

# KDDI Smart Mobile Safety Manager

## 4G LTEケータイ向け 利用手引き

2017年2月21日  
KDDI株式会社

# はじめに


本手引きは、「KDDI Smart Mobile Safety Manager 4G LTE ケータイプラン」（以下、KDDI SMSM 4G LTE ケータイプラン）と4G LTE ケータイの組合せサービスにより、法人様向け業務用端末としてご利用頂くことを目的としています。

KDDI ビジネスオンラインサポート（以下、KBOS）は、複数サービスを一つのログインで利用できるWebサイトです。まずは、KBOSのサービス登録を行った後、KDDI SMSMの利用手続きを行いますので、ご留意願います。

- ① KBOSサイトからKDDI SMSMサービス利用手続き
- ② KDDI SMSMの機能概要
- ③ KDDI SMSMの設定事例

4G LTE ケータイへのアプリケーションインストール設定手順

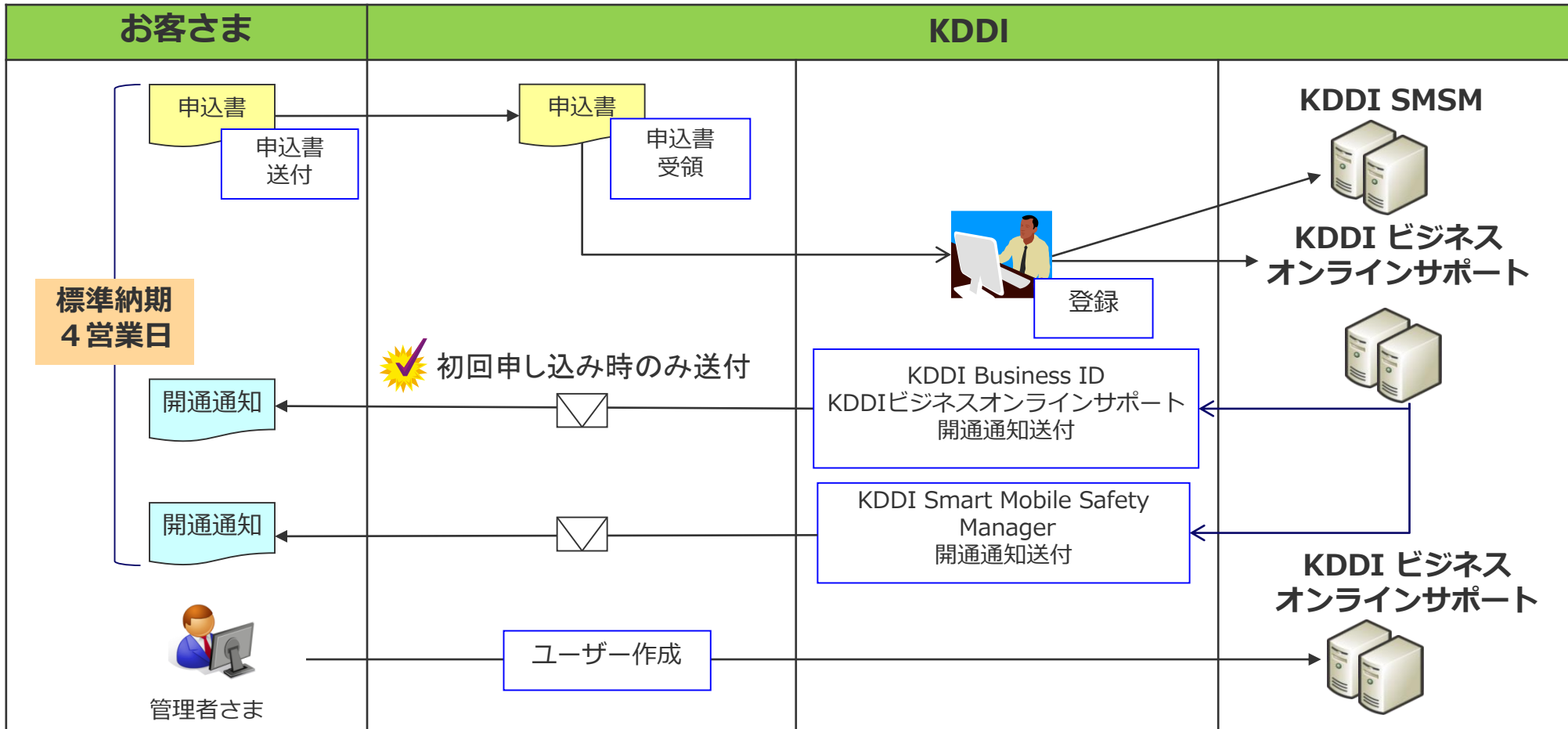
はじめに	2	<b>KDDI SMSM管理者（機器削除）</b>	<b>45</b>
目次	3	<b>KDDI SMSM管理者（設定事例）</b>	<b>49</b>
<b>KDDIビジネスオンラインサポート（KBOS）でのサービス利用について</b>	<b>4</b>	➤ 設定例	50
➤ お申込みフロー	5	➤ 管理プロファイル デバイス制御	52
➤ 初期設定のお知らせ	6	➤ 管理プロファイル パスワードポリシー	54
➤ 初期設定	7	➤ 管理プロファイル 位置情報ポリシー	55
		➤ 管理プロファイル 共通アドレス帳	57
		➤ 管理プロファイル アプリケーション禁止	63
<b>サービス利用設定</b>	<b>12</b>	➤ 管理プロファイル Webフィルタリング	66
➤ KBOS画面	13	➤ 環境設定	70
		➤ 管理プロファイル	72
<b>KDDI SMSM管理サイト画面</b>	<b>24</b>	<b>4G LTEケータイへの</b>	
➤ 管サイト画面（トップ画面）	26	<b>KDDI SMSM エージェントソフト導入</b>	<b>74</b>
➤ 管理サイト画面（機器情報一覧）	27	<b>KDDI SMSM エージェントソフトアップデート</b>	<b>78</b>
➤ 管理サイト画面（機器単体情報）	28		
➤ 管理サイト画面（ユーザー情報）	29	<b>KDDI SMSMユーザー画面</b>	<b>81</b>
➤ 管理サイト画面（組織情報）	31	ユーザー画面	82
➤ 管理サイト画面（メニュー→「管理プロファイル情報」→「設定ポリシー」）	33	ユーザー画面（リモートロック実施）	86
		ユーザー画面（リモートロック解除）	87
<b>KDDI SMSM管理者（リモートロック、ワイプ）</b>	<b>37</b>	➤ ユーザー画面（ワイプ実施）	88
➤ 管理者（リモートロック実施）	39		
➤ 管理者（リモートロック解除）	41		
➤ 管理者（リモートワイプ実施）	42		



# KDDI ビジネスオンラインサポート (KBOS) サービス利用について

# お申込みフロー

サービスのお申込みから開通までの処理です




 「KDDIビジネスオンラインサポート」「KDDI Business ID」が初回申し込みの場合のみ、  
 「KDDIビジネスオンラインサポート」「KDDI Business ID」の開通通知が別途送付されます。

# 初期設定（KBOS開通通知）

ユーザー初期設定のKBOS開通通知が届きますので、メール内のURLへアクセスします。

メール送付元：[mail-bizportal@mail.bizportal.kddi.com](mailto:mail-bizportal@mail.bizportal.kddi.com)

メールタイトル：【KDDI ビジネスオンラインサポート】ユーザー初期設定のお願い

\*\*\*\*\*

お客様管理者名　さま

【KDDI ビジネスオンラインサポート】サービスのユーザー登録申請が行われました。  
下記URLへアクセスし、初期設定を実施くださいますようお願いいたします。

[URL:https://businessportal.kddi.com/otu/init/\\*\\*\\*\\*\\*](https://businessportal.kddi.com/otu/init/*****)

【ユーザーID】 xx-yyyy@www.com

●ワンタイムURLの有効期限は7日間です。  
期限が切れてしまった場合、下記のログインURLにアクセスし、「パスワードを忘れた方はこちら」よりパスワード再設定を実施してください(上記ユーザーIDの入力が必要です)。

【ログインURL】 <https://businessportal.kddi.com/login>

このメッセージは送信専用のメールアドレスから送信しているため、返信いただいても回答できません。

\*\*\*\*\*

# 初期設定（パスワード設定）

パスワードの初期設定を行います。  
入力後、「次へ」ボタンを押します。

## パスワード設定

🏠 パスワード > 📧 通知先メールアドレス > 👁️ 確認 > 完了

ユーザID:

パスワード

パスワードを入力してください。

パスワード(確認)

再度パスワードを入力してください。

次へ



## ヒント

ログイン時に使用するパスワードを設定してください。

半角英数/記号(英字と数字必須)、8文字以上で入力してください。

過去に利用したパスワード(直近3回分)は設定できません。

# 初期設定（通知先メールアドレス設定）

通知先メールアドレスを入力して、「確認」ボタンを押します。

※通知先メールアドレスは、ログインパスワードを忘れた場合、パスワード再設定メールを受信するメールアドレスです。

## 通知先メールアドレス設定

✓ パスワード > ✉ 通知先メールアドレス > 👁 確認 > 完了

パスワードを忘れた場合に再設定依頼メールを送付する宛先となります。

### 通知先メールアドレス

通知先メールアドレスを入力してください。

戻る

確認



### ヒント

ユーザ作成時に管理者が入力した内容が表示されます。

ログイン後に変更できます。



# 初期設定（通知先メールアドレス設定確認）

ユーザーIDを確認して、「完了」ボタンを押します。

## 設定確認

✓パスワード > ✓通知先メールアドレス > 👁️確認 > 完了

完了ボタンをクリックすると、設定した内容でログインできるようになります。

ユーザID: ██████████@██████████

パスワード: 設定済

通知先メールアドレス: 設定済

[戻る](#) [完了](#)



# 初期設定（通知先メールアドレス設定完了）

初期設定が完了しましたので、「閉じる」ボタンを押します。



# ユーザー初期設定完了のお知らせ

ユーザー初期設定が完了しますと、【KDDI ビジネスオンラインサポート】より、ユーザー登録完了のお知らせメールが届きます。

メール送付元：[mail-bizportal@mail.bizportal.kddi.com](mailto:mail-bizportal@mail.bizportal.kddi.com)

メールタイトル：【KDDI ビジネスオンラインサポート】ユーザー登録完了のお知らせ

\*\*\*\*\*

お客様管理者名 さま

【KDDI ビジネスオンラインサポート】サービスへのユーザー登録が完了いたしました。  
下記URLからログインしてください。

【ログインURL】

<https://businessportal.kddi.com/login>

【ユーザーID】

xx-yyyy@www.com

このメッセージは送信専用のメールアドレスから送信しているため、返信いただいても回答できません。

\*\*\*\*\*



# サービス利用設定

# KBOS画面

下記サイトよりログインします。

<https://businessportal.kddi.com/login>



Designing The Future  
**KDDI**

ユーザID

パスワード

次回以降、ユーザIDの入力を省略する

Log in

[パスワードを忘れた方はこちら](#)

[利用規約はこちら](#)

# KBOS画面

メニューバーから「ユーザー」を選択します。  
プルダウンメニューから「ユーザー追加」を選択します。



# KBOS画面

必要事項を入力後、「確認」ボタンを押します。  
(※印は必須入力項目です。)

姓 <small>*</small>	名 <small>*</small>
<input type="text" value="国際"/>	<input type="text" value="太郎"/>
姓(カナ)	名(カナ)
<input type="text" value="コクサイ"/>	<input type="text" value="タロウ"/>
所属	
<input type="text" value="総務部"/>	
権限 <small>*</small>	
<input type="text" value="ユーザ"/>	
サービス利用電話番号	
<input type="text" value="090XXXXXXXX"/>	
ユーザID(メールアドレス) <small>*</small>	
<input type="text" value="test1502@kddi.com"/>	
パスワード設定方法	
<input checked="" type="radio"/> ユーザが設定 (設定案内メールを通知先メールアドレス宛に送信)	
<input type="radio"/> 仮パスワードを設定	
通知先メールアドレス <small>*</small>	
<input type="checkbox"/> メールアドレスとは別のメール通知先を指定する。	
ログイン条件 <small>*</small>	
<input type="text" value="デフォルト"/>	
着信認証電話番号	
<input type="text" value="090XXXXYYYY"/>	

**ヒント**  
現在登録されている情報が表示されていますので、変更したい箇所のみ編集してください。  
\*印は必須入力項目です。

**権限**  
ユーザ:登録済サービスへのシングルサインオンが利用できます。※ KDDI Business ID の契約が必要です。  
管理者:ユーザやサービスの管理、デバイスの購入、セキュリティ設定等ができます。

**ユーザID(メールアドレス)**  
メールアドレス(例: abc@example.com)を入力してください。

**通知先メールアドレス**  
初期設定に必要なメール等が送信されます。ユーザはログイン後に変更できます。

**ログイン条件**  
ログインする際の認証条件を選択できます。“デフォルト”では、IDとパスワードによる認証となっています。  
KDDI Business ID を利用している場合、“セキュリティ設定”タブより、条件を追加できます。

**サービス利用電話番号**  
サービスをご利用にあたり、電話番号を必要とするサービスをご登録される際にこの電話番号が利用されます。

**着信認証電話番号**  
着信認証時に利用する電話番号です。  
070・080・090ではじまる携帯電話番号のみ設定可能です。  
ユーザはログイン後に変更できます。

**確認**

# KBOS画面

入力内容を確認後、「完了」ボタンを押します。  
(※印は必須入力項目です。)

Home	ユーザ	サービス	セキュリティ	契約情報	ダウンロード	ヘルプ
------	-----	------	--------	------	--------	-----

## ユーザ追加(確認)

姓名	国際 太郎
姓名(カナ)	コクサイ タロウ
所属	
権限	ユーザ
サービス利用電話番号	
ユーザID(メールアドレス)	test1502@kddi.com
パスワード設定方法	ユーザが設定 (設定案内メールを通知先メールアドレス宛に送信)
通知先メールアドレス	test1502@kddi.com
ログイン条件	デフォルト
着信認証電話番号	

戻る 完了



# KBOS画面

メニューバーから「ユーザー」を選択します。  
プルダウンメニューから「ユーザー一覧」を選択します。



# KBOS画面

ユーザー一覧から該当ユーザーのメールアドレスを選択します。

Home ユーザ サービス セキュリティ 契約情報

## ユーザー一覧

ユーザIDまたは姓で検索できます。

メニュー

ユーザ	ステータス	前回ログイン日時
① @ [redacted] [redacted]	未設定	
② @ [redacted] [redacted]	未設定	
③ @ [redacted] [redacted]	有効	2016/05/25 16:45:00
④ @ [redacted] [redacted]	有効	2016/05/31 13:06:53

ステータスフィルター

- 全て 20
- 有効 17
- 一時停止 0
- パスワードロック 0
- 未設定 3

メールアドレス  
ユーザー名

# KBOS画面

KDDI SMSMサービスの登録状態は、「未登録」になっています。  
利用可能な状態にするため、「サービス情報」タグからサービス名  
「KDDI Smart Mobile Safety Manager(4G LTEケータイプラン)」を  
選択します。

The screenshot shows the KBOS user interface. At the top, there is a navigation bar with tabs: Home, ユーザ (selected), サービス, セキュリティ, and 契約情報. Below the navigation bar, there is a breadcrumb trail: < ユーザー一覧. The main content area is titled 'ユーザ詳細'. Underneath, there are two tabs: ユーザ情報 and サービス情報 (selected). The 'サービス情報' tab displays a table with the following content:

サービス名/アカウント	サービス登録状態
KDDI Smart Mobile Safety Manager(4GLTEケータイプラン)	未登録

A red box highlights the service name 'KDDI Smart Mobile Safety Manager(4GLTEケータイプラン)', and a hand icon points to it. To the right of the table, there is a 'ヒント' (Hint) section with the text: ユーザが利用するサービスを登録できます.

# KBOS画面

契約番号欄から「Mxxxxxxx」、「利用者」を選び「確認」ボタンを押します。

Home ユーザ サービス セキュリティ 契約情報

## KDDI Smart Mobile Safety Manager(4GLTEケータイプラン)登録(入力)

契約番号	権限
M:XXXXXXXX	利用者

**ヒント**  
**契約番号**  
紐づけを行うKDDI Smart Mobile Safety Manager(4GLTEケータイプラン)の契約番号を指定します。  
**権限**  
KDDI Smart Mobile Safety Manager(4GLTEケータイプラン)におけるユーザの権限を指定します。

キャンセル 確認

# KBOS画面

KDDI SMSMサービスの登録確認を行い、「完了」ボタンを押します。

Home ユーザ サービス セキュリティ 契約情報

KDDI Smart Mobile Safety Manager(4GLTEケータイプラン)登録(確認)

契約番号	権限
M:XXXXXXXX	利用者

戻る 完了

# KBOS画面

本サービスの登録状態が「登録済」になりましたら、サービス利用設定の完了です。メニューバーの「Home」を押します。

The screenshot shows the KBOS user interface. At the top is a navigation bar with icons for Home, User, Service, Security, and Contract Information. Below this is a breadcrumb trail for 'User List' and a title 'User Details'. There are two tabs: 'User Information' and 'Service Information'. The 'Service Information' tab is active, showing a table with columns for 'Service Name/Account', 'Service Registration Status', and 'Hint'. The first row shows 'KDDI Smart Mobile Safety Manager(4GLTEケータイプラン)' with a status of 'Registered' (登録済) highlighted by a red box and a hand icon pointing to it. A hint message states 'Users can register services they use.'

サービス名/アカウント	サービス登録状態	ヒント
KDDI Smart Mobile Safety Manager(4GLTEケータイプラン)	登録済	ユーザが利用するサービスを登録できます。

# KBOS画面

KDDI SMSMのアイコンが表示されますので、アイコンを押します。  
別ウィンドウが開き、KDDI SMSMの管理サイト画面が表示されます。





# KDDI S M S M 管理サイト画面の概要



# 管理サイト画面（基本機能）

管理サイトでは、機器/組織情報閲覧、ユーザー情報の確認及び管理、セキュリティポリシーに合わせた端末管理などができます。

機能	概要
トップ	企業コード、認証コードの確認や各機能画面へアクセスすることができます。
機器情報閲覧	機器の新規登録/編集/削除、機器への管理プロファイルの割り当て、機器の位置情報の確認等ができます。
ユーザー認証	ユーザーの追加/編集/削除や、ユーザーが所有する機器の確認等ができます。
組織情報管理	組織の追加/編集/削除、組織に割り当てている管理プロファイルの確認/変更等ができます。
メニュー	以下の機能画面にアクセスできます。
管理プロファイル作成/適用	機器をカスタマイズするための設定パックです。6つの設定ポリシー（①デバイス制限、②パスワード、③位置情報、④共通アドレス帳、⑤アプリケーション禁止、⑥Webフィルタリング）を組み合わせて作成することができます。
環境設定	管理サーバーとの通信間隔や、メール通知等の設定ができます。
管理・機器ログ	機器に対する設定や操作の記録が確認できます。

# 管理サイト画面（トップ画面）

The screenshot shows the top page of the KDDI Smart Mobile Safety Manager. The header includes the title 'KDDI Smart Mobile Safety Manager', a notification count '0件のアラート', and navigation links for 'トップ' (highlighted with a red box), '機器', 'ユーザー', '組織', 'メニュー', and '管理者'. A left sidebar contains navigation items: '資産' (highlighted), '機器', 'ユーザー', '組織', '設定管理', '管理プロファイル', '環境設定', and '管理・機器ログ'. The main content area displays several metrics with callouts:

- 機器数/契約数**: 2/100. Callout: 契約数および管理者用サイトで管理されている機器数を表示します.
- アラート機器数**: 0件. Callout: アラート状態（無通信状態機器やパスワードポリシー違反機器）の発生件数を表示します.
- ロック・ワイプ中機器数**: 0件. Callout: ロック/ワイプの実施件数を表示します.
- 企業コード**: sarufp. Callout: 企業コード/認証コードを表示します.
- 認証コード**: sarufp.

Additional callouts provide context:

- A green callout on the right states: ヘッダ部分は各機能へのリンクとなっています.
- Another green callout on the right states: 数字をクリックすると対象端末を確認することができます.
- A green callout at the bottom right states: 端末側のSMSM設定の際、必要となります.
- A green callout on the bottom left states: トップ画面から各機能へアクセスすることができます.

# 管理サイト画面（機器情報一覧）

KDDI Smart Mobile Safety Manager 0件のアラート トップ **機器** ユーザー 組織 メニュー 管理者

表示条件: すべての機器

<input type="checkbox"/>	機器名	所有者	電話番号	通信日時	プロフィール	状態	備考
<input type="checkbox"/>	KYF31 [ ]	管理者	080 [ ]	17日前	(所属組織に従う: セキュリティ強度: 強)		(なし)
<input type="checkbox"/>	新規スタッフ 田中さん用	代行管理者	090 [ ]	(なし)	(所属組織に従う: セキュリティ強度: 強)		(なし)

アクション

- 機器の新規登録
- CSVの読み込み
- CSV一括エクスポート
- 選択した機器を削除

組織の一覧を表示します  
組織を選択すると、所属する機器を一覧表示します

機器名や所有者によるソート  
(▲▼)、操作したい端末を選択できます

「アクション」配下は、実行可能なメニューを表示します  
機器削除を行う場合は、画面中央に表示しています機器のチェックボックスにチェックを入れます

# 管理サイト画面（機器単体情報）

KDDI Smart Mobile Safety Manager 0件のアラート [トップ](#) **機器** [ユーザー](#) [組織](#) [メニュー](#) [管理者](#)

組織

全体 (2)

営業チーム (0)

経営企画チーム (0)

製品企画チーム (1)

表示条件:

<input type="checkbox"/>	機器名	所有者	電話番号	通信日時	プロフィール	状態	備考
<input checked="" type="checkbox"/>	KYF31 [080-XXXX-XXXX]	管理者	080-XXXX-XXXX	17日前	(所属組織に従う: セキュリティ強度: 強)		(なし)
<input type="checkbox"/>	新田 〇〇	代行管理者	090-XXXX-XXXX	(なし)	(所属組織に従う: セキュリティ強度: 強)		(なし)

< 1 >

選択された機器はハイライトされます

機器を選択する場合は、機器名のところをクリックします

にチェックを入れても選択されたことになりません

選択された機器の情報閲覧や各種操作を実施することができます

< 所有者の機器

080-XXXX-XXXX

 KYF31 [080-XXXX-XXXX]

機種名  
KYF31

所有者  
管理者

通信日時  
2016/04/15 15:47:16

プロフィール  
(所属組織に従う: セキュリティ強度: 強)

備考  
(なし)

同期する  
この機器に対して同期を行います。 >

設定を変更する  
この機器の設定を変更します。 >

# 管理サイト画面（ユーザー情報）

KDDI Smart Mobile Safety Manager 0件のアラート [トップ](#) [機器](#) [ユーザー](#) [組織](#) [メニュー](#) [管理者](#)

組織	名前 ^	ユーザーID ⇅	組織 ⇅	種別 ⇅	機器数 ⇅	備考	アクション
全体 (2)	代行管理者		製品企画チーム	管理者	1	(なし)	<a href="#">ユーザー追加</a>
営業チーム (0)	管理者	admin	(なし)	管理者	1	(なし)	<a href="#">ユーザー編集・削除</a>
経営企画チーム (0)							
製品企画チーム (1)							

< 1 >

各メニューをクリックすると、KDDI ビジネスオンラインサポートの画面が、別ウィンドウで表示されます  
ユーザー管理（登録、削除）はKDDI ビジネスオンラインサポートの管理画面より行います

# 管理サイト画面（ユーザー情報）

KDDI Smart Mobile Safety Manager

0件のアラート

🏠 トップ

📱 機器

👤 ユーザー

👥 組織

☰ メニュー

👤 管理者

組織

全体 (2)

営業チーム (0)

経営企画チーム (0)

製品企画チーム (1)

名前 ▲	ユーザーID ⇅	組織 ⇅	種別 ⇅	機器数 ⇅	備考
代行管理者	██████████	製品企画チーム	管理者	1	(なし)
管理者	admin	(なし)	管理者	1	(なし)

名前 ▼



< ユーザー



管理者

管理者

カンリシャ

ユーザーID

admin

メールアドレス

admin@██████████

組織

(なし)

備考

(なし)

画面中央のユーザーをクリックすると、詳細情報が確認できます

ユーザー利用の機器を表示します

ユーザーの所属組織を変更します

ユーザーの機器

このユーザーが所有する機器を表示します。 >

ユーザーの設定を変更する

このユーザーの設定を変更します。 >

# 管理サイト画面（組織情報）

KDDI Smart Mobile Safety Manager

0件のアラート | ホーム | 機器 | ユーザー | **組織** | メニュー | 管理者

組織	選択中の組織	
設定名	組織名	管理プロフィール
全体	全体	セキュリティ強度：強

組織	配下の組織	
営業チーム	組織名	管理プロフィール
経営企画チーム	営業チーム	(所属組織に従う:セキュリティ)
	経営企画チーム	セキュリティ強度：強

詳細

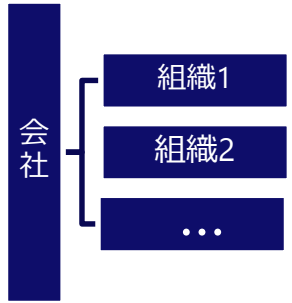
- この階層に新規作成 >
- 編集 >

作成された組織の設定内容を一覧表示します

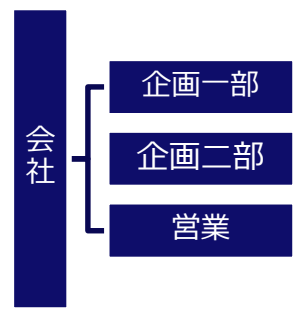
この層に新規作成：「全体」の「配下の組織」を作成します

編集：「全体」に適用する管理プロフィールを選択します

運用一例：



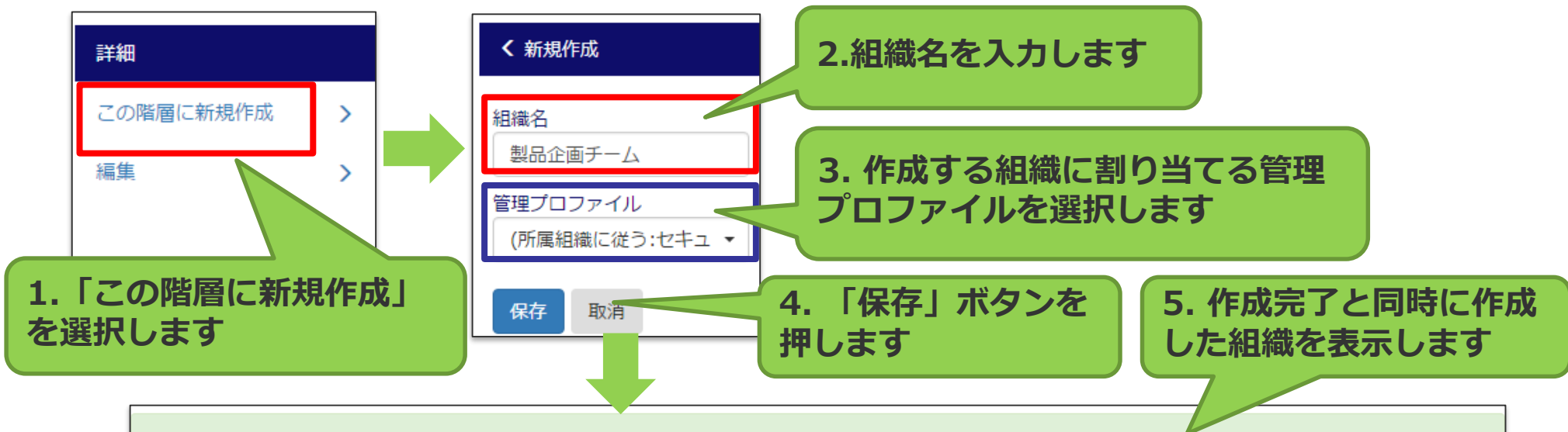
本機能では、1階層により、端末を管理できます。  
**端末は認証された時、既定で「全体」に所属し、「全体」の設定ポリシーは適用されます。**  
他組織に端末を変更したい場合、端末の所属組織を変更します。



# 管理サイト画面（組織情報）

「全体直下」に組織作成および管理プロフィール設定する場合、画面右サイドの「詳細」より作成します。

※管理プロフィールは、マニュアル「3.1.5 管理プロフィール」を参照願います。



組織を作成しました。

組織	選択中の組織	管理プロフィール	詳細
設定名	組織名		編集 >
全体	製品企画チーム	(所属組織に従う:セキュリティ強度:強)	削除 >
営業チーム			
経営企画チーム			
製品企画チーム			



# 管理サイト画面

(メニュー → 「管理プロフィール情報」 → 「設定ポリシー」)

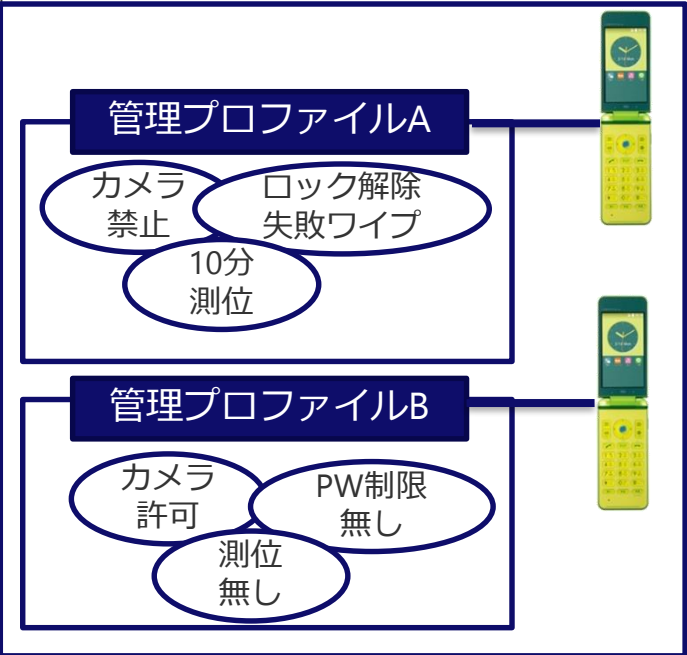
## 管理プロフィール

<input type="checkbox"/>	プロフィール名	デバイス制限	パスワード	位置情報	連絡先	アプリケーション禁 止	Webフィルタリ ング
<input type="checkbox"/>	データ	(設定なし)	(設定なし)	(設定なし)	A	(設定なし)	(設定なし)
<input type="checkbox"/>	サンプル	サンプル	サンプル	サンプル	サンプル	サンプル	サ

- アクション
- 新規作成
- 選択したプロフィールを削除
- 設定ポリシー**
- デバイス制限
- パスワード
- 位置情報
- 連絡先
- アプリケーション禁止
- Webフィルタリング

「アクション」では、  
新たな管理プロフィールを  
作成および削除することが  
できます

「設定ポリシー」は、6つ  
の規制を設定することが  
できます



管理プロフィール/設定ポリシー

本機能では初めに「設定ポリシー」配下の各規制内容（次頁参照）を作成し、次にそれらを「管理プロフィール」としてまとめます。管理プロフィールは、紐つけられた端末に一斉同期をかけることが可能です。

# 管理サイト画面

(メニュー → 「管理プロフィール情報」 → 「設定ポリシー」)

The screenshot displays the '管理プロフィール' (Manage Profiles) section of the KDDI Smart Mobile Safety Manager. A table lists profiles, with 'サンプル' (Sample) selected. A context menu is open over the selected row, offering '同期' (Sync), '編集' (Edit), and '削除' (Delete) options. A red box highlights the 'メニュー' (Menu) button in the top navigation bar and the context menu. A green arrow points from the '編集' option to a detailed 'プロフィールを変更' (Edit Profile) form on the right, which contains fields for profile name, device restrictions, password, location info, network, application restrictions, and web filtering.

プロフィール名	デバイス制限	パスワード	位置情報	連絡先	アプリケーション禁止	Webフィルタリング
<input type="checkbox"/> データ	(設定なし)	(設定なし)	(設定なし)	A	(設定なし)	(設定なし)
<input checked="" type="checkbox"/> サンプル	サンプル	サンプル	サンプル	サンプル	サンプル	サンプル

同期 >  
編集 >  
削除 >  
設定内容

プロフィール名  
サンプル  
デバイス制限  
サンプル  
パスワード  
サンプル  
位置情報  
サンプル  
連絡先  
サンプル  
アプリケーション禁止  
サンプル  
Webフィルタリング  
サンプル

保存 取消

選択した管理プロフィールに対して、同期/編集/削除を実施することができます

管理プロフィールを削除する場合は、プロフィール名の□にチェックを入れて、「削除」を押します

「編集」を押すと、右側の表示が変わり、6つの規制内容を変更することができます。変更した後は、「保存」ボタンを押します

# 管理サイト画面

(メニュー → 「管理プロフィール情報」 → 「設定ポリシー」)

## <デバイス制限>

設定名  
test

カメラ制限

- 許可
- 禁止

SDカード制限

- 許可
- 禁止

Bluetooth制限

- 変更しない
- 有効にする
- 無効にする

Wi-Fi制限

- 変更しない
- 有効にする
- 無効にする

保存 取消

設定名は任意に入力できます

## <共有アドレス帳>

設定名

入力してください。

保存 取消

共有アドレス帳として配信することができます

共有アドレス帳

設定名  
サンプル

新規作成

登録状況  
300/3000

選択した設定を削除

設定名

test : 連絡先3つ

共有アドレス帳インポート

共有アドレス帳エクスポート

編集

「Bluetooth制限」は管理サイトから端末に適用した後、端末側からは変更できません

一方、「Wi-Fi制限」は、適用した後、端末利用者は端末側から設定を変更できます。  
次の同期時に設定は再度適用されます

# 管理サイト画面

(メニュー → 「管理プロフィール情報」 → 「設定ポリシー」)

## <位置情報測位>

## <パスワードポリシー>

設定名

入力してください。

エージェントによる測位

- 測位しない
- エージェント起動時のみ測位する
- 定期的に測位する

分ごと

※端末の位置情報の場合、測位を行う

※エージェントの場合、位置情報を

※この設定値は、

使用します。管理

定値は、エージェ

の通信間隔」で設

保存 取消

設定名は任意に入力できます

- PIN  
GRATINA 4Gでは「ロックNo.」と表示（数字のみ）
- パスワード  
英字のみ
- 数字を含むパスワード  
英数字

設定名

パスワードポリシー

- 端末の設定を変更しない
- 制限なし
- 以下の制限を設定する

解除方法

- PINまたはパスワード
- パスワード
- 数字を含むパスワード

文字数

5 文字以上

オプション

制限を満たしていない場合にパスワードの再設定を強制する

パスワードの再利用

- 端末の設定を変更しない
- 制限なし
- 再利用を禁止 5 回前のパスワードまで

パスワードの有効期限

- 端末の設定を変更しない
- 有効期限なし
- 日時を指定 30 日

自動ロックまでの時間

自動ロックまでの時間

- 端末の設定を変更しない
- 30秒  1分  2分  3分  5分  10分  30分
- 時間を指定 15 分

ロック解除失敗時の設定

- 端末の設定を変更しない
- 10 回失敗でリモートロック

リモートロックメッセージ

10 回失敗でワイプ

△ 対象機器のデータを消去します。実行後に取り消すことはできませんので、ご注意ください。

- リモートロック/ワイプを行わない

保存 取消



# KDDI S M S M 管理者 (リモートロック、ワイプ)

# 管理者（リモートロックの留意事項）

## 注意点

ロックのアラームにて「鳴動する」を選択し、リモートロックを実施する場合、マナーモードを無視し、最大音量にて端末に通知します。

※解除されない限り、鳴り続けます。

## 対応方法

**以下の方法に従い、鳴動解除が可能となります。**

- ユーザーが端末の電源を切る。
- ユーザーが端末上で解除コード入力にてロック解除する。  
※解除コードによるロック解除を「許可する」に設定する必要がある。  
ロック解除されると、鳴動の停止、端末画面にてUnlockの表示および「待ち受け」画面に戻ります。
- 管理者が管理者サイトから、「ロックを解除する」を実施する

# 管理者（リモートロック実施）

リモートロックは、「機器」タブから対象機器を選択します。  
次に、右側の「ロックする」を押します。

KDDI Smart Mobile Safety Manager

0件のアラート

トップ

機器

ユーザー

組織

メニュー

組織

全体 (1)

営業本部 (0)

情報本部 (0)

表示条件： すべての機器

機器名

<input type="checkbox"/>	機器名	所有者	電話番号	通信日時	プロフィール	状態	備考
<input type="checkbox"/>	KYF31 [070 ]	(なし)	070	1日前			(なし)

1. 対象機器を選択します

2. 「ロックする」を選択します

< 所有者の機器

ロックする  
現在ロックされていません。

ロックを解除する  
機器のロックを解除します。

ワイプする  
この端末の情報を初期化します。

パスワードを変更する  
この機器のパスワードを変更・解除します。

ログを見る  
この機器のログを表示します。

機器を削除する  
この機器を削除します。

# 管理者（リモートロック実施）

画面がグレーアウトし、端末をロックする際の条件を選び、実行します。

この端末をロックする

ロックメッセージ

ロック時のアラーム

鳴動する  鳴動しない

解除コードによるロック解除

許可する  許可しない

端末の状態によっては反映に時間がかかる場合があります。

実行 取消

3. 端末画面に表示できるメッセージ（200文字まで）を入力できます

リモートロック時にアラームを鳴動させたくない場合は、「鳴動しない」を選択します

「許可する」で端末側にてリモートロックの解除ができます

4. 「実行」ボタンを押します

最終実行日時: 2016/05/31 17:45:04

ロックする  
現在ロックされていません。

ロックを解除する  
機器のロックを解除します。

ワイプする  
この端末の情報を初期化します。

パスワードを変更する  
この機器のパスワードを変更・解除します。

ログを見る  
この機器のログを表示します。

機器を削除する  
この機器を削除します。



# 管理者（リモートロック解除）

「機器」タブから対象機器を選択し、「ロックを解除する」を押します。  
ロックを解除するウィンドウが表示されますので、「実行」を押します。

The screenshot displays a mobile device management interface. On the left, a modal dialog box titled "この端末のロックを解除する" (Unlock this device) is shown. The dialog contains the text "端末の状態によっては反映に時間がかかる場合があります。" (Depending on the device status, it may take time to reflect). At the bottom of the dialog, there are two buttons: "実行" (Execute) and "取消" (Cancel). The "実行" button is highlighted with a red border, and a blue hand icon points to it. On the right side of the screen, a list of management actions is visible. The action "ロックを解除する" (Unlock device) is highlighted with a red border, and a blue hand icon points to it. Other actions include "連絡帳をバックアップする" (Backup contacts), "ロックする" (Lock device), "ワイプする" (Wipe device), "パスワードを変更する" (Change password), and "ログを見る" (View logs).

この端末のロックを解除する

端末の状態によっては反映に時間がかかる場合があります。

実行 取消

連絡帳をバックアップする  
最終実行日時: 2016/07/29 16:52:52

ロックする  
現在ロックされていません。

ロックを解除する  
機器のロックを解除します。

ワイプする  
この端末の情報を初期化します。

パスワードを変更する  
この機器のパスワードを変更・解除します。

ログを見る  
この機器のログを表示します。

# 管理者（リモートワイプ実施）

リモートワイプは、「機器」タブから対象機器を選択し、「ワイプする」を押します。  
※リモートワイプを行いますと、取り消しができませんのでご注意ください。

KDDI Smart Mobile Safety Manager 0件のアラート トップ 機器 ユーザー 組織 メニュー

組織 表示条件： すべての機器

機器名	所有者	電話番号	通信日時	プロフィール	状態	備考
<input type="checkbox"/> KYF31 [070 ]	(なし)	070	1日前			(なし)

1. 対象機器を選択します

2. 「ワイプする」を選択します  
「ワイプする」メニューは右側画面の下方にあります

所有者の機器

- ロックする  
現在ロックされていません。
- ロックを解除する  
機器のロックを解除します。
- ワイプする  
この端末の情報を初期化します。
- パスワードを変更する  
この機器のパスワードを変更・解除します。
- ログを見る  
この機器のログを表示します。
- 機器を削除する  
この機器を削除します。

# 管理者（リモートワイプ実施）

リモートワイプの「実行」を行うと、端末の初期化が実施されます。

この端末をワイプする

**警告**  
端末のデータを初期化します。実行後に取り消すことはできません。よろしければ、「初期化に同意する」にチェックをいれて、「実行」ボタンを押してください。

初期化に同意する  
 SDカードのデータも初期化する

端末の状態によっては反映に時間がかかる場合があります。

実行 取消

3. 「初期化に同意する」にチェックするのは必須です  
「SDカードのデータも初期化する」は任意です

4. 「実行」ボタンを押します

# 管理者（リモートワイプ実施）

リモートワイプの確認は、「機器」選択し、該当端末の状態が「ワイプ済」になっていることを確認します。

KDDI Smart Mobile Safety Manager 0件のアラート [トップ](#) **機器** [ユーザー](#) [組織](#) [メニュー](#)

表示条件：   機器名

<input type="checkbox"/>	機器名	所有者	電話番号	通信日時	プロファイル	状態	備考
<input type="checkbox"/>	KYF31 [070- ]	(なし)	070- ]	2分前		<b>ワイプ済</b>	(なし)



# KDDI S M S M 管理者 (機器削除)

# 管理者（機器削除）

端末が故障し、新たな端末に置換された場合、故障した端末情報は残っています。その場合、管理者により故障端末情報を削除します。また、端末の回線解約した場合も同様に、端末情報の削除が必要になります。

「機器」タブを押して、現在登録されている機器名が表示されます。  
※削除対象機器をクリックし、ボックス□にチェックを入れます。  
次に、所有者の機器欄配下にある「機器を削除する」を押します。

KDDI Smart Mobile Safety Manager

0件のアラート [ホーム](#) [機器](#) [ユーザー](#) [組織](#) [メニュー](#)

表示条件: [すべての機器](#)

<input type="checkbox"/>	機器名	所有者	電話番号	通信日時	プロフィール	状態	備考
<input type="checkbox"/>	KYF31 [0703 J( ... )]	(なし)	0703	19分前	(所属組織に従う: 設定なし)		(なし)
<input checked="" type="checkbox"/>	KYF31 [0703 J]	(なし)	0703	4時間前	(所属組織に従う: 設定なし)		(なし)

所有者の機器

- 0703 KYF31 | |

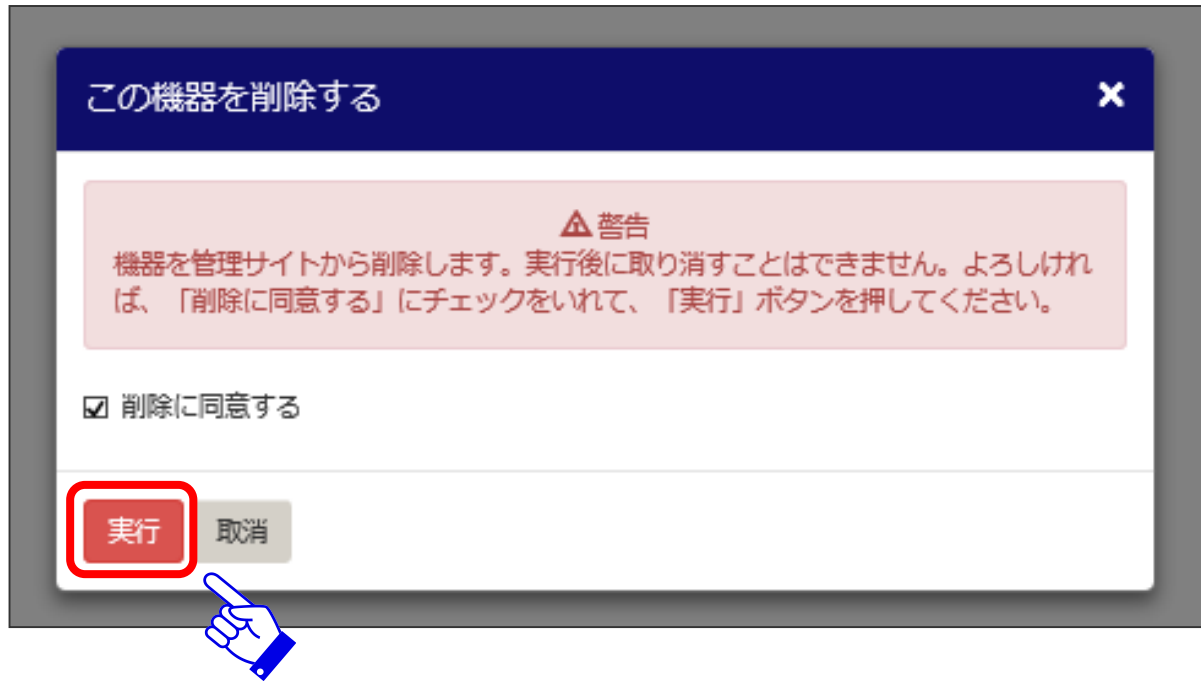
機種名 KYF31  
所有者

- [パスワードを変更する](#)  
この機器のパスワードを変更・解除します。
- [ログを見る](#)  
この機器のログを表示します。
- [機器を削除する](#)  
この機器を削除します。

※削除対象機器：同一の電話番号で、かつ通信日時が古い日時が表示されています。

# 管理者（機器削除）

機器削除の確認ウィンドウが表示されますので、  
チェックボックスをクリックし、「実行」ボタンを押します。



# 管理者（機器削除）

削除対象機器が、管理画面より消えていること確認します。  
※「メニュー」タブの機器・管理ログから確認できます。

KDDI Smart Mobile Safety Manager 0件のアラート [トップ](#) [機器](#) [ユーザー](#) [組織](#) [メニュー](#) [!](#)

組織 表示条件: [すべての機器](#)  機器名

組織	機器名	所有者	電話番号	通信日時	プロフィール	状態	備考
全体 (1)							
営業本部 (0)							
情報本部 (0)							
<input type="checkbox"/>	KYF31 [0703 ]( )	(なし)	0703	27分前	(所属組織に従う: 設定なし)		(なし)

アクション  
[機器の新規登録](#)  
[CSVの読み込み](#)  
[CSV一括エクスポート](#)

KDDI Smart Mobile Safety Manager 0件のアラート [トップ](#) [機器](#) [ユーザー](#) [組織](#)

管理・機器ログ 種別:  管理ログ  機器ログ  
オプション:  通知対象のみ  
期間: 発生日時  から  まで  
キーワード:

種別	通知	発生日時	受信日時	概要
		2016/09/	2016/09/	ユーザー「[...]」が機器「KYF31 [0703: ]」を削除しました。







# KDDI S M S M 管理者（設定事例）

# 設定例

【前提】 全端末共有して、以下のセキュリティポリシー条件で端末の運用を行う場合。

1. デバイス制限	SDカード制限	禁止
	Wi-Fi制限	無効にする
2. パスワードポリシー	文字数	6文字以上
	その他設定	▶ 制限を満たしていない場合にパスワードの再設定を強制する
		▶ パスワードを10回失敗したら、ロックをかける。
	▶ メッセージ内容：ロック解除先まで連絡する旨を通知する	
3. 位置情報ポリシー	エージェントによる測位	エージェント起動時のみ測位する
4. 共有アドレス帳	共有アドレス帳を配信	csvファイル形式で管理します
5. 禁止アプリケーション	LINE	パッケージ名：jp.naver.line.android
6. Webフィルタリング	ホワイトリスト	<a href="https://www.google.co.jp/">https://www.google.co.jp/</a> の利用を許可する
	参考：カテゴリフィルタ	フィルター中設定（ITサービスで辞書サイト <a href="http://dictionary.goo.ne.jp/">http://dictionary.goo.ne.jp/</a> を許可する）
7. 環境設定	エージェント共通管理	管理サーバーとの通信間隔1日
	ログメール通知	リモートロック、リモートワイプ
	無通信検知	指定日数通信がない機器を検知：6日間

# 設定例

セキュリティポリシー条件に基づき、「メニュー」タブの「管理プロファイル」配下にある、各規制毎にファイルを作成致します。作成後、一つの「管理プロファイル」としてまとめます。

KDDI Smart Mobile Safety Manager

0件のアラート    🏠 トップ    📱 機器    👤 ユーザー    👥 組織    ☰ メニュー

資産

機器数/契約数

1/10

ユーザー

組織

設定管理

アラート機器数

0 件

管理プロファイル

環境設定

管理・機器ログ

ロック・ワイプ中機器数

0 件

- 管理プロファイル
  - ▶ デバイス制限
  - ▶ パスワードポリシー
  - ▶ 位置情報ポリシー
  - ▶ 共有アドレス帳
  - ▶ アプリケーション禁止
  - ▶ Webフィルタリング
- 環境設定
- 管理・機器ログ

# 管理プロフィール デバイス制御

管理プロフィール配下にある「デバイス制御」を選択します。  
下記画面に遷移しますので、右側「アクション」欄の「新規作成」をクリックします。

KDDI Smart Mobile Safety Manager

0件のアラート

🏠 トップ

📱 機器

👤 ユーザー

👥 組織

☰ メニュー ▾

デバイス制限

■ 設定名

設定名

サンプル

カメラ制限

禁止

SDカード制限

禁止

USB接続制限

禁止

Bluetooth制限

変更しない

Wi-Fi制限

有効にする

発信先制限

制限しない

編集

削除

アクション

新規作成

選択した設定を

ヒント

端末の各種機能の使用制限ができません。



# 管理プロフィール デバイス制御

デバイス制限

■ 設定名

□ サンプル

設定名

サンプル

カメラ制限

許可  
 禁止

SDカード制限

許可  
 禁止

USB接続制限

許可  
 禁止

Bluetooth制限

変更しない  
 有効にする  
 無効にする

Wi-Fi制限

変更しない  
 有効にする  
 無効にする

発信先制限

制限しない  
 制限する

① 設定名を記入します。  
例：サンプル

② 利用条件に基づき、選択します。  
SDカード制限：禁止  
Wi-Fi制限：無効にする

③ 上記設定後、「保存」ボタンを押します。

④ 設定名欄に「サンプル」が表示されます。

発信先制限：「制限する」を選択した場合、  
「共有アドレス帳」で配信された連絡先のみ電話発信が可能となります。

次に「パスワードポリシー」の設定を行います。

# 管理プロファイル パスワードポリシー

管理プロファイル配下にある「パスワードポリシー」を選択します。  
下記画面に遷移しますので、右側「アクション」欄の「新規作成」をクリックします。

KDDI Smart Mobile Safety Manager

0件のアラート

トップ

機器

ユーザー

組織

メニュー

パスワードポリシー

設定名

サンプル

パスワードポリシー

端末の設定を変更しない

制限なし

以下の制限を設定する

解除方法:

PINまたはパスワード

パスワード

数字を含むパスワード

文字数:

6文字以上

オプション:

制限を満たしていない場合にパスワードの再設定を強制する

パスワードの再利用

端末の設定を変更しない

制限なし

再利用を禁止 5 回前のパスワードまで

パスワードの有効期限

端末の設定を変更しない

有効期限なし

日時を指定 30 日

設定名欄に「サンプル」が表示されましたら、次に「位置情報ポリシー」の作成に移ります。

- ① 設定名を記入します。
- ② 各項目を設定し、パスワードポリシーを作成します。  
文字数：6文字以上  
制限を満たしていない場合にパスワードの再設定を強制する  
パスワードを10回失敗したら、ロックをかける  
メッセージ内容：  
ロック解除先まで連絡する旨を通知する
- ③ 上記設定後、「保存」ボタンをクリックします。



自動ロックまでの時間

端末の設定を変更しない

30秒  1分  2分  3分  5分  10分  30分

時間を指定 15 分

ロック解除失敗時の設定

端末の設定を変更しない

10回失敗でリモートロック

リモートロックメッセージ

リモートロックになりました。解除は、次の連絡先まで電話してください。  
XX-XXXX-XXXX

10回失敗でワイプ

△ 対象機器のデータを消去します。実行後に取り消すことはできませんので、ご注意ください。

リモートロック/ワイプを行う

保存 取消

# 管理プロフィール 位置情報ポリシー

管理プロフィール配下にある「位置情報ポリシー」を選択します。  
下記画面に遷移しますので、右側「アクション」欄の「新規作成」をクリックします。

KDDI Smart Mobile Safety Manager

0件のアラート

🏠 トップ

📱 機器

👤 ユーザー

👥 組織

☰ メニュー

位置情報ポリシー条件を設定します

- ① 設定名を記入します
- ② 位置情報ポリシー  
エージェントによる測位  
起動時のみ測位する

③ 上記設定後、「保存」ボタンをクリックします

設定名欄に「サンプル」が表示されたら、次に「共有アドレス帳」の作成に移ります。

※端末の位置情報の取得設定条件が必要となりますので、次頁をご確認願います。

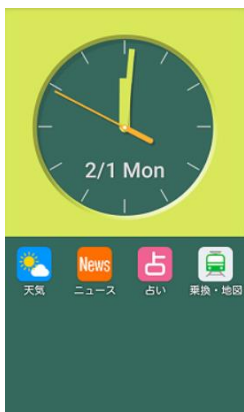
# 端末の位置情報設定

「センターキー」

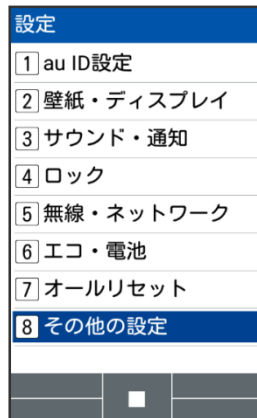
①待ち受け画面の状態で 「センターキー」を押します。



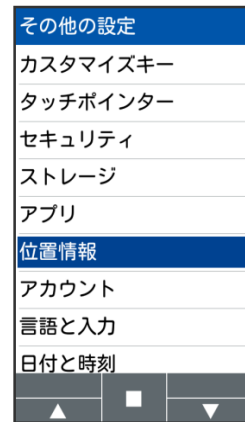
「電源/終話キー」



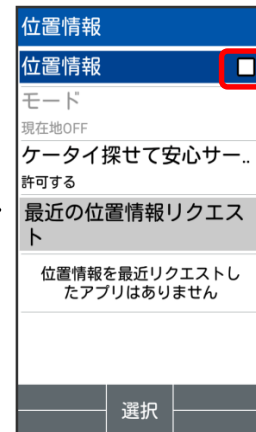
③「8」その他の設定を押します。



④「位置情報」を押します。



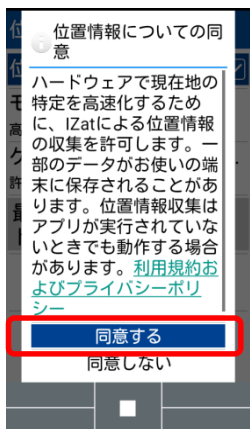
⑤「位置情報」を押します。



⑥「位置情報」に「レ」が表示されます。



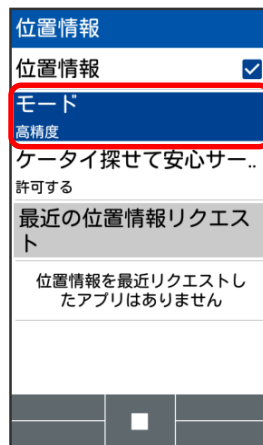
⑦「同意する」を押します。



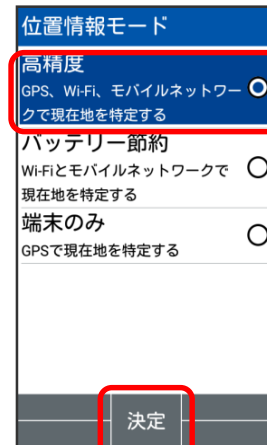
⑧画面表示が⑥に戻ります。



⑨「モード」を押します。



⑩「高精度」を確認し、「センターキー」を押します。



「電源/終話キー」を押しますと、待ち受け画面に戻ります。





# 管理プロフィール 共有アドレス帳

まず、連絡先情報が含まれたCSVファイルを事前に準備します。

- ① 設定名欄から該当ファイルを選択します。
- ② 「共有アドレス帳インポート」ボタンを押します。

KDDI Smart Mobile Safety Manager

0件のアラート

🏠 トップ

📱 機器

👤 ユーザー

👥 組織

☰ メニュー

共有アドレス帳

新規作成

選択した設定を削除

設定名

共有アドレス帳インポート

共有アドレス帳エクスポート

登録状況

0/3000

編集

①

②

<インポート用連絡先ファイルイメージ>

姓	名	姓(フリガナ)	名(フリガナ)	電話番号	メールアドレス	電話番号2	メールアドレス2	電話番号3	メールアドレス3
国際	太郎	コクサイ	タロウ	TEL:09000001000	test1501@kddi.com	TEL:09000000999	test1502@kddi.com	TEL:09000009999	test1503@kddi.com
国内	太郎	コクナイ	タロウ	TEL:09000002000	test1504@kddi.com	TEL:09000000888	test1505@kddi.com	TEL:09000008888	test1506@kddi.com
海外	太郎	カイガイ	タロウ	TEL:09000003000	test1507@kddi.com	TEL:09000000777	test1508@kddi.com	TEL:09000007777	test1509@kddi.com

- ・1管理プロフィールは、「最大50件」まで作成可能です。
- ・1管理プロフィールに連絡先の作成が「最大3000件」まで登録可能です。

# 管理プロフィール 共有アドレス帳

KDDI Smart Mobile Safety Manager

0件のアラート

🏠 トップ

📱 機器

👤 ユーザー

👥 組織

☰ メニュー

共有アドレス帳設定に戻る

共有アドレス帳インポート

ダウンロードしたファイルを編集し、「次へ」ボタンを押してください。

ダウンロード 次へ

① インポート用のCSVファイル (update\_values.csv) を管理者のPC機器へセーブするため、「ダウンロード」ボタンを押します。

② PCにセーブしたCSVファイルに、アドレス帳を更新し、「次へ」ボタンを押します。

共有アドレス帳設定に戻る

共有アドレス帳インポート アップロード

編集したCSVファイルをアップロードしてください。

参照...

アップロード

③ 「参照」ボタンでCSVファイルを選びます。

④ 「アップロード」ボタンを押します。

# 管理プロフィール 共有アドレス帳

KDDI Smart Mobile Safety Manager

0件のアラート

トップ

機器

ユーザー

組織

メニュー

データ確認中

×

データ確認中です。  
ブラウザを開いたまましばらくお待ちください。

全 3 件中 0 件完了 (0%) / エラー0件

入力データのチェック終了を待ちます。

エラーが発生したら、CSVファイルの内容を確認、  
修正します。

共有アドレス帳設定に戻る

下記内容でよろしければ「インポート実行」ボタンを押してください。

**⑤**

インポート実行

行	GUID(新規追加の場合は空欄)	姓	名	姓(フリガナ)	名(フリガナ)	電話番号	メールアドレス	電話番号2	メールアドレス2	電話番号3	メールアドレス3	削除(削除する:1)	備考
1		国際	太郎	コクサイ	タロウ	TEL:09000001000	test1501@kddi.com	TEL:09000000999	test1502@kddi.com	TEL:09000009999	test1503@kddi.com		
2		国内	太郎	コクナイ	タロウ	TEL:09000002000	test1504@kddi.com	TEL:09000000888	test1505@kddi.com	TEL:09000008888	test1506@kddi.com		
3		海外	太郎	カイガイ	タロウ	TEL:09000003000	test1507@kddi.com	TEL:09000000777	test1508@kddi.com	TEL:09000007777	test1509@kddi.com		

⑤インポート用のデータを再確認し、「インポート実行」ボタンを押します。

インポート中

×

インポート中です。  
ブラウザを開いたまましばらくお待ちください。

全 3 件中 0 件完了 (0%) / エラー0件

インポートの終了を待ちます。

※アドレス帳の新規追加の場合、  
「GUID」を空欄にします。

# 管理プロフィール 共有アドレス帳

KDDI Smart Mobile Safety Manager

0件のアラート

🏠 トップ

📱 機器

👤 ユーザー

👥 組織

☰ メニュー

インポートに成功しました。

CSVダウンロード

CSVアップロード

確認

完了

共有アドレス帳設定に戻る

⑥

全 3件

行	GUID(新規追加の場合は空欄)	姓	名	姓(フリガナ)	名(フリガナ)	電話番号	メールアドレス	電話番号2	メールアドレス2	電話番号3	メールアドレス3
1		国際	太郎	コクサイ	タロウ	TEL:09000001000	test1501@kddi.com	TEL:09000000999	test1502@kddi.com	TEL:09000009999	test1503@kddi.com
2		国内	太郎	コクナイ	タロウ	TEL:09000002000	test1504@kddi.com	TEL:09000000888	test1505@kddi.com	TEL:09000008888	test1506@kddi.com
3		海外	太郎	カイガイ	タロウ	TEL:09000003000	test1507@kddi.com	TEL:09000000777	test1508@kddi.com	TEL:09000007777	test1509@kddi.com

⑥インポート成功のメッセージが表示されましたら、（状態は「完了」に遷移します）  
「共有アドレス帳設定に戻る」を押します。

共有アドレス帳の作業が終了しましたら、次に「アプリケーション禁止」の作成に移ります。

# 管理プロフィール 共有アドレス帳

共有アドレス帳の編集はCSVファイルで行い、管理サイトにインポートします。

- ① 設定名欄から該当ファイルを選択します。
- ② 「共有アドレス帳エクスポート」ボタンを押します。

KDDI Smart Mobile Safety Manager

0件のアラート

トップ

機器

ユーザー

組織

メニュー

共有アドレス帳

新規作成

選択した設定を削除

設定名

共有アドレス帳インポート

共有アドレス帳エクスポート

設定名

サンプル

登録状況

0/3000

編集

エクスポートファイルで編集後、P59～P61と同様の手順でアドレス帳のインポートを行います。

<エクスポートファイルイメージ>

姓	名	姓(フリガナ)	名(フリガナ)	電話番号	メールアドレス	電話番号2	メールアドレス2	電話番号3	メールアドレス3
国際	太郎	コクサイ	タロウ	TEL:090000001000	test1501@kddi.com	TEL:090000009999	test1502@kddi.com	TEL:090000009999	test1503@kddi.com
国内	太郎	コクナイ	タロウ	TEL:090000002000	test1504@kddi.com	TEL:090000008888	test1505@kddi.com	TEL:090000008888	test1506@kddi.com
海外	太郎	カイガイ	タロウ	TEL:090000003000	test1507@kddi.com	TEL:090000007777	test1508@kddi.com	TEL:090000007777	test1509@kddi.com

# 管理プロファイル アプリケーション禁止

管理プロファイル配下にある「アプリケーション禁止」を選択します。  
画面が切替りますので、左側「アプリケーション禁止」欄の「新規作成」をクリックします。

KDDI Smart Mobile Safety Manager

0件のアラート

🏠 トップ

📱 機器

👤 ユーザー

👥 組織

☰ メニュー

アプリケーション禁止

設定名

新規作成

選択した設定を削除

設定名

利用禁止

サンプル

①

保存

取消

②

0/100

設定名

利用禁止

サンプル

禁止アプリケーション

アプリケーション名

LINE

パッケージ名

jp.naver.line.android

保存

取消

③

④

指定アプリケーションの利用禁止を設定します。

- ① 「アプリケーション禁止」配下の「新規作成」をクリックし、ファイル名を作成します。
- ② 「保存」ボタンをクリックすると、「設定名」配下にファイル名が表示されます。
- ③ 禁止アプリケーションの情報として、禁止アプリケーション名、パッケージ名を設定し、
- ④ 「保存」ボタンをクリックします。 パッケージ名の取得方法は、次頁で説明します。

# 管理プロフィール アプリケーション禁止

端末にインストールされているアプリケーション情報は、以下URLから取得できます。

<http://www.optim.co.jp/promotion/smsm/pdf/FPAppslist.pdf>

※4G LTEケータイプリセットアプリ制限可否一覧

例えば、「LINE」を制限したい場合。

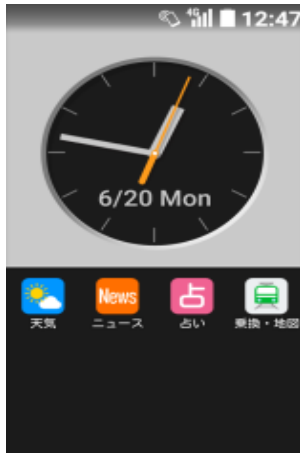
- ①上記一覧表からLINEを探します。
- ②アプリ制限の対応可否が「○」となっていたら、アプリケーション禁止メニューにおいて、アプリ名欄に「LINE」、パッケージ名欄に「jp.naver.line.android」を記入します。



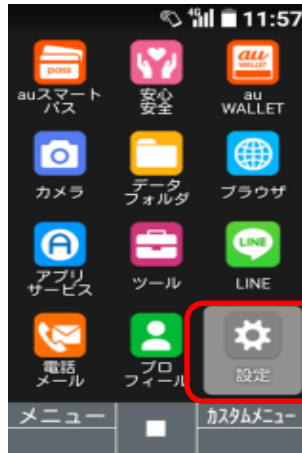
# LINEアプリの非表示設定【端末での作業】

待受け画面上の「LINE」を非表示にする場合は、以下の操作を行います。  
なお、アプリアイコン自体は消えません。（端末側にて表示設定も可能です）

TOP画面



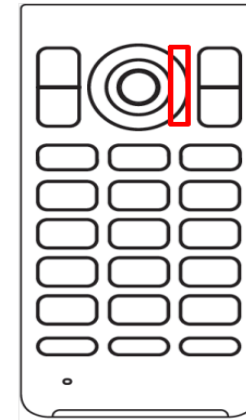
① 設定を選択



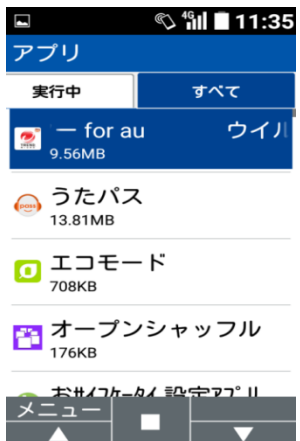
② 【8 その他の設定】を選択 ③ 【アプリ】を選択



④ 【下記右ボタンを2度押し】



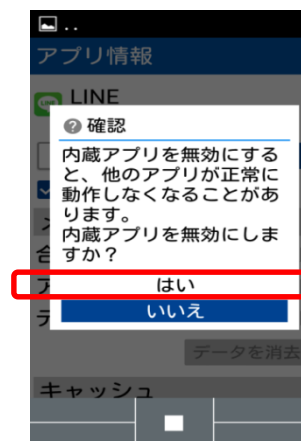
⑤ 【搭載アプリ】すべて表示  
となります。



⑥ スcrollさせて【LINE】を  
選択します。



⑦ 【無効にする】を選択する。⑧ 【はい】を選択して  
【OK】を選択。



⑨ メニュー画面にて  
アプリ【不明】になって  
いればOKです。



# 管理プロファイル Webフィルタリング (要オプション契約)

管理プロファイル配下にある「Webフィルタリング」を選択します。  
画面が切替りますので、左側「Webフィルタリング」欄の「新規作成」をクリックします。

KDDI Smart Mobile Safety Manager

0件のアラート

🏠 トップ

📱 機器

👤 ユーザー

👥 組織

☰ メニュー

Webフィルタリング

設定名  
サンプル

新規作成

選択した設定を削除

■ 設定名

禁止方式

許可するURLを指定する (指定されていないURLは禁止)  
 禁止するURLを指定する (指定されていないURLは許可)

保存 取消

Webフィルタリングの「許可」(ホワイトリスト)あるいは「禁止」(ブラックリスト)のURLを指定します。(どちらか一方になります)

Webフィルタリング

設定名  
サンプル

新規作成

選択した設定を削除

設定名

サンプル

禁止方式

許可するURLを指定する (指定されていないURLは禁止)  
 禁止するURLを指定する (指定されていないURLは許可)

登録状況  
1/1000

URL一覧 (先頭部分の一致による比較)

URL  
https://www.google.co.jp/

編集

+

① 「Webフィルタリング」配下の「新規作成」をクリックし、ファイル名を作成します。  
② 「保存」ボタンをクリックすると、「設定名」配下にファイル名が表示されます。

③次に、指定するURLの情報を入力します。  
入力終わりましたら、「+」を押します。  
これにより、URL情報が登録できます。

④禁止方式を変更する場合は、「編集」ボタンを押します。

# 参考：管理プロファイル Webフィルタリング (要オプション契約)

特定サイトへのアクセスを制限する機能「WEBフィルター」のオプション（有償：月額料金 200円/台）として、カテゴリフィルターがご利用できます。

※カテゴリフィルター：特定カテゴリ（不法、ギャンブルなど）に分類されるサイトへのアクセスを制限します。

標準機能Webフィルタリングとオプションのカテゴリフィルターを併用する場合、以下の動作となります。

## 1. 許可するURLを指定する（ホワイトリスト）

⇒ カテゴリフィルターの制限対象であるURLでも、登録されたURLは例外として許可します。

## 2. 禁止するURLを指定する（ブラックリスト）

⇒ カテゴリフィルターの制限対象でないURLでも、登録されたURLは例外として禁止します。

カテゴリフィルタ  
ー規制時の端末画  
面



# 参考：管理プロファイル Webフィルタリング (要オプション契約)

管理プロファイル配下にある「Webフィルタリング」を選択します。  
画面が切替りますので、左側「Webフィルタリング」欄の「新規作成」をクリックします。  
設定名を入力し、「カテゴリフィルター選択」より強度（フィルター 中設定）を選択します。  
次に、URLフィルター指定方式 で 「許可するURLを指定する」を選び、「保存」ボタンを押します。  
最後に URL指定リスト欄に 許可するURLを入力（<http://dictionary.goo.ne.jp/>）し「+」ボタンを押します。

KDDI Smart Mobile Safety Manager 0件のアラート トップ 機器 ユーザー 組織 メニュー

Webフィルタリング

新規作成  
選択した設定を削除

設定名

サンプル2

カテゴリフィルター選択  
フィルター 中設定

制限するカテゴリ

不法	アダルト・フェティシズム	セキュリティ	出会い	ギャンブル
ショッピング	コミュニケーション	ITサービス	過激な表現	青年・成人向け
趣味と娯楽	広告	迷惑メール		

URLフィルター指定方式  
許可するURLを指定する

URL指定件数  
1/1000

URL指定リスト (先頭部分の一致による比較)

URL  
http://dictionary.goo.ne.jp/

編集

# 参考：カテゴリフィルター制限一覧

		カテゴリレベル名		
カテゴリ種別		低設定	中設定	高設定
制限 カテゴリ	不法	閲覧不可	閲覧不可	閲覧不可
	アダルト・フェティシズム	閲覧不可	閲覧不可	閲覧不可
	セキュリティ	閲覧不可	閲覧不可	閲覧不可
	出会い	閲覧不可	閲覧不可	閲覧不可
	ギャンブル	閲覧不可	閲覧不可	閲覧不可
	コミュニケーション	閲覧不可	閲覧不可	閲覧不可
	過激な表現	閲覧不可	閲覧不可	閲覧不可
	青年・成人向け	閲覧不可	閲覧不可	閲覧不可
	趣味と娯楽	閲覧不可	閲覧不可	閲覧不可
	広告	可能	閲覧不可	閲覧不可
	迷惑メール	可能	閲覧不可	閲覧不可
	ショッピング	可能	閲覧不可	閲覧不可
	ITサービス	可能	閲覧不可	閲覧不可
	金融	可能	可能	閲覧不可
	ニュース	可能	可能	閲覧不可
	各種サービス	可能	可能	閲覧不可
	プロバイダ・ポータル・ホスティング	可能	可能	可能
	ビジネス・経済	可能	可能	可能
	生活と暮らし	可能	可能	可能
	医療と健康	可能	可能	可能
	学術・教育	可能	可能	可能
政治・行政	可能	可能	可能	
各種産業	可能	可能	可能	

# 環境設定

「メニュー」タブから「環境設定」を選択します。画面が切替りますので、左側の「環境設定」欄から「エージェント共通管理」をクリックします。

KDDI Smart Mobile Safety Manager 0件のアラート トップ 機器 ユーザー 組織 **メニュー**

環境設定  
個人設定  
**エージェント共通管理**  
ログメール通知  
無通信検知  
設定バックアップ

管理サーバーとの通信間隔

分数指定:  分  
 時間指定:  時間  
 日数指定:  日

※機種によって端末のスリープ中は通信が行われないことがあります。  
※通信間隔が短い場合、端末のバッテリー消費が早まる可能性があります。

管理サーバーと通信できなかった場合

なにもしない  
 指定分数後にロック:  分  
 指定時間後にロック:  時間  
 指定日数後にロック:  日

※通信間隔の設定によってはロックまでに時間がかかることがあります。

ロックメッセージ

リモートロックの解除コード

端末でのエージェント停止・ライセンス解除・アンインストールの制限

制限なし  
 パスワードの入力:

**保存** 取消

環境設定の内容は、全ての機器に適用されます。  
機器が管理サーバーと定期的に同期する間隔および同期できなかった場合の端末へのリモートロック等を指定します。

①管理サーバーとの定期的な同期（通信間隔）を設定します。「エージェント共通管理」の「日数指定」を1日 で設定します。

②設定条件の入力が終了しましたら、「保存」ボタンを押します。  
※リモートロック解除コードの設定、変更可能です。

# 環境設定

環境設定

個人設定

エージェント共通管理

**ログメール通知**

無通信検知

設定バックアップ

①

メール通知タイミング

随時  1日1回  一時停止

メール通知対象ログ

リモートロック

リモートワイプ

スクリーンロック設定のパスワード変更

無通信検知

スクリーンロック解除失敗時のリモートロック・ワイプ

アプリケーション使用禁止

位置情報設定の変更

言語

日本語

メール送信先

管理者

機器のユーザー

メール送信先(カスタム)

保存 取消

環境設定

個人設定

エージェント共通管理

ログメール通知

**無通信検知**

設定バックアップ

②

無通信検知

指定時間通信がない機器を検知: [ ] 時間

指定日数通信がない機器を検知: [6] 日間

なにもしない

保存 取消

## ②無通信検知

端末の長期利用がない場合を想定し、サーバとの無通信期間が「指定日数」の間で通信がない機器を検知します。  
指定日数：6日間 とします。

## ①ログメール通知

リモートロックやリモートワイプ等が行われた場合に、メールで通知することができます。「ログメール通知」欄からメール通知対象事項は、「リモートロック」、「リモートワイプ」メール送信先としては、「管理者」に設定します。

# 管理プロフィール

「メニュー」タブから「管理プロフィール」を選択します。  
画面が切替りますので、右側の「アクション」欄から「新規」をクリックします。

KDDI Smart Mobile Safety Manager 0件のアラート [トップ](#) [機器](#) [ユーザー](#) [組織](#) [メニュー](#)

管理プロフィール

<input type="checkbox"/>	プロフィール名	デバイス制限	パスワード	位置情報	共有アドレス帳	アプリケーション禁止	Webフィルタリング
<input type="checkbox"/>	サンプル	サンプル	サンプル	サンプル	サンプル	サンプル	サンプル

プロフィールの新規作成

プロフィール名

入力してください。

デバイス制限  
(設定なし)

パスワード  
(設定なし)

位置情報  
(設定なし)

共有アドレス帳  
(設定なし)

アプリケーション禁止  
(設定なし)

Webフィルタリング  
(設定なし)

① 設定名を記入します。

② セキュリティポリシー条件に沿って作成した各ファイルを「▼」をクリックして、選定します。

③ 選定が終了しましたら、「保存」ボタンを押します。

④ プロフィール名欄に、作成したプロフィール名が表示されることを確認します。



# 管理プロフィール

組織	選択中の組織	
設定名	組織名	管理プロフィール
全体	全体	(設定なし)
営業本部	配下の組織	
情報本部	組織名	管理プロフィール
	営業本部	(所属組織に従う:設定なし)
	情報本部	(所属組織に従う:設定なし)

詳細
<a href="#">この階層に新規作成</a>
<a href="#">編集</a>

組織	選択中の組織	
設定名	組織名	管理プロフィール
全体	全体	サンプル
営業本部	配下の組織	
情報本部	組織名	管理プロフィール
	営業本部	(所属組織に従う:サンプル)
	情報本部	(所属組織に従う:サンプル)

< 編集
組織名 全体
管理プロフィール サンプル
<a href="#">保存</a> <a href="#">取消</a>

全端末共有のセキュリティポリシーを設定する場合、

- ① メニューの「組織」から、「詳細」→「編集」を選択します。
- ② 管理プロフィールで作成したファイル名（例：サンプル）を選びます。
- ③ 「保存」ボタンを押します。新しい端末がKDDI SMSMサーバと接続された時点で、新しい端末に管理プロフィールが配信されます。（セキュリティポリシーが適用されます）



# 4G LTEケータイへの KDDI SMSM エージェントソフト導入

# はじめに

4G LTE ケータイにKDDI SMSMのエージェントソフトをインストールおよびKDDI SMSMサービス利用のための※ライセンス認証が必要です。主な手順は以下のとおりです。

## ① 4G LTE ケータイへのKDDI SMSMエージェントソフトの導入

- ・インストーラの起動
- ・インストール実施

## ② 4G LTE ケータイ側でのKDDI SMSM利用のためのライセンス認証

※ライセンス認証には、「企業コード」、「認証コード」が必要です。

両コードは、KDDI SMSMの管理サイト（トップ画面）にて確認できます。

# KDDI SMSMエージェントソフト導入方法

4G LTEケータイの電源を入れてから、導入作業完了するまでの手順は以下のとおりです。  
画面遷移図（④～⑨）は次頁を参照願います。

- ① 4G LTEケータイの電源を入れますと、画面上に 「ようこそauへ」 が表示されますので、センターキーを押します。
- ② 端末初期設定の画面が表示されますので、「設定」（再度、センターキー）選択します。
- ③ au ID設定の画面が表示されますので、「クリア」キーを選択します。
- ④ ホーム画面（時計、アプリが表示）になりますので、次の文字、数字を入力します。  
**\*#\*#7676#\*#\*** （自動的にエージェントソフトがインストールされます）
- ⑤ インストールが正常に終了しますと、KDDI SMSMの画面が表示されます。
- ⑥ KDDI SMSM画面の 「ライセンス認証」を選択します。
- ⑦ 利用規約画面が表示れますので、同意にチェックし、「OK」を選択します。
- ⑧ 権限付与の確認画面が表示されますので、「はい」を選択します。
- ⑨ ライセンス認証画面に遷移しますので、以下の情報を入力し、「送信」ボタンを選択します。  
**企業コード（必須）、認証コード（必須）、ユーザーID（任意）**
- ⑩ 認証が終了しますと、「設定が完了しました」が表示されます。
- ⑪ 「クリア」キーを選択しますと、ホーム画面に遷移します。

※⑥～⑨の作業途中で、ホーム画面に戻った場合は、以下の手順で再開できます。

「センター」キー押下 → 「アプリサービス」選択 → プリセット一覧から「KDDI Safety Manager」選択

# KDDI SMSエージェントソフト導入方法

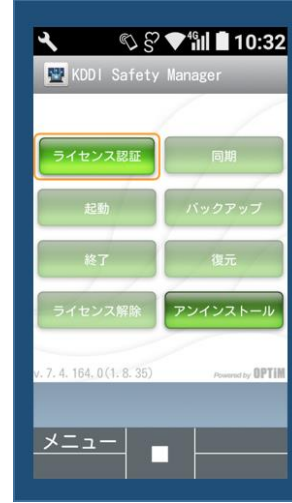
## 1. インストーラ起動



## 2. インストール実施



## 3. インストール完了



## 4. ライセンス利用



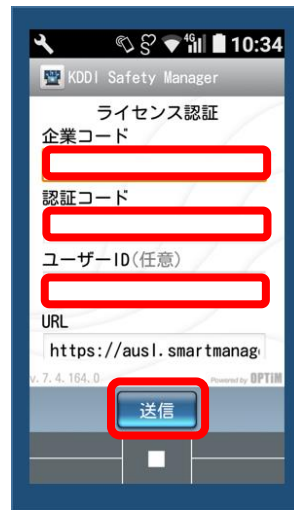
## 5. ライセンス利用



## 6. 権限付与



## 7. ライセンス認証



## 8. ライセンス認証中



## 9. ライセンス認証完了



# KDDI SMSMエージェントソフトウェアアップデート

SMSMエージェントアプリ（以下、エージェント）が最新ではない場合、端末にはエージェントの新バージョン通知が表示されます。その通知を選択していただくと、エージェントのアップデートが可能です。

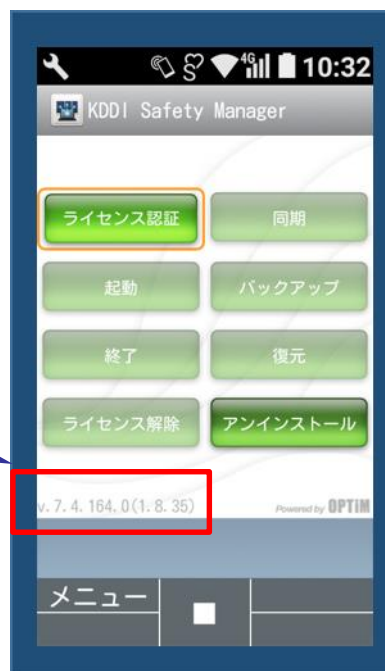
アップデート前に通知を誤って消してしまった場合は、同期をすることで再度通知ができます。

※エージェントのバージョンが 7.4.200.0未満の場合、**Wi-Fi経由でのみ**アップデート可能となります。

バージョンが 7.4.200.0以上の場合は、**Wi-Fiと4G LTE経由の両方**で可能アップデート可能です。

※7.4.200.0のバージョンは2016/11/29リリースされたものです。

ここでバージョン  
を確認できます。



※左記は参考画面です。  
実際の最新バージョンとは異なります。

# KDDI SMSエージェントソフトウェアアップデート

Wi-Fi経由(2.4GHz帯)でアップデートを行う場合、Wi-Fiの利用設定を行います。4G LTEでアップデートする場合、次のスライドにお進みください。

「センターキー」  
「カメラキー」

①待ち受け画面の状態  
「センターキー」を押します。

②「設定」を選択し、  
「センターキー」を押します。

③「無線・ネットワーク」を  
選択し、「センターキー」  
を押します。

④「Wi-Fi」を選択し、「セ  
ンターキー」を押します。

⑤Wi-Fi設定がOFFの場  
合、「Wi-Fi」を選択し、「セ  
ンターキー」を押します。



⑥接続するWi-Fiネット  
ワークを選択し、「セン  
ターキー」を押します。

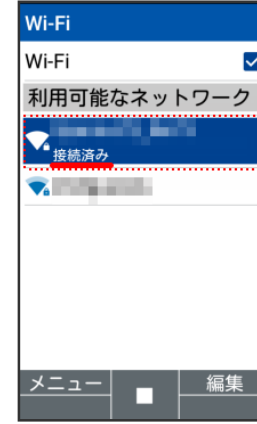
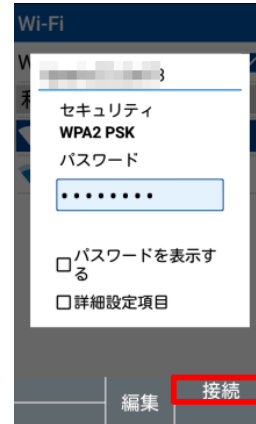
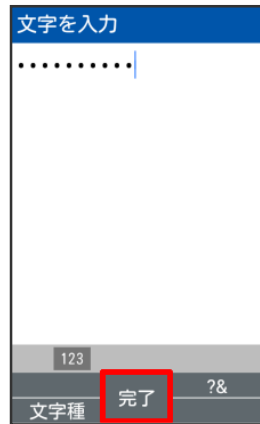
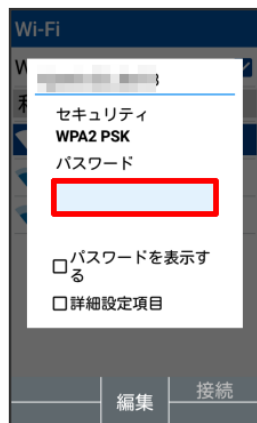
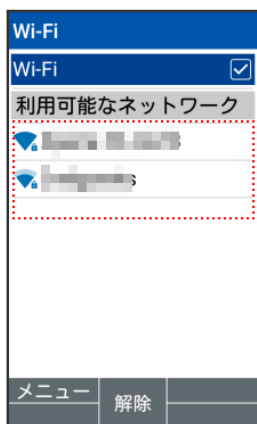
⑦パスワードの項目を  
選択し、「センターキー」  
を押します。

⑧パスワードを入力し、  
「センターキー(完了)」  
を押します。

⑨「カメラキー(接続)」を  
選択し、「センターキー」  
を押します。

⑩選択したSSIDの下に  
「接続済み」と表示が出  
ます。

「電源/終話キー」  
を押しますと、  
待ち受け画面に戻  
ります。



# KDDI SMSエージェントソフトウェアアップデート

①待ち受け画面の状態  
で新バージョン通知  
を確認します。



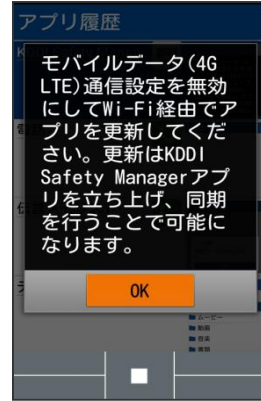
②待ち受け画面の状  
態で「カーソルキー」  
の下を押します。



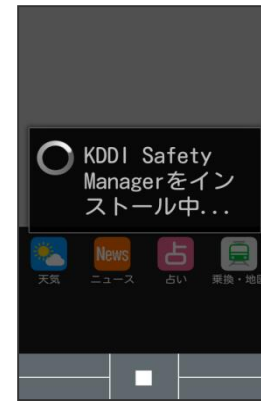
③通知画面で下  
記表示を確認し、  
センターキーを  
押します。



④下記メッセージ、を確  
認し、センターキーを  
押します。  
(表示されないケース有)



⑤エージェントのアップ  
デートが行われます。



⑥エージェントのアップ  
デートが終了する  
と、待ち受け画面に  
戻ります。



⑦待ち受け画面でセン  
ターキーを押し、カーソ  
ルキーで「設定」を選び、  
センターキーを押します。



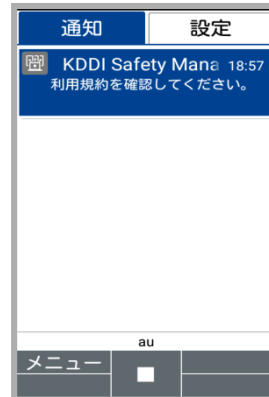
⑧しばらくすると利用規約  
の確認メッセージが表示  
されます。



⑨待ち受け画面の状  
態で「カーソルキー」  
の下を押します。



⑩通知画面で下記表  
示を確認し、センタ  
ーキーを押します。



⑪【利用規約に同意す  
る】にチェック後【OK】  
を押します。



⑫アプリのバージョンが  
7.4.220を確認し、「電源/  
終話キー」を押します。







# SMSM ユーザー画面

# ユーザー画面

ユーザー用サイト上では、端末利用者自身で、端末の同期、端末の位置確認、およびロック/解除/ワイプを実施することができます。

なお、管理者は以下の作業を予め行って下さい。これにより「ユーザー用サイト」への利用が可能となります。

- ① KBOS画面のメニューバーの「ユーザー」から「ユーザー追加」を行います。  
※サービス利用設定（P.14～P.16）を参考にして下さい。
- ② KBOS画面の「ユーザー」から「ユーザー一覧」を選び、該当ユーザーへのKDDI SMSMの登録作業を行います。  
※サービス利用設定（P.17～P.22）を参考にして下さい。

---

## ユーザー用サイト

ユーザー認証/位置情報確認

---

同期

---

連絡帳バックアップ

---

ロック実施/解除

---

ワイプ実施

---

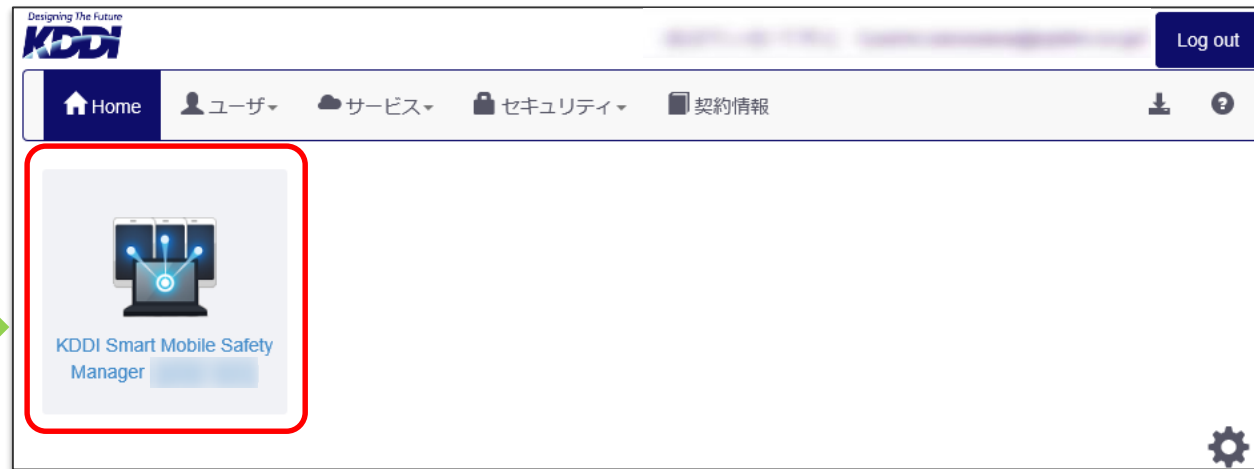
# ユーザー画面

サービス一覧に表示されている「KDDI Smart Mobile Safety Manager」を選択します。

KDDI Business Online Support  
(以下、KBOS) へのログイン



利用可能なサービス一覧



KDDI Business Online Support上で権限が「ユーザー」の場合、上記アイコンから「ユーザー用サイト」へ遷移します。

# ユーザー画面

端末を操作するためには、ログインするユーザーと機器が紐づいている必要があります。  
端末認証時、「ユーザーID」を入力しておくことで、ユーザーと機器は紐づきます。

## KBOSへのログイン



## 利用可能な機能一覧



# ユーザー画面（端末との同期実施）

端末利用者(ユーザー)は手動で  
端末側から同期できます。



「同期」の際、※「センタープッシュ」を利用するため、Wi-Fi通信のみでなく、モバイルデータ通信回線が開通しており、かつ利用可能な状態であることが必要となります

※センタープッシュは、センター側からの起動により、指定のau携帯電話のアプリケーション等を起動させる機能です

# ユーザー画面（リモートロック実施）



# ユーザー画面（リモートロック解除）



1. 「ロックを解除する」を押します



2. 「ロック解除」を押します



3. ロック解除指示が送信されました

# ユーザー画面（ワイプ実施）

リモートワイプを行いますと、取り消しができませんのでご注意願います。

1. 「ワイプする」を押します

2. 「初期化に同意する」のを押します。

3. 「ワイプ」ボタンを押します

4. ワイプ指示が送信されました

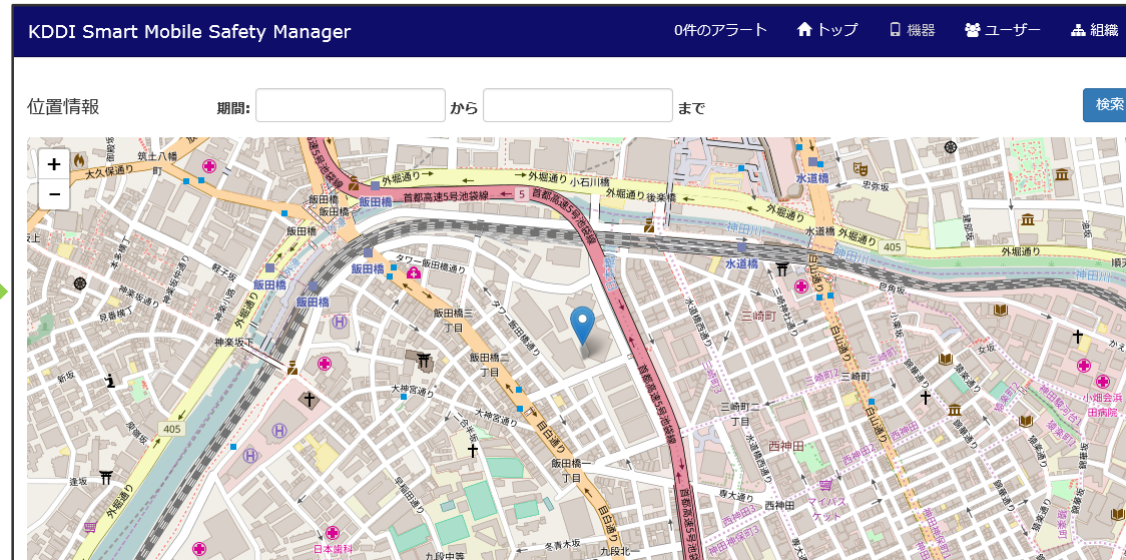
## 初期化同意前のボタン

ユーザーが「初期化に同意する」にチェックをするまで、ワイプボタンは非活性化され、押下できません。





# ユーザー画面 (位置情報を確認)



*Designing The Future*

**KDDI**