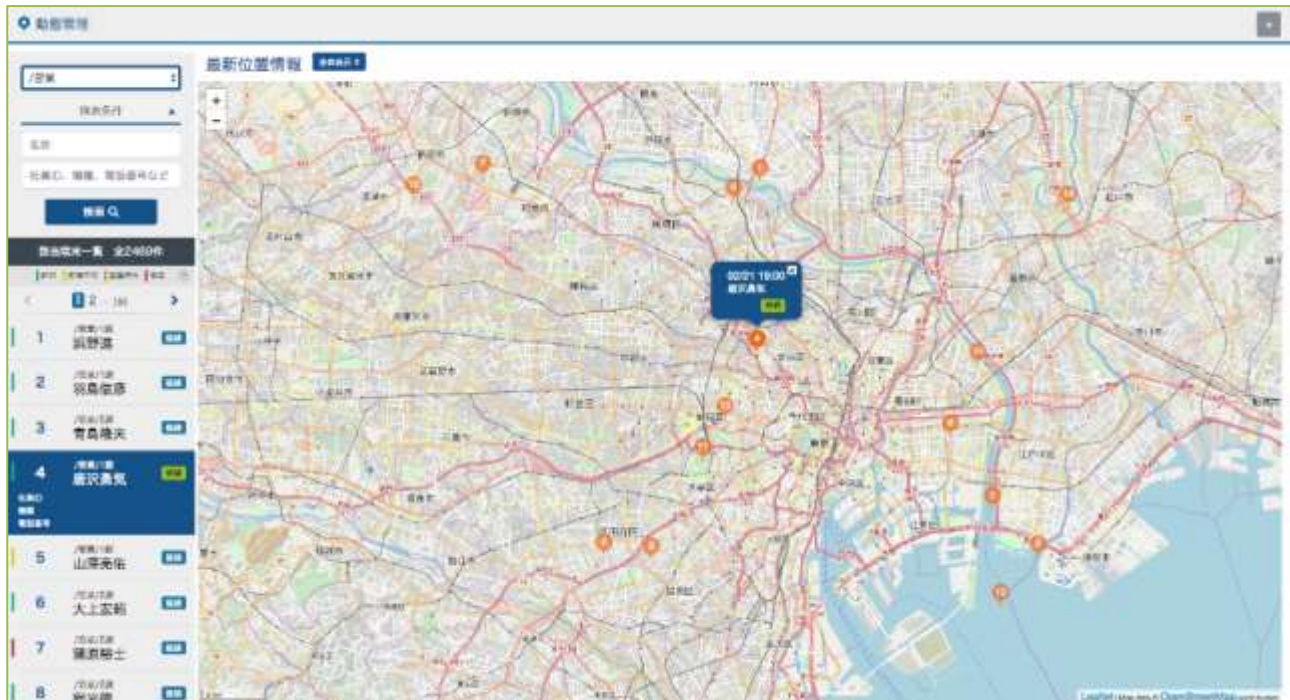
関連情報➡[「端末情報編集」](#)

関連情報➡[「登録表示設定」](#)

4. 動態管理画面

メニューの「動態管理」ボタンから動態管理の専用管理画面を表示できます。

【最新位置情報画面】



■グループ選択

選択したグループに所属した端末を検索できます。

ログインしている管理者アカウントが管理権限を持つグループのみ選択可能です。

「全体」を選択すると、管理権限を持つ全てのグループが検索対象となります。

■検索条件

検索条件

名前

社員ID、機種、電話番号など

検索

条件を入力し、選択グループ内から端末を検索できます。

■該当端末一覧

動態管理ステータス

端末毎の許可状況等が色別に表示されます。

- ユーザーにより動態管理が許可されています。
- 許可状態ですが位置情報設定がOFFのため取得できません。
- ユーザーによる動態管理の同意回答待ちです。
- ユーザーにより動態管理が拒否されています。

検索された端末が1ページ15件まで表示されます。

端末をクリックすることで、該当する番号の取得位置情報が表示されます。

直近24時間以内の取得位置情報がない場合はグレイアウトで表示されます。

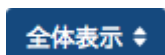
番号横には端末毎の動態管理の許可状況等が色別に表示されます。

■最新位置情報

検索された端末の24時間以内の最新位置情報がマップに表示されます。

一度に表示される端末は該当端末一覧に表示された15件(1ページ分)までです。

■全体表示

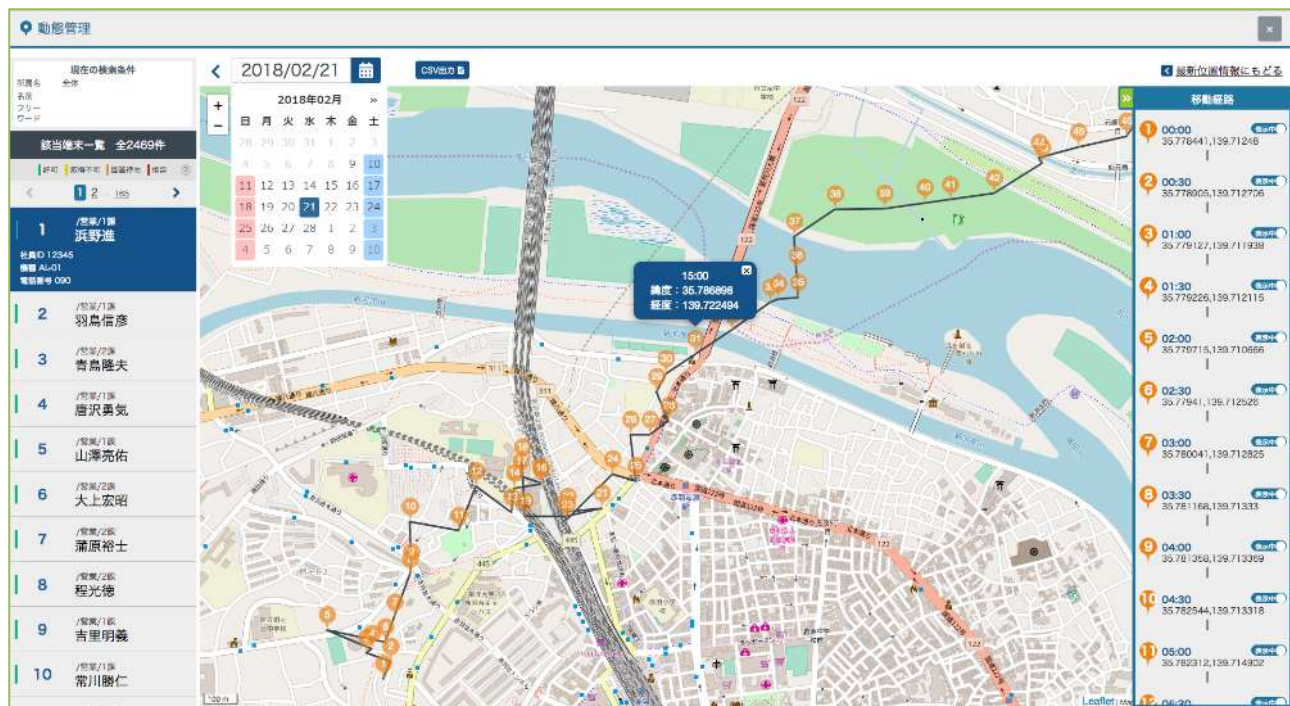


位置情報全体が表示されるようにマップを再表示します。

■経路

端末の移動経路を表示する画面へ遷移します。

【移動経路画面】



選択された端末の移動経路がマップに表示されます。

■表示日

2018/02/21

移動経路の表示日を選択できます。

クリックすることでカレンダーが表示されます。また、直接入力で指定も可能です。

※表示できるのは過去 30 日分までの位置情報です。

※日を跨いでの移動経路は表示できません。



移動経路表示日を 1 日進める、または 1 日戻します。



移動経路の表示日をカレンダーから選択できます。

■CSV 出力

CSV出力

移動経路を CSV 形式で出力できます。

出力項目: 取得時間, 緯度, 経度, 取得タイプ, 精度, 表示状態

■位置情報(取得時刻・緯度経度)



マップ、または移動経路でクリックした番号の取得位置情報が表示されます。

■移動経路



表示日の移動経路が一覧で表示されます。

クリックすると該当番号の位置情報がマップに拡大表示されます。

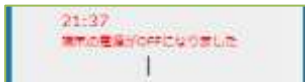


「表示中」をクリックすることでマップ上で該当番号を非表示にできます。
誤検知された不要な位置情報の非表示等にご利用ください。



位置情報の取得に失敗した場合、経路は表示されません。

■端末状態ログ



端末状態のログが移動経路一覧に表示されます。

位置情報が表示されていない時間帯の状態確認等にご利用ください。

《表示ログ》

「端末の電源が ON になりました」

「端末の電源が OFF になりました」

「位置情報の取得を開始しました」

「位置情報の取得を停止しました」

「端末の位置情報機能が ON になりました」

「端末の位置情報機能が OFF になりました」

「OS 自動省電力モードが ON になったため、以降位置情報が取得しづらくなります」

「OS 自動省電力モードが OFF になりました」

「ユーザーにより動態管理が許可されました」

「ユーザーにより動態管理が拒否されました」



Android OS により通知されるログを表示するため、
端末や端末の状態によっては誤検知される場合があります。

1. 概要

端末の「アプリ利用時間」「データ通信量」情報を集計し、専用の管理画面で統計情報を確認できます。
統計情報は端末の「所属グループ毎」と「端末毎」に表示できます。

■アプリ利用時間

【所属グループ統計情報】

- ・アプリ毎の合計利用時間
- ・アプリ毎の 1 台の平均利用時間
- ・アプリ毎の利用端末台数

【端末統計情報】

- ・アプリ毎の合計利用時間

■データ通信量

【所属グループ統計情報】

- ・端末毎の合計データ通信量

【端末統計情報】

- ・アプリ毎の合計データ通信量

※対応バージョン

アプリ利用時間 : Android OS 5.0 以降、SPPM Agent v3.26 以降

データ通信量 : Android OS 6.0 以降、SPPM Agent v3.31 以降

※STAR-MDM フル機能パックまたは STAR-MDM 拡張プランをご契約いただいたお客様は、無償でご利用いただけます。

※取得データの閲覧期間は 90 日間です。

【ご利用にあたっての注意】

- ・ アプリの利用状況は位置情報は端末利用者のプライバシー情報となるため、あらかじめ必ず端末利用者の許諾を取ってください。
- ・ SPPM Agent v3.01 未満で端末登録した端末で、アプリ使用時間、通信量の取得を行うためには、SPPM Agent v3.42 以降にバージョンアップする必要があります。
- ・ 集計対象となるグループに所属している端末数の上限は 5000 台までです。
SPPM 管理画面にログインしている管理者が管理している各グループの所属台数が 5001 以上では利用統計画面を開くことができないためご注意ください。

2. 申し込み方法

動態管理の申し込みは 2018 年 8 月 1 日を以って不要となりました。

管理画面の設定のみでご利用いただけます。

3. 設定方法

【動態管理 / 利用統計 利用設定】

その他＞動態管理／利用統計 利用設定 で利用統計を「利用する」設定にします。

※マスター管理者でのみ設定が可能です。

※詳細情報は「[動態管理／利用統計 利用設定](#)」をご覧ください。

【所属グループ設定】

利用統計では端末のグループ設定が必須となります。所属設定がない端末は利用統計画面の集計結果に表示されません。

・グループ管理でグループを作成する。

その他＞グループ管理から、端末利用者が所属するグループを作成してください。

・端末毎に所属先を設定する。

端末情報編集画面の【利用者情報】で所属先のグループを選択してください。

関連情報➡[「グループ管理」](#)

関連情報➡[「端末情報編集」](#)

【管理アカウント設定】

・管理者アカウントに管理グループを追加する。

その他＞管理者管理から、各管理者アカウントに設定させる管理グループを追加してください。

・管理者アカウントの管理グループ権限で「利用統計」を ON にする。

管理者アカウントの管理グループの権限設定で「利用統計」を ON にしてください。

※権限を設定されていない管理アカウントではメニューの『利用統計』ボタンをクリック時に利用できない旨のメッセージが表示されます。

(一般管理者とマスター管理者では表示内容に差分がございますのでご注意ください。)

※動態管理 / 利用統計の利用設定前の状態では権限操作はできません。

関連情報➡[「グループ管理」](#)

関連情報➡[「管理者管理」](#)

【端末適用】

・ポリシーを作成する

ポリシー管理から利用統計ポリシーを作成してください。

・端末に「動態管理」機能を適用する。

端末編集画面から作成した利用統計ポリシーを選択し、上書保存します。

※端末情報編集画面に「利用統計」を表示するには「登録表示設定」の利用統計にチェックを付けます。

関連情報➡[「端末情報編集」](#)

関連情報➡[「登録表示設定」](#)

4. 利用統計画面

メニューの「利用統計」ボタンから利用統計の専用管理画面を表示できます。

■機能を選択

「アプリ利用時間」と「通信量」から表示したい機能を選択できます。

■グループ選択

選択したグループに所属した端末を検索できます。

ログインしている管理者アカウントが管理権限を持つグループのみ選択可能です。

■検索条件

グループを選択するとグループ選択のプルダウン下に表示されます。

条件を入力し、選択グループ内から端末を検索できます。

※「アプリ利用時間」と「通信量」はグループ単位での集計となります。

検索条件で検索された端末一覧での集計表示ではないためご注意ください。

■該当端末一覧

該当端末一覧 全2件	
1	/営業/1課 山田
2	/営業/1課 鈴木

検索された端末が表示されます。

※表示日のアプリ利用情報がない端末はグレーアウトされます。
端末を選択すると端末個別のアプリ利用情報を確認できます。

■表示日

2018/02/21 日

利用統計の表示日を選択できます。

クリックすることでカレンダーが表示されます。また、直接入力で指定も可能です。

※当日のデータは表示対象外です。前日以前のデータが集計対象となります。

※表示できるのは過去 90 日分までです。

※利用通信量の場合は期間指定が可能です。



利用統計の表示日を 1 日進める、または 1 日戻します。



利用統計の表示日をカレンダーから選択できます。

4-1. アプリ利用時間

【アプリ利用時間画面 TOP】

■グループ選択時表示



選択したグループに所属している端末のアプリ利用統計情報が1日単位で表示されます。

※アプリの画面を表示している時間が集計されます。

- ① 選択したグループ内でアプリ利用情報がある端末の台数が表示されます。
アプリ利用情報がない端末は台数に含まれません。
- ② 選択したグループ内で利用されたアプリの一覧が表示されます。
- ③ アプリの「合計利用時間」「1台の平均利用時間」「利用端末台数」統計情報が表示されます。
グラフはグループ内での最大値を基準に作成されます。
- ④ 「合計利用時間」「1台平均利用時間」「利用端末台数」から選択した項目が濃く表示されます。
また、項目を選択した状態で「ソート」をクリックすると、対象項目のデータを基に「降順/昇順」でアプリ一覧が並び替えられます。

「合計利用時間」選択

1	電話アプリ com.incallui	137時間48分 2時間12分/台 37台				
---	-----------------------	-----------------------------	--	--	--	--

「1台平均利用時間」選択

1	電話アプリ com.incallui	137時間48分 2時間12分/台 37台				
---	-----------------------	-----------------------------	--	--	--	--

「利用端末台数」選択

1	電話アプリ com.incallui	137時間48分 2時間12分/台 37台				
---	-----------------------	-----------------------------	--	--	--	--

■端末選択時表示



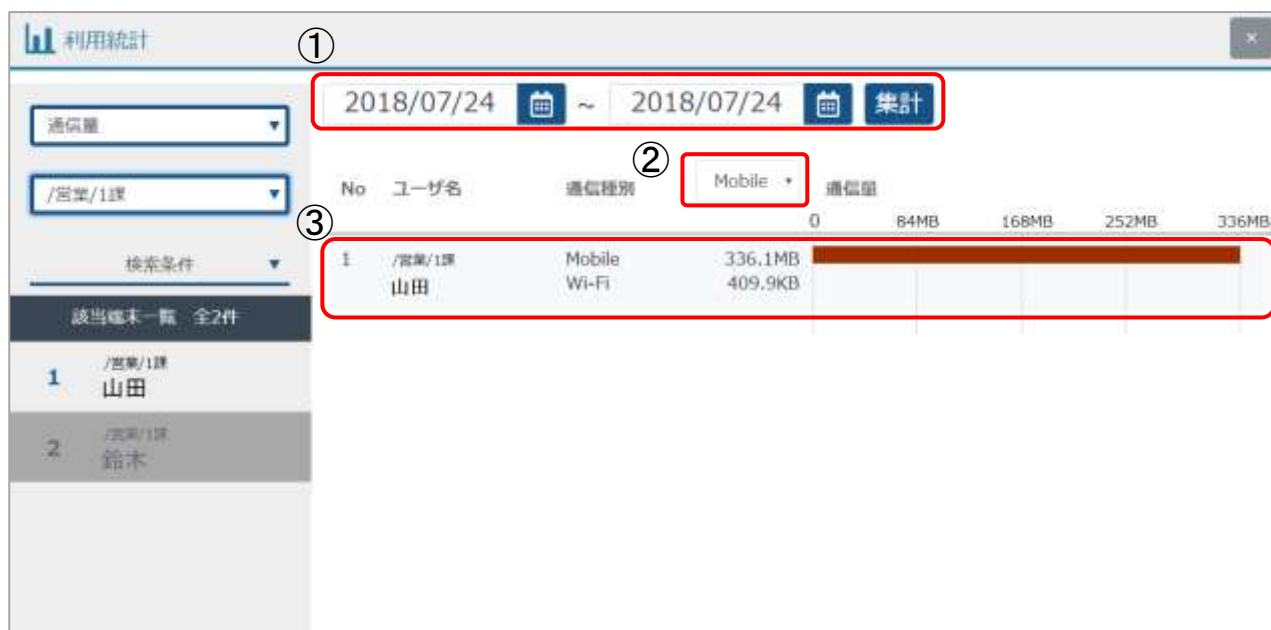
該当端末一覧で端末を選択すると、その端末で利用されたアプリの一覧が表示されます。

表示できる情報は「合計利用時間」のみです。

4-2. 通信量

【アプリ通信量画面 TOP】

■グループ選択時表示



選択したグループに所属している端末のデータ通信量情報が表示されます。

通信量は「WiFi 通信」と「モバイル通信(SIM 通信)」に分けて集計されます。

① 集計対象の期間を設定し、右側の「集計」ボタンを押下すると対象の期間の通信量が表示されます。
※集計が可能な期間は最大1ヶ月です。

② Mobile/WiFi 毎で通信量の多い順にソートをかけることができます。
※Mobile を選択している場合は Mobile の通信量の多い順に、
WiFi を選択している場合は WiFi の通信量の多い順にソートがかけられます。



③ 端末毎の Mobile/WiFi の通信量を一覧で確認することができます。
また通信量のグラフはグループ内での最大値を基準に作成されます。

■端末選択時表示

該当端末一覧で端末を選択すると、端末の集計期間中の通信量がグラフで表示されます。



また、画面を下にスクロールすると、端末の合計通信量とアプリ毎の通信量が確認できます。

利用統計

通信量

/営業/1課

検索条件

該当端末一覧 全2件

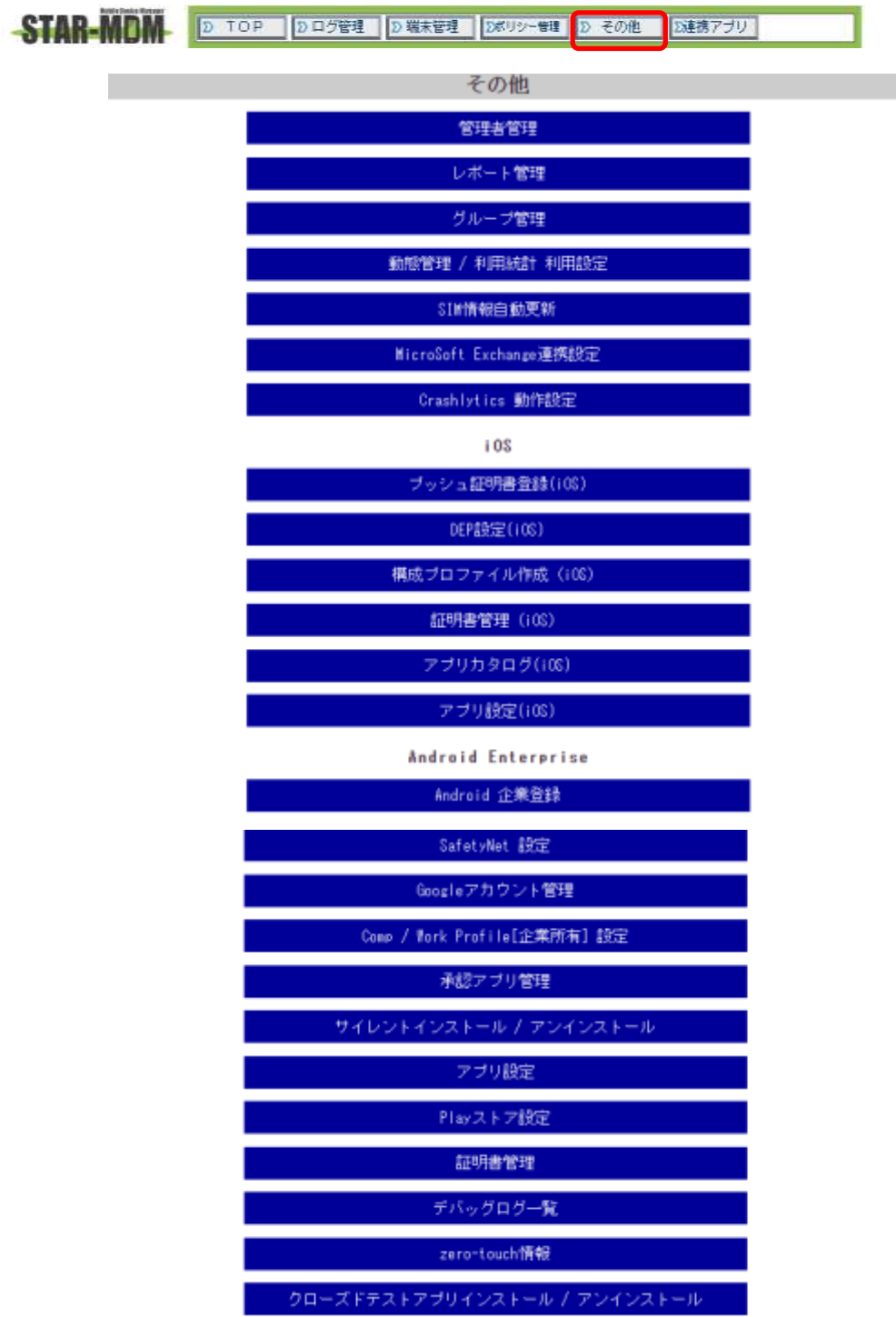
No	アプリ名	通信種別	通信量
合計		Mobile	2.7GB
		Wi-Fi	48.1MB
1	テザリング tethering	Mobile	2.2GB
		Wi-Fi	0B
2	Chrome com.android.chrome	Mobile	243.0MB
		Wi-Fi	9.8MB
3	YouTube com.google.android.youtube	Mobile	86.2MB
		Wi-Fi	48.7KB
4	Google Play開発者サービス com.google.android.gms	Mobile	56.4MB
		Wi-Fi	4.4MB
5	Slack com.Slack	Mobile	37.8MB
		Wi-Fi	505.9KB

① 通信事業者のデータ通信量とは異なる場合があります。

② サーバーに送信される前にアンインストールされたアプリの通信量データは、「アンインストール済みアプリ」と表示されます。

1. その他画面

メニューバーの[その他]をクリックすると、「その他」画面が表示されます。



iOS項目についてはiOS管理者マニュアルをご参照ください。

Android Enterprise項目については「Android Enterpriseマニュアル」をご参照ください。

2. 管理者管理

[管理者管理]をクリックすると、管理者の追加、削除、及びパスワード変更を含む編集のための「管理者一覧画面」が表示されます。

管理者管理 - 管理者一覧画面

選択	設定権	権限	編集	管理者ID	管理者名	電話番号	メールアドレス
☐	1	設定	編集				qa@axseed.co.jp
☐	1	設定	編集				r_tanaka@axseed.co.jp
☐	1	設定	編集				
☐		設定	編集				
☐	1	設定	編集				
☐	1	設定	編集				

・権限設定権を持つユーザをマスター管理者と呼びます。
 ・権限設定権を持たないユーザを管理者と呼びます。
 ・マスター管理者は他のユーザに権限設定権を付与できます。
 ・マスター管理者は必ず1名設定されている必要があります。
 ・マスター管理者は基本ポリシーの編集をできます。
 ・管理者ID欄に「(停止)または(凍結)」と表示されているアカウントは解除を行わないと利用できません。解除は「編集」から行うことができます。
 ※解除操作はシステム管理者または、マスター管理者が実行可能です。

[新規作成]をクリックすると、新たに管理者IDとパスワードを設定できます。

その後、利用開始に際して付与された管理者IDを削除してください。これにより、管理者ID及びパスワードの両方が自前のものになるので安全です。

管理者IDを削除するには、削除したい管理者IDの左横にあるチェックボックスにチェックを入れて、[削除]をクリックします。管理者IDが一つしかない場合には、その一つを削除することはできません。



一つしか設定していない管理者ID／パスワードを忘れると、STAR-MDM管理サーバのすべての情報を初期化しからの再設定が必要となります。管理者ID／パスワードは忘れないように注意してください。

設定権に「1」が付いているユーザーがマスター管理者、空欄になっているユーザーが管理者となります。マスター管理者は他のユーザーの情報を変更できますが、管理者は他のユーザーの情報を変更することはできません。

パスワードを変更したい場合には、変更したいアカウント名の左横の[編集]をクリックしてください。
 次のような「管理者情報更新画面」が表示されます。

「パスワード」及び「パスワード確認」の欄に新しいパスワードを入力することで、管理者パスワードを変更することができます。



- ・パスワードは英数字記号 8～32 字で設定してください。
- ・英字と数字を 1 文字以上含んで設定してください。
- ・パスワード確認用のテキストボックスは、ペーストと右クリックが禁止されます。

パスワード入力失敗によってアカウントが停止・凍結されている場合、「停止・凍結解除」のボタンが表示されます。解除する場合はボタンをクリックしてください。

■接続許可IPアドレス

「接続許可IPアドレス」に入力されたIPアドレス以外からのログインを制限できます。

※IPアドレスは複数入力可能です。その際はIPアドレスを「,(カンマ)」で区切って入力してください。

例) 「11.111.111.1,22.222.22.2」



- 接続許可 IP アドレスの設定により、管理画面へ一切ログインできなくなる場合があるため
 最低1つは IP アドレス制限無しのマスター管理者を用意することを推奨します。

■権限設定

権限設定にチェックを入れてユーザーデータを更新することで、そのユーザーをマスター管理者にすることが可能です。尚、マスター管理者は企業内に最低1名は必要となるため、すべてのマスター管理者を削除したり、全てのユーザーから権限設定のチェックを外したりすることはできません。

権限を設定したい場合は、変更したいアカウント名の左横の『設定』をクリックしてください。
次のような「権限設定」画面が開きます。

新しく管理グループを登録するには、[管理グループ追加]をクリックします。
次のような「グループ権限設定」画面が開きます。

監視指示処理権限									
端末ロック	ハードリセット	位置情報取得	データ消去	即時応答	パスワードリセット	ライセンスキーリセット	アンインストール有効化	端末再起動	デバッグログ取得
☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

機能権限							
サーバ監視開始通知	緊急時	異常検知・通知	Agent管理	パスワード管理	デバイス制御	宛先電話番号履歴	宛先電話番号登録
☒	☒	☒	☒	☒	☒	☒	☒
位置情報取得	アプリ配信	利用アプリ登録	アプリ一覧	アプリ固定化	Wi-Fi接続切断	接続切断履歴	ファイル配信
☒	☒	☒	☒	☒	☒	☒	☒
端末番号無効化	お子(設定)	アプリ管理(iOS)	構成プロファイル配信(iOS)	リモート監視	メッセージ配信	構成プロファイル登録(iOS)	利用アプリ検知(iOS)
☒	☒	☒	☒	☒	☒	☒	☒
AVR管理	電話帳配信	IEP設定(iOS)	VPN管理配布(iOS)	アプリアンインストール解除	動作管理	利用統計	IPアドレス検索
☒	☒	☒	☒	☒	☐	☐	☐
キオスク管理							
☐							

グループ選択

選択グループ

☐ /

☐ /開発部(部)/

元に戻す 戻る 新規作成

この画面では、操作できる権限の設定とそれを適用するグループを指定します。チェックの入っているものが権限有りとなります。また、最も上位のグループは “/” と表示されています。この “/” を選択した場合は、すべての端末に対して、ここで指定された権限を持つことになります。

必要な権限設定を行ったら[新規作成]をクリックして保存してください。保存後は次のような画面になります。

「✓」の付いている項目が権限を持っている項目となります。ポリシーの権限を空欄にした場合、当該グループに含まれる端末に対してポリシーを適用することや、ポリシーを作成することができません。緊急時指示の権限を空欄にした場合、該当端末の「緊急時指示画面」で指示ボタンが表示されなくなります。

尚、複数のグループの権限を追加して設定することが可能ですが、下記のような制限があります。

例.

グループ"/"に対して全権を許可。

グループ"/東京本社"に対して緊急時指示のみ許可。

上記のように上位のグループで権限設定を実施している場合、上位グループで設定された権限が優先されるため、上記例の場合、"/東京本社"に対しても全権を持つことになります。

誤って権限を設定した場合は、当該グループの左横に表示される[編集]をクリックして「グループ権限設定」画面を開き、編集を行ってください。

※ユーザー権限の変更は、一度ログアウトした後に有効になります。

※管理者にグループ権限が設定されている場合、ログ管理画面に表示されるログは、そのグループに属す端末のものになります。

※管理者にグループ権限が設定されている場合、[そのグループ]と[そのグループの下層に位置するグループ]に属する端末に関する通知のみ、管理者に届きます。

<例>

管理グループ「/東京本社/営業企画部」に所属する端末のアラートメールについては

「/」の管理権限を持つ管理者、

「/東京本社」の管理権限を持つ管理者、

「/東京本社/営業企画部」の管理権限を持つ管理者に送信。

※ポリシー一括設定にてポリシーを適用する場合、権限の無いグループに所属している端末を「端末管理」画面上で選択することはできません。管理者の権限設定、または端末の所属グループを確認してください。

※新機能(ポリシー)が追加された場合は自動で権限の設定はされませんので、個別に権限設定が必要になります。

【「マスター管理者」と「管理者」について】

管理者には「マスター管理者」と「管理者」の2種類あります。

「マスター管理者」は管理者の追加や権限の設定を行うことができます。

「管理者」は端末の管理を行うことができますが、管理者の追加や権限の設定はできません。

	マスター管理者	管理者
権限の設定	○	×
グループの追加	○	×
管理者の追加	○	×
他の管理者が作成したポリシーの変更	○ *1	×
自身が作成したポリシーの変更	○ *1	○ *1
緊急時指示	○ *1	○ *1
管理下の端末のCSV連携	○	○
その他のAndroid Enterprise 機能	○	×

*1:ポリシーの追加、変更、削除、緊急指示は、権限設定で許可されたものののみ実施可能です。

3. レポート管理

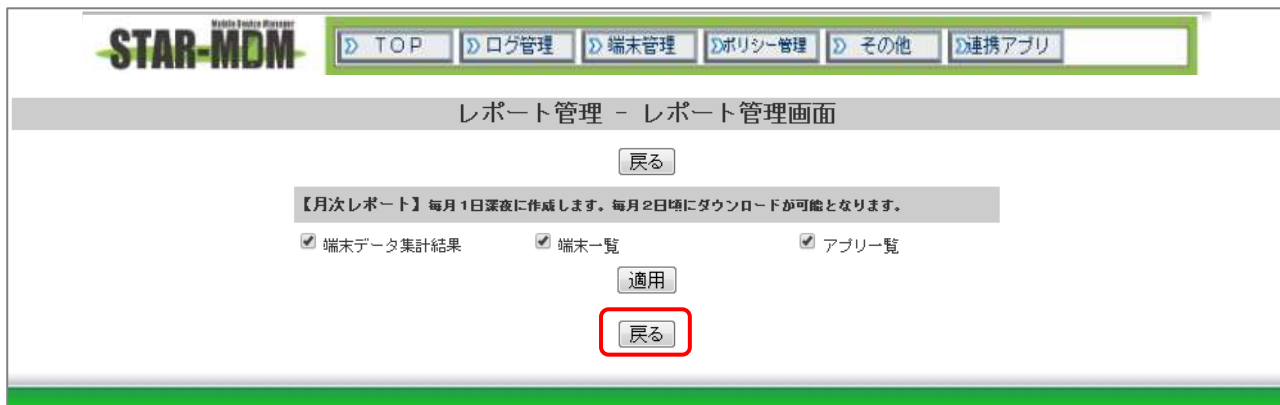
STAR-MDMで管理している端末情報やアプリ一覧などをレポートとして出力する設定を行う機能です。

【レポート出力設定について】



①.管理画面メニューから「その他」⇒「レポート管理」ボタンを押すと上記の画面が表示されます。





②.月次でレポートを出力したい項目にチェックを入れて、適用ボタンを押します。

項目は下記の内容から選択できます。

■「端末データ集計結果」:

管理画面に登録されている端末の OS 別集計データ、機種別集計データ、Android OS バージョン別集計データ、iOS バージョン別集計データが統計グラフと共に出力されます。

■「端末一覧」:

管理画面に登録されている端末の電話番号、氏名、機種名、IMEI、Wi-Fi MAC アドレス、OS、OS バージョン、API レベル、E-SDK レベル、Agent ver、端末メールアドレス、PC メールアドレス、所属が一覧で出力されます。

■「アプリ一覧」:

管理画面に登録されている端末の電話番号、端末 ID、アプリ名、パッケージ名、バージョン、更新日時が一覧で出力されます。

■「緊急指示操作ログ集計結果」

緊急指示(端末ロック指示・データ消去・ワイプ(端末初期化))が実施された統計データが出力されます。

☆レポート出力設定について

レポートは毎月1日の深夜の時間帯に出力処理を実行します。

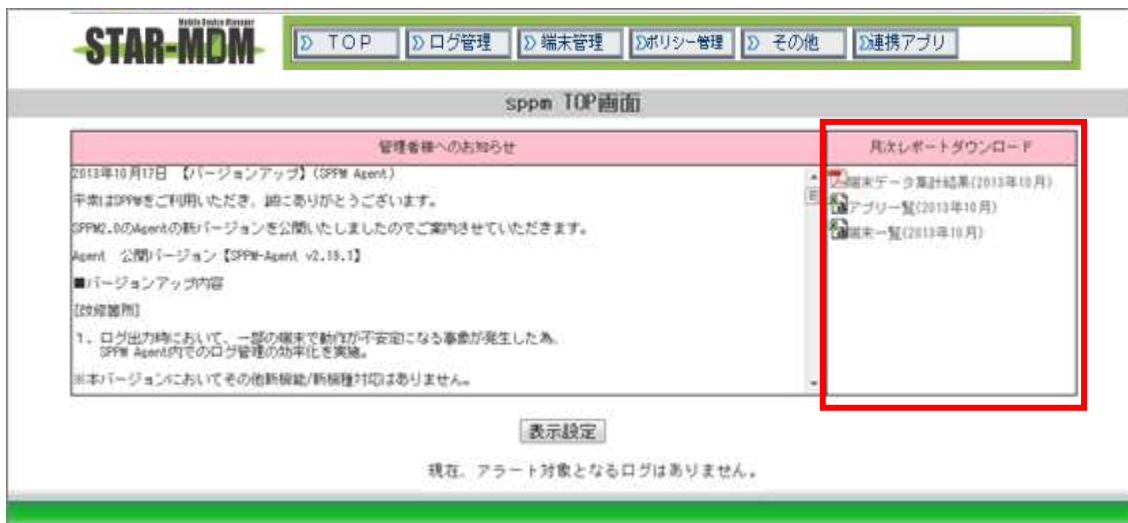
出力処理以前にチェックを付けた項目のみレポート生成されます。

権限設定権を持つユーザである マスター管理者のみレポート管理機能の項目が表示され、設定を行うことができます。

👉 [「マスター管理者」と「管理者」について](#)

【レポートダウンロードについて】

レポートはSTAR-MDM管理画面TOPからダウンロードできます。月次レポートの出力設定を行い、毎月1日の出力処理が完了すると、STAR-MDM管理画面TOPに各種レポートが生成されています。



①. レポートダウンロード欄のデータをクリックすると、該当データがダウンロードできます。

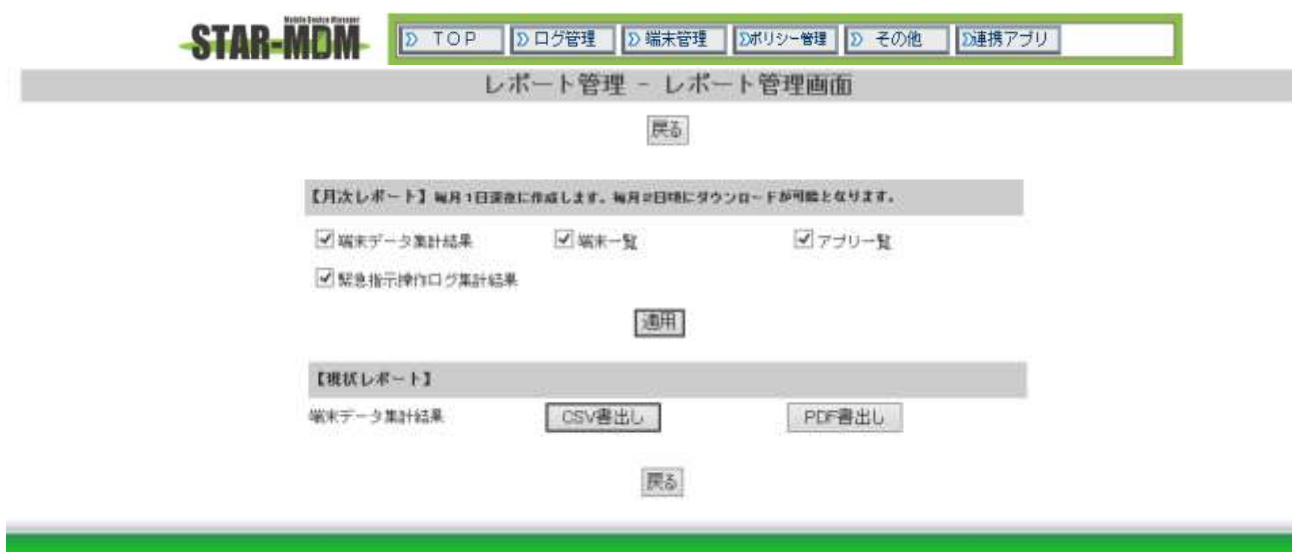
☆レポートダウンロードについて

権限設定権を持つユーザである マスター管理者のみレポートダウンロード欄が表示され、ダウンロードを行うことができます。

レポートのダウンロード可能期間は出力から3ヶ月間となります。3ヶ月経つと自動削除されます。

【現状レポートについて】

現状レポートの書出しボタンをクリックすると、現時点でのSTAR-MDMで管理している端末情報を出力します。



4. グループ管理

「グループ管理」の項目は、マスター管理者のみに表示されます。

管理者ではグループを作成することはできません。

グループ管理

グループ新規登録

グループポリシー管理

戻る

グループ新規登録

《グループ登録について》

グループ管理 - グループ 新規登録

グループ名称:

登録

グループ名称は「/」で区切る形で入力してください。登録文字数は1,000文字までとなります。
例、/東京本社/営業企画部/営業一課

グループ情報 未登録

グループ名称の欄にグループ名を入力して、[登録]をクリックします。

グループ名は「/」で区切った形で階層を指定します。部署名は文字コード順で並ぶ為、必要に応じて先頭に001などコードを指定してください。

尚、グループ名称に指定に利用することが出来る文字は下記の通りです。

- ・半角英数字、半角記号(# \$ % & () _)、全角文字 (Windows機種依存文字は除く)

グループが登録されると、以下のようにグループ名称がリスト表示されます。

グループ管理 - グループ 新規登録

グループ名称:

登録

グループ名称は「/」で区切る形で入力してください。登録文字数は1,000文字までとなります。
例、/東京本社/営業企画部/営業一課

チェックしたグループを削除

削除	グループ名称
☐	/大塚支社
☐	/東京本社
☐	/東京本社/営業部
☐	/東京本社/営業部/第三課
☐	/東京本社/経理部

《グループ削除について》

管理者管理 - 権限設定

管理グループ追加 管理グループ削除 (チェックした管理グループが削除されます)

グループ	権限	権限	権限	権限	権限	権限	権限	権限
☐ 基本	端末ロック	ハードリセット	位置情報取得	データ消去	異動記録	パスワードリセット	ライセンスキーリセット	アンインストール有効化
	サードパーティ連携	緊急時	異常検知・通報	Agent管理	パスワード管理	デバイス制御	宛先番号検索	宛先番号制御
	位置情報取得	アプリ制御	利用アプリ制御	アプリ一覧	API設定	Wi-Fi接続制御	接続先URL制御	ファイル配布
	端末番号通知	Wi-Fi 設定	アプリ管理(追加)	構成プロファイル配布				
☐ 基本 / 営業	端末ロック	ハードリセット	位置情報取得	データ消去	異動記録	パスワードリセット	ライセンスキーリセット	アンインストール有効化
	サードパーティ連携	緊急時	異常検知・通報	Agent管理	パスワード管理	デバイス制御	宛先番号検索	宛先番号制御
	位置情報取得	アプリ制御	利用アプリ制御	アプリ一覧	API設定	Wi-Fi接続制御	接続先URL制御	ファイル配布
	端末番号通知	Wi-Fi 設定	アプリ管理(追加)	構成プロファイル配布				

戻る

「管理者管理」の「管理者一覧画面」>「権限設定」画面から、削除するグループのチェックボックスにチェックを入れて[チェックした管理グループを削除]をクリックし、当該グループの管理権限を削除します。

上記が完了した後、「グループ管理」の「グループ 新規登録」画面にて、上記で削除をしたグループ名称のチェックボックスにチェックを入れて[チェックしたグループを削除]をクリックし、グループを削除します。

グループ管理 - グループ 新規登録

グループ名称:

グループ名称は、[/]で区切る形で入力してください。登録文字数は1,000文字までとなります。
例: /東京本社/営業企画部/営業一課

削除	グループ名称
☐	/大塚支社
☐	/東京本社
☐	/東京本社/営業部
☐	/東京本社/営業部/第三課
☐	/東京本社/経理部

尚、グループの削除が完了しますと端末にはグループが設定されませんので、新たにグループを設定してください。

グループポリシー管理

作成したグループごとに、ポリシーを適用させることができます。

「対象グループ」から該当のグループを選択し、ポリシーを適用してください。

※反映されるタイミングは、サーバー端末間通信時となります。

端末管理 - 端末情報編集画面

対象グループ

グループ選択

グループ

1/1営業部

2/2開発部

3/3総務部

ポリシー設定

サーバー/端末部通信	基本ポリシー	ポリシー編集
緊急時	<適用中のポリシーを優先>	ポリシー編集
異常検知・通報	<適用中のポリシーを優先>	ポリシー編集
Agent管理(Android)	<適用中のポリシーを優先>	ポリシー編集
Agent管理(Windows)	<適用中のポリシーを優先>	ポリシー編集
パスワード管理	<適用中のポリシーを優先>	ポリシー編集
デバイス制御	<適用中のポリシーを優先>	ポリシー編集
電話番号履歴	<適用中のポリシーを優先>	ポリシー編集
電話番号制限	<適用中のポリシーを優先>	ポリシー編集
位置情報取得	<適用中のポリシーを優先>	ポリシー編集
アプリ配信	<適用中のポリシーを優先>	ポリシー編集
利用アプリ制限(Android)	<適用中のポリシーを優先>	ポリシー編集
利用アプリ制限(Windows)	<適用中のポリシーを優先>	ポリシー編集
アプリ一覧	<適用中のポリシーを優先>	ポリシー編集
APN固定化	<適用中のポリシーを優先>	ポリシー編集
Wi-Fi接続先制限	<適用中のポリシーを優先>	ポリシー編集
Wi-Fi設定	<適用中のポリシーを優先>	ポリシー編集
接続先URL制限	<適用中のポリシーを優先>	ポリシー編集
端末番号義務化	<適用中のポリシーを優先>	ポリシー編集
ファイル配布	<適用中のポリシーを優先>	ポリシー編集
アプリ管理(iOS)	<適用中のポリシーを優先>	ポリシー編集
構成プロファイル配信(iOS)	<適用中のポリシーを優先>	ポリシー編集
SIM監視	<適用中のポリシーを優先>	ポリシー編集
メッセージ配信	<適用中のポリシーを優先>	ポリシー編集
構成プロファイル削除(iOS)	<適用中のポリシーを優先>	ポリシー編集
KNOX管理	<適用中のポリシーを優先>	ポリシー編集
利用アプリ検知(iOS)	<適用中のポリシーを優先>	ポリシー編集
電話帳配信	<適用中のポリシーを優先>	ポリシー編集
DEF設定(iOS)	<適用中のポリシーを優先>	ポリシー編集
VPN管理配布(iOS)	<適用中のポリシーを優先>	ポリシー編集
アプリアンインストール制限	<適用中のポリシーを優先>	ポリシー編集
制限管理	<適用中のポリシーを優先>	ポリシー編集
利用統計	<適用中のポリシーを優先>	ポリシー編集
中央スク管理	<適用中のポリシーを優先>	ポリシー編集
Android Enterprise (Opa_BuiltProfile)		
緊急時	<適用中のポリシーを優先>	ポリシー編集
デバイス制御	<適用中のポリシーを優先>	ポリシー編集

[0]件の端末にポリシーの適用を行ってもよろしいですか?

元に戻す 戻る 設定初期化 適用

5. 動態管理 / 利用統計 利用設定

「動態管理」「利用統計」の機能を有効にするための設定を行えます。

※「動態管理 / 利用統計 利用設定」の項目は、マスター管理者にのみ表示されます。

マスター管理者IDでログインし、「利用する」の項目のチェックボックスにチェックを入れ「適用」ボタンをクリックすると動態管理/利用統計のそれぞれの機能を利用することができます。

動態管理 / 利用統計 利用設定		
機能名称	利用する	利用状況
動態管理	☐	動態管理は有効ではありません。
利用統計	☐	利用統計は有効ではありません。

※動態管理/利用統計は位置情報等の個人情報を扱うため、利用者へ許諾を得た上でご利用ください。
※一度、機能を有効にすると無効にする事は出来ません。

マスター管理者が有効にした場合、利用状況の欄に有効にした日時と管理者IDが履歴として表示されます。

動態管理 / 利用統計 利用設定		
機能名称	利用する	利用状況
動態管理	☒	[2018-07-11 15:34:33.896]に[]が[ON]にしました。
利用統計	☒	[2018-07-11 15:34:33.896]に[]が[ON]にしました。

※動態管理/利用統計は位置情報等の個人情報を扱うため、利用者へ許諾を得た上でご利用ください。
※一度、機能を有効にすると無効にする事は出来ません。

【申込書によりご利用中のお客様】

申込書によりご利用されているお客様は、利用状況には「申込書によりスターネット株式会社が有効にしました。」と表示されます。

動態管理 / 利用統計 利用設定		
機能名称	利用する	利用状況
動態管理	☒	申込書によりスターネット株式会社が有効にしました。
利用統計	☒	申込書によりスターネット株式会社が有効にしました。

※動態管理/利用統計は位置情報等の個人情報を扱うため、利用者へ許諾を得た上でご利用ください。
※一度、機能を有効にすると無効にする事は出来ません。

● 利用設定は有効にすると無効にする事はできません。

● 「動態管理 / 利用統計 利用設定」画面から有効に設定しても、管理者権限の動態管理/利用統計の項目にチェックがない場合はメニューバーの「動態管理」「利用統計」ボタンは有効になりません。

6. SIM情報自動更新



利用中の携帯電話をスマートフォンに置き換えるケースでは、各ユーザーが持っているSIMをスマートフォンの初期設定時に使うことが困難です。その場合は、管理者が用意した初期設定用のSIMやWi-Fi通信でSTAR-MDMの初期設定を行うことが可能です。

- ①「SIM情報自動更新」の項目で[自動更新する]にチェックを入れ、[上書保存]してください。
- ②管理者が用意した初期設定用のSIMやWi-Fi通信を用いて、端末にSTAR-MDMの初期設定を行い、設定が完了した端末をユーザーに渡します。
- ③端末を受け取ったユーザーが自分のSIMを装着し、端末を起動すると、SPPM AgentはSTAR-MDM管理サーバへの定期通信（ポーリング）を開始します。
- ④[自動更新する]にチェックが入っていると、端末からSTAR-MDM管理サーバへの定期通信時に、装着してあるSIMの電話番号が端末情報に反映され、端末一覧の端末電話番号も変更されます

8. Crashlytics設定

Crashlytics 動作設定

Crashlytics 動作設定

Crashlytics は端末内において SPPM Agentが異常終了した際にエラー情報を Crashlyticsサーバにアップロードします。
エラー情報にはIMEIやユーザ情報は含まれません。

☒ Crashlytics 機能を有効化する。

元に戻す

戻る

保存

Crashlytics は SPPM Agent が異常終了を起こした際にエラー情報等を収集する為の機能であり、SPPM Agent の安定性の向上を目的とした機能です。

収集される情報に関しては異常終了に関する情報のみで、ユーザ情報や端末の IMEI などは含まれませんが、一部の情報は Crashlytics のサーバ内に格納されます。

尚、本機能はSTAR-MDMサーバの管理画面設定により停止する事も可能です。

※SPPM Agent v3.66 以降では、非対応です。

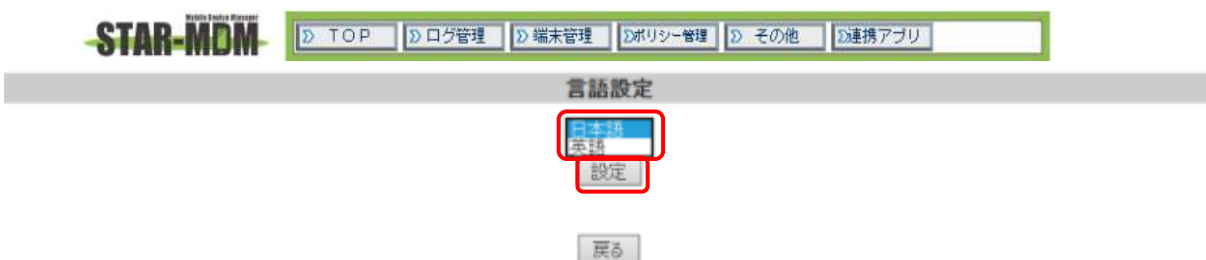
9. 言語表示設定

本機能はSTAR-MDMの管理画面表示言語を、英語と日本語に切り替える事ができます。

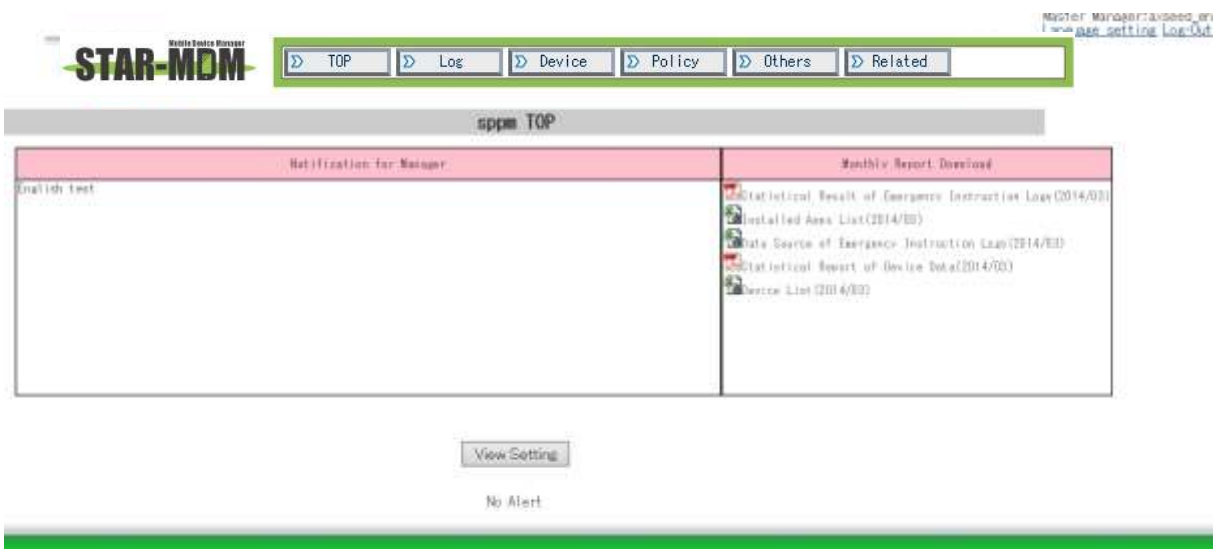
【言語切り替えについて】



STAR-MDM管理画面の右上に表示されている管理者情報下の「言語設定」を選択します。



言語設定画面が表示されるので、日本語か英語を選択し「設定」ボタンを押下します。



設定した言語で管理画面が表示されます。言語を再度切り替える場合は同様の手順となります。



言語切り替え設定は設定時にログインしている管理者のみ適用となります。

その他の管理者には適用されません。

10. デバッグログ一覧

Android Enterprise 端末から受け取ったデバッグログを、ダウンロードすることができます。

※あらかじめ、緊急指示画面にて「デバッグログ取得指示」を実施する必要があります。

「デバッグログ取得指示」の詳細は、「[緊急時](#)」ポリシーをご参照ください。

デバッグログ一覧		
※作成されて30日経過したデバッグログは自動で削除されます。		
端末ID	電話番号	作成日
		2020/03/18 15:40
		2020/03/18 15:40
	none	2020/03/18 15:40
	none	2020/03/18 15:40
		2020/03/18 15:39
	none	2020/03/18 15:39

【デバッグログダウンロード方法】

端末 ID 欄のうち、デバッグログをダウンロードしたい端末の ID 情報をクリックしてください。

デバッグログの Zip ファイルがダウンロードされます。

※デバッグログの保存期間は 30 日間です。保存期間終了後は自動的にデータは削除されます。

【デバッグログが無い場合】

ダウンロード可能なデバッグログが 1 つも存在しない場合、以下のような画面が表示されます。

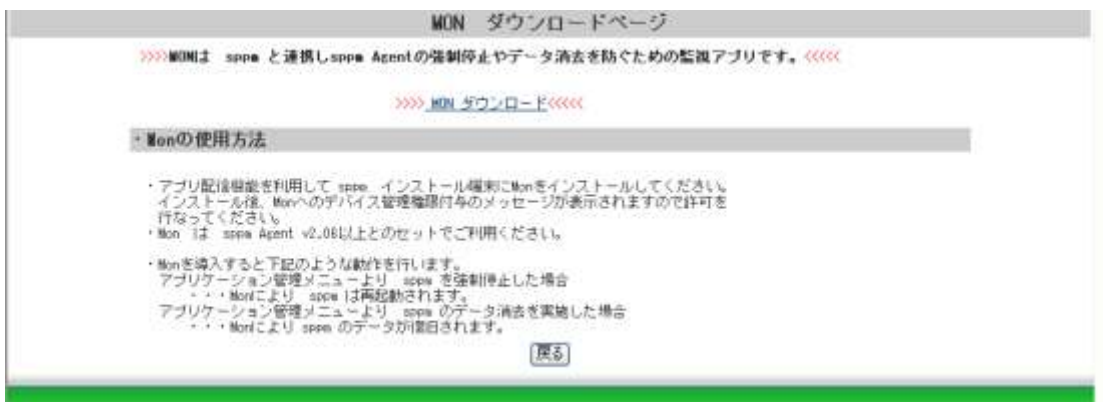
デバッグログ一覧		
※作成されて30日経過したデバッグログは自動で削除されます。		
端末ID	電話番号	作成日
作成済みのデバッグログがありません。		

1. 連携アプリ画面

メニューバーの[連携アプリ]をクリックすると、「連携アプリ」画面が表示されます。



2. Mon(SPPM監視ソフト)



SPPM Agentの強制停止やデータ消去を防ぐための監視アプリです。

Monのインストール用ファイル(apk)は、本画面の[MON ダウンロード]をクリックして入手してください。各端末へのインストールは、STAR-MDMの「アプリ配信」機能にて可能です。

関連情報 [「アプリ配信」](#)

Monはデバイス管理権限を持ったソフトとして動作します。インストール後、SPPM Agentのインストール時と同様にデバイス管理権限付与の確認メッセージが表示されますので[有効にする]を選択してください。

※メッセージ内容に端末の仕様に依存します。

※Monはユーザーインターフェースを持たないため、インストールを行っても端末のアプリトレイにアイコンは表示されません。

3. AV連携アプリ



BBソフトサービス株式会社の「Internet Virus Wall(IVW)」のウイルス／マルウェア対策アプリが用意されています。併用してのアンチウイルスエンジンでウイルス／マルウェア検知を行うこともできます。

STAR-MDMと各ウイルス／マルウェア対策アプリは、下記の連携を実現します。

- STAR-MDM管理サーバに登録済みの端末へのウイルス対策アプリのリモートインストール
- ウイルス対策アプリの稼働状況の把握(端末管理画面での一覧表示)
- ウイルス／マルウェア検知時にアラート通知(管理画面表示とメール通知)
- 検知したウイルス／マルウェアのアンインストールを義務化(別途アプリ一覧ポリシー適用が必須)
- 検知したウイルス／マルウェアのアンインストールの表示とメール通知
- 端末ユーザーによるウイルス対策アプリの停止の検知とメール通知
- 端末ユーザーによるウイルス対策アプリのアンインストールの検知とメール通知
- ウイルス対策アプリのライセンス期限の表示とメール通知(7日前から)
- ウイルス対策アプリのライセンス切れの表示とメール通知

これら一連の機能により、管理者はSTAR-MDMの管理画面でウイルス対策アプリの稼働状況を把握することができ、IT監査に必要な情報を得ることができます。

【動作環境】

以下の OS バージョンの端末にてご利用いただけます。

Internet Virus Wall : Android OS 4.x～13.x

【連携状態表示等】

端末一覧画面

自動更新

登録表示設定

一覧表示設定

データ並替

CSV連携

DEP端末更新

ON

☐ 2(端末製造)法適用

全選択

選択済:

ポリシー適用

検索条件:

追加

解除

選択	品名・品ス	種別	形態	端末識別番号	カテゴリー	利用状況	DEP動作稼働日時	Lockout	キオスク管理	DEP1 設定
☐	         	端末	指立	none			未インストール			
☐	         	端末	指立	xxxx			未インストール			
☐	         	端末	指立	xxxx			未インストール			
☐	         	端末	指立				 稼働中/2022-12-31 18:07:28			
☐	         	端末	指立	none			未インストール			
☐	         	端末	指立	none			未インストール			
☐		端末								
☐		端末								
☐	         	端末	指立	xxxx			未インストール			
☐		端末								
☐		端末								
☐		端末								
☐		端末								
☐	         	端末	指立	none						
☐	         	端末	指立	xxxx			 稼働中/2022-07-21 17:01:00			
☐		端末								
☐		端末								
☐		端末								
☐	         	端末	指立	none			未インストール			
☐		端末								

「端末一覧画面」にて、連携設定したウイルス／マルウェア対策アプリの稼働状況を確認できます。

■未インストール

端末にアプリがまだインストールされていないことを示します。

■稼働中

アプリが正常に稼働していることを示しています。

■停止中

アプリの初期設定が完了していない場合や、アプリが強制停止または削除されていることを示しています。

■ 端末状態シグナル

ウイルス／マルウェアを検知すると当該端末のアラート・シグナルが赤に変わります。

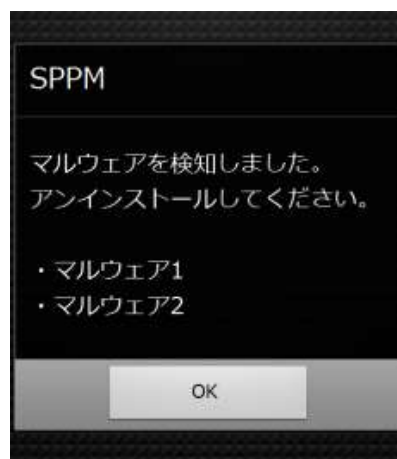
また、「アプリ一覧」ポリシーで“アプリ一覧を取得する”が適用されている場合、ウイルス／マルウェアを検知すると、「端末情報画面」の「インストールアプリ一覧」にて以下のように背景を赤色で表示します。

インストールアプリ一覧		利用アプリ制限設定作成	リスト取得日 2012-03-26 21:32:59
アプリ名	バージョン	パッケージ名	更新日時
AllBroadcastReceiver	0.3	jp.co.axseed.android.abr	
CA'zCAFE	1.0.0	com.nec.android.nmc.cazcafe	
Cメール	2.3.3	com.android.mms	
EICAR Anti Virus Test	1.0	uk.co.extorlan.EICARAntiVirusTest	
ES ファイルエクスプローラー	1.6.1.3	com.esstrongs.android.pop	
Eメール	1.5.2	com.aplixcorp.email	
Flash Player Settings	11.1.111.7	com.adobe.flashplayer	
G'zGEAR	1.0	com.nec.android.nmc.gzgear.menu	
GREEマーケット	2.1.0	jp.gree.android.pf.greeapp1753	
Gmail	2.3.5.2	com.google.android.gm	
Google+ 通知	2.0.00	com.google.android.gm.notifications	

端末では、検知したウイルス／マルウェアを以下のように表示（一度に複数検知した場合は全部を表示）し、[OK] ボタンで各ウイルス／マルウェアのアンインストール画面を表示します。

※一度に複数検知した場合は、検知したウイルス／マルウェアを全部表示します。

[キャンセル] をクリックしても、アンインストールが実行されるまで、アンインストール画面を表示し続けることで、端末ユーザーにウイルス／マルウェアのアンインストールを義務付けます。



ウイルス／マルウェアの検知、アンインストール、また IVW というウイルス／マルウェア対策アプリの強制停止などは、すべてログに記録されます。

※ウイルス／マルウェアの検知／アンインストールをログに出力するにはアプリ一覧を有効にしたポリシーの適用が必要です。

Internet VirusWall(IVW)



IVWのインストール用ファイル(apk)ファイルは、本設定画面の[IVWダウンロード]／[マニュアルダウンロード]をクリックして入手してください。各端末へのインストールは、STAR-MDMの「アプリ配信」機能にて可能です。

関連情報  [「アプリ配信」](#)

連携設定にて[連携する]を選択すると、「端末一覧画面」で連携状況を把握できるようになります。

IVWは、STAR-MDMの利用状況と連動するため、ライセンスキーがありません。従って各端末へのライセンスキーの設定や利用期限等を管理するといった手間が不要です。

また、以下の場合に、その端末の属するグループの管理者及び端末ユーザーへ通知メールを送信することができます。

- ・マルウェアを検知した際
- ・マルウェアのアンインストールを確認した際(アプリ一覧ポリシーを別途適用する必要があります)
- ・IVWをユーザーがアプリ管理画面等で停止させた際
- ・IVWをユーザーがアンインストールした際

IVWをインストールしている場合、端末一覧画面で「最終接続日時」が確認できます。

IVW/最終接続日時	
	稼働中/2022-04-26 13:23:54



IVW の初回スキャン時、「SCAN START」のボタン押下時、「クラウドポーリング間隔」で設定した時間で通信が発生した場合などに最終接続日時が更新されます。

【IVWインストール・起動手順】



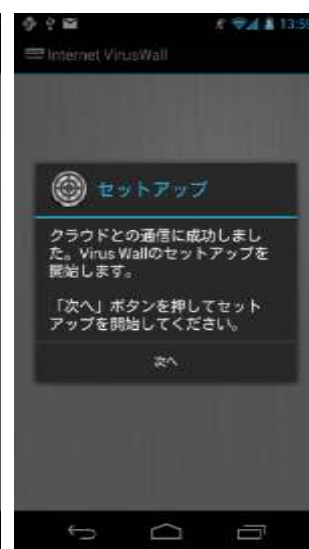
①



②



③



④

- ① IVWを起動し、「ストレージ」の権限ダイアログが表示されたら「許可」をタップします。
- ② [使用許諾契約書に同意してVirus Wallを利用する]をタップします。
- ③ クラウドサーバと通信してセットアップが準備されます。
- ④ [次へ]をタップします。



⑤



⑥



⑦



⑧

- ⑤ セットアップの開始の画面になりますので、[開始]をタップします。
- ⑥ セットアップが開始されます。
- ⑦ 初期スキャンが実行されます。
- ⑧ 初期スキャンが完了すると利用可能となります。端末の[ホーム]ボタンあるいは[バック]ボタンをタップして、IVWを終了してください。

4. E-SDK専用モジュールアプリ

SPPM Agent v2.18 以降の Agent と Samsung Galaxy 端末向けの専用モジュールアプリを端末にインストールする事でさらに詳細な制御をする事が可能になりました。

E-SDK を用いた Samsung Galaxy 端末向けの新機能は、フル機能パックで利用可能です。

尚、Galaxy 端末毎に対応している E-SDK バージョンが異なり、利用できる機能に違いがありますので下記機能対応表でご確認ください。

※端末の E-SDK バージョンは SPPM (Agent 2.18 以降) 起動後のメニュー画面で確認ができます。

※E-SDK バージョン 4 以降の端末では、SPPM Agent v2.29 以降がインストールされていれば、E-SDK モジュールアプリを別途インストールする必要はありません。

	機能詳細	対応 E-SDK バージョン
位置情報取得ポリシー	位置情報取得指示の際に、GPS 機能を自動的に有効にします。	3.0 以上
	「位置情報取得後に GPS 機能を OFF にする。」にチェックを付けると、位置情報取得終了時、または位置情報取得解除時に、GPS 機能が自動的に OFF になります。	3.0 以上
端末暗号義務化ポリシー	外部ストレージの暗号利用を義務化します。	3.0 以上
デバイス制御ポリシー	Wi-Fi テザリングを制限します。従来の制限方法と異なり、有効にするボタンがグレースアウトします。	2.0 以上
	USB テザリングを制限します。従来の制限方法と異なり、有効にするボタンがグレースアウトします。	2.0 以上
	外部 SD カードを制限します。従来の制限方法と異なり、マウントするボタンがグレースアウトします。	2.0 以上
	OS のバージョンアップを制限します。	3.0 以上
	USB を接続した際の MTP モードを制限します。	2.0 以上
	USB 接続時のマストレージ接続を制限します。	2.0 以上
	USB デバッグ機能を制限します。	2.0 以上
	USB ストレージへの接続を制限します。	4.0 以上
	NFC の利用を制限します。	2.0 以上
	壁紙の変更を制限します。	3.0 以上
	マイク機能を制限します。	2.0 以上
	ホームボタン押下時のホームアプリの起動を制御します。	2.0 以上
	ホームボタン長押しでのアプリ履歴表示を制限します。	3.0 以上
	ボリュームアップボタンを無効化します。	3.0 以上
	ボリュームダウンボタンを無効化します。	3.0 以上
	バックボタンを無効化します。	3.0 以上
	メニューボタンを無効化します。	3.0 以上
	電源ボタンを無効化します。	3.0 以上
	擬似ロケーション機能を制御します。	2.0 以上

デバイス制御ポリシー	擬似ロケーション機能を制御します。	2.0 以上
	端末初期化操作を制限します。	2.0 以上
	ステータスバーを非表示にします。	3.0 以上
	電源ボタン長押し時の”電源を切る”を制限します。	3.0 以上
	スクリーンキャプチャ操作を制限します。	2.0 以上
	Google クラッシュレポートを無効にします。	3.0 以上
	Google バックアップを制限します。	2.0 以上
	アプリ履歴キーを制限します	3.0 以上
	セーフモードでの端末の起動を制限します	4.0 以上
	アクティブキーを無効化します。	3.0 以上
利用アプリ制限ポリシー	apk 展開禁止設定時のアプリインストール抑止 (Google Play アプリも可) *1	1.0 以上
	利用アプリ制限ポリシーで禁止しているアプリを制限します。 制限時は SPPM Home 未設定でも禁止アプリは非表示します。*2	2.0 以上
	apk 展開禁止設定時に”提供元不明のアプリ”設定を制限します。	2.0 以上
アプリ配信ポリシー	アプリ配信機能でのサイレントインストール*1	1.0 以上
アプリアンインストール制限 ポリシー	アプリアンインストール制限ポリシーのリストに追加されたアプリのアンインストールを制限します。	1.0 以上

☆ワンポイント:E-SDK対応Agentについて

E-SDK 対応の SPPM Agent は v2.18 以降です。

*1 の機能については SPPM Agent v2.21 以降、E-SDK モジュール v1.1.0 以降で利用可能です。

*2の機能についてはSPPM Agent v2.28.2以降、E-SDKモジュールv1.1.0以降で利用可能です。

【E-SDKモジュールアプリ インストール手順】

- ① E-SDK モジュールは管理画面の「連携アプリ」⇒「Samsung E-SDK モジュール」を選択すると、ダウンロードページに進みます。



- ② Samsung E-SDK モジュールダウンロードページのダウンロードリンクを選択して、モジュールファイルを PC に保存します。

モジュールファイル保存後は STAR-MDM の「アプリ配信」機能を利用して、端末への配信・インストールを行ってください。

関連情報 [「アプリ配信」](#)

Samsung E-SDKモジュールダウンロードページ

>>>>E-SDKモジュールは GalaxyシリーズのE-SDK提供機能を利用する為のモジュールです。<<<<<

>>>> [E-SDK モジュールダウンロード](#) <<<<<

Samsung E-SDKモジュールについて

Samsung E-SDKモジュールは、Samsung端末に実装された MDM機能を利用する為のモジュールです。
SPPM Agent v2.18以降がインストールされた端末にインストールし、利用することが可能です。

なお、E-SDKには端末によって対応しているバージョンが異なります。
SPPMをセットアップした端末では、SPPM Agentのメニュー画面で対応するE-SDKのバージョンを確認する事が可能です。

表記例
SPPM Agent:ver2.18
E-SDK 2.0
なお、E-SDK非対応の端末では 表示は行われません。
また、E-SDKモジュールが未インストールの状態ではバージョン表示はグレー表示となります。

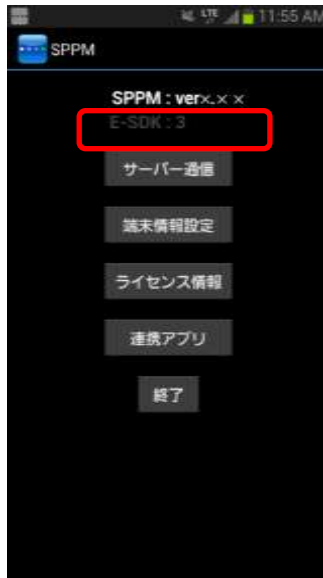
【Galaxy端末 E-SDKモジュールアプリのインストール・バージョン確認方法】



- ①. 端末に E-SDK のモジュールアプリのインストールが完了
- ②. インストール完了後「デバイス管理機能の起動」画面が表示されるので「開始」を選択
- ③. アプリ一覧から SPPM のアプリを起動



④



⑤

- ④. SPPM Agent のバージョン下に、端末の対応 E-SDK のバージョンが表示されます
 ⑤. モジュールアプリがインストールされていない場合はバージョンがグレースアウト

◎E-SDKモジュールアプリのアンインストールについて

E-SDK モジュールアプリをアンインストールする場合は、必ず全て許可設定にしたデバイス制御ポリシーを適用してからアンインストールしてください

【Galaxy端末 E-SDKバージョン4以上の端末について

E-SDKバージョン『4』以上の端末ではSPPM Agent v2.29以降をインストールする事で、E-SDKモジュールを別途インストールする必要はありません(別途KNOXライセンス有効化が必要)

☞「[KNOXライセンス有効化](#)」

また該当端末でSPPM Agent v2.29にバージョンアップした時E-SDKモジュールがインストールされていると、サイレントアンインストールをします。

5. Sony Xperia E-API

Sony Xperia 端末向け独自 MDM 機能である「E-API 機能」を利用した MDM 機能が利用できます。当機能は SPPM Agent v2.26 に内蔵されているので、Agent 以外の別アプリケーションをインストールする必要はありません。

E-API を用いた Sony Xperia 端末向けの新機能は、フル機能パックで利用可能です。

尚、Xperia 端末毎に対応している E-API バージョンが異なり、利用できる機能に違いがあります。各機種の E-API バージョンは弊社までお問い合わせください。

	機能詳細	対応 E-API バージョン
緊急時ポリシー データ消去	OS4.2 以上でも SD カードの個別データ削除をします。	4.0 以上 ※SPPM Agent v2.28 以降
端末暗号義務化ポリシー	外部ストレージの暗号利用を義務化します。	3.0 以上 ※SPPM Agent v2.26 以降
デバイス制御ポリシー	Bluetooth HANDSFREE デバイス制御で Bluetooth を禁止していても Bluetooth HandsFree (ヘッドセット) の接続のみ個別許可をします。	3.0 以上 ※SPPM Agent v2.28 以降
	On the AirOS upgrade 端末操作での OS バージョンアップを制限します。 ※PC 接続によるバージョンアップも完全に制限する場合は PC_OS_UPGRADE と MassStorage を制限してください。	3.0 以上 ※SPPM Agent v2.26 以降
	“緊急時省電力モード” 緊急時省電力モードの利用を制限します。 ※緊急時省電力モードを ON にすると、端末再起動をして制限します。	3.0 以上 ※SPPM Agent v2.28 以降
	外部 SD カード OS4.4 以上でも外部 SD カードをアンマウントします。	3.0 以上 ※SPPM Agent v2.28 以降
	USB Debugging USB デバッグモード機能を制限します。 ※USB デバッグモードを ON にすると、端末再起動をして制限します。	5.0 以上 ※SPPM Agent v2.28 以降
	MassStorage USB 接続時のファイルアクセスを制限します。	5.0 以上 ※SPPM Agent v2.28 以降
	ADD Guest User 端末にゲストユーザの追加を制限します。	6.0 以上 ※SPPM Agent v2.28 以降
	設定 パスワード変更と暗号化を除く端末の設定を制限します。	7.0 以上 ※SPPM Agent v3.05 以降
	セーフモード セーフモードでの端末の起動を制限します。	8.0 以上 ※SPPM Agent v3.06 以降
	スモールアプリ スモールアプリの使用を制限します。	3.0 以上 ※SPPM Agent v2.28 以降

	・Power OFF 電源オフ操作を制限します。	8.0 以上 ※SPPM Agent v3.09 以降
	・AUTO_BOOT 充電時オートブートモードを制御できます。	8.0 以上 ※SPPM Agent v3.09 以降
	・PC_OS_UPGRADE Xperia Companion によるソフトウェア修復時の OS アップグレードを制限します。	8.0 以上 ※SPPM Agent v3.09 以降
	・SCREEN SLEEP 画面のスリープを制限します。	8.0 以上 ※SPPM Agent v3.09 以降
	・FACTORY RESET BY USER 端末初期化操作を制限します。	9.0 以上 ※SPPM Agent v3.09 以降
	・FACTORY RESET ALL 端末初期化操作を制限します。 システムによるリセットや緊急時ポリシーによるリセットも制限します。	9.0 以上 ※SPPM Agent v3.09 以降
	・トップに固定するパッケージ名 指定したアプリを開くとトップ画面に固定します。	8.0 以上 ※SPPM Agent v3.09 以降
	・スクリーンショット スクリーンショットキャプチャ操作を制限します。	5.0 以上 ※SPPM Agent v3.09.1 以降
	・Home Key ホームボタンを無効化します。	8.0 以上 ※SPPM Agent v3.10.1 以降
	・Volume Key ボリュームキーを無効化します。	9.0 以上 ※SPPM Agent v3.10.1 以降
	・Back Key バックボタンを無効化します。	8.0 以上 ※SPPM Agent v3.10.1 以降
	・Status Bar ステータスバーを非表示にします。 ※パスワード認証画面ではステータスバーが表示されます。	8.0 以上 ※SPPM Agent v3.10.1 以降
	・アプリ履歴キー アプリ履歴キーを制限します。	8.0 以上 ※SPPM Agent v3.10.1 以降
利用アプリ制限ポリシー	利用アプリ制限ポリシーで禁止しているアプリを制限します。 制限時は SPPM Home 未設定でも禁止アプリは非常時します。	3.0 以上 ※SPPM Agent v2.28 以降
	apk 展開禁止設定時に“提供元不明のアプリ”設定を制限します。	7.0 以上 ※SPPM Agent v3.04 以降
アプリ配信ポリシー	アプリ配信機能でのサイレントインストール	7.0 以上 ※SPPM Agent v2.40 以降
アプリアンインストール制限 ポリシー	アプリアンインストール制限ポリシーのリストに追加されたアプリのアンインストールを制限します。	6.0 以上 ※SPPM Agent v3.13 以降

6. SHARP モジュールアプリ

SHARP 端末向けの専用モジュールアプリを端末にインストールする事でさらに詳細な制御をする事が可能となります。

- ❗ SHARP モジュールは OS9 以降の端末は未対応です。
- ❗ Android Enterprise 端末で SHARP モジュール機能は利用できません。

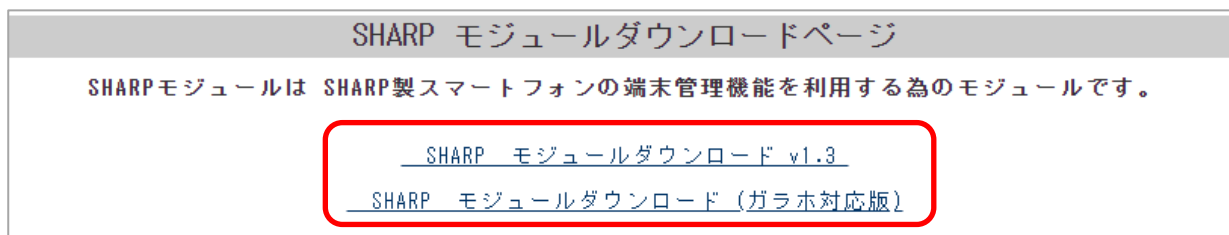
【SHARP モジュールアプリ インストール手順】

- ① SHARP モジュールは管理画面の「連携アプリ」⇒「SHARP モジュール」を選択すると、ダウンロードページへ進みます。



- ② SHARP モジュール ダウンロードページのダウンロードリンクをクリックして、モジュールファイルを PC に保存します。

※ガラホ端末の場合は、「ガラホ対応版」のモジュールをダウンロードしてください。



- ③ モジュールファイル保存後は SPPM の「アプリ配信」機能を利用して、端末への配信・インストールを行ってください。

関連情報⇒「[アプリ配信](#)」

【機能一覧】

機能名	機能内容	対応 OS	SHARP モジュール	SPPM Agent
On the AirOS upgrade	OS のバージョンアップを制限します。 (docomo 端末のみの機能です)	OS6～7	V1.0 以降	v3.22 以降
		OS8.x	V1.1 以降	
パスワードリセット機能	端末に設定されているパスワードをリセットします。	OS6～7	V1.0 以降	
		OS8.x	V1.1 以降	
USB 制限	USB 接続を制限します。	OS6～8.x	v1.2 以降	v3.51 以降
外部 SD カード制限	外部 SD カードを強制アンマウントします。			
USB テザリング	USB テザリングを制限します。		V1.3 以降	V3.53 以降

7. コールピックアップ

コールピックアップ

コールピックアップ

☒ コールピックアップ機能を有効化する。

元に戻る

戻る

保存

コールピックアップ機能では、内線電話システムのコールピックアップ専用番号が登録された「専用ダイヤルボタン」を端末パスワード画面に設ける事で、簡単に内線をスマートフォンで受話する事が可能になります。尚、本機能を利用するには各通信事業者が提供しているコールピックアップ機能に対応した内線サービスの契約が必要です。

【コールピックアップ機能の切替】

コールピックアップ

コールピックアップ

☒ コールピックアップ機能を有効化する。

☒ 先頭が"0"の発信番号の登録を許可する。

元に戻る

戻る

保存

■コールピックアップ機能を有効化する。

チェックを入れる事で端末で専用番号の登録が可能になります。

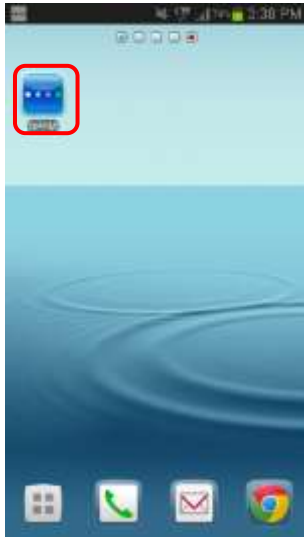
- 
 コールピックアップ機能を利用するには、各事業者が提供しているコールピックアップ機能に対応した内線サービスの契約が必要です。
- 
 コールピックアップ機能は、AndroidOS3.0 以上の端末でお使いいただけます。
- 
 コールピックアップ機能が表示されない場合は、ポリシーの変更や再適用を行ってください。
 ※変更・再適用するポリシーはどの種類でも可能です。

■先頭が“0”の発信番号の登録を許可する。

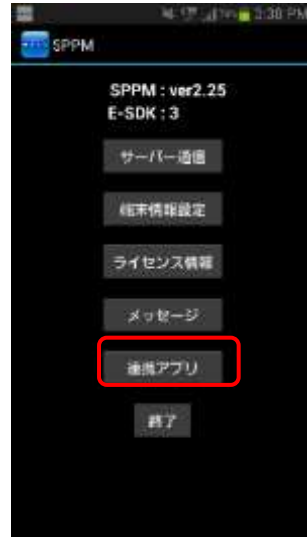
チェックを入れる事で 0 から始まる番号の登録が可能になります。

- 
 番号登録時に先頭 0 番が入力できない場合は、ポリシーの変更や再適用を行ってください。
 ※変更・再適用するポリシーはどの種類でも可能です。

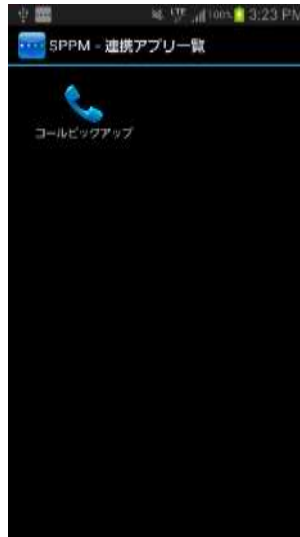
【コールピックアップ番号登録・削除について】



①



②



③



④

- ①端末で SPPM Agent を起動
- ②メニューから「連携アプリ」を選択
- ③連携アプリの「コールピックアップ」を選択
- ④コールピックアップの登録画面で「追加」を選択



⑤



⑥



⑦



⑧

- ⑤ダイヤルリンクの表示名・番号を入力します
- ⑥ダイヤルリンクアイコンの色を選択し、保存をします。
- ⑦保存が完了するとコールピックアップ登録一覧に表示されます
- ⑧削除する場合は登録一覧の横にチェックを入れて、削除を選択します



⑨



⑩

⑨ダイヤルリンクアイコンの『高さ(大きさ)』を設定します

⑩パスワード画面に表示される、ダイヤルリンクアイコンの表示位置を選択します

【コールピックアップの操作について】



①



②

① 定をした表示位置(上・中・下のいずれか)にダイヤルリンクアイコンが表示されるので、タップします

② 電話アプリが起動し、登録されている番号へ発信をします

【コールピックアップ利用時のパスワード解除について】



①端末のロック解除を『パスワード』に設定していた場合、ダイヤルアイコンが表示されていると、パスワード入力できません。

※パターン・PIN の場合は入力できます

②ダイヤルアイコン横に表示されている『×』を選択します

③ダイヤルアイコンが非表示になり、パスワードの入力ができます

◎コールピックアップ機能利用時の電源メニュー操作について

Android OS 4.1コールピックアップ機能有効化状態では、パスワード画面上に表示される電源メニューはタップしても機能しません(電源メニューを閉じる場合は、電源ボタンを押してください)

電源メニューを利用する場合は、パスワード解除後に再度電源長押しで電源メニューを表示してください。

【パスワード解除前】



【パスワード解除後】



8. アプリポータル

アプリポータル機能では、管理画面にて設定した各アプリの Google Play ページへのリンクを一覧で端末に表示できます。端末キッティング時に Google Play からインストールしたいアプリや、ユーザーへの使用推奨アプリを予め設定しておくことで、ユーザーが個別に検索しインストールする手間を省くことができます。



アプリの新規追加機能は非対応となりました。

アプリポータル

◆連携設定

☒ 連携する
☐ 連携しない

◆認証設定

☒ 有効にする
☐ 無効にする

アプリポータルID: test
 パスワード: 1234

検索ワード: Google 検索

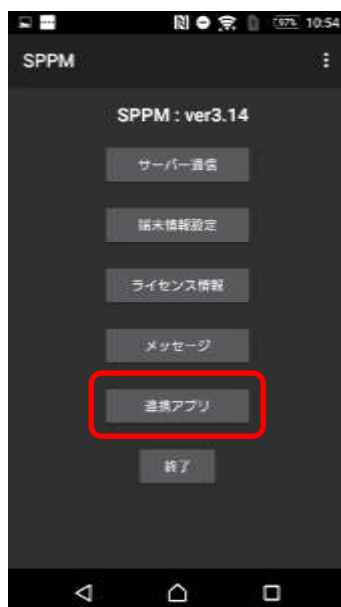
アイコン	アプリ名	パッケージ名	削除
	Google	com.google.android.googlequicksearchbox	削除
	Google Chrome: 高速で安全	com.android.chrome	削除

元に戻す 戻る 保存

【連携設定】

■連携する / 連携しない

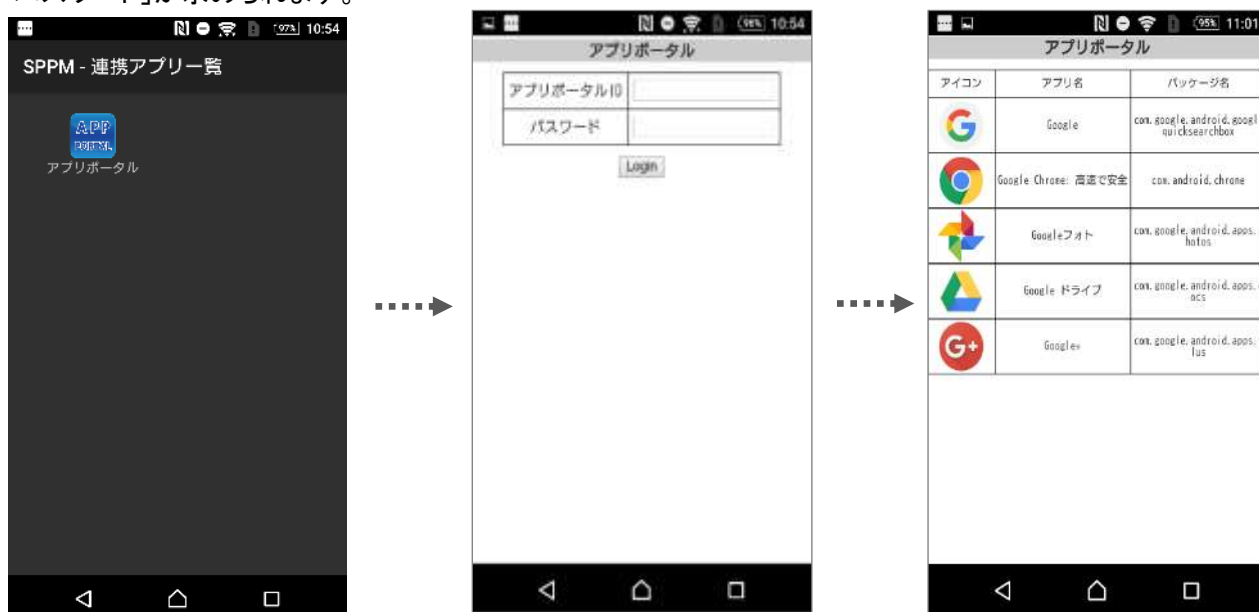
「連携する」にチェックを入れると、SPPM Agent の「連携アプリ」一覧にアプリポータルアイコンが表示されます。



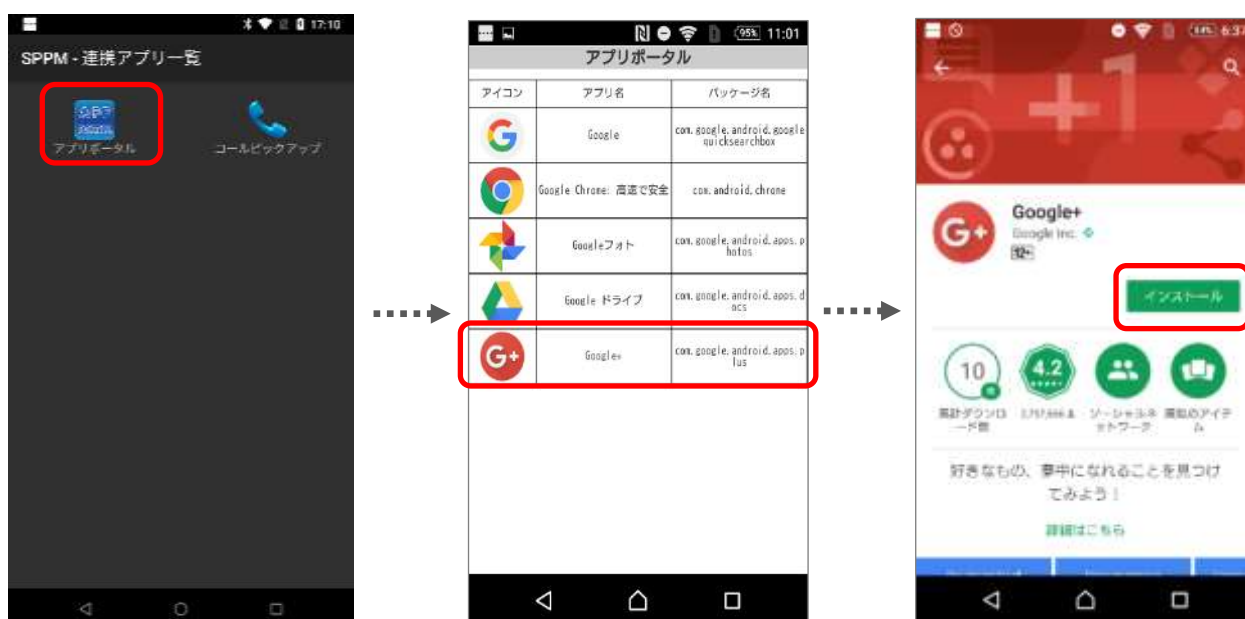
【認証設定】

■有効にする / 無効にする

「有効にする」にチェックをいれると、端末からアプリポータル画面へアクセスする際に、「アプリポータル ID」と「パスワード」が求められます。



《アプリポータルからアプリをインストールする方法》



- ① アプリポータルアイコンをタップ
- ② インストールしたいアプリをタップ
- ③ Google Play Store が開くのでインストール

アプリポータルからアプリのインストールを行う場合は、利用アプリ制限ポリシーで

「Google Play」と「ブラウザ」の制限を外してお使いください

関連情報 ➡ [「利用アプリ制限」](#)

1. 他の端末管理システムとの併用

例えば、Exchange Serverにもパスワード義務化や紛失時の端末初期化といった端末管理機能があります。こういった端末管理機能を併用しますと、互いに設定を変更し合う競合状態に陥ることで制御不能となり、正常に利用できなくなります。

STAR-MDMをご利用の場合には、Exchange Server等の他のMDM機能を端末に適用しないようにしてください。実験的に適用した場合には、必ず管理サーバ側で設定解除し、さらに端末メモリのクリア（工場出荷状態への復帰）をしてから、STAR-MDMをご利用ください。

2. 端末の識別方法

STAR-MDMでは、端末固有のIDでIMEI(International Mobile Equipment Identifier)を用いて端末の識別と管理を行います。

従って、SIMを取り替えてもSTAR-MDMは機能し続け、ポリシーは堅持されます。しかしながら、電話着信指示による即時ポーリングや、緊急時処理（端末ロック指示、データ消去、ハードリセット）は、SIM差し替えにより使えなくなります。

3. SIM未装着の場合の機能制限

端末にSIMが未装着の場合、あるいはSIM装着が出来ない端末の場合、下記の機能が制限されます。

1. 端末一覧画面での電話番号表示
2. 電話着信指示による緊急時処理、ポリシー変更即時反映
3. Googleプッシュ・サービス（GCM/C2DM/FCM※FCM）

※Googleプッシュ・サービスが利用可能なケースもありますが、保証しておりません。

※Android OSは、SIMが変わるとGoogleアカウントのパスワード入力を求めます。正しく入力されないとGoogleプッシュ・サービスが有効になりません。

4. 機種依存

最新の情報は弊社までお問い合わせください。

※非対応機種/AgentでSTAR-MDMを利用した場合は動作保証外となります。

以上