

# あんしんセキュリティ



## マニュアル

第 3.3 版

株式会社 NTTドコモ

2024年12月11日

## ■ 目次

第 1 章 「あんしんセキュリティ」アプリとは	5
サービス別 利用可能な機能	5
機能	6
利用料金	7
対応機種・動作環境	7
第 2 章 アプリを使い始める	8
「あんしんセキュリティ」をインストールする	8
初期設定する	9
省電力機能の設定を行う	1 6
第 3 章 セキュリティ対策状況を確認する	1 8
ホーム画面の説明	1 8
第 4 章 セキュリティチェック、脅威の検出レポートを確認する	2 0
レポートを表示する	2 0
レポート画面の説明	2 1
詳細レポート画面	2 2
第 5 章 セキュリティに関するニュースを見る	2 3
ニュースを表示する	2 3
ニュースを評価する	2 3
第 6 章 セキュリティスキャン機能を確認する	2 4
セキュリティスキャン機能とは	2 4
セキュリティスキャンの種類・対象	2 4
セキュリティスキャン画面を確認する	2 4
セキュリティスキャンの設定を確認する	2 6
セキュリティスキャンで脅威を検出したら？	3 2
ログの確認	3 6
第 7 章 危険サイト対策を確認する	3 7
危険サイト対策とは	3 7
危険サイト対策画面を確認する	3 7
危険サイト対策の設定を確認する	3 9
危険サイト対策で脅威を検出したら？	3 9
第 8 章 アプリチェックを確認する	4 1

アプリチェックとは	4 1
アプリチェック画面を確認する	4 1
アプリチェックの設定を確認する	4 2
アプリチェックでアプリ一覧を確認する	4 2
第 9 章 危険 Wi-Fi 対策を確認する	4 4
<hr/>	
危険 Wi-Fi 対策とは	4 4
危険 Wi-Fi 対策画面を確認する	4 4
危険 Wi-Fi 対策の設定を確認する	4 4
危険 Wi-Fi 対策で脅威を検出したら？	4 5
位置情報の使用が OFF の場合	4 7
第 10 章 迷惑電話対策を確認する	4 8
<hr/>	
迷惑電話対策とは	4 8
発着信時に表示される画面を確認する	4 8
迷惑電話対策の主な機能	4 9
迷惑電話対策画面を確認する	5 0
迷惑電話対策の設定を確認する	5 0
迷惑電話で危険・迷惑な電話を検出した場合の対処方法	5 2
迷惑電話番号を検索する	5 6
第 11 章 迷惑メール対策を確認する	5 7
<hr/>	
迷惑メール対策設定とは	5 7
迷惑メール対策設定画面を確認する	5 7
第 12 章 SMS フィルタリングを確認する	5 9
<hr/>	
SMS フィルタリング機能とは	5 9
SMS フィルタリング機能の設定について	5 9
SMS フィルタリング設定方法	6 2
迷惑メッセージフォルダの確認方法	6 3
迷惑なメッセージを受信した場合	6 4
第 13 章 ダークウェブモニタリングを確認する	6 5
<hr/>	
ダークウェブモニタリングとは	6 5
モニタリング情報を登録する	6 5
モニタリング情報を削除する	6 8
流出を検知したら	6 9
検知結果通知の設定	7 1
検知詳細画面の見方	7 2
第 14 章 各機能の設定を変更する	7 3
<hr/>	
アカウント	7 3
設定画面	7 4

第 15 章 サービス利用上の注意点 7 6

---

ご利用にあたって 7 6

通信について 7 8

端末の動作環境について 7 8

---

# 第1章 「あんしんセキュリティ」アプリとは

あんしんセキュリティアプリは、以下のサービスをご利用いただけるアプリです。

- ・あんしんセキュリティ
- ・あんしんセキュリティ トータルプラン ※マルチアカウント利用者も含まれます
- ・あんしんセキュリティ スタンダードプラン
- ・あんしんセキュリティ 無料プラン
- ・あんしんセキュリティ（迷惑SMS対策）※1
- ・あんしんセキュリティ（プライバシー）※1

毎日使っているメール、アプリ、WEBサイト、Wi-Fiや個人情報。セキュリティは大丈夫なのか心配になりますね。

そんなときは、ウイルス、危険サイト、危険 Wi-Fi、迷惑メール、迷惑電話対策や個人情報の流出検知などドコモがおすすめするセキュリティサービスをまとめて管理できる「あんしんセキュリティアプリ」で、あんしん・安全にスマートフォン・タブレットを利用してください。

※1 新規での契約受付は終了しています

## サービス別 利用可能な機能

機能	あんしん セキュリティ トータル プラン※3	あんしん セキュリティ スタンダード プラン	あんしん セキュリティ	あんしん セキュリティ 無料プラン	あんしん セキュリティ (プライバシー)	あんしん セキュリティ (迷惑 SMS 対策)	契約なし
セキュリティスキャン	○	○	○	○	○	○	○
危険サイト対策	○	○	○	-	-	-	-
アプリチェック	○	○	○	-	-	-	-
危険 Wi-Fi 対策	○	○	○	○	-	-	-
迷惑電話対策 ※1	○	○	○	-	-	-	-
迷惑メール対策	○	○	○	-	-	-	-
迷惑 SMS 対策 ※1	○	○	-	-	-	○	-
ダークウェブモニタリング	○	○	-	-	○	-	-
PC セキュリティ	○	-	-	-	-	-	-
レポート ※2	○	○	○	○	-	-	-
ニュース	○	○	○	○	○	○	○

○：利用可能、-：利用不可

※1 タブレットではご利用できません。

※2 ご利用のサービスにより、レポートの機能が異なります。

※3 マルチアカウント利用者は、PC セキュリティ以外のあんしんセキュリティ トータルプランと同じ機能を利用できます。

PC セキュリティはあんしんセキュリティ トータルプランもしくはネットワークセキュリティをご契約された d アカウントを設定することで利用可能です。

## 機能

機能	概要
セキュリティスキャン	スマートフォンやタブレットをスキャンし、有害アプリ等から保護します。
危険サイト対策	詐欺サイト、ウイルス配布サイトなど危険なサイトを閲覧すると警告画面を表示します。
アプリチェック	アプリが個人情報を外部送信していないかをチェックし、注意レベルを一覧表示します。
危険Wi-Fi対策	通信内容を改ざんされたり、盗み見られたりする可能性がある危険な Wi-Fi スポットに接続すると、警告画面を表示します。
迷惑電話対策	しつこいセールスなどの迷惑な番号や、詐欺などの危険な番号の発着信時に警告画面を表示したり、電話番号に紐づく企業名や、飲食店名を表示します。 また、発着信以外でも電話番号を入力すると危険な番号や発信元情報を確認できます。
迷惑メール対策	詐欺などの危険なメールを含む迷惑メールを自動で判定し、迷惑メールフォルダへ振り分けます。
SMS フィルタリング	詐欺などの危険なメッセージを含む迷惑 SMS を自動で判定し、迷惑メッセージフォルダへ振り分けます。
ダークウェブモニタリング	お客様の個人情報が流出していないかモニタリングし、流出を検知したらお知らせします。
PC セキュリティ	PC 向けのセキュリティ対策です。コンピューターウイルス、スパイウェア、ネット詐欺、不正アクセスなど、様々な脅威に対しパソコン (Windows, Mac) の保護対策をします。
レポート	定期的にチェック数や脅威の発見数をレポートします。月ごとに見ることができるので、傾向を把握することも可能です。
ニュース	ウイルスなどの脅威や、セキュリティのトレンド情報を定期的に配信します。

## 利用料金

---

セキュリティ管理機能の一部、レポート管理機能の一部、およびニュース機能は、無料でご利用いただけます。

「あんしんセキュリティ」は、ドコモ回線のご契約がないお客様もお申込みいただけます。

「あんしんセキュリティ トータルプラン」「あんしんセキュリティ スタンダードプラン」「あんしんセキュリティ 無料プラン」は、ドコモ回線のご契約がないお客様はお申込みいただけません。

全ての機能を利用するには以下のご契約が必要となります。

あんしんセキュリティ	月額使用料 220 円（税込）
あんしんセキュリティ トータルプラン	月額使用料 1078 円（税込）
あんしんセキュリティ スタンダードプラン	月額使用料 550 円（税込）

※ドコモメールがご利用いただけない場合、迷惑メール対策はご利用できません。

※「あんしんセキュリティ」アプリのダウンロード、およびアプリの利用に伴うパケット通信料が別途かかります。

※海外でもご利用いただけますが、通信料金にご注意ください。

## 対応機種・動作環境

---

Android 9.0 以上のドコモスマートフォン・タブレット

一部非対応機種につきましては、対応機種一覧 ([https://www.nttdocomo.co.jp/service/anshin\\_security/compatible\\_model/index.html](https://www.nttdocomo.co.jp/service/anshin_security/compatible_model/index.html)) をご参照ください。

## 第2章 アプリを使い始める

### 「あんしんセキュリティ」をインストールする

あんしんセキュリティサービスをご契約の回線をご利用の場合、アプリは自動的にインストールされます。  
以下、あんしんセキュリティサービスをご契約されていない場合、または個別にあんしんセキュリティをインストールする場合の手順です。

1



dメニューを表示し、「おすすめのサービスをもっと見る」をタップ

2



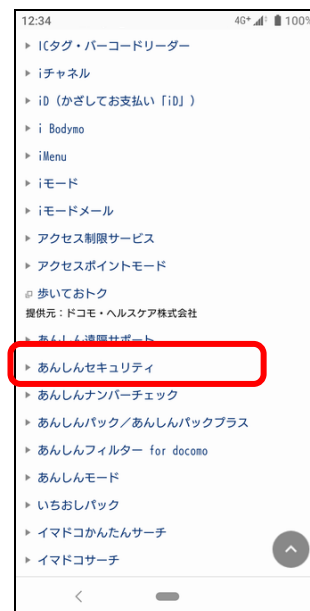
「おすすめのサービス一覧へ」をタップ

3



「50音順一覧へ」をタップ

4



「あんしんセキュリティ」をタップ

5



「ダウンロード」をタップ

6



「インストール」または「アップデート」をタップ

7



アイコンが追加されます

※「あんしんセキュリティ」の容量は約 55M バイトです。  
※ドコモ回線に契約していない場合はドコモアプリ管理の「契約中サービス」に表示されない為、本手順にてアプリをインストールしてください。



# 初期設定する

インターネットに接続して操作してください。

1



アイコンをタップ

2



スプラッシュ画面が表示されます

3



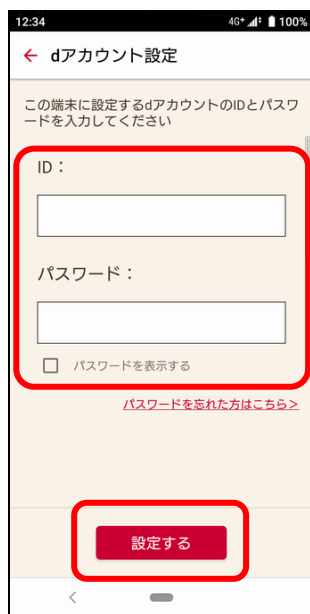
「規約に同意して利用を開始」をタップ

4



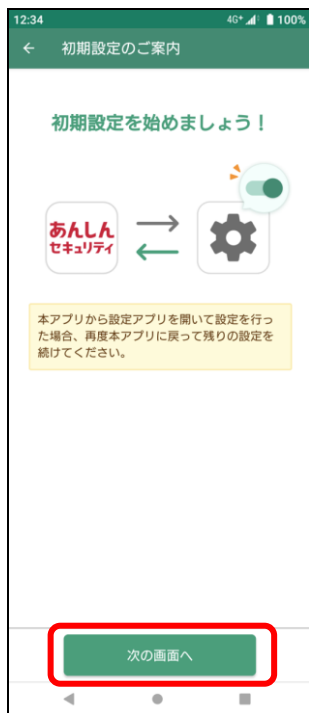
「初期設定を開始する」をタップ

5 dアカウント未設定時



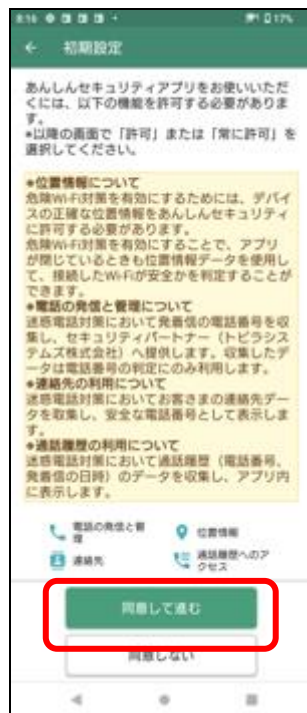
dアカウント未設定の場合、dアカウントのIDとパスワードを入力し、「設定する」をタップ(※1)

6



「次の画面へ」をタップ

7



説明を読み、「同意して進む」をタップ

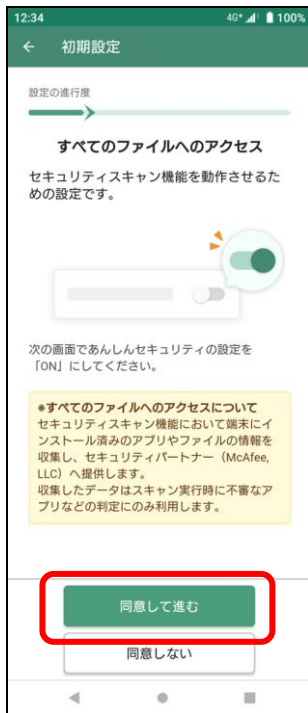
8



「許可」をタップ

※1 dアカウント未設定時のみ表示されます。

## 9 ※Android 11.0 以降



「同意して進む」をタップ(※2)

## 10 ※Android 11.0 以降



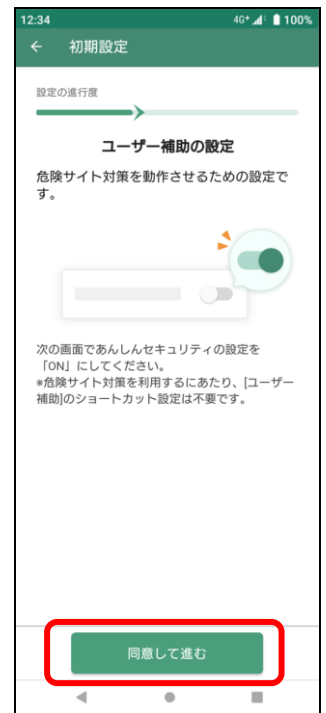
「あんしんセキュリティ」をタップ

## 11 ※Android 11.0 以降



すべてのファイルへのアクセスを ON に変更  
その後アプリを起動

## 12



「設定画面を起動する」をタップ

## 13



「あんしんセキュリティ」をタップ

## 14



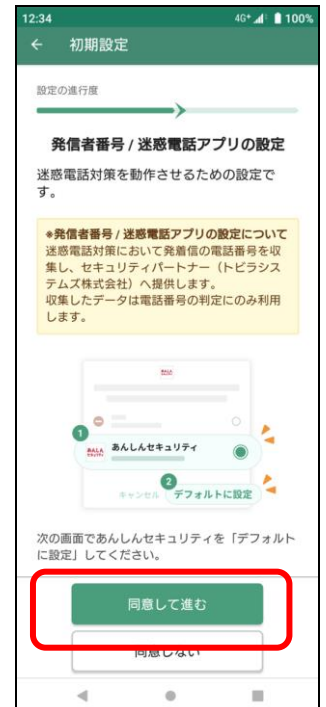
「あんしんセキュリティ」の使用を ON に変更

## 15



「許可」をタップ  
その後アプリを起動

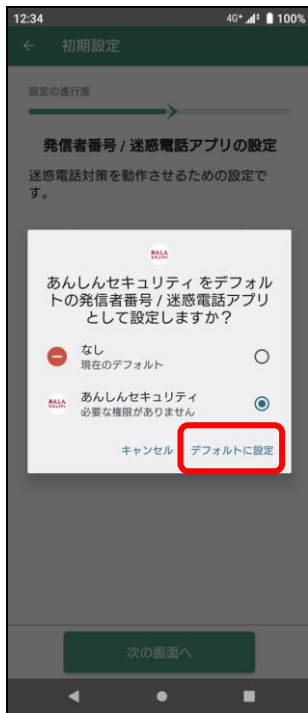
## 16 ※Android 12.0 以降



「同意して進む」をタップ(※3)

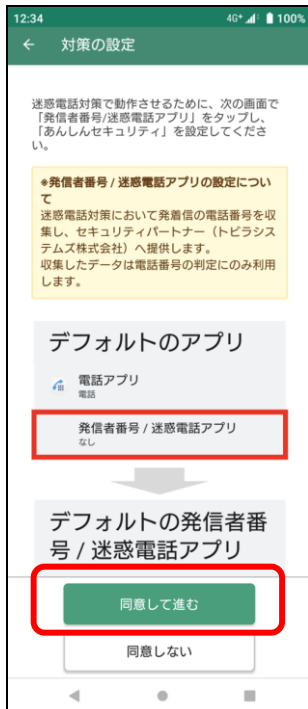
※2 Android 11.0 以降のみ表示されます。  
※3 Android 12.0 以降のみ表示されます。

## 17 ※Android 12.0 以降

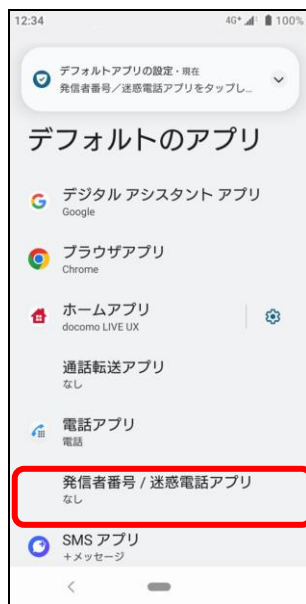


あんしんセキュリティを選択し、「デフォルトに設定」をタップ

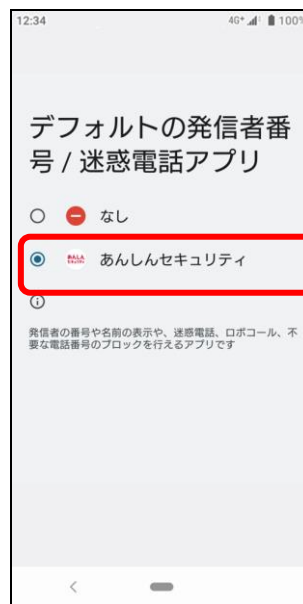
※ Android 12.0 以降 「16」「17」の設定のかわりに以下案内が表示される場合があります



「同意して進む」をタップ(※3)



「発信者番号 / 迷惑電話アプリ」をタップ



「あんしんセキュリティ」をタップ

18



「次の画面へ」をタップ

19



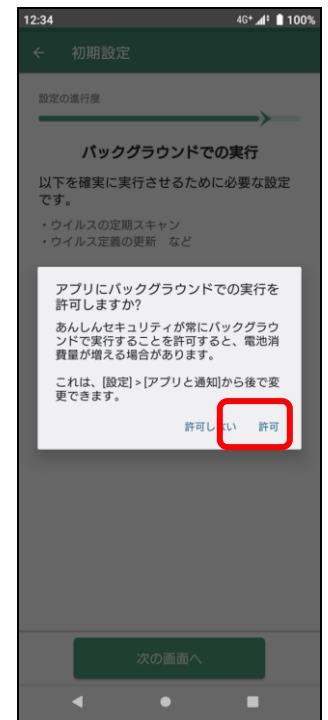
「他のアプリの上の表示を許可」ボタンをONに変更  
その後アプリを起動

20



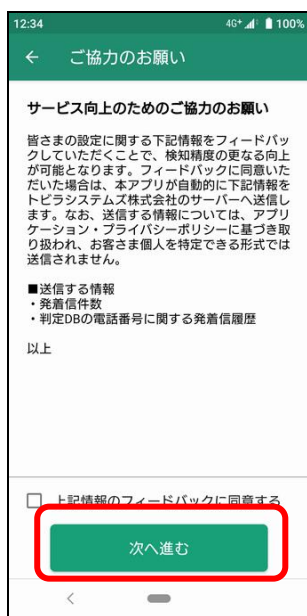
「次の画面へ」をタップ

21



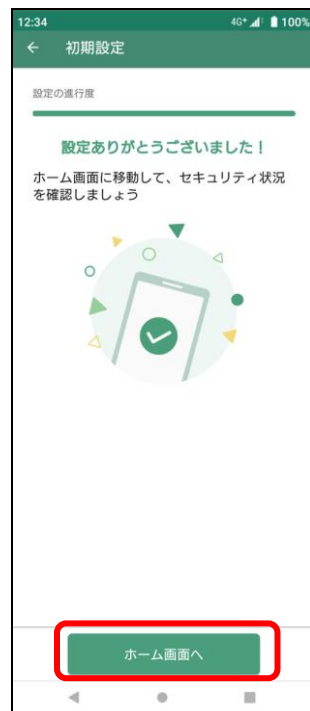
「許可」をタップ

22



説明を読み、「次へ進む」をタップ  
※フィードバックに同意いただける場合は  
チェックを入れてから「次へ進む」をタップ

23



「ホーム画面へ」をタップ

24



ホーム画面が表示されます

25 ※契約なしのホーム画面



無料機能の「スキャン」のみ一覧に表示  
されます

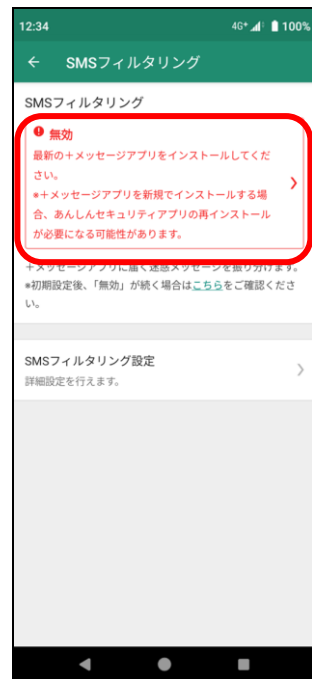
あんしんセキュリティ トータルプラン、あんしんセキュリティ スタンダードプラン、マルチアカウント利用者、あんしんセキュリティ（迷惑SMS対策）ご契約の場合は、引き続き以下の設定を行ってください。

## 26



「迷惑SMS」をタップ

## 27



有効を確認。無効の場合、赤枠箇所をタップし、有効に設定

詳しくは、第12章を参照してください。

あんしんセキュリティ トータルプラン、あんしんセキュリティ スタンダードプラン、マルチアカウント利用者、あんしんセキュリティ (プライバシー) ご契約の場合は、引き続き以下の設定を行ってください。

## 28



「プライバシー」をタップ

## 29



「次に進む」をタップ

## 30



「モニタリング対象が設定されていません」をタップ

## 31



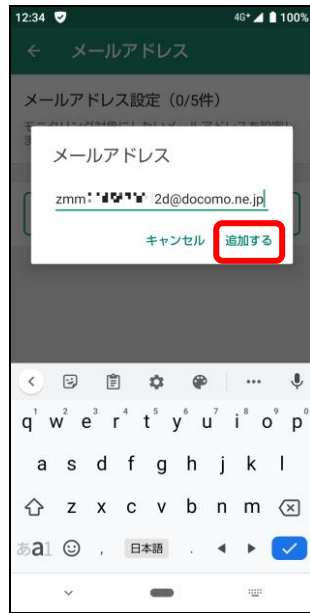
「メールアドレスを設定していきましょう」をタップ

### 32



「メールアドレスを追加」をタップ

### 33



モニタリングしたいメールアドレスを入力し、「追加する」をタップ

### 34



モニタリング対象としてメールアドレスが登録されました。

他の情報をモニタリング対象として登録する場合、第 13 章を参照してください。

■ あんしんセキュリティ トータルプラン、あんしんセキュリティ スタンダードプラン、あんしんセキュリティサービス未契約の場合

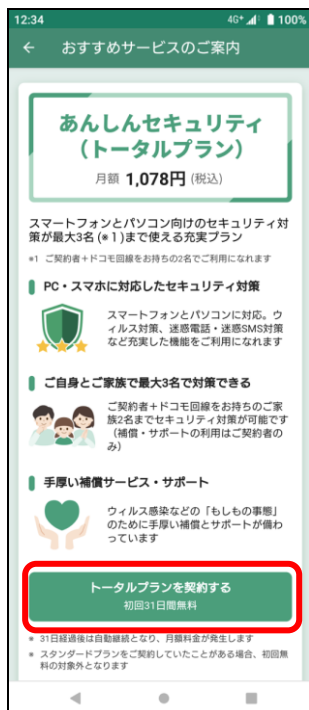
あんしんセキュリティ トータルプラン、あんしんセキュリティ スタンダードプラン、あんしんセキュリティサービスが未契約の場合、ホーム画面からサービスの契約を行うことができます。

1



バナーをタップ

2



契約したいサービスをタップすると、サービス契約ページが表示されますので、案内に従って操作してください

## 省電力機能の設定を行う

Android 9.0 以降の機能である「省電力機能」において、本アプリが『対象アプリ』となっている場合、バックグラウンド通信は行えないため、データベースの更新や認証が想定通りに実施されず、データベースが最新の状態にならない可能性があります。以下の手順を行っていただき、「省電力機能」において、本アプリを『対象外アプリ』に設定してください。 ※端末の設定状況により、通知タップ後の操作が異なります。

### ■「バックグラウンドでの実行を許可する」の設定

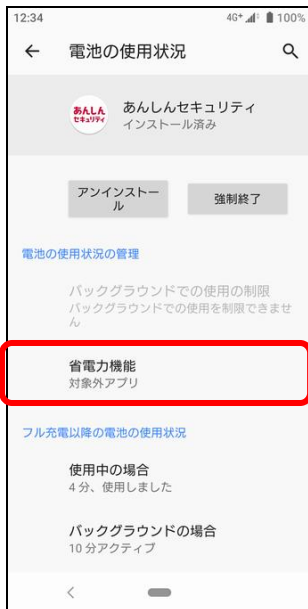


### ■「バックグラウンドでの使用の制限を解除」の設定



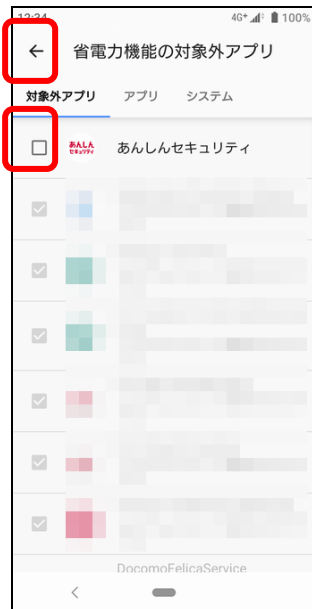


5



「バックグラウンドでの使用の制限」が選択できないため「省電力機能」をタップ

6



本アプリを「対象外アプリ」から外すため、チェックをタップし、「←」をタップ

7



「バックグラウンドでの使用の制限」をタップ

8



「解除」をタップ

9



「バックグラウンドでの使用の制限」が解除されます

## 第3章 セキュリティ対策状況を確認する

ご利用中のスマートフォン／タブレットのセキュリティ対策状況を確認することができます。

### ホーム画面の説明



タップして、オプションメニューを表示します

タップして、お知らせを表示します

現在のセキュリティ対策状況が表示されます

タップして、設定画面を表示します

タップして、それぞれのセキュリティ対策アプリ、サービス設定画面を表示します

タップして、セキュリティチェック、脅威の検出レポートを表示します

タップして、ニュース一覧を表示します

#### ■ ! が表示されたときの対応方法



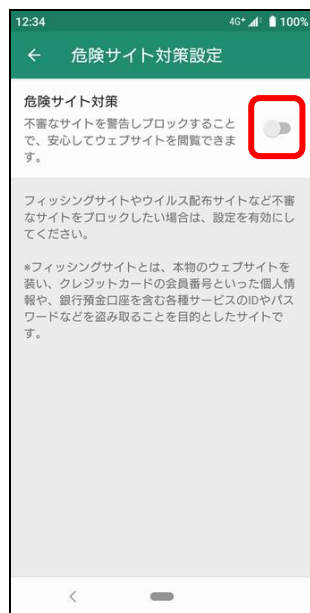
! が表示されている場合、各機能が動作していない場合があります。以下の表の通り、対応してお使いください。（※1）

ステータス	状況	対応方法
未設定	機能を有効にするための設定が完了していない	設定を完了してください
停止中	アプリの設定はすべて完了しているが、ユーザ自身が機能を停止させている	安全にご利用いただくため、機能を有効にしてください
脅威検出中	脅威を発見している	各セキュリティアプリで脅威を確認し、対処してください

## 未設定




## 停止中



「設定画面を起動する」をタップして、初期設定を行ってください

セキュリティ対策を有効にしてください

※1 迷惑メール対策は、設定を変えても  マークが反映されるまで最長 1 日かかる場合があります。

## 第4章 セキュリティチェック、脅威の検出レポートを確認する

### レポートを表示する

ご利用中のスマートフォン／タブレットのセキュリティレポートを確認することができます。

セキュリティスキャン、危険サイト対策、アプリチェック、危険 Wi-Fi 対策、迷惑電話対策、迷惑メール対策、SMSフィルタリングごとに、レポートを表示しますので、ご利用いただいている端末の状況がわかります。

※レポートの件数は当日分まで表示されます。(迷惑メール対策のみ前日)

※SMS フィルタリングは+メッセージアプリの「迷惑メッセージ」フォルダに振り分けられたメッセージ数と検出数が一致しない場合があります。

1



「レポート」をタップ

2



すべての機能の総チェック数と、検出数が表示されます

3



下にスクロールすると、機能別に詳細レポートを表示できます

## レポート画面の説明



## 詳細レポート画面

セキュリティスキャン、危険サイト対策、アプリチェック、危険 Wi-Fi 対策、迷惑電話対策、迷惑メール対策は詳細なレポートを確認できます。

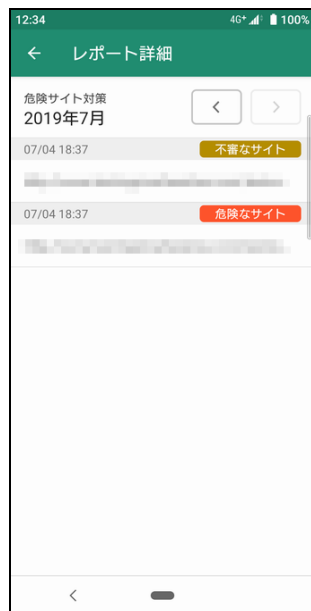
※SMS フィルタリングは詳細レポート画面がございません。

### ウイルスチェックレポート



検出されたウイルスや、不審なプログラムが表示されます

### 危険サイトブロックレポート



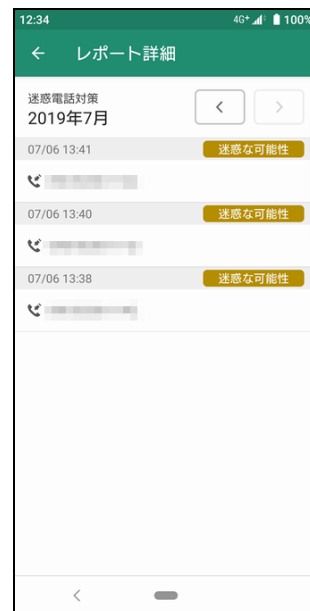
不審なサイトや、危険なサイトと判定されたサイトの一覧が表示されます

### 危険 Wi-Fi 検知レポート



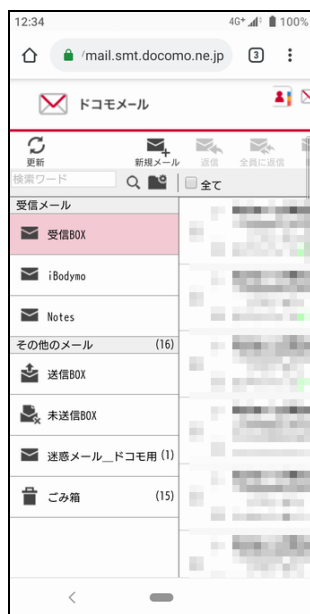
危険な Wi-Fi と判定された Wi-Fi スポット一覧が表示されます

### 迷惑電話警告レポート



迷惑電話や危険電話と判定された一覧が表示されます

### 迷惑メールレポート



迷惑メールレポートの場合、ドコモメール (Web 版)が表示されます

## 第5章 セキュリティに関するニュースを見る

セキュリティに関するニュースを定期的に配信しますので、最新のセキュリティ動向を把握し、安全にスマートフォンをご利用ください。

### ニュースを表示する

1



「ニュース」をタップ

2



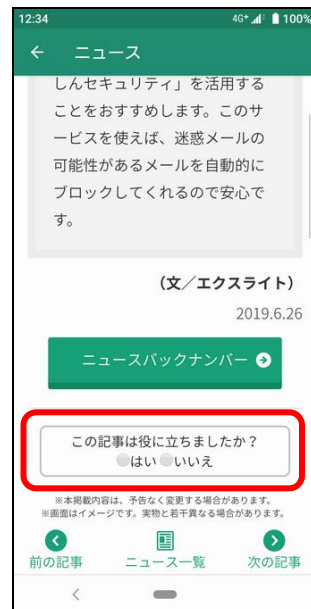
読みたいニュース記事をタップ

3



下にスクロールすることができ、ニュース  
気が表示されます

4

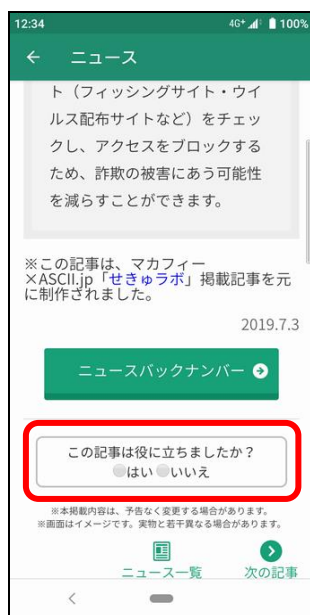


「ニュース一覧」「前の記事」「次の記事」  
をタップすると他の記事へ遷移します

### ニュースを評価する

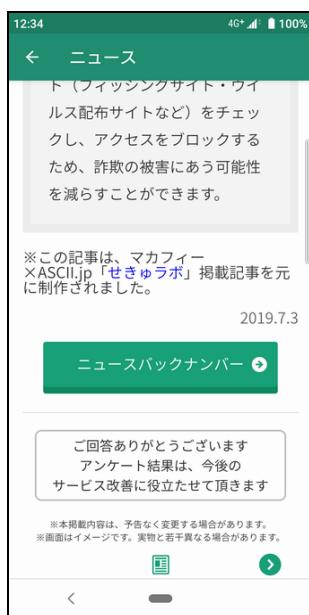
ニュース記事がお客さまに役立ったかアンケートにご協力ください。  
今後のニュース配信に活用させていただきます。

1



「はい」または「いいえ」をタップ

2



アンケートを受け付けました

## 第6章 セキュリティスキャン機能を確認する

### セキュリティスキャン機能とは

ファイルやアプリをスキャンする事で、ウイルスなどの不審なアプリ（ファイル）から端末を保護します。

### セキュリティスキャンの種類・対象

セキュリティスキャンには3種類のスキャン機能があります。

- ・**リアルタイムスキャン** …… 端末起動時・SD カードの挿入時・アプリのインストール時を指定し、リアルタイムにスキャンします。
- ・**スケジュールスキャン** …… 任意の設定（アプリスキャン・フルスキャン）において、指定した時刻にスキャンします。
- ・**手動スキャン** …… 任意の設定（アプリスキャン・フルスキャン）において、直ぐにスキャンします。

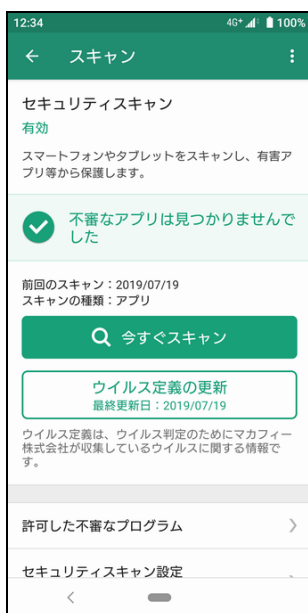
セキュリティスキャンでは以下の対象からウイルスを検出します。

- ・**一般のファイル** …… txt、.doc、.so などですが、拡張子依存はありません
- ・**圧縮ファイル** …… zip、gzip、bzip2、cab、sis、MIME、tar、Unix ELF、MMS、PE (Microsoft Portable Executable)、E32 (Symbian EPOC32)、MSO (MicroSoft Office binary format)
- ・**メディアファイル** …… ビデオ、オーディオ、画像など
- ・**パッケージ** …… インストールアプリ

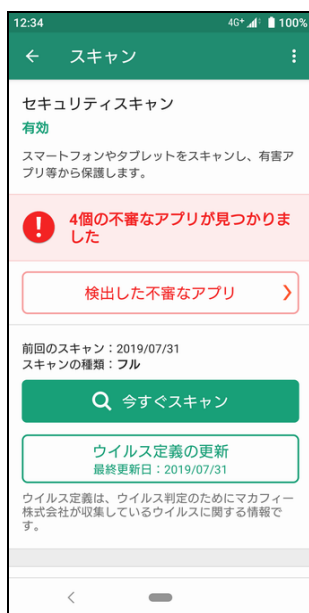
### セキュリティスキャン画面を確認する

セキュリティスキャン画面を確認することができます。

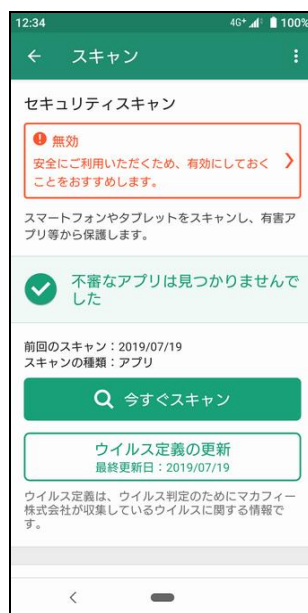
#### 1 ※通常時



#### 2 ※脅威発見時



#### 3 ※設定無効時

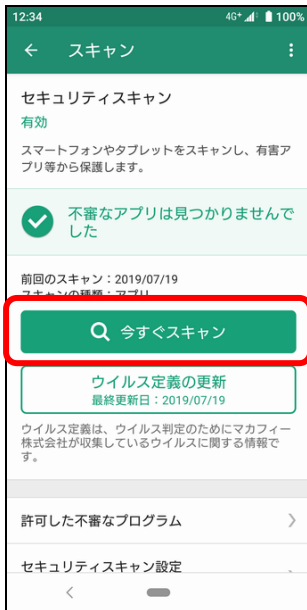




# 今すぐスキャン

今すぐスキャンをタップすると直ちにセキュリティスキャンが実行されます。

1



今すぐスキャンタップ

2



今すぐスキャン中

3



今すぐスキャン完了

4



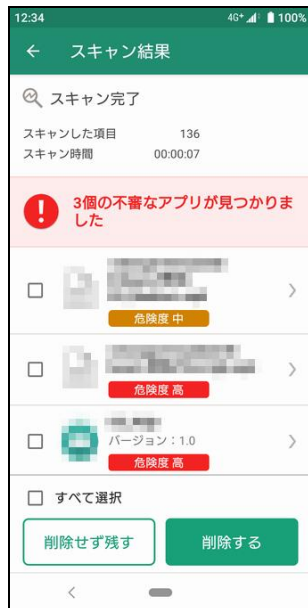
今すぐスキャン中止

5



今すぐスキャン表示隠し

6



今すぐスキャン脅威検出

## ウイルス定義の更新

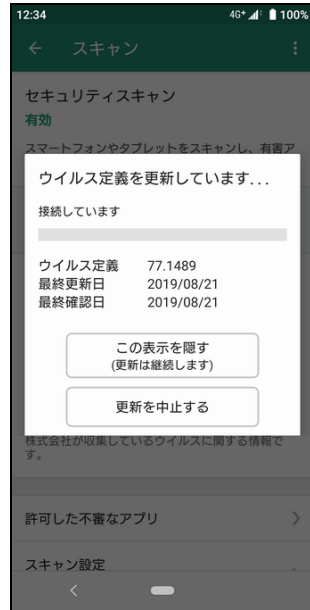
ウイルス定義の更新をタップするとウイルスの定義ファイルを最新にすることができます。

1



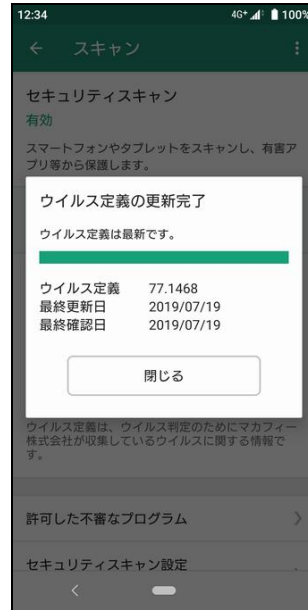
ウイルス定義更新トップ

2



ウイルス定義更新中

3



ウイルス定義更新完了

4



ウイルス定義更新失敗

## セキュリティスキャンの設定を確認する



リアルタイムスキャンの設定を行います(初期値：有効)

定期スキャンの設定を行います(初期値：有効)

定期ウイルス定義の更新を行います(初期値：有効)

スキャンの種類を設定します(初期値：フルスキャン)

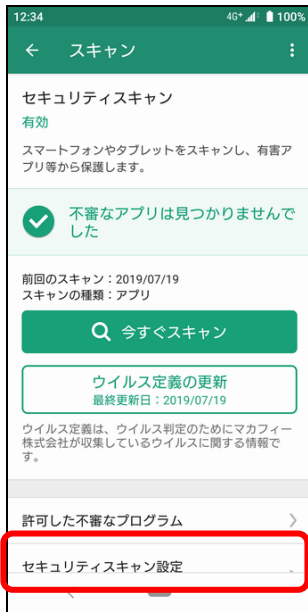
不審なアプリスキャンの有無を設定します(初期値：ON)

不審なアプリを検出した際に通知の有無を設定します(初期値：ON)

## リアルタイムスキャン

リアルタイムスキャンの設定ができます。

1



「セキュリティスキャン設定」をタップ

2



「リアルタイムスキャン」をタップ

3

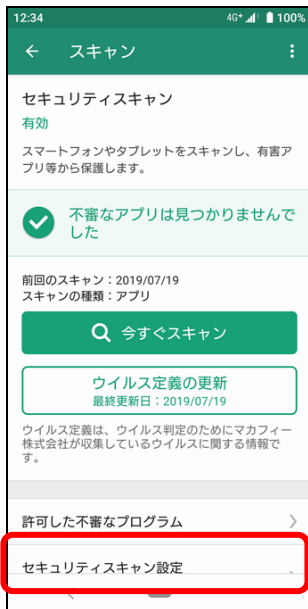


リアルタイムスキャンの有効/無効や、スキャンの対象・タイミングなどを設定できます

## 定期スキャン

定期スキャンの設定ができます。

1



「セキュリティスキャン設定」をタップ

2



「定期スキャン」をタップ

3



定期スキャンの有効/無効や、実行スケジュールなどを設定できます

4



間隔を毎日/毎週のどちらかで設定できます。  
※毎週に設定した場合、さらに曜日を設定できます。

5



実行する曜日を設定できます。

6

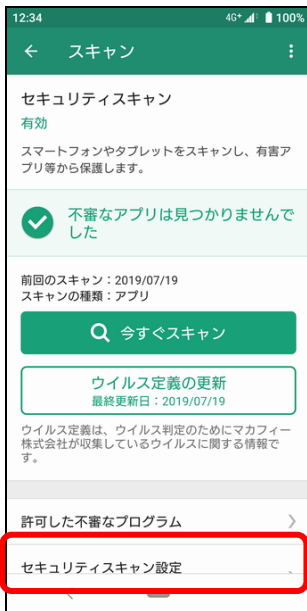


実行する時間を設定できます。

## 定期ウイルス定義更新

定期ウイルス定義更新の設定ができます。

1



「セキュリティスキャン設定」をタップ

2



「定期ウイルス定義更新」をタップ

3



定期ウイルス定義更新の有効/無効や、実行スケジュールなどを設定できます

4



間隔を毎日/毎週のどちらかで設定できます。  
※毎週に設定した場合、さらに曜日を設定できます。

5



実行する曜日を設定できます。

6

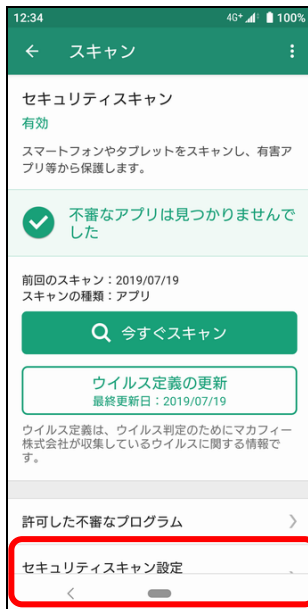


実行する時間を設定できます。

## スキャンの種類

スキャンの種類の設定ができます。

1



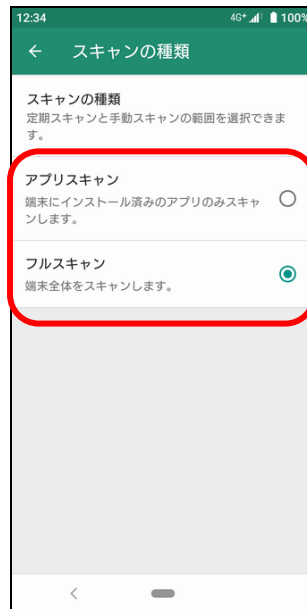
「セキュリティスキャン設定」をタップ

2



「スキャンの種類」をタップ

3

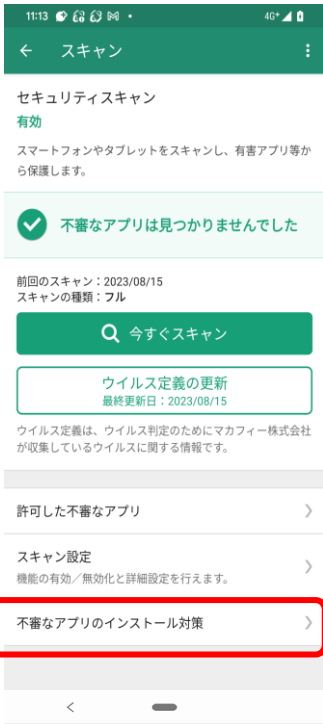


スキャンする範囲を選択します

# 不審なアプリのインストール対策

知らない間に不審なアプリをインストールすることを防ぐための設定です。

1



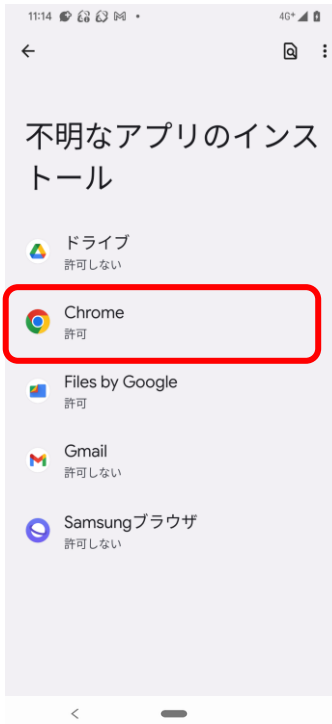
「不審なアプリのインストール対策」をタップ

2



「設定を確認」をタップ

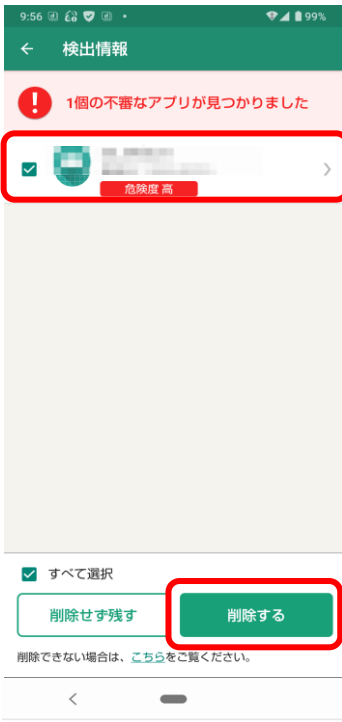
3



Chrome などのブラウザからの不明なアプリのインストールを「許可しない」に設定します。

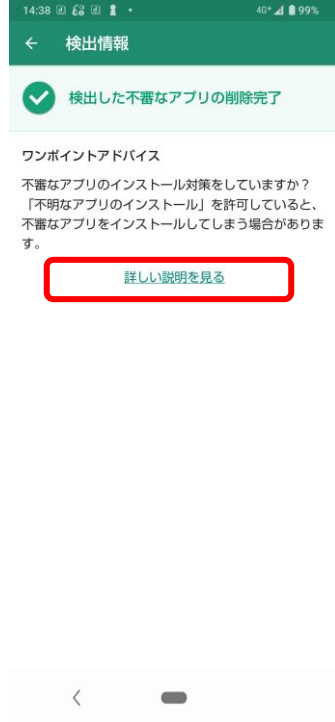
※また、不審なアプリ検出時には不審なアプリの削除完了後に、不審なアプリのインストール対策状況を確認できます。

1



「削除する」をタップし不審なアプリを削除する

2



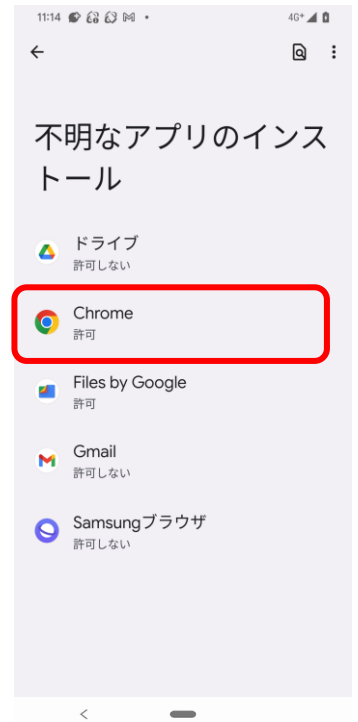
「詳しい説明を見る」をタップ

3



「設定を確認」をタップ

4



Chrome などのブラウザからの不明なアプリのインストールを「許可しない」に設定します。

# セキュリティスキャンで脅威を検出したら？

## 脅威検出時の対応

セキュリティスキャンで脅威が発見されるとホーム画面のスキャンのアイコンが変化します。タップし、詳細を確認し対処してください。

1



「スキャン」をタップ

2



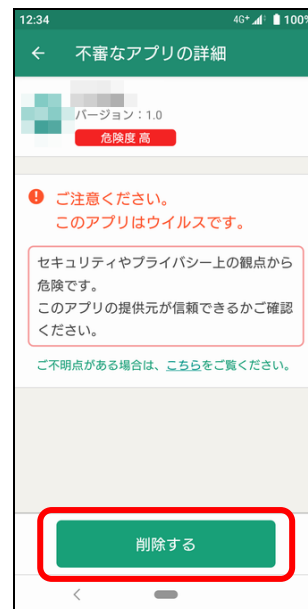
「検出した不審なアプリ」をタップ

3



対処を行うアプリをタップ

4



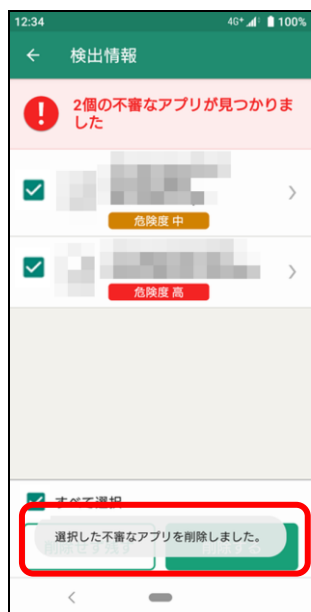
「削除する」をタップ

5



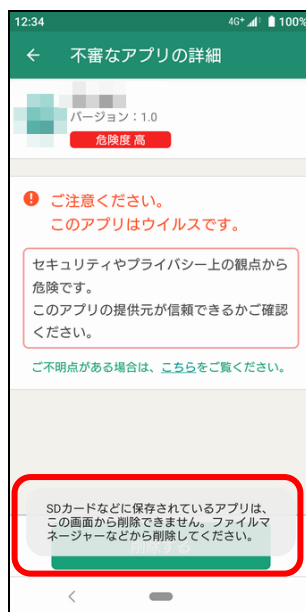
「OK」をタップ

6



該当アプリが削除されます。

7



5で「キャンセル」をタップした場合は上記の様な警告が表示されます

8 ※複数まとめて削除する場合



脅威アプリ一覧で複数選択し、削除することも可能です。  
※0A.00.10000以降のアプリでは最初からすべてにチェックが入っております

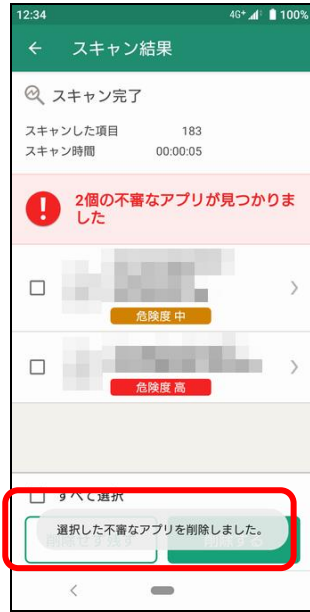


9



「OK」をタップ  
 ※OSの制御上、選択したアプリの回数  
 上記画面が表示されます。

10



該当アプリが削除されます。

11 ※リアルタイムスキャン検出時



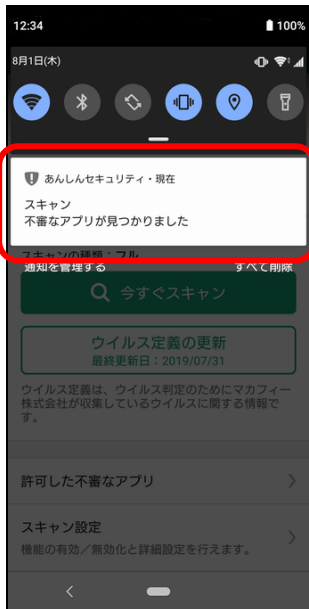
リアルタイムスキャンでの脅威検出時は  
 ポップアップで警告が表示されますので、  
 直接この画面から削除できます。

※SD カードなどに保持されているアプリはこの画面から削除できません。  
 ファイルマネージャーなどから削除してください。

## 脅威検出時の確認方法

脅威が検出された場合は以下の方法で確認ができます。確認後の対処については「脅威検出時の対応」をご参照ください。

1



通知をタップ

2



脅威アプリ一覧が表示されます。

3 ※リアルタイムスキャン検出時



リアルタイムスキャンでの脅威検出時は  
 ポップアップで警告が表示されますので、  
 直接この画面から削除できます。

4



不審なアプリの削除完了後、「詳しい説明を見る」をタップすることで、不審なアプリのインストール対策状況を確認できます。

## 脅威を許可リストに追加する対応方法

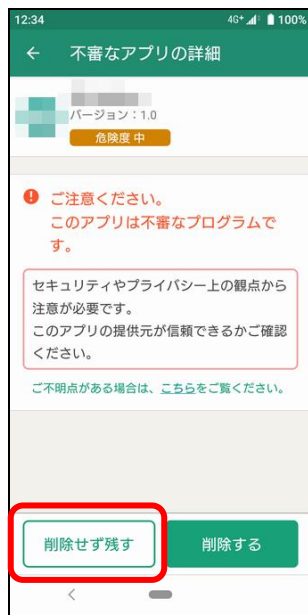
脅威検知されたアプリを許可リストに追加し脅威として検知しないようにするには以下の対応を行います。

1



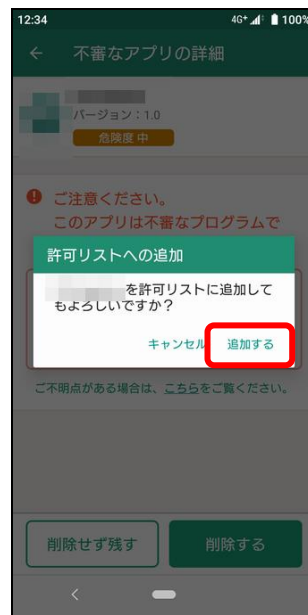
許可リストに追加したいアプリをタップ

2



「削除せず残す」をタップ

3



「追加する」をタップ

4



許可リストに追加されます。

5 ※複数まとめて追加する場合



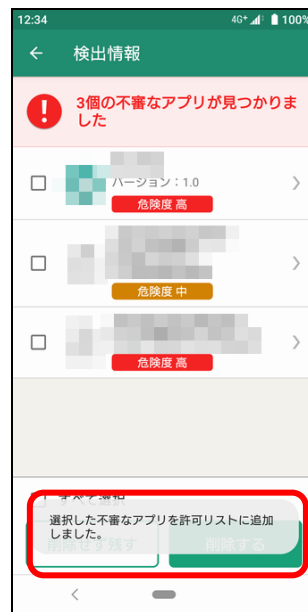
脅威アプリ一覧で複数選択し、追加することも可能です。  
※0A.00.10000 以降のアプリでは最初からすべてにチェックが入っております

6



「追加する」をタップ

7



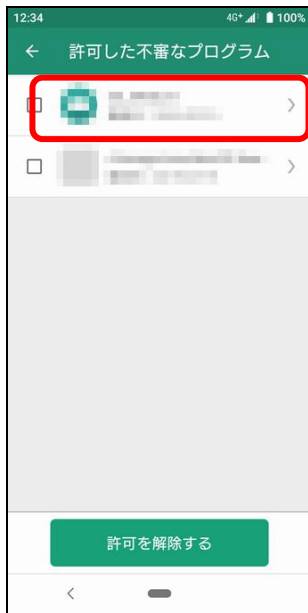
許可リストに追加されます。

8



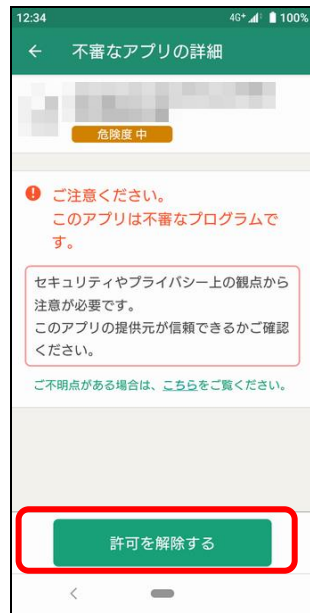
許可リストに追加したものを確認する場合はスキャントップより「許可した不審なアプリ」をタップ

9



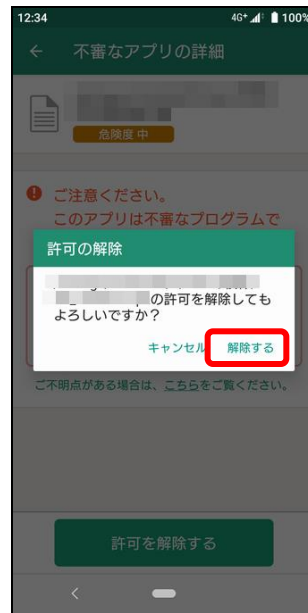
許可したアプリの一覧が表示されます。  
許可リストより削除したい場合は該当の  
アプリをタップ

10



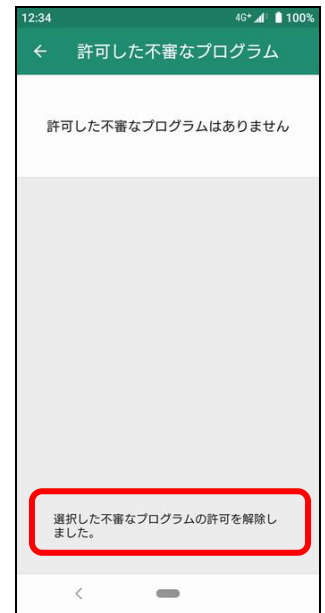
「許可を解除する」をタップ

11



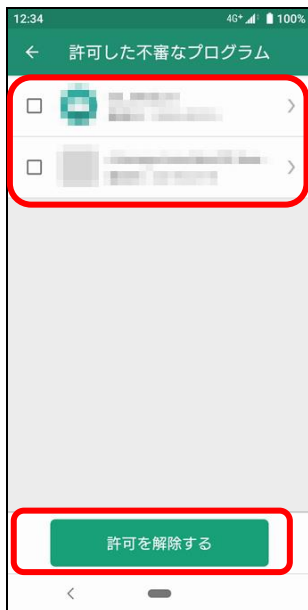
「解除する」をタップ

12



許可リストより削除されます。  
※解除した直後は不審なプログラムとして  
検知されません。「今すぐスキャン」にて  
手動にてスキャンいただくか、「定期スキャン」にて再度チェックいただいた際に不  
審なプログラムとして検知されます。

13 ※複数まとめて解除する  
場合



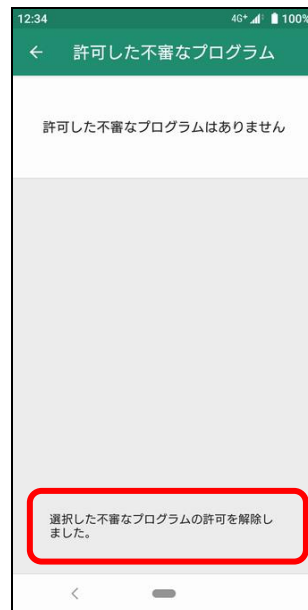
複数アプリをまとめて解除したい場合は  
該当のアプリを選択し「許可を解除す  
る」をタップ

14



「解除する」をタップ

15



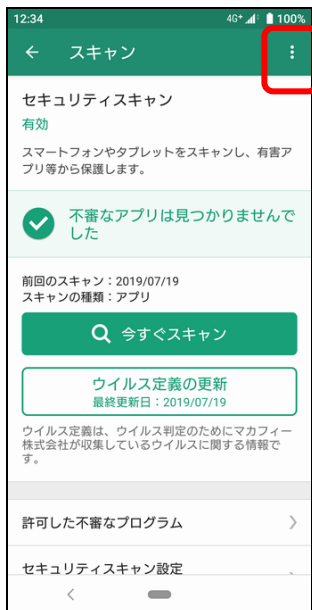
許可リストより削除されます。  
※解除した直後は不審なプログラムとして  
検知されません。「今すぐスキャン」にて  
手動にてスキャンいただくか、「定期スキャン」にて再度チェックいただいた際に不  
審なプログラムとして検知されます。

16

## ログの確認

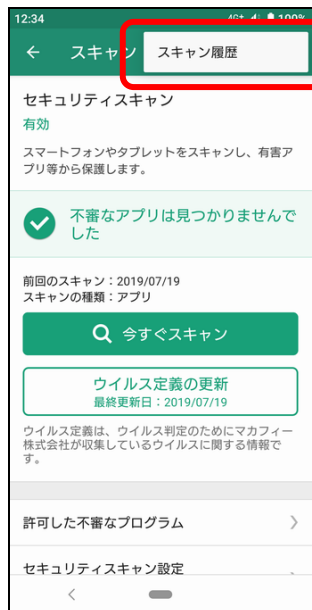
セキュリティスキャンの稼働状況をご確認いただけます。

1



右上のメニューボタンをタップ

2



「スキャン履歴」をタップ

3



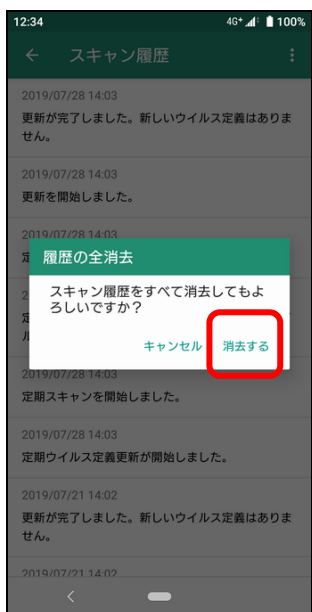
右上のメニューボタンをタップ

4



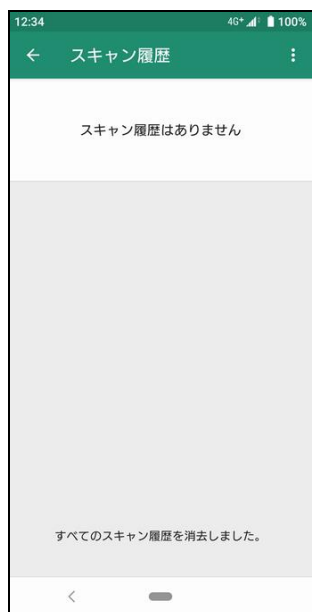
「履歴の全消去」をタップ

5



「消去する」をタップ

6



スキャン履歴が削除されます

## 第7章 危険サイト対策を確認する

### 危険サイト対策とは

端末搭載のブラウザや SNS アプリで問題あるサイトにアクセスする際にフィッシングサイトやウイルス配信サイトかどうかをチェックし、該当した場合に警告画面を表示し、ブロックします。

対応しているブラウザは以下となります。

- ・Chrome
- ・Samsung 社端末に標準搭載されたブラウザ
- ・あんしんフィルター for docomo (青少年向け)

※その他のブラウザでも動作する場合がありますが、動作保証外となります。

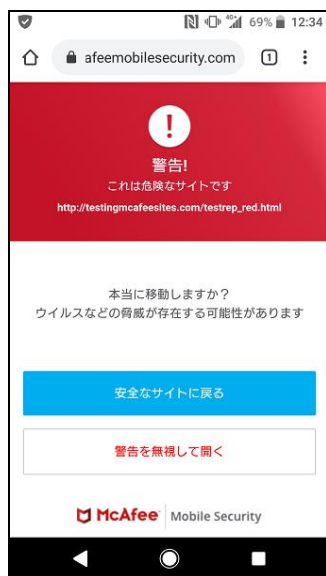
対応している SNS は以下となります。

- ・Facebook
- ・Instagram (対象 OS : 13 以上)
- ・LINE
- ・Messenger
- ・X (Twitter)

### 危険サイト対策画面を確認する

端末掲載のブラウザの場合はブラウザアプリ内に表示します。

#### 1 ※危険なサイトにアクセス



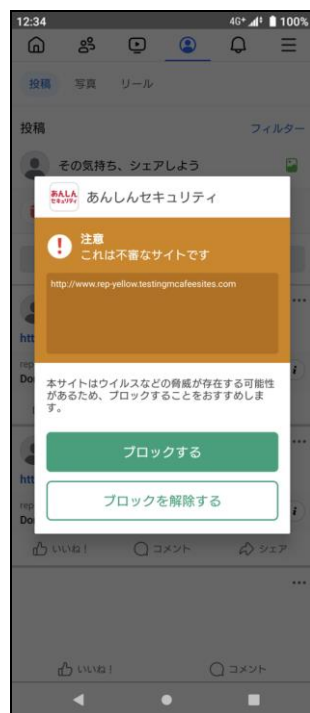
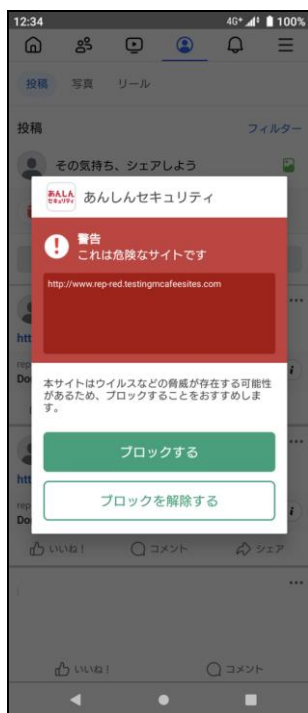
#### 2 ※不審なサイトにアクセス



SNS アプリの場合はポップアップで表示します。  
※X（Twitter）ではブラウザアプリ内に表示します。

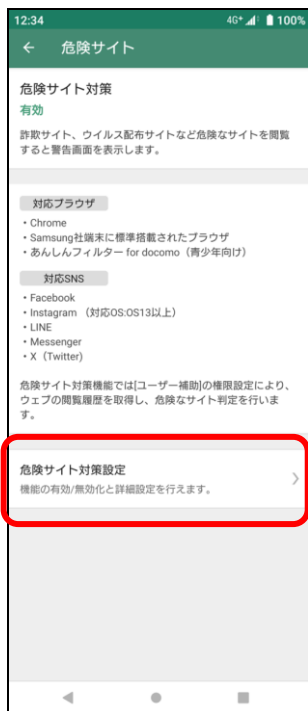
**1** ※危険なサイトにアクセス

**2** ※不審なサイトにアクセス



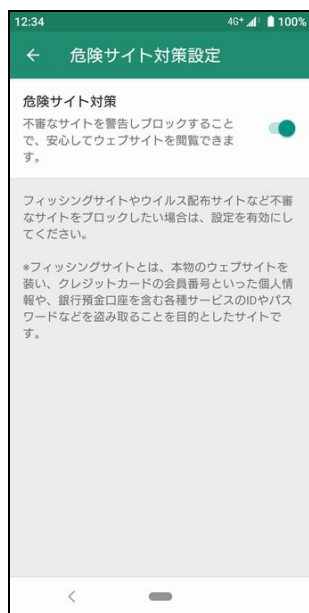
## 危険サイト対策の設定を確認する

1



「危険サイト対策設定」をタップ

2



危険サイト対策設定が表示されます

## 危険サイト対策で脅威を検出したら？

ご利用中のスマートフォン／タブレットがセキュリティの脅威を発見した場合、あんしんセキュリティのホーム画面で確認することができます。

### ■ ブラウザでの危険サイトアクセス時



タップして、直前に開いた安全なサイトに戻ります

タップして、警告されたサイトを開きます  
※安全なサイトであることを確認のうえ、開いてください。

■ SNS アプリでの危険サイトアクセス時



警告されたサイトをブロックします

警告されたサイトのブロックを解除します  
※安全なサイトであることを確認のうえ、開いてください。



## 第8章 アプリチェックを確認する

### アプリチェックとは

インストール済アプリを対象に、個人データに関与し、外部送信の可能性のあるアプリをチェックし、McAfee LLC の評価結果をもとに、確認することができます。

※アプリチェックは、お客様の個人データを取得する機能が搭載されているアプリをお知らせすることで、お客様の当該アプリの利用に関する注意喚起を促すものです。ウイルスを検出・駆除等を行ったり、お客様の個人データの送信を停止したりする機能ではありません。

アプリの提供元が信頼できるかどうかを確認し、チェック結果を参考に、不審と思われるアプリはアンインストールすることをおすすめします。

※McAfee LLC での評価済みアプリのみ表示されます。

### アプリチェック画面を確認する



タップして、今すぐインストールアプリのチェックを行います。

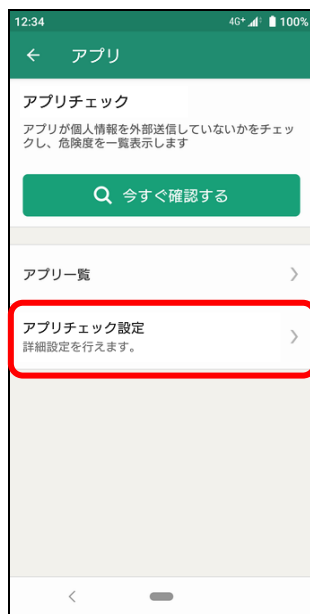
タップして、アプリ一覧ページを表示します。

タップして、設定画面を表示します。

## アプリチェックの設定を確認する

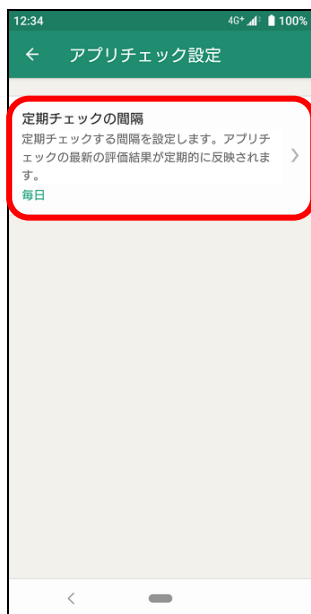
アプリチェックを確認することができます。

1



「アプリチェック設定」をタップ

2



「定期チェックの間隔」をタップ

3

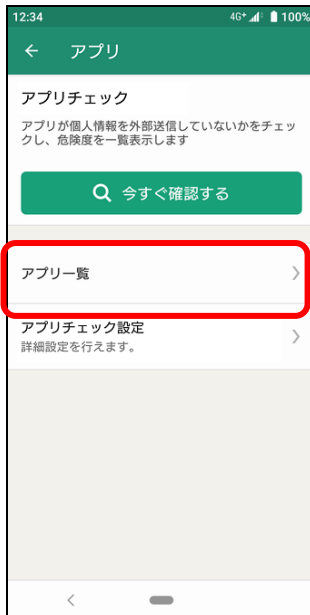


チェックする間隔の設定を変更できます。

## アプリチェックでアプリ一覧を確認する

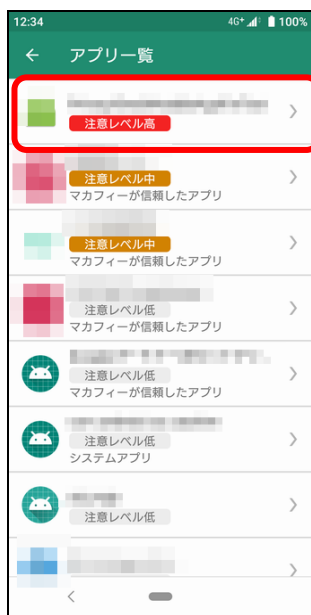
アプリ一覧より、インストールされているアプリの危険度などを確認することができます。

1



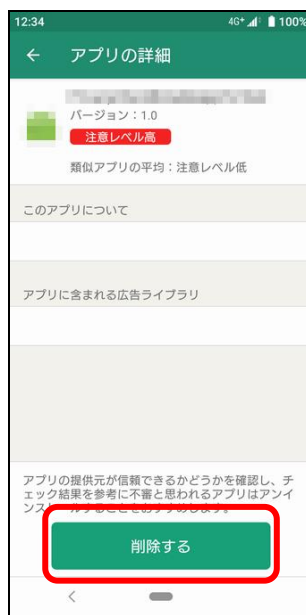
「アプリ一覧」をタップ

2



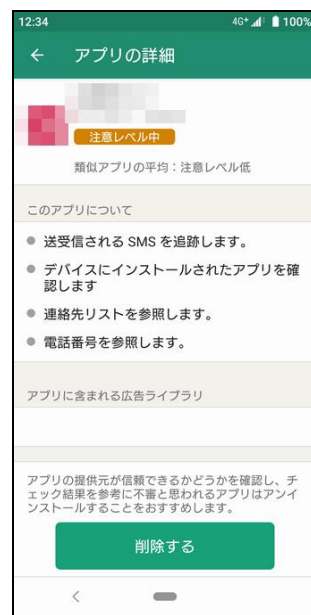
端末にインストールされているアプリの一覧が表示されます。アプリをタップすると該当アプリの詳細が確認できます。

3



中身を確認いただき、不要なものであれば、「削除する」をタップし、削除を実施してください。

4



## 5 ※注意レベル低



## 6 ※注意レベルなし

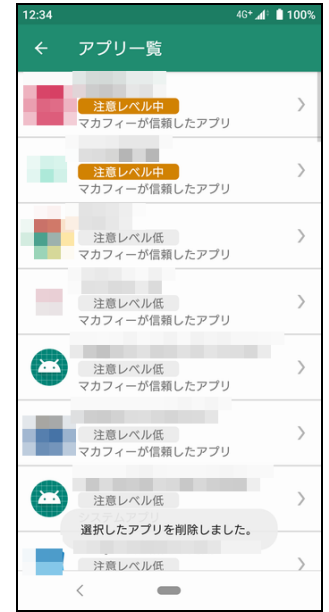


## 7



「OK」をタップ

## 8



該当のアプリが削除されます

## 第9章 危険 Wi-Fi 対策を確認する

### 危険 Wi-Fi 対策とは

危険 Wi-Fi 対策は Wi-Fi に接続した際に、通信を監視される可能性のある Wi-Fi がチェックする機能です。危険な Wi-Fi に接続した場合に警告画面を表示します。

### 危険 Wi-Fi 対策画面を確認する

#### 1 ※Wi-Fi 未接続時



#### 2 ※安全な Wi-Fi 接続時



#### 3 ※信頼した Wi-Fi 接続時



#### 4 ※危険な Wi-Fi 接続時



### 危険 Wi-Fi 対策の設定を確認する

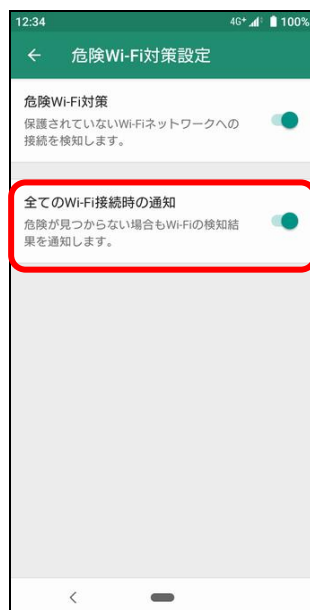
危険 Wi-Fi 対策の設定を確認・変更することができます。

#### 1



「危険 Wi-Fi 対策設定」をタップ

#### 2



「全ての Wi-Fi 接続時の通知」を ON に設定することで、安全な Wi-Fi 接続時にも通知をさせることができます。

#### 3



ON にすると安全な Wi-Fi 接続時に上記の様な通知がされます。

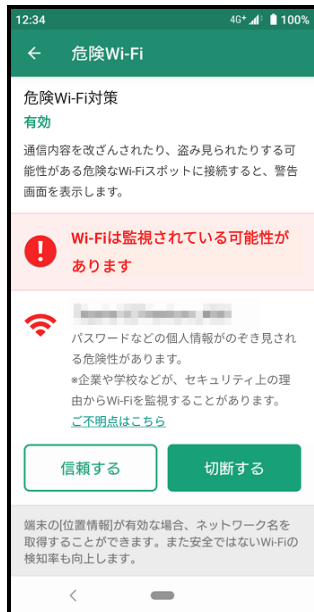
## 危険 Wi-Fi 対策で脅威を検出したら？

ご利用中の端末で危険な Wi-Fi を検知した場合、ポップアップ表示によりお知らせをいたします。尚、「あんしんセキュリティ」アプリを起動し、「危険 Wi-Fi」をタップいただくことで、同様な内容を確認することができます。

### 1 ※ポップアップ表示



### 2 ※アプリ内表示



### 3 ※通知画面



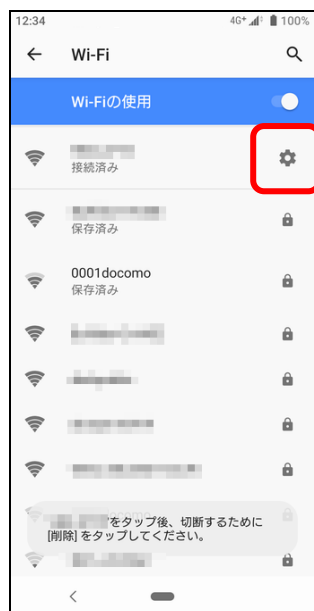
## ■ Wi-Fi の切断を行う場合

### 1



「切断する」をタップ

### 2



現在接続している危険な Wi-Fi の設定をタップ



「削除」をタップ

※ Wi-Fi の切断方法については、機種及び OS バージョンにより異なりますので、詳細はご利用機種の説明をご確認ください。

## ■ Wi-Fi を信頼する場合

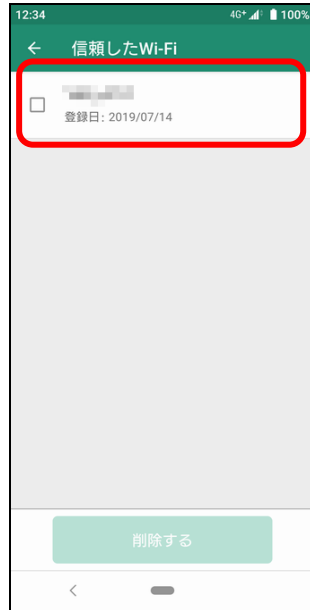
※信頼するときは、安全な Wi-Fi であることを確認のうえ、実施してください。

1



「履歴の全消去」をタップ

2



信頼した Wi-Fi 一覧に追加されます

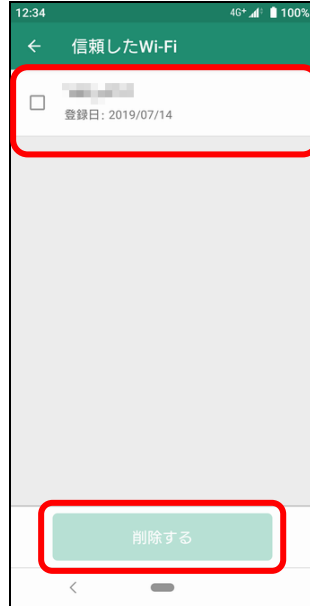
## ■ 信頼した Wi-Fi を確認・削除する場合

1

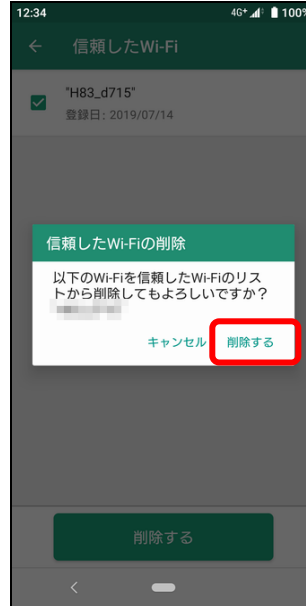


「危険 Wi-Fi 対策設定」をタップ

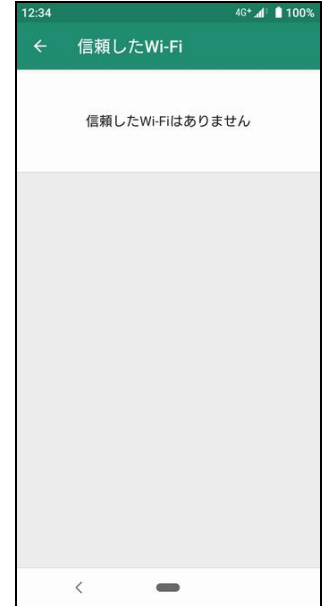
2



信頼した Wi-Fi 一覧が表示されます  
信頼した Wi-Fi のリストから削除するには Wi-Fi を選択し、「削除する」をタップ



「削除する」をタップ



信頼した Wi-Fi リストより削除されます

## 位置情報の使用が OFF の場合

Android8.1 以降の端末をお使いの方は「位置情報」が有効でない場合、接続先のネットワーク名称が取得できず、「信頼する」のボタンが無効となります。ネットワーク名称の確認および、ボタンの有効化のために「位置情報」を有効にしてください。

### 1 ※危険な Wi-Fi に接続中



### 2 ※安全な Wi-Fi に接続中



「信頼する」ボタンが無効となります

## 第10章 迷惑電話対策を確認する

### 迷惑電話対策とは

迷惑電話対策機能は電話番号をチェックし、必要に応じて発着信中の警告をする機能です。

本機能を有効にすることで、通話を介して金銭をだまし取ろうとするなどの危険な行為や執拗に勧誘をするなどの迷惑な行為から守ります。

端末の電話帳に登録されていない公共施設や企業、飲食店などの電話番号の発着信に対して、ハローページ等の情報を用いて発信元の名称を表示するので、より安心して通話ができるようになります。

※ハローページはN T Tの登録商標です。ハローページ掲載の個人名義情報については表示対象外となります。

### 発着信時に表示される画面を確認する

#### 1 ※着信時



着信先情報のバナーが表示されます。

#### 2 ※発信時

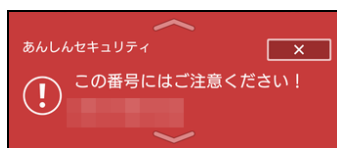


発信先情報のバナーが表示されます。

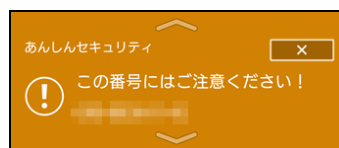


迷惑電話対策が有効な場合、発着信時の表示画面には以下の種類がございます。

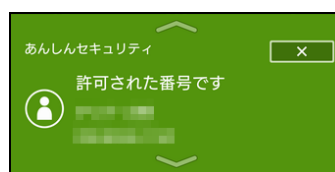
危険な可能性の高い番号



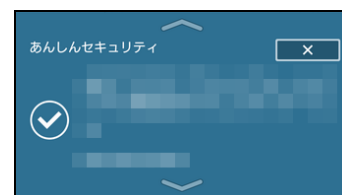
迷惑な可能性の高い番号



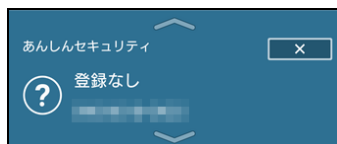
電話帳登録済みの番号からの着信



左記に該当せず、電話番号データベースに登録されている番号



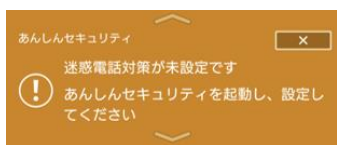
いずれにも該当しない番号



迷惑電話対策が無効な場合、発着信時の表示画面には以下の種類がございます。

迷惑電話対策未設定

※Android 12.0 以降



## 迷惑電話対策の主な機能

迷惑電話対策の主な機能としては以下のものがあります。

### ■ 発着信時の警告

番号のチェック結果に応じて「警告」をします。

### ■ 着信時の発信元表示

飲食店や企業などの電話番号からの着信の発信元を表示します。

### ■ 発信時の発信先表示

発信時に飲食店や企業などの電話番号の発信先を表示します。

### ■ 履歴

危険な可能性が高い発着信と迷惑の可能性が高い発着信などの履歴を見ることができます。

## 迷惑電話対策画面を確認する

### ■ メイン画面



迷惑電話判別や発信元情報の検索を行います。

タップして、設定画面を表示します。

発信履歴表示の絞り込みを行います。

発信履歴の消去を行います。

電話の掛けなおしを行います。

## 迷惑電話対策の設定を確認する

### 「許可された番号をお知らせ」するには？

電話帳に登録された番号から発信時に許可された番号として通知します。

1



「迷惑電話対策設定」をタップ

2



「許可された番号の通知」を設定する

3



発信時に「許可された番号です」と通知されるようになります。

## フィードバック情報の送信

通知の精度の更なる向上が可能になるため、ご協力をお願いします。

尚、お客様個人を特定できる形式では送信されません。

1



「迷惑電話対策設定」をタップ

2



「フィードバック情報の送信」を ON に設定する

## 迷惑電話のデータベースの更新

通常迷惑電話のデータベースは自動にて更新されます。手動で更新を実施したい場合は以下となります。

**1**

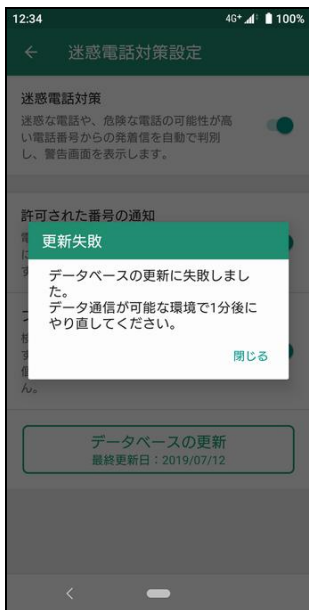
「迷惑電話対策設定」をタップ

**2**

「データベースの更新」をタップ

**3**「データベースの更新中」に切り替わりま  
す**4**

データベースが更新されます

**5 ※更新失敗時**

通信の関係などでデータベースの更新が失敗した場合、通信が可能な場所で再度お試しください。

**迷惑電話で危険・迷惑な電話を検出した場合の対処方法****発着信時の操作について**

迷惑電話対策が有効な場合、発着信時に以下のような画面が表示されます。

**■ 着信時**



タップして、電話に出ずに切ります

タップして、電話に出ます

タップして、表示を閉じます

タップしながら上下に移動することで、表示する箇所を移動することができます。

## ■ 発信時



タップして、設定画面を表示します

タップして、表示を閉じます

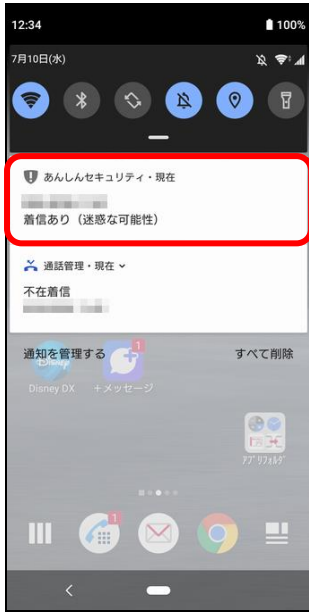
タップしながら上下に移動することで、表示する箇所を移動することができます。

タップして、電話を切ります。

## 不在着信の通知について

危険な電話と迷惑な電話に関しては、受信者が電話に出なかった場合、通知に「着信あり(危険な可能性/迷惑な可能性)」と表示されます。

1



通知に「着信あり(危険な可能性/迷惑な可能性)」と表示

2



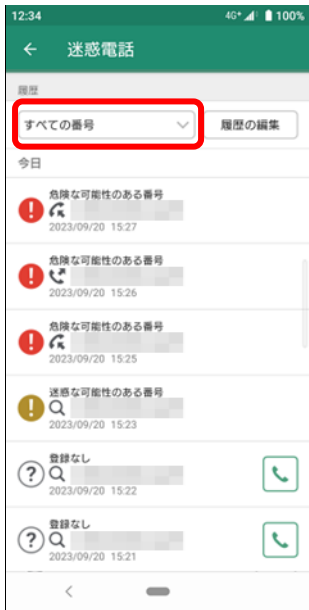
履歴を表示

## 履歴の操作

発着信の履歴は絞り込みや、履歴の削除をすることができます。

### ■ 発着信履歴の絞り込みを行う場合

1



通知に「着信あり(危険な可能性/迷惑な可能性)」と表示

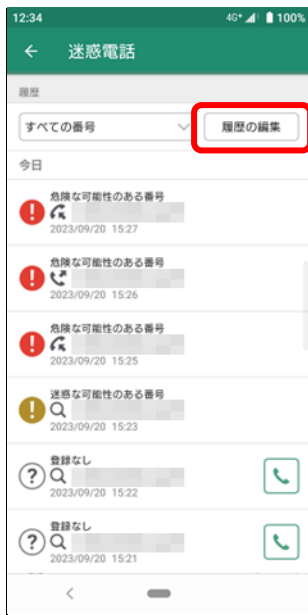
2



履歴を表示

### ■ 発着信履歴の削除を行う場合

1



「履歴の編集」をタップ

2



削除したい番号を選択し、「消去する」をタップ

3



「消去する」をタップ

4



履歴が削除されます

## 迷惑電話番号を検索する

メールやメッセージに含まれる電話番号がしつこいセールスなどの迷惑な番号や、詐欺などの危険な番号でないかを調べることができます。

### ■ 検索方法

1



調べたい電話番号を入力して 🔍 をタップ

2



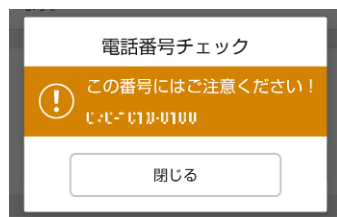
「閉じる」をタップ  
※危険な電話の場合、「この番号にはご注意ください!」と表示されます。

### ■ 検索結果

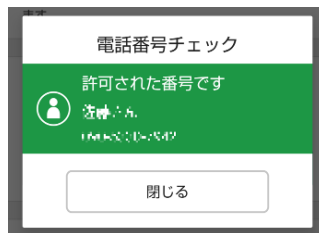
危険な可能性の高い番号



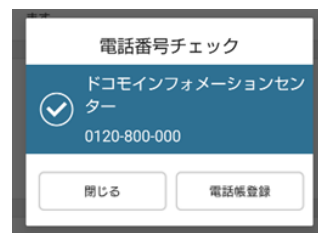
迷惑な可能性の高い番号



電話帳登録済みの番号(※)



左記に該当せず、電話番号データベースに登録されている番号



いずれにも該当しない番号



※ご利用端末の電話帳およびドコモ電話帳に登録済みの番号



# 第11章 迷惑メール対策を確認する

## 迷惑メール対策設定とは

迷惑メールと判定したメールを自動で振り分け、専用の迷惑メールフォルダに保存します。

※ドコモメールがご利用いただけない場合、迷惑メール対策はご利用できません。

## 迷惑メール対策設定画面を確認する

迷惑メール対策の設定を行い、安全にメールを利用しましょう。

詳細な迷惑メールおまかせブロックの設定方法は、NTT ドコモのコーポレートサイトをご確認ください。

[https://www.nttdocomo.co.jp/service/omakase\\_block/setting/index.html](https://www.nttdocomo.co.jp/service/omakase_block/setting/index.html)

### ■ 迷惑メールおまかせブロックが停止中の場合

1



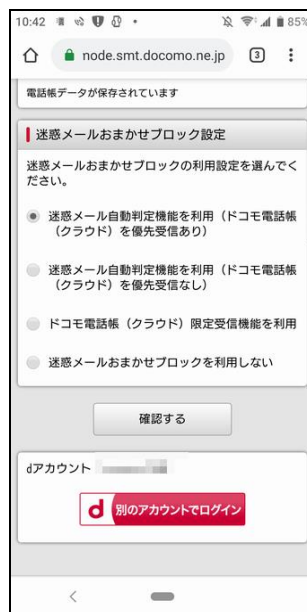
「迷惑メール」をタップ

2



「迷惑メールおまかせブロック設定」をタップ

3



迷惑メールおまかせブロックの設定を行ってください

## ■ 迷惑メールおまかせブロックが動作の場合

1



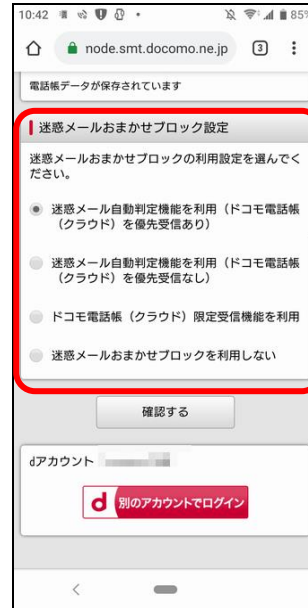
「迷惑メール」をタップ

2



「迷惑メールおまかせブロック設定」をタップ

3



迷惑メールおまかせブロック設定が確認  
できます

## 第12章 SMS フィルタリングを確認する

### SMS フィルタリング機能とは

メッセージアプリに送られてくるなりすましやフィッシング詐欺など、不審と判定されたメッセージ※ 1 を自動で専用フォルダに振り分けるサービスです。安心・安全にメッセージをご利用になれます。

※1 メッセージとは、Android は +メッセージアプリで受信した SMS および +メッセージ。

### SMS フィルタリング機能の設定について

SMS フィルタリングの設定を行い、安全に +メッセージアプリを利用しましょう。

SMS フィルタリングが有効であることを確認します。

詳細な +メッセージアプリの設定方法は、NTT ドコモのコーポレートサイトをご確認ください。

[https://www.docomo.ne.jp/service/plus\\_message/](https://www.docomo.ne.jp/service/plus_message/)

### SMS フィルタリングの有効／無効を確認

SMS フィルタリング機能には、有効と無効があります。

#### 有効画面例



SMS フィルタリング機能が有効の画面

#### 無効画面例



SMS フィルタリング機能が無効の画面

### SMS フィルタリングが無効の場合

SMS フィルタリングが無効画面は、以下の 3 パターンがあります。

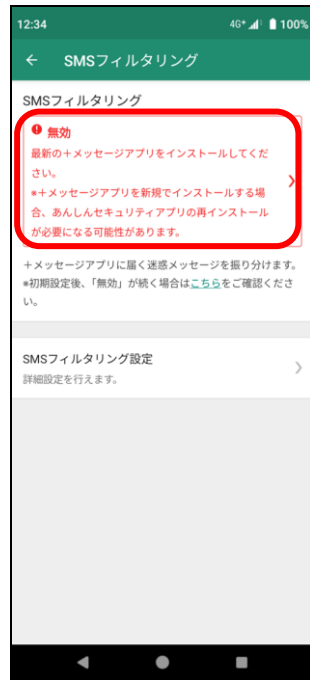
- +メッセージアプリが未インストールもしくは古いバージョンの場合

1



「迷惑 SMS」をタップ

2



「最新の+メッセージアプリをインストールして下さい」と表示、そこをタップ

3



最新の+メッセージアプリのインストール画面にてインストール

■ +メッセージアプリの初期設定が完了していない場合

1



「迷惑 SMS」をタップ

2



「機能を有効にするために、+メッセージアプリの初期設定を行って下さい」と表示、そこをタップ

3



+メッセージアプリの初期設定を行う  
※ 詳細は+メッセージアプリのコーポレートサイト参照

■ +メッセージアプリのSMSフィルタリングが無効になっている場合

1



「迷惑 SMS」をタップ

2



「SMS フィルタリング設定を有効にしてください」と表示、そこをタップ  
※ SMS フィルタリング設定方法 [へ](#)

## SMS フィルタリングが有効の場合

SMS フィルタリングの有効画面は、以下の 2 パターンがあります。

+メッセージアプリがデフォルト（標準）のメッセージアプリに設定されていない場合、基本的には迷惑メッセージフォルダへ自動振り分けは行われません。

■ +メッセージアプリがデフォルト（標準）の SMS になっている場合

1



「迷惑 SMS」をタップ

2



この有効画面の場合、迷惑メッセージを別フォルダに振り分けます

■ +メッセージアプリがデフォルト（標準）のSMSになっていない場合

基本的には、+メッセージアプリに届く迷惑なメッセージは振り分けられません。通知でお知らせします。

1



「迷惑SMS」をタップ

2



基本的には、+メッセージアプリに届く迷惑なメッセージは振り分けられません。通知でお知らせします。

## SMS フィルタリング設定方法

SMS フィルタリングの設定方法です。

■ 無効に設定する場合

1



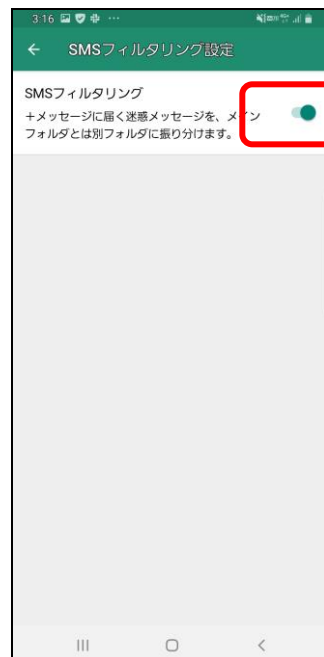
「迷惑SMS」をタップ

2



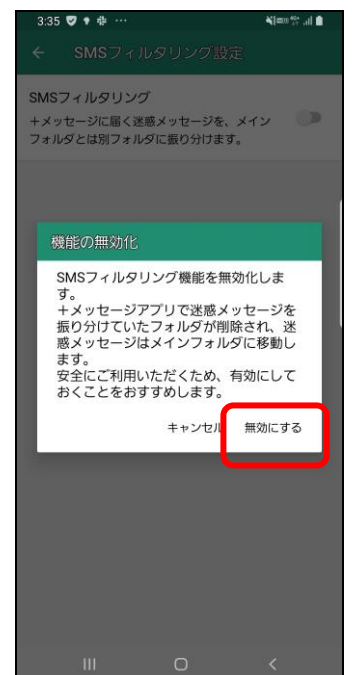
「SMSフィルタリング設定」をタップ

3



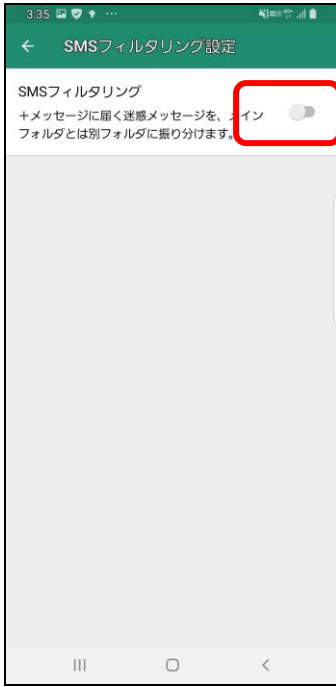
タップする

4



「無効にする」をタップ

# 5



無効になったことを確認

## 迷惑メッセージフォルダの確認方法

迷惑メッセージフォルダは、+メッセージアプリで自動的に作成されます。

+メッセージアプリから、「迷惑メッセージ」フォルダを確認できます。

詳細な+メッセージアプリの設定方法は、NTT ドコモのコーポレートサイトをご確認ください。

[https://www.docomo.ne.jp/service/plus\\_message/](https://www.docomo.ne.jp/service/plus_message/)

# 1



メッセージをタップ  
「迷惑メッセージ」フォルダがあることを確認

「迷惑メッセージ」フォルダが自動作成されていることを確認

## 迷惑なメッセージを受信した場合

---

迷惑なメッセージを受信した場合、自動的に「迷惑メッセージ」フォルダへ振り分けられます。

※ 詳細な+メッセージアプリの設定方法は、NTT ドコモのコーポレートサイトをご確認ください。

[https://www.docomo.ne.jp/service/plus\\_message/](https://www.docomo.ne.jp/service/plus_message/)

### 1



迷惑な SMS を受信すると「迷惑メッセージ」フォルダへ自動的に振り分けられます。



# 第13章 ダークウェブモニタリングを確認する

## ダークウェブモニタリングとは

お客様の個人情報が出ていないかモニタリングし、流出を検知したらお知らせします。

## モニタリング情報を登録する

流出をモニタリングする情報を登録します。

メールアドレス、ID（ログイン名）、クレジットカード番号、銀行口座番号、電話番号、パスポート番号を登録できます。

1



「プライバシー」をタップ

2



「モニタリング対象設定」をタップ

3



「メールアドレス」をタップ

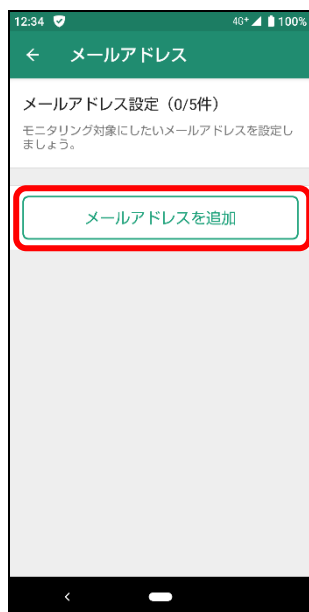
### ■ メールアドレスを登録する場合

1



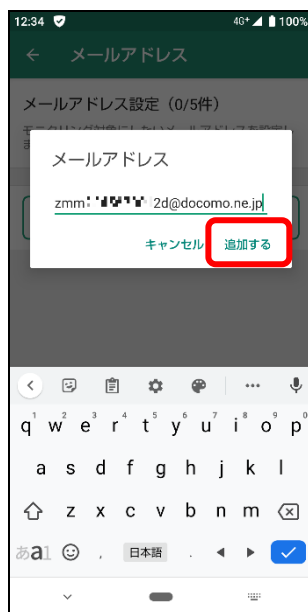
「メールアドレスを設定していきましょう」をタップ

2



「メールアドレスを追加」をタップ

3



メールアドレスを入力し、「追加する」をタップ

4



メールアドレスは最大 5 件登録できます。

■ ID (ログイン名) を登録する場合

1



「ID (ログイン名) を登録してみましょう」をタップ

2



「d アカウントを追加」をタップ

3



「追加する」をタップ

4



ID (ログイン名) は 1 件のみ登録できます。

■ クレジットカード番号を登録する場合 ※手入力により登録

1



「クレジットカード」をタップ

2



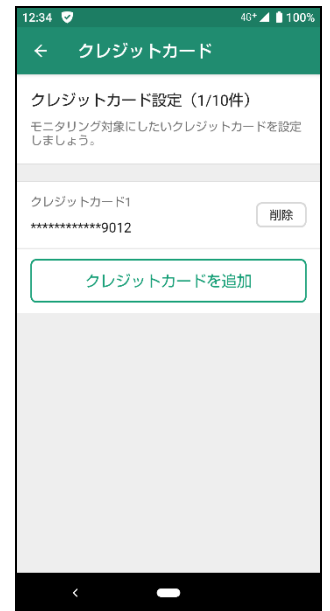
「クレジットカードを追加」をタップ

3



クレジットカード番号を入力し、「追加する」をタップ

4



クレジットカード番号は最大 10 件登録できます。

## ■ 銀行口座番号を登録する場合

1



「銀行口座」をタップ

2



「銀行口座を追加」をタップ

3



銀行口座情報を入力し、「追加する」をタップ

4



銀行口座番号は最大 10 件登録できます。

## ■ 電話番号を登録する場合

1



「電話番号」をタップ

2



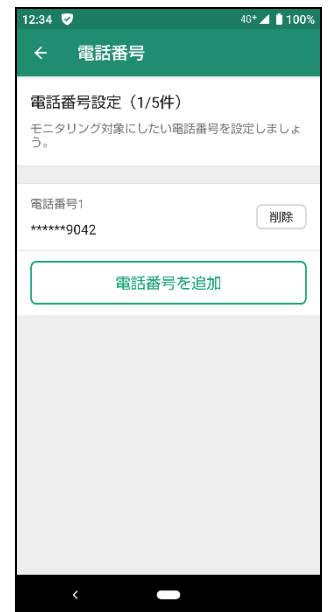
「電話番号を追加」をタップ

3



電話番号を入力し、「追加する」をタップ

4



電話番号は最大 5 件登録できます。

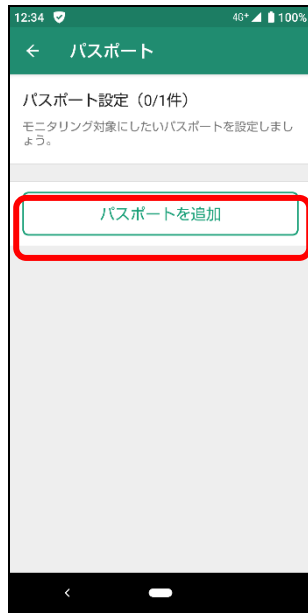
## ■ パスポート番号を登録する場合

1



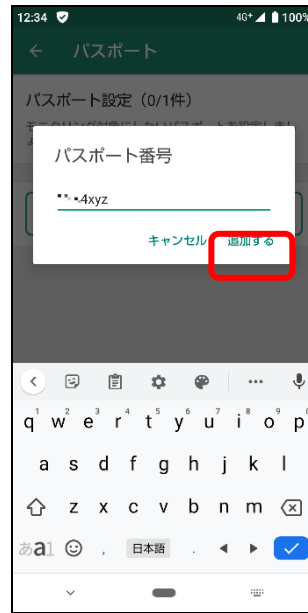
「パスポート」をタップ

2



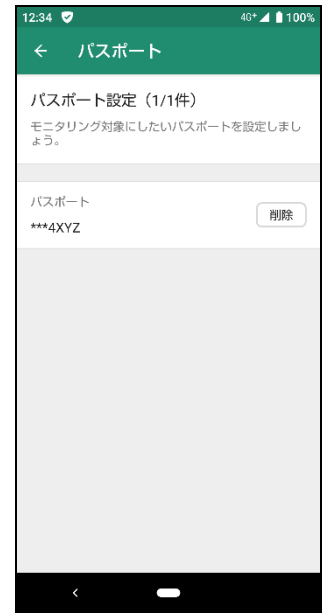
「パスポートを追加」をタップ

3



パスポート番号入力し、「追加する」をタップ

4



パスポート番号は 1 件のみ登録できます。

## モニタリング情報を削除する

モニタリングをする情報を変更する場合、登録済みの情報を削除し新たに登録してください。  
ここではメールアドレスを削除する操作を記載しますが、他の情報も同様の操作で削除できます。

1



削除するメールアドレスの「削除」をタップ

2



「削除する」をタップ

3



## 流出を検知したら

流出を検知すると、検知ダイアログが表示されます。

「確認する」をタップし、至急確認してください。

未確認の検知結果がある場合、定期的に通じます。

定期的な通知が不要の方は、「検知結果通知の設定」で通知を無効に変更してください。

1



「確認する」をタップ

2



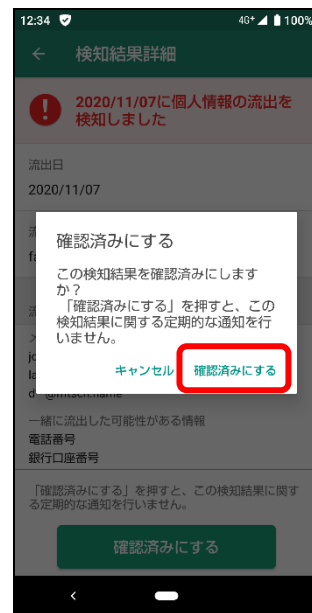
確認する情報をタップ

3



スクロールして対処方法を確認し、「確認済みにする」をタップ

4



「確認済みにする」をタップ  
※必ず対処方法を確認いただき、お客様ご自身の判断にて「確認済み」に変更してください。

5



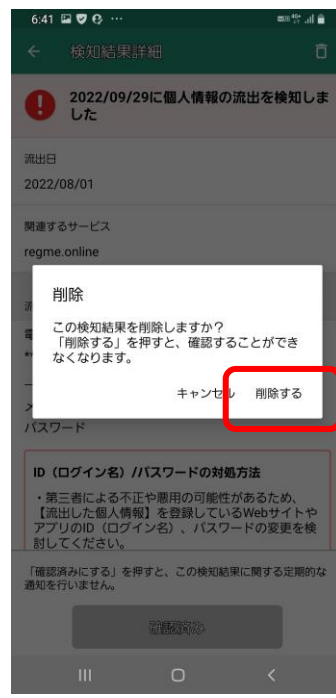
検知結果を履歴として残さず削除したい場合は、引き続き以下を行ってください。

6



右上のゴミ箱マークをタップ

7



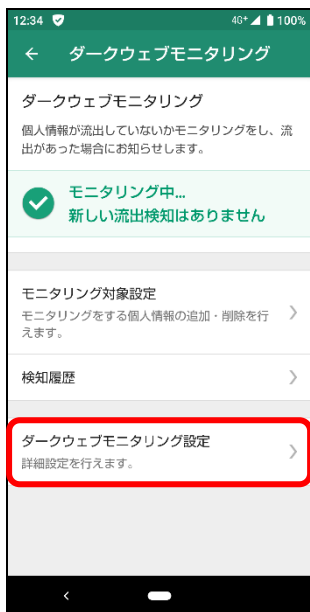
「削除する」をタップして削除

## 検知結果通知の設定

未確認の検知結果がある場合、定期的に通知します。

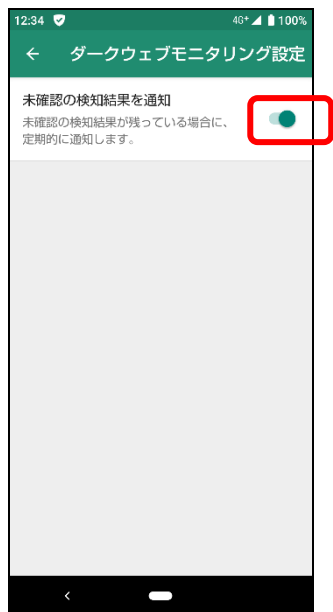
通知が不要の方は、下記の手順で通知を無効に変更してください。

1



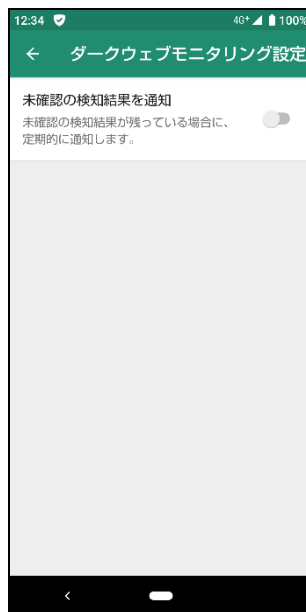
「ダークウェブモニタリング」をタップ

2



トグルボタンをタップ

3



有効にする場合は再度トグルボタンをタップしてください。

## 検知詳細画面の見方

12:34 4G+ 100%

← 検知結果詳細

❗ 2020/11/07に個人情報の流出を検知しました

流出日  
2020/11/07

関連するサービス  
turner.name

流出した個人情報

ID (ログイン名)  
adel\*\*\*\*\*

一緒に流出した可能性がある情報  
メールアドレス  
電話番号  
銀行口座番号  
クレジットカード番号

ID (ログイン名) の対処方法

- ・ 第三者による不正や悪用の可能性があるため、ID (ログイン名) とパスワードの変更を検討してください。  
※複数のWebサイトやアプリで同じID (ログイン名) ・パスワードをご利用の場合は、同様の対策をしてください。
- ・ 流出したID (ログイン名) がdアカウントと一致しています。  
お客様のdアカウントに対しても、同様の対策をしてください。  
[dアカウントのID・パスワード変更はこちら](#)
- ・ ドコモではdアカウントパスワード無効化設定を提供しています。

パスワードの変更を検討してください。

銀行口座番号の対処方法

- ・ ご利用の銀行口座明細を確認し、身に覚えのない不審な入出金を確認した場合は、金融機関に相談してください。
- ・ ご利用の銀行口座明細は定期的に確認してください。
- ・ 第三者による不正や悪用の可能性があるため、銀行口座を登録しているWebサイトやアプリのID (ログイン名) とパスワードの変更を検討してください。

その他

個人情報流出時の対処方法は[こちら](#)

「確認済みにする」を押すと、この検知結果に関する定期的な通知を行いません。

確認済みにする

流出を検知した日付

情報が流出した日付

関連するサービス (ドメイン)  
※サービスが分からないときは「不明」と表示されます

検知した情報

検知した情報と一緒に流出した可能性がある情報

タップして、詳細な対処方法を表示します

流出した情報の対処方法  
※流出した情報の種類ごとに対処方法を表示します

タップして、詳細な対処方法を表示します



## 第14章 各機能の設定を変更する

ホーム画面で左上のメニューボタンを押すとナビゲーションメニューが表示されます。

### ■ ナビゲーションメニュー



## アカウント

アカウント画面ではログインしている d アカウントや、現在の「あんしんセキュリティ」サービスの契約状態を確認することができます。未契約の場合、サービスの詳細を確認することができます。

### 契約中



契約中の場合、契約しているアカウントが表示され、契約中のサービスが表示されます

### 契約なし



未契約の場合、ログインしている d アカウントが表示され、契約状態に「未契約」と表示されます

### d アカウント未ログイン



d アカウント未ログインの場合、「ログインしていません」と表示され、契約状態に「不明」と表示されます

■ dアカウントでのログイン、ログイン ID を変更する場合

1 ※未ログインの場合



「d アカウントの設定」をタップ

2 ※既にログイン中の場合



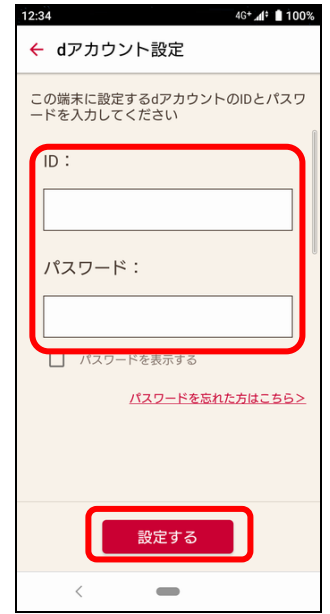
「d アカウントの変更・解除」をタップ

3



「ご利用中の d アカウントを設定」をタップ

4



ID・パスワードを入力し、「設定する」をタップ

設定画面

各種通知の設定や、利用情報の送信、常駐アイコンについて設定ができます。

■ 設定画面



おすすめのセキュリティサービスの案内を通知します

月初に前月分のレポートを通知します

毎週 1 本程度ニュース配信時に通知を行います

端末で設定が完了していない項目がある場合に通知を行います

端末の上部の通知バーにアイコンを表示します

アプリの利用状況を送信します。送信された情報は今後の改善に利用いたします  
また、個人が特定できるような状態での送信はいたしません

検知時の通知表示の設定を変更します  
※Android14.0 以降で表示されます



## 第15章 サービス利用上の注意点

---

### ご利用にあたって

---

#### 【サービス全般】

- ご利用には、本アプリのインストールおよび初期設定が必要です。
- FOMA/Xi/5Gご契約のドコモ UIM カードが挿入されていない場合、本アプリのインストールやアップデートができない場合があります。
- アップデートの際、ご利用規約とアプリケーション・プライバシーポリシーへの同意が必要な場合があります。同意しない場合、本アプリはご利用できません。
- お客さまのご利用の方法によっては、ご利用端末の消費電力が増加し連続通話（通信）時間・連続待受時間が短くなる場合があります。
- ご利用端末の設定で文字サイズを大きくした場合、本アプリのレイアウトが崩れたり文字が切れたりする場合があります。
- 本アプリをインストールいただかなくても、迷惑メールおまかせブロックをご利用いただくことは可能です。
- docomo Application Manager（ドコモアプリ管理） アプリのバージョンが最新でない場合、本アプリが正常に動作しない場合があります。最新のバージョンをインストールの上ご利用ください。
- タスクキラー機能により本アプリを強制停止した場合や、本アプリと同等機能を有するアプリがインストールされていた場合、本アプリは正常に動作しない場合があります。
- インターネットへ接続できない場合や、ウイルス定義ファイルの更新や危険サイトの照会時などに McAfee LLC の定めるサーバが利用できない場合、「あんしんセキュリティ」申込者の認証時などに弊社が定めるサーバが利用できない場合、本アプリは正常に動作しない場合があります。
- 本アプリを端末の RAM 容量が少ない状態で利用した場合、本アプリは正常に動作しない場合があります。RAM の容量を確保した上でご利用下さい。

#### 【セキュリティスキャン】

- セキュリティスキャンにて検出されるセキュリティの危険は、McAfee LLC が提供するウイルス定義ファイルとマルウェア評価データベースにより対応可能な危険のみであり、すべてのセキュリティの危険の検出を保証するものではありません。
- スキャンの実行中やウイルス定義ファイルの更新中に、本サービス対応端末のレスポンスや通信速度が低下する場合があります。
- ウイルス定義ファイルの更新中・マルウェア評価データベース照会中に通信が切れた場合、本機能は正常に動作しない場合があります。
- 各種スキャン機能が動作しても、全ての動作がログに保存されるわけではありません。

#### 【危険サイト対策】

- 危険サイト対策にて注意喚起されるサイトは、McAfee LLC が定める URL リストにより対応可能なサイトのみであり、すべての危険サイトの検出を保証するものではありません。
- 対応ブラウザは Chrome ブラウザ、Samsung 社端末に標準搭載されたブラウザ、およびあんしんフィルター for docomo（青少年向け）でご利用になれます（その他のブラウザでも動作する場合があります）。但し、シークレットモード等秘匿性のある状態ではご利用になれません。
- 対応 SNS アプリは Facebook、Instagram（対応 OS：OS13 以上）、LINE、Messenger、X（Twitter）でご利用になれます。
- 危険サイト対策をご利用中は、お客さまのサイトアクセスした URL が危険サイトであるかを判定するため、本アプリが McAfee LLC のサーバに当該 URL 等の情報を通知します。お客さまは、危険サイト対策のご利用にあたり、本アプリがかかる通知を行うことを承諾するものとします。
- 一部のサービス対応端末にて危険サイト対策による注意喚起の表示が遅れる場合や、サイトアクセスの方法等によって危険サイト対策が機能せず注意喚起が表示されない場合があります。
- サイトアクセスなどの通信が遅くなることがあります。
- ブラウザの戻る／進むボタンを利用した場合、注意喚起画面が表示されない場合があります。

#### 【アプリチェック】

- アプリチェックにて注意喚起されるアプリは、McAfee LLC が定める検出ロジックによりお客様の個人データを取得する機能が搭載されているアプリであり、すべての個人データを取得するアプリの検出を保証するものではありません。
- アプリチェックは、お客様の個人データを取得する機能が搭載されているアプリをお知らせすることで、お客様の当該アプリの利用に関する注意喚起を促すものです。ウイルスを検出・駆除等を行ったり、お客様の個人データの送信を停止したりする機能ではありません。
- プライバシー評価データベース照会中に通信が切れた場合、本機能は正常に動作しない場合があります。

#### 【危険 Wi-Fi 対策】

- 危険 Wi-Fi 対策にて注意喚起される Wi-Fi は、McAfee LLC が定める検出ロジックにより検出可能な Wi-Fi のみであり、すべての危険な Wi-Fi の検出を保証するものではありません。
- マルチコネクション機能を搭載している機種において、マルチコネクション機能が ON の状態で適用アプリケーションに「あんしんセキュリティ」が含まれている場合、Wi-Fi 接続時の表示が遅れることがあります。

#### 【迷惑電話対策】

- パケット通信を利用した通話アプリ（LINE、Skype など）の発着信には対応していません。
- 「キャッチホン」サービス等による通話中の着信については、本サービスの動作保証外です。
- 本サービスは、お客様の対象端末の発着信について、トビラシステムズ株式会社の提供するデータベースに基づき、当該番号が迷惑電話の蓋然性の高い電話番号であるかの判定結果を提供します。
- 全ての迷惑電話等が正しく判定されることを保証するものではありません。
- 発信者番号の通知がない場合（「非通知設定」、「公衆電話」、「通知不可能」等）、迷惑電話の蓋然性の高い電話番号であるかの判定結果の提供は行いません。
- 電話帳に登録されていない電話番号の発着信について、全ての公共施設や企業、飲食店などの発信元の名称を正しく表示されることを保証するものではありません。パケット通信／データ通信ができない状態の発着信は、発信先・発信元の名称を表示することができません。

#### 【迷惑メール対策】

- ドコモメールがご利用いただけない場合、迷惑メール対策はご利用できません。
- 迷惑メール対策が利用できない場合、バージョン 05.10.00000 未満をご利用の方は、すべての設定が完了してもホーム画面のセキュリティ状況は 100% になりません。最新バージョンにアップデートの上ご利用ください。

#### 【SMS フィルタリング】

- +メッセージアプリで受信したメッセージの情報を、トビラシステムズ社のサーバへ送信します。また、送信された情報は迷惑 SMS の判定のみに使用します。
- 迷惑 SMS 受信時に、+メッセージアプリがデフォルト（標準）の SMS 設定されていない場合、基本的には「迷惑メッセージ」フォルダに振り分けられません。
- 一度迷惑と判定された SMS の送信元からの SMS は、全て「迷惑メッセージ」フォルダに振り分けられます。
- その他、+メッセージの動作に関しては、+メッセージのサービスサイトをご確認ください。

[https://www.docomo.ne.jp/service/plus\\_message/](https://www.docomo.ne.jp/service/plus_message/)

- あんしんセキュリティ トータルプラン、あんしんセキュリティ スタンダードプラン、あんしんセキュリティ（迷惑 SMS 対策）を解約した場合、「迷惑メッセージ」フォルダが削除されるまでしばらく時間がかかります。

#### 【ダークウェブモニタリング】

- 本サービスは、F-Secure Corporation の提供するダークウェブモニタリングシステムにより、お客様が登録した情報の流出をモニタリングします。
- 本サービスは、流出の検知をお知らせするものであり、検知した情報の対処はお客様ご自身で行っていただく必要があります。
- 本サービスのご契約者の個人情報のみをモニタリング対象として設定するようにお願いしています。

詳細はご利用規約を参照ください。

あんしんセキュリティ（プライバシー）：

[https://www.docomo.ne.jp/service/anshin\\_security\\_privacy/regulation.html](https://www.docomo.ne.jp/service/anshin_security_privacy/regulation.html)

あんしんセキュリティ トータルプラン：

[https://www.docomo.ne.jp/service/anshin\\_security\\_total\\_plan/regulation.html](https://www.docomo.ne.jp/service/anshin_security_total_plan/regulation.html)

あんしんセキュリティ スタンダードプラン：

[https://www.docomo.ne.jp/service/anshin\\_security\\_standard\\_plan/regulation.html](https://www.docomo.ne.jp/service/anshin_security_standard_plan/regulation.html)

※本サービス契約以外の電話番号の設定について

サービス契約者ご本人名義の携帯電話番号（キャリア問わず）、固定電話番号であれば、設定可能です。

## 通信について

---

- 本アプリの利用には、パケット通信料／データ通信料（本アプリのダウンロードやホーム画面の更新時、ウイルス定義ファイルの更新時、危険サイト対策による危険サイトの検出、マルウェア評価・プライバシー評価データベースの照会時、電話番号判定のためのデータベース更新時の通信時、電話帳登録外の発着信での発信先・発信元の名称表示時など）がかかります。
- 本サービスはホーム画面の更新などのため、自動で通信します。
- サーバと通信できない状態ではアプリを利用できません。通信環境の良い状態で利用してください。
- ドコモ回線をご利用のお客さまが海外で本アプリをご利用になる場合には、当社が別に定める場合を除き、すべての通信に対し、契約約款に定める国際ローミング利用料がかかります。この場合、パケット定額サービスをご契約されていても、パケット定額サービスなどの適用対象外となります。

## 端末の動作環境について

---

- ご利用端末の機能や環境により、本アプリが正常に動作しない場合があります。
  - ご利用端末のオペレーションソフト（OS）の仕様変更等により、本アプリの機能や動作に影響を与える場合があります。
  - 本サービスをご利用される端末の種類や端末の状況によっては、本サービスに基づく警告表示が遅れるなど、警告表示や発信先・発信元名称表示がされない場合があります。
  - 以下の場合、本サービスが正常に動作しない可能性があります。必ずご利用前に設定を確認してください。
    - ①タスクキラー機能により本アプリを強制停止した場合
    - ②本アプリと類似する他のアプリ等がインストールされていた場合
    - ③本アプリの警告画面よりも前面で画面を表示するアプリ等がインストールされている場合
- ※上記以外の場合でも、端末固有の機能やご利用の環境により、本アプリが正常に動作しない場合があります。