（リンク付き文書）

なとりコイン　利用者説明書（補足 版）

2024. 8.27　Ver.2.3

名取市役所 ＤＸ推進室

Tel：022-748-6816　Fax：022-384-9030

補足説明書　目次

補足説明書　目次

3.　安心して利用するために

４．技術的な参考情報

目次へ戻る

自分のスマホの電子メールアドレスを確かめる

【 Android端末 】

- **Google メールの場合**

①Chrome画面の「設定」アイコンをタップします。
②設定画面でご自分の名前の部分をタップします。
③メールアドレスが表示されます

Google メール

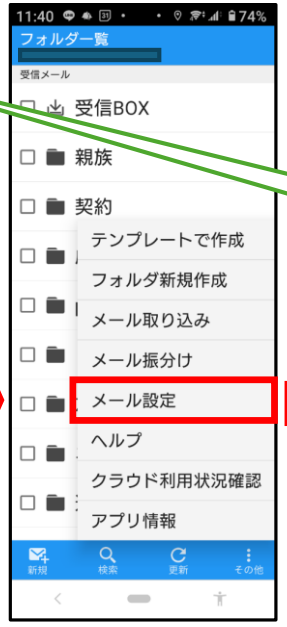
・Chrome ブラウザの右上隅の「⋮」マークをクリック

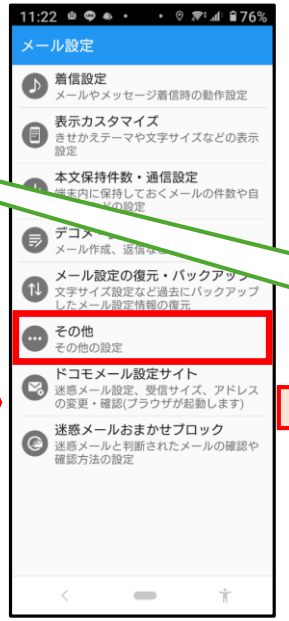
・Google 電子メール（Gmail）の自分のメールアドレスが確認できます

Docomo メール

Docomo メールの場合

①スマホ画面下部のDocomoメールアプリのアイコンをクリックします。
② ［その他］-［メール設定］-［その他］-舞アドレス」をタッチします。





・Docomoメールの自分のメールアドレスが確認できます

・Docomoメールの自分のメールアドレスが確認できます

目次へ戻る

自分のスマホの電子メールアドレスを確かめる

【ＩＯＳ端末】

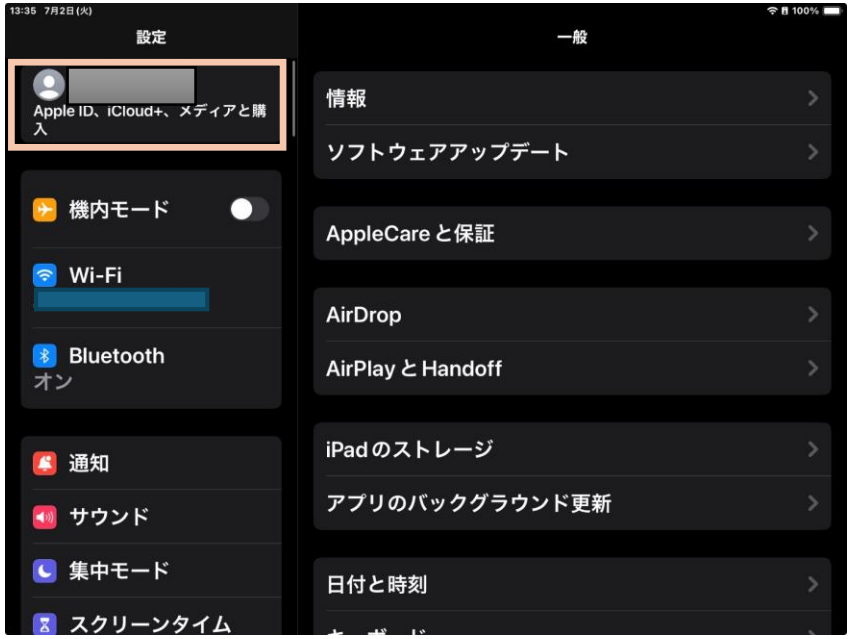
・「設定」アプリを開きます。
・左上の「名前」をタップすることで、メールアドレスが表示されます。

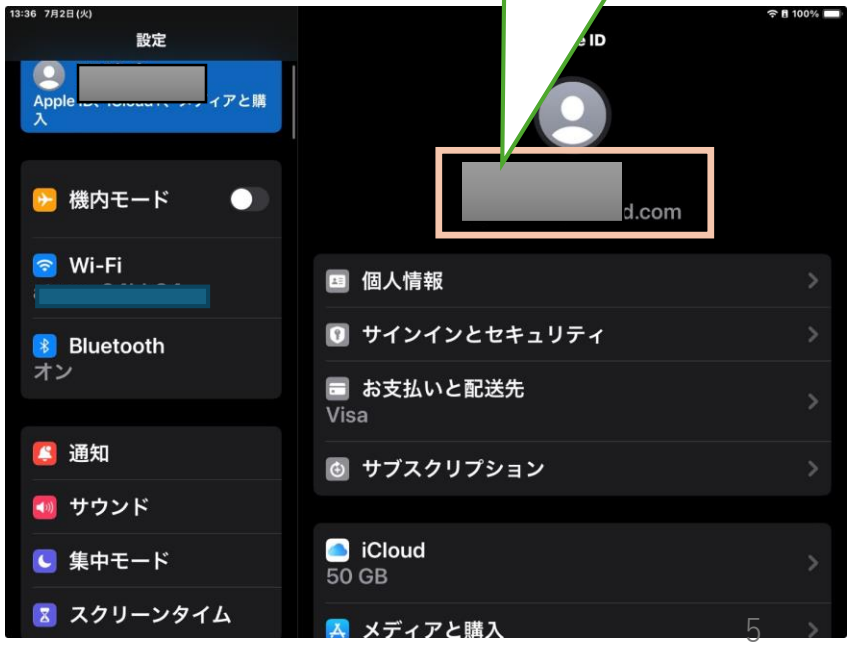
・ＩＯＳの電子メールアプリでは、自分で保持しているさまざまなメールアドレス毎に送受信管理ができます。

例：　☐ iCloud　☐ Biglobe
　　☐ Gmail　☐ Outlook
など

・ＩＯＳ端末での自分のメールアドレスが確認できます

［設定］アプリをクリック





目次へ戻る

「Google レンズ」の活用

　スマートフォンのカメラを使って、目の前にあるものの情報を瞬時に読み取り、以下のようなことが出来ます。

①　外国語の看板やメニューを翻訳する。

②　植物や動物の種類を特定する。

③　類似の商品を（家電、バッグ、洋服など）を検索する。

④　手書きのテキストをスマホにコピーする。

⑤　ＱＲコードやバーコードをスキャンする。

⑥　ランドマーク・建物などの史実やお店の営業時間などを調べる。

※iOS の場合、「Google アプリ」をインストールすることで、実現できます。

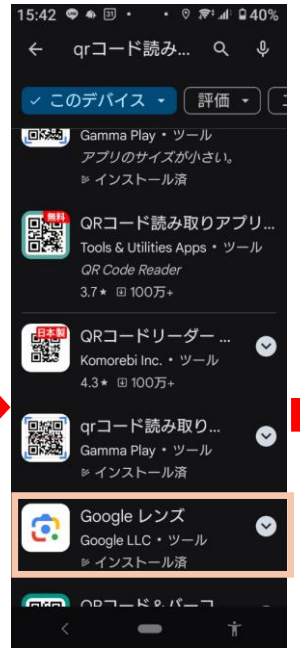
Google フォト の場合、Google レンズで検索できるのは「保存済みの写真のみ」なので、起動したカメラでも検索できる Google アプリのほうが使い勝手が良いと思われます。

目次へ戻る

Google レンズで、QRコードの読み取り

●アプリの検索を行う
・「QRコード 読み取り」

※この事例では、既に「Google レンズ機能」はインストール済み



●Qoogle レンズアプリを「インストール」または「開く」

●Qoogle レンズアプリを「インストール」または「開く」
●「検索」をクリック

●カメラ機能が働きだす。

●QRコードに応じた情報が画面に表示される。

●対応するアプリを呼び出すか確認画面が表示される。

□ 「インストール」（新規にインストール）
□ 「開く」（既にインストール済みの場合

ここから先に進めない場合

●「らくらくスマホ」の「インターネット」から起動する標準ブラウザでは、QRコード読取の際にカメラが起動しないケースがあります。

メニューの「Google」から「Chrome」でのご利用をお願いします。
なおChromeでは、Chromeにカメラの使用許可設定が必要になります。

※先の頁の「●らくらくスマホ で カメラが起動しない」を参照ください。7

目次へ戻る

PDFファイル の活用

●PDF形式のファイルを参照する場合は、Adobe社が提供するAcrobat Reader が必要です。

（他の同等なアプリを利用するという選択肢もあります。）

※スマホの機種によっては、最初からPDFを読み込むためのアプリが付属していないことがあります。

PDF ファイルの参照例（なとりコイン利用店）

PDF 文書を参照できます

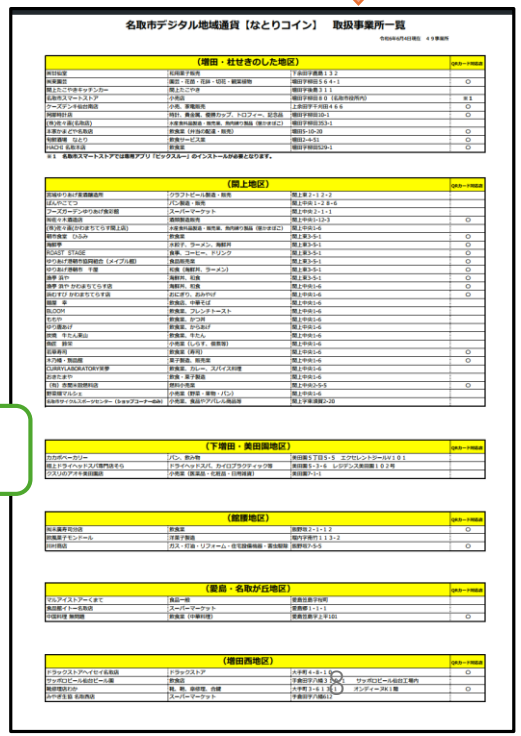
Acrobat Reader のインストール

「Play ストア」をクリック

① 検索欄に、「pdf リーダー」 と入力
② 検索結果に、いくつかのアプリが表示
③ Adobe Acrobat Reader を選択

① Adobe Acrobat Reader 画面が表示されたら、
☐ インストール または
☐ 開くを選択

① Adobe Acrobat Reader が使える環境が整いました。



目次へ戻る

2. スマートフォンの使い勝手をよくするために

【 操作性 】

Web 型アプリを、ホーム画面に設定する

（ホーム画面にショートカットを置く）

■ Android の場合　　■ iPhone,iPadの場合

【 操作性 】

ブックマークに登録する

・メニューバーをクリック
・「ブックマーク」をクリック
・現在参照しているWebページが「ブックマーク」に登録される

【 解説 】

スマホ上で動く「アプリ」と「Webブラウザー型アプリ」の違い

【 操作性 】

パスワードマネージャー による ＩＤ/パスワード関連付けの修正

・ID と パスワード の関連付けに関する、修正処理を行います。
・パスワード管理機能を有する主要なブラウザとしては、Google Chrome、Edge、Firefox、Safari などがあります。

【 操作性 】

ブラウザーのタブを閉じる

●タブを閉じる理由
① パフォーマンスとメモリーの最適化
　～ システムリソースの節約
② 整理と作業効率　～ 特定のタスクに集中
③ セキュリティとプライバシー漏洩のリスク軽減

目次へ戻る

Web 型アプリを、ホーム画面に設定する（1/3）

●Google Chrome、Safari からは、「ホーム画面に追加する」機能があります。

●Yahoo！ ブラウザーからは、「ホーム画面に追加する」機能はありません。
→　利便性を高めるには、以下の方法をとることができます。

①　他のブラウザ（Chrome、Safari）を使用し、ホーム画面上に登録されたアイコンから入る。またはブックマークを利用する

②　「ナトぽた」から入る

●ホーム画面に追加したいアプリ

- ナトぽた
- なとりコイン（Web版）
- Gmail（アプリ版）

など

目次へ戻る

Web 型アプリを、ホーム画面に設定する（2/3）

●Android スマートフォンの場合

・ホーム画面へショートカットを作成すると、

ブラウザ起動も含め、スムーズにアクセスできるようになります。

（バージョンにより画面が異なります）

目次へ戻る

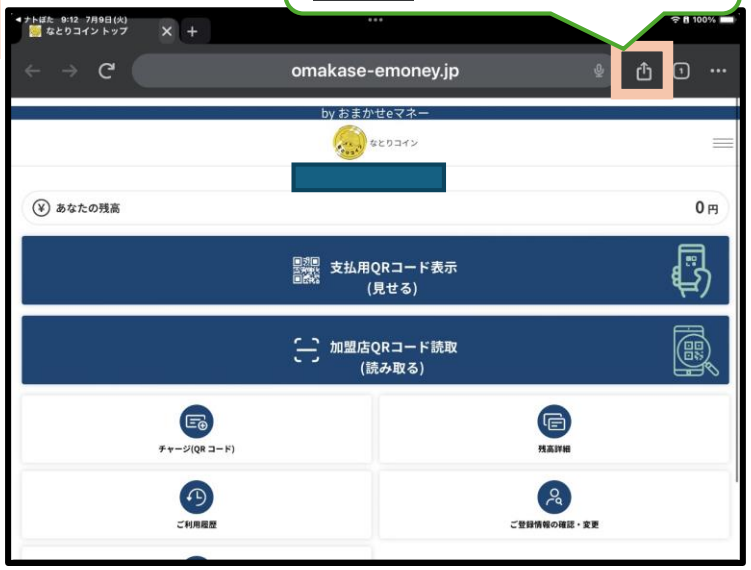
Web 型アプリを、ホーム画面に設定する（3/3）

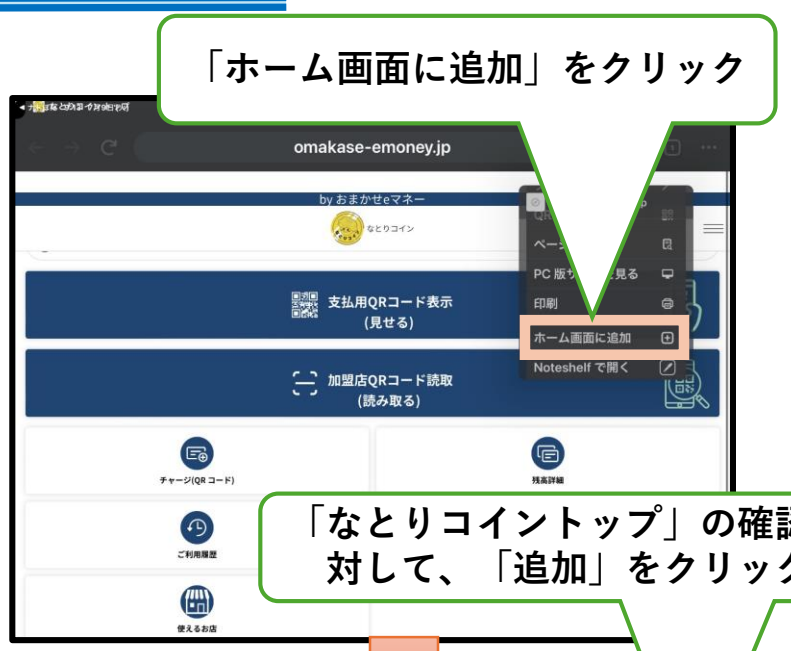
● iPhone,iPad の場合

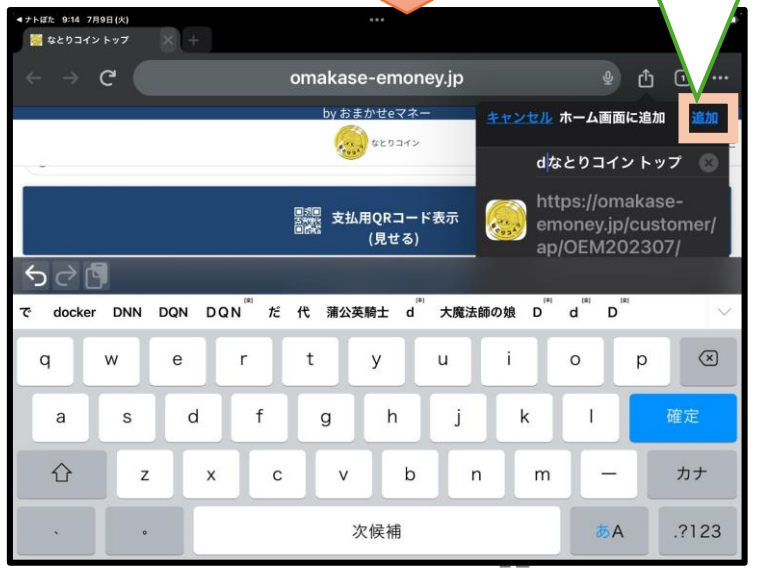
・ホーム画面へショートカットを作成すると、

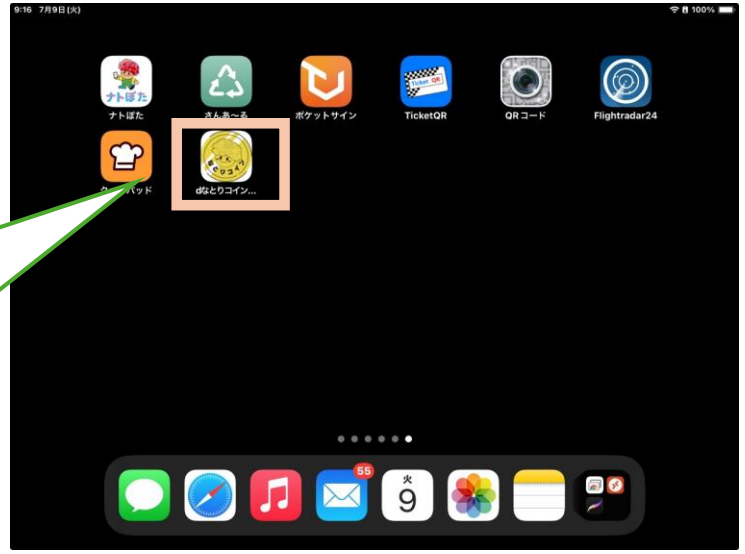
ブラウザ起動も含め、スムーズにアクセスできるようになります。

（バージョンにより画面が異なります）









●ホーム画面に、「なとりコイン」が設定されます。

●今後は、このアイコンをクリックすることで、利用することができます。

目次へ戻る

ブックマークに登録する(1/2)

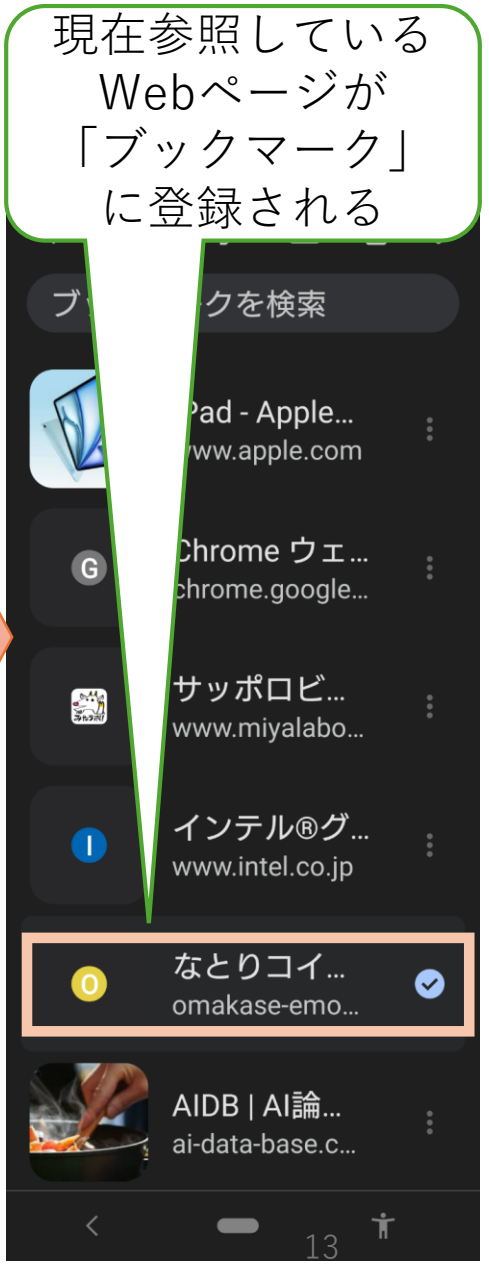
●Android スマートフォンの場合

● ブックマークに登録すると、ブラウザからスムーズにアクセスできるようになります。

（登録方法はバージョンにより画面が異なります。）

活用手順

登録手順



目次へ戻る

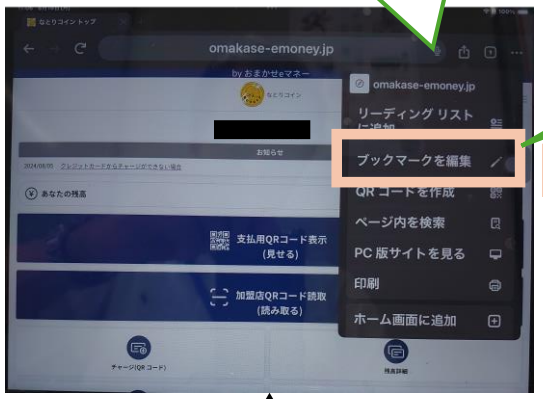
ブックマークに登録する(2/2)

● iPhone,iPad の場合

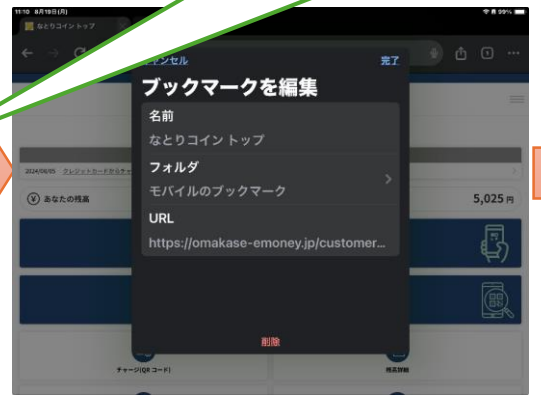
● ブックマークに登録すると、ブラウザからスムーズにアクセスできるようになります。

（登録方法はバージョンにより画面が異なります。）

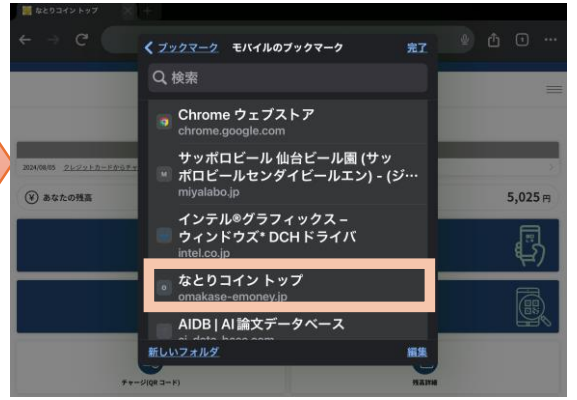
登録手順




をクリック



「ブックマークを登録（編集）をクリック

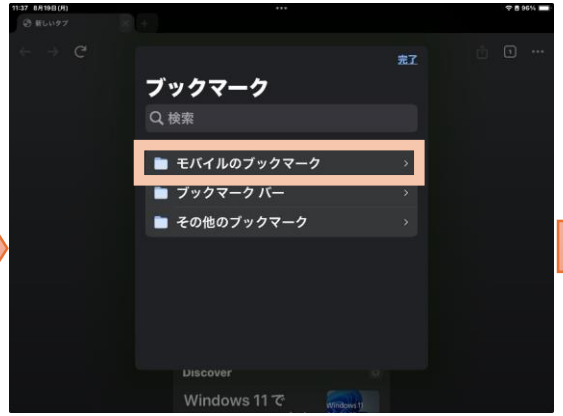


「なとりコイン」呼び出し

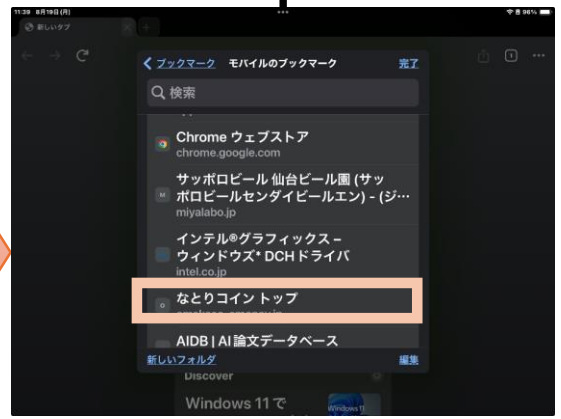
活用手順

… をクリック

「ブックマーク」をクリック



既に登録していた「なとりコイン」をクリックして画面呼び出し



※このブックマークに登録する方法よりも、先の「Web 型アプリを、ホーム画面に設定する」ほうが使い勝手が良いと思われます。

目次へ戻る

スマホ上で動く「アプリ」と 「Webブラウザー型アプリ」の違い

スマートフォン上で動作するアプリと、Webブラウザーを通して動くアプリ（Webアプリ）の違いは以下のとおりです。

【 スマホアプリ（ネィティブアプリ） 】
・ユーザーはアプリケーションストアからダウンロードして端末にインストールします。
・端末の機能（カメラ、プッシュ通信など）をフル活用できます。
オフラインでも利用可能です。

【 Webアプリ 】
・ダウンロードは不要で、Webブラウザー上で直接動作します。
・**インターネット経由で提供されるため、オフラインでは利用できません。**
・サーバー側で管理され、ユーザーの端末に依存しない特徴があります。

　どちらを選ぶかは、機能や利用目的によります。
スマホアプリは安定性が高く、ネィティブ機能を活用できますが、Webアプリは手軽に利用でき、インストール不要です。

※従来は、「アプリ＝特定の作業のみを行うソフトウェア」という位置づけでしたが、**現在はアプリへの機能追加がかなり進んで、例えばLINE のようにきわめて多様な用途で使えるものが普及しています。（スーパーアプリ）**

パスワードマネージャー による　ＩＤ/パスワード関連付けの修正

【 パスワードマネージャー 】

・パスワード管理機能を有する主要なブラウザとしては、

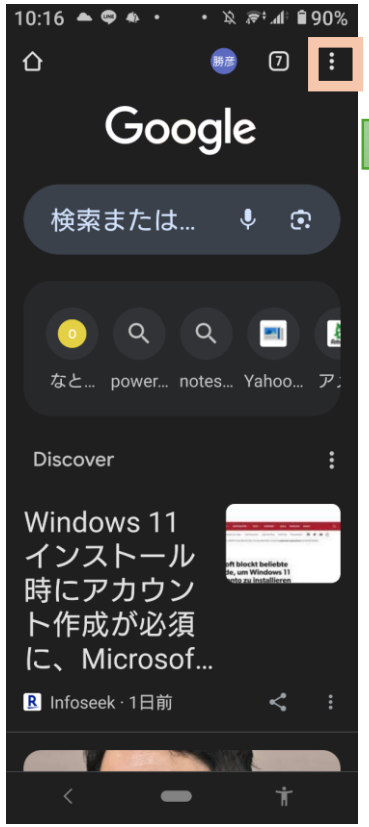
Google Chrome、Edge、Firefox、Safari などがあります。

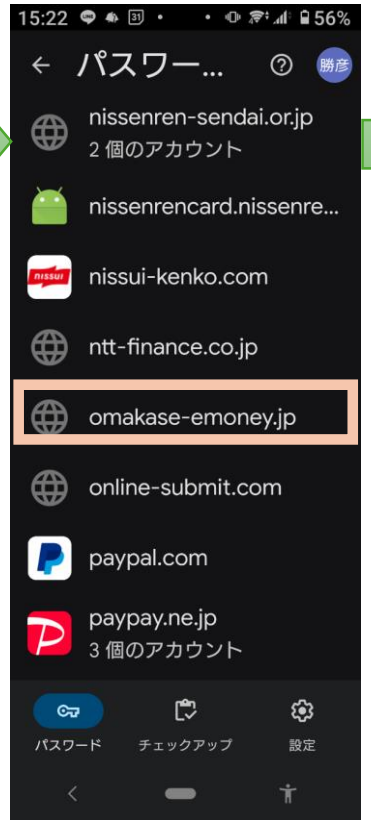
・**アカウントにログインする画面で、自動的にパスワードが表示される**など便利な面がありますが、ブラウザー利用のいろんな処理をやっていると、逆に混乱をきたすことがあります。

例：
｛間違えたままのＩＤやパスワードが残っていたり、パスワードを変更してもそれが反映されないなど｝

・このような場合に、**ID と パスワード の関連付けに関する、修正処理**を行います。

・パスワードは、クラウド上でセキュリティ上の安全管理がなされていますが、悪意のある攻撃から完全に安心とは言い切れない面があります。





本人認証

指紋認証など

画面を下にスクロールして、「omakase-emoney.jp」をクリック

・間違えて登録したＩＤがあれば、「削除」します。
・複数のIDを使うなどして、「煩雑」状態に陥った時には、「編集」も行わず、すべて削除してしまい改めて新規登録するほうが混乱しなくて済みます。

目次へ戻る

ブラウザーのタブを閉じる

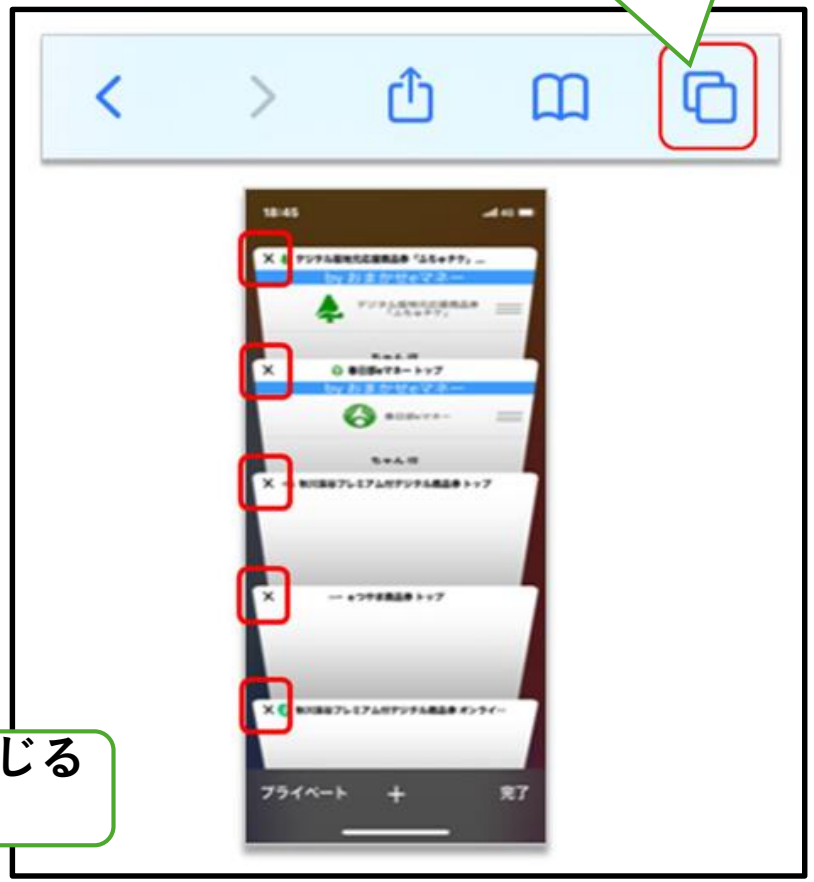
Android Chromeの場合

今、利用していない「不要なタブ」をチェックして消す

すべてのタブを閉じることも可能

Saffari の場合

右上隅の
をクリックすることで、各タブ一覧が表示されます。



不要なタブシートの、
「X」欄をチェックしていきます。

【 ブラウザーのタブを閉じる理由 】

① パフォーマンスとメモリーの最適化　～　システムリソースの節約
② 整理と作業効率　～　特定のタスクに集中
③ セキュリティとプライバシー漏洩のリスク軽減

目次へ戻る

（解説）メールの種類 と フリーメールの利用

◎ **プロバイダーメール：**
　インターネットのプロバイダー（Jcom や OCN 、Biglobe など）が提供

◎ **キャリアメール：**
　ドコモやａｕ、ソフトバンクなどの携帯電話会社（キャリア）が提供

▲ **フリーメール：**
　登録するだけで無料で使うことができる

例：　□ Gmail　□ Yahoo！メール　□ Outlook メール

●フリーメールは、ブラウザを通して無料で利用できるメールサービスで、次の特徴があります。

■氏名や住所が必要ない
■匿名性がある
■使い捨て可能（いわゆる捨てアド）

　しかし、メールアドレスの中でも**フリーメールアドレスはワンタイム認証に利用することは推奨されていません。**

●銀行のオンライン送金サービスなどでは、**ワンタイム認証**（振込等のお取引の際に、お手続きごとに変わる1回きりの使い切りパスワード）をメールで受け取り認証を行います。

　しかし、メールアドレスの中でもフリーメールアドレスは、ワンタイム認証に推奨されていません。

（フリーメールアドレスを避け、
「携帯電話・スマートフォンのメールアドレス」
「プロバイダ・勤務先のメールアドレス」
を使用するように注意喚起が行われています。）

目次へ戻る

キャリアメール　受信設定方法（1/4）

設定手順

準備

携帯電話会社のメールアドレス（@docomo.ne.jp / @ezweb.ne.jp / @softbank.ne.jp 等）をご利用の方は、下記手順により「@omakase-emoney.jp」 及び 「@ntt-card.co.jp」ドメインからのメールを受信を許可する設定にしてから、申込をお願いいたします。

- NTTドコモ（受信リスト設定）
- au（受信リスト設定）　※「必ず受信」のチェックを入れてください
- SoftBank（受信許可リスト設定）

NTTドコモの方

dメニュー⇒My docomo⇒設定⇒メール⇒メール設定⇒「受信リスト設定」

auの方

■Androind：
「auメールアプリ」⇒「画面左上のメニューキー」⇒「アドレス変更／迷惑メール設定」⇒「迷惑メールフィルターの設定／確認へ」

■iPhone：事前にWi-Fiをオフにしてください
「safari」⇒「右下の📖」⇒「auサポート」⇒「迷惑メール対策を知りたい」⇒「迷惑メールフィルター設定」⇒
「設定方法など詳しくはこちら」⇒「迷惑メールフィルター トップ」

softbankの方

My SoftBank⇒「迷惑メール対策」⇒「許可するメールの登録」の「登録する」

目次へ戻る

キャリアメール　受信設定方法（docomo）（2/4）

（1）【受信リスト設定】を押下

（2）設定を利用するを押下

（3）【さらに追加する】を押下

（4）表示した入力欄にドメインを入力

@omakase-emoney.jp
@ntt-card.co.jp

（5）【確認する】を押下

（6）設定内容をご確認のうえ、【設定を確定する】を押下

目次へ戻る

キャリアメール　受信設定方法（softbank）　(3/4)

「許可するメールの登録」の「登録する」を押します。

メールアドレスを入力し、指定方法を選択します。

アドレス入力
@omakase-emoney.jp
@ntt-card.co.jp

「部分一致」を選択

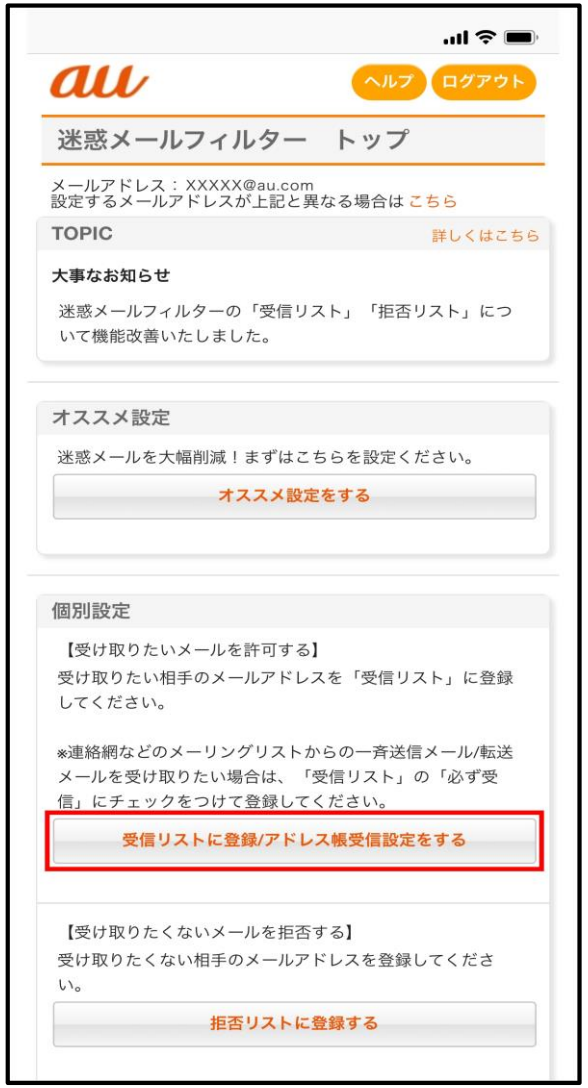
「次へ」を押します。

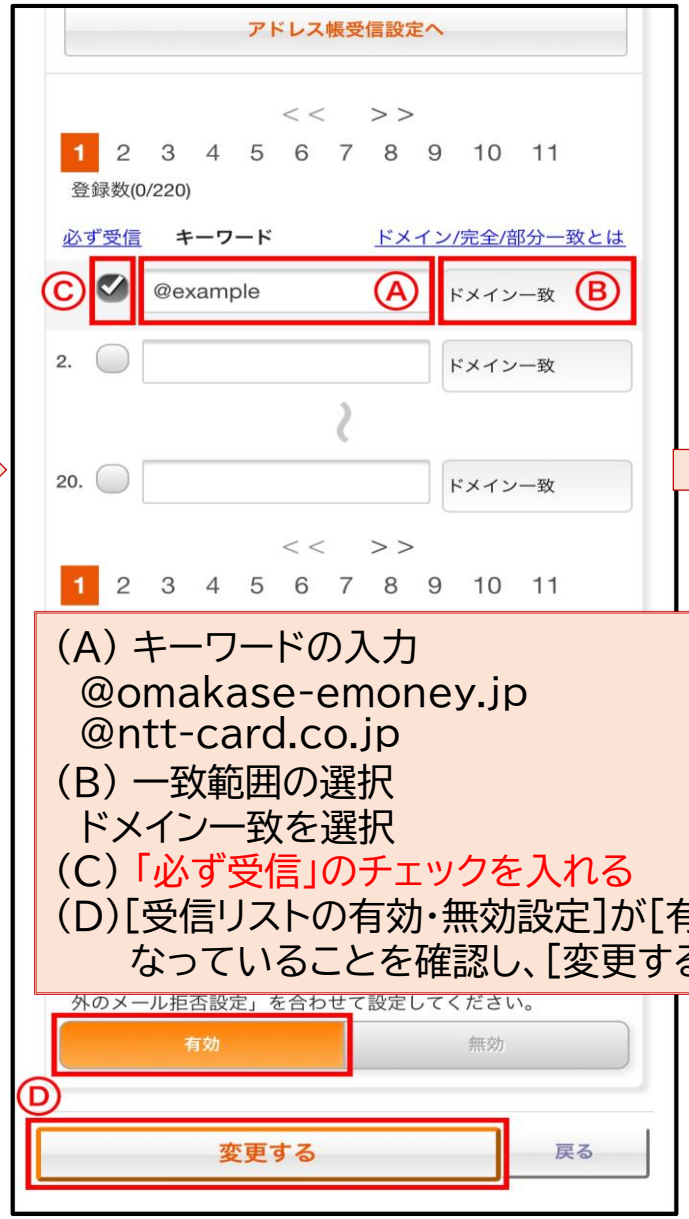
「登録する」を押します。

目次へ戻る

キャリアメール受信 設定方法（au） (4/4)

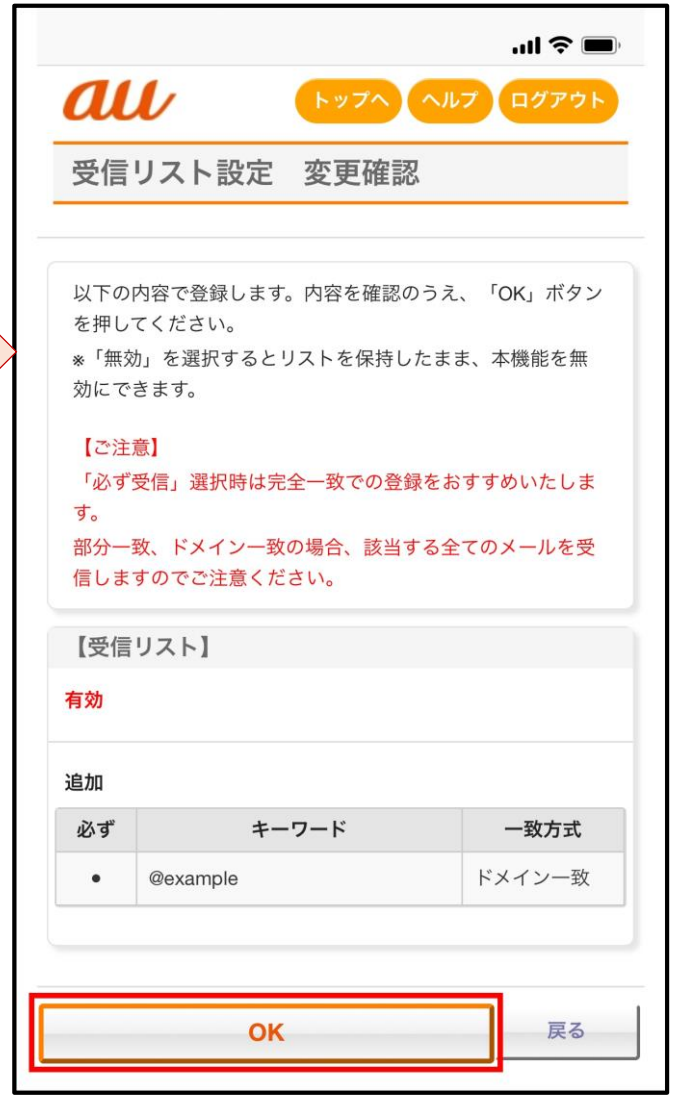
［受信リストに登録／
アドレス帳受信設定をする］を選択





（A）キーワードの入力
@omakase-emoney.jp
@ntt-card.co.jp
（B）一致範囲の選択
ドメイン一致を選択
（C）「必ず受信」のチェックを入れる
（D）［受信リストの有効・無効設定］が［有効］に
なっていることを確認し、［変更する］を選択

［OK］を選択



目次へ戻る

設定したメールアドレスに届かない 場合の対処

●新規登録の際の、本登録を行うためのURLが、 設定したメールアドレスに届かない

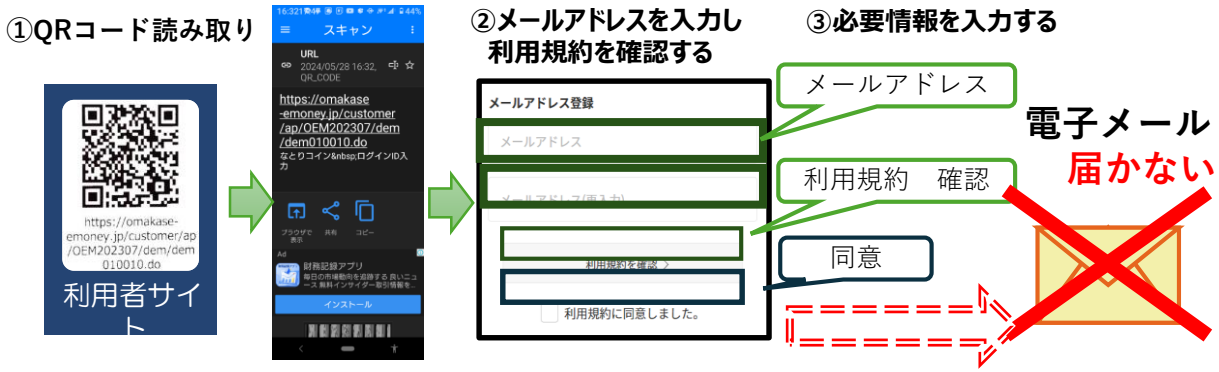
→

■ご利用の携帯電話（スマホ）の設定をご確認いただき、「@omakase-emoney.jp」ドメインからのメールを受信できるよう設定変更していただき、再度お申込みください。

■ auの携帯電話およびメールアドレス（@au.com／@ezweb.ne.jp）をご利用のお客様の場合、「迷惑メールおまかせ規制」の自動設定が適用されてメール受信が拒否されている可能性があります。

設定方法など詳しくは、以下のauホームページをご参照ください。
https://www.au.com/support/service/mobile/trouble/mail/email/filter/recommend/auto/

■ iCloudのメールアドレス（@icloud.com/@me.com 等）をご利用のお客様の場合、「迷惑メール」フォルダに振り分けられている場合がございます。迷惑メールフォルダも合わせてご確認ください。



□ インターネット接続が困難

・利用者サイトへのログインにはインターネット接続が必要です。

・ご利用の端末からWebサイトの閲覧ができるかご確認ください。

なお、以下の**推奨ブラウザ**でアクセスするようお願いします。
・iOS（iPhone、iPad等）の場合：Safari
・Androidの場合：Chrome、FireFox

□ メールアドレスの間違い

□ 届いたが「迷惑メール」扱い

・メールアプリ内の、「迷惑」フォルダーを参照して処理続行

□ そもそも届かず、「迷惑メール」扱い

「迷惑メール受信拒否設定の解消方法」 （次頁）

目次へ戻る

迷惑メール受信拒否設定 の解消方法

【 目的 】

・「なとりコイン」等において、利用者情報の登録や当選メールを、スマホ側で確実に受け取れるように環境設定しておく。（スマホの機種によって、既定値を変える必要あり）

【 具体的対策 】

・自分のスマホの「メール設定」処理で、以下の手続きをする。

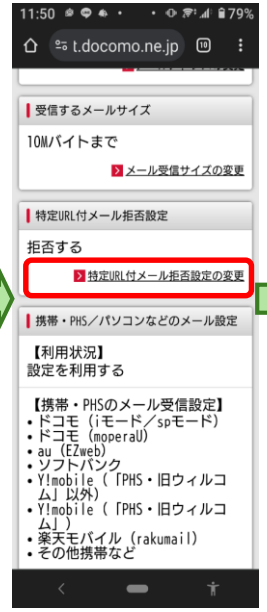
① 特定URL付きメール拒否設定を「拒否しない」に設定する。

② 「@omakase-emoney.jp」ドメインからのメール受信設定。（迷惑メールと間違えられる事の防止）

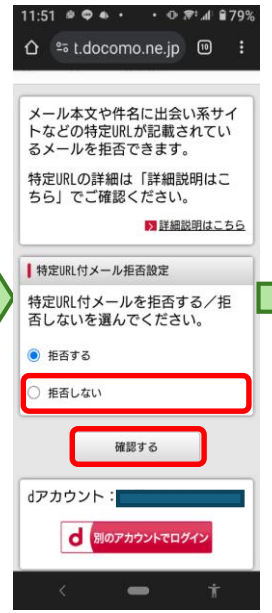
特定URL付きメール拒否設定

メール設定内容の確認

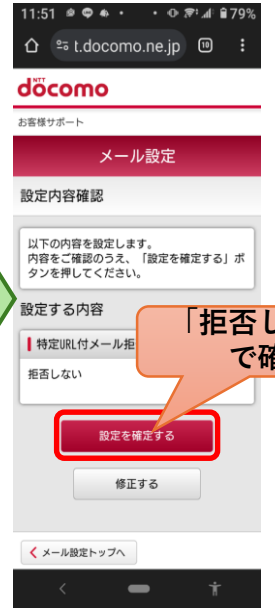
特定URL付メール拒否設定の変更



「拒否しない」選択



「拒否しない」確定

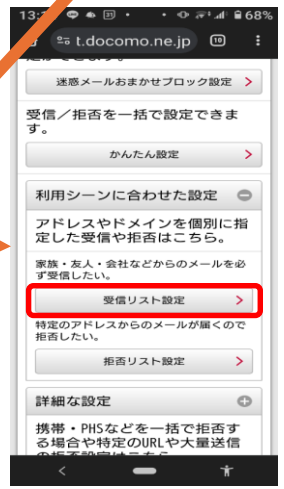


「拒否しない」で確定

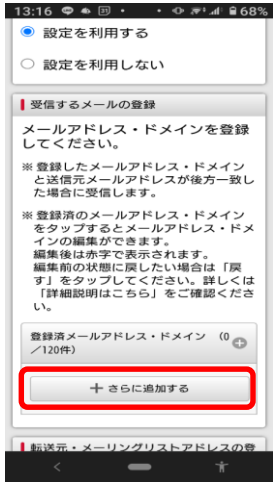
「@omakase-emoney.jp」ドメインからのメール受信設定

ドコモ の場合　→　My docomo

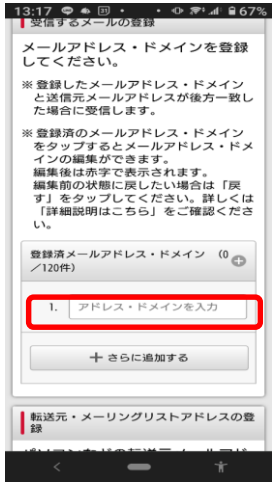
メール各種設定



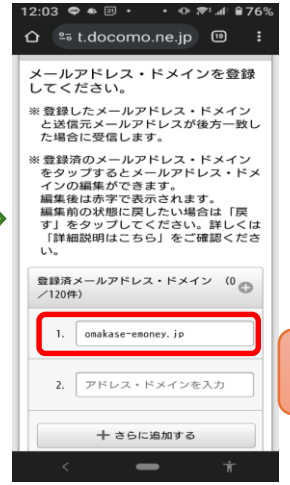
受信リスト設定



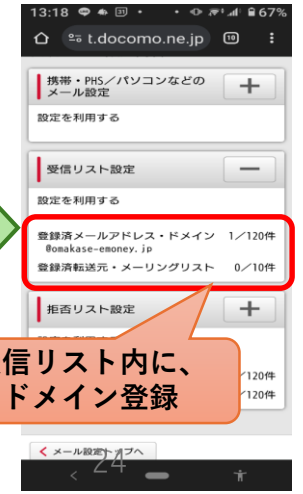
さらに追加する



「@omakase-emoney.jp」を入力



「（画面下にスクロールして）「確認する」



受信リスト内に、ドメイン登録

目次へ戻る

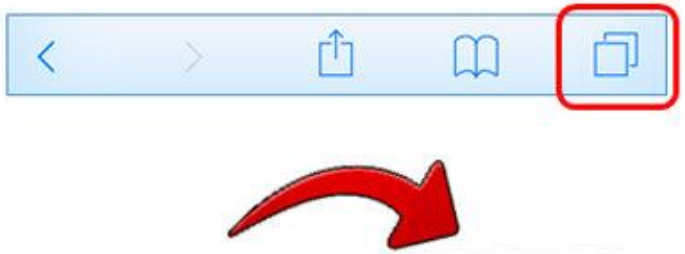
「プライベートブラウズモード」OFF の設定

●ブラウザに、｛閲覧履歴、Cookie、フォームに入力した値｝を保存しない機能。
　ただし、Web上の機能が使えなくなる可能性がある。

● 「ログイン状態を保存」にチェックを入れても、毎回ログオンを求められる　場合の対処

<iPhone/iPad>

⇒プライベートブラウズモードをOFFにして接続を行ってください



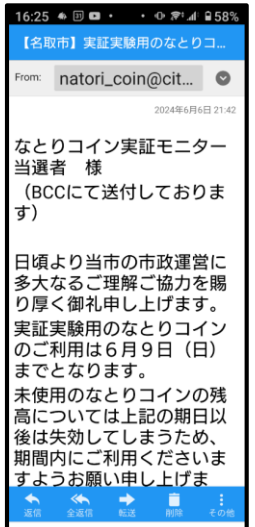
<Androidスマートフォン>

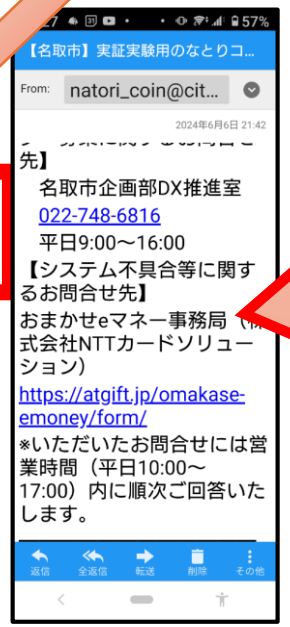
⇒シークレットモードをOFFにして接続を行ってください

シークレット
モード

目次へ戻る

実証モニター通知～ブラウザ接続時に、ＩＤ登録エラー への対応





Yahoo！ブラウザでは
パスワードマネージャーの機能はない

→　この確認画面が表示されない可能性あり

電子メールアドレスは、正しく入れること

ＩＤ、パスワードが不明

ログインID通知＆
パスワード設定申込

●ID、パスワード、電子メールアドレス不明のときは、なとりコインの利用者登録からやり直す。
→
「ログインＩＤ およびパスワードを忘れた方」
を選択

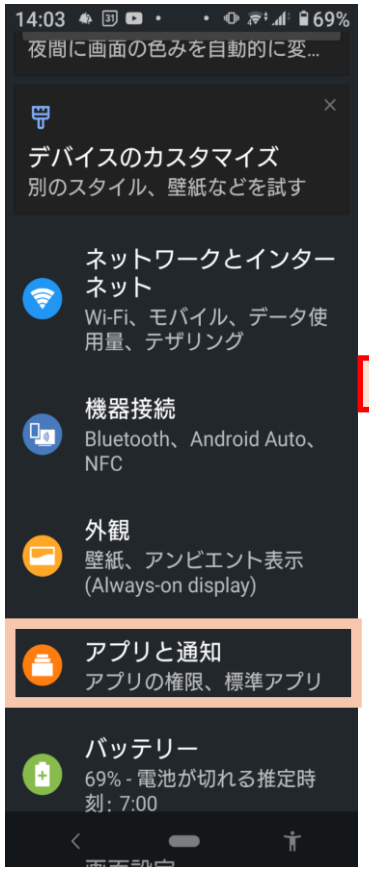
ID登録完了

目次へ戻る

Webブラウザの既定値を、Chrome に設定する方法

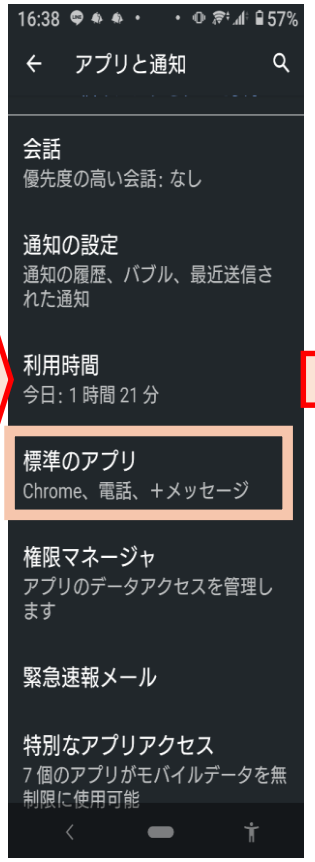
・**設定アプリから「アプリケーション」を選択し、「ブラウザアプリ」を選択**します。

・標準にしたいアプリを選択して、
「**デフォルトアプリの設定**」から
ブラウザを選択します。

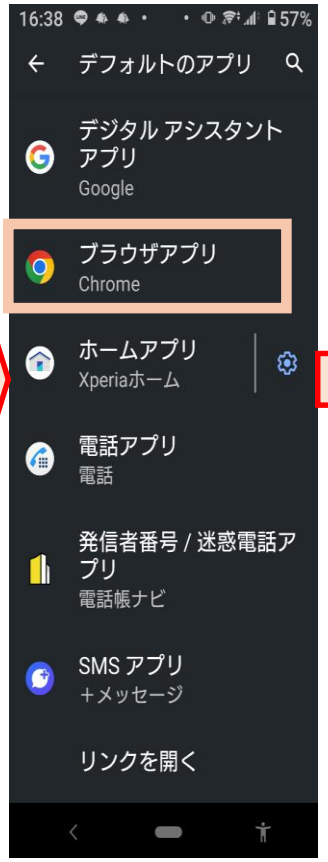


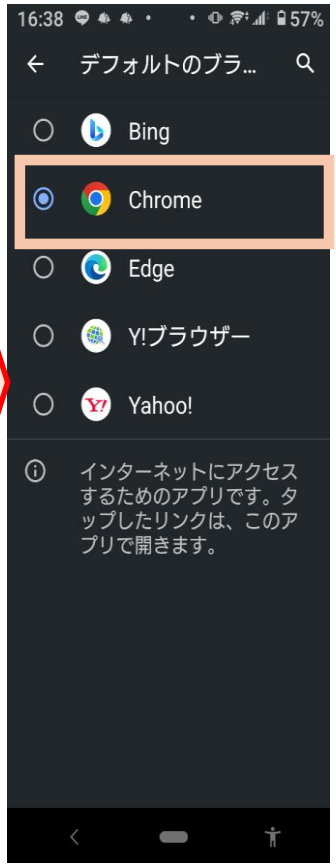
・**設定アプリを開き、スクロールして、「アプリと通知」を呼び出す。**

「**詳細設定**」を選択



「**標準のアプリ**」-「**ブラウザアプリ**」を選択





・**デフォルト（既定値）のブラウザとして、「Chrpme」を選択**

目次へ戻る

Webブラウザで、専用サイトが正常に起動しない

（次の画面へ遷移しない、カメラが起動しない　等）

●専用サイトへのアクセスにはインターネット環境が必要です。

ご利用の端末からWEBサイトの閲覧が可能か確認下さい。

なお、以下の推奨環境での利用をお願いします。

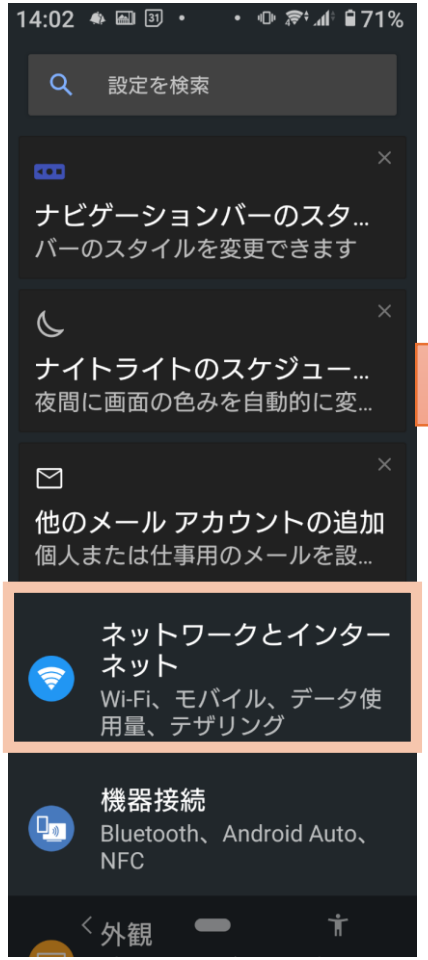
【推奨環境】

＜ブラウザ＞

・Androidの場合：Chrome、Firefox

・iOS（iPhone、iPad等）の場合：Safari

＜OS＞　・最新バージョン



ネット環境の確認

【設定】-【ネットワークとインターネット】

目次へ戻る

Chromeのインストール方法

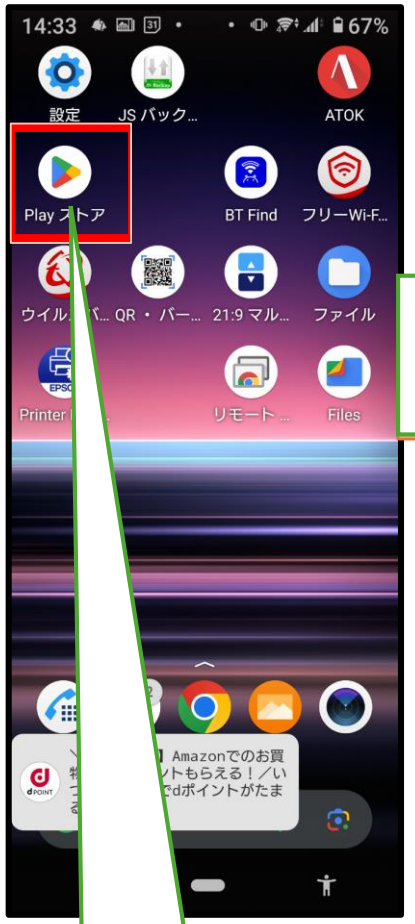
【 Chromeのインストール方法 】

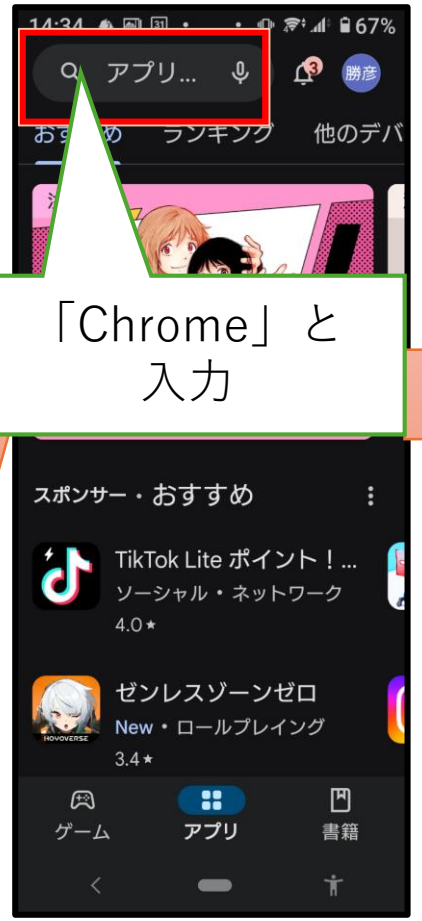
＜Android端末＞

1. Android端末（スマホやタブレット）でGoogle PlayのChromeのページへ移動
2.「インストール」→「同意」をタップ

＜iOS端末（iPhone、iPad）＞

1. iOS端末（iPhone、iPad）でApp StoreのChromeのページへ移動
2.「入手」→「インストール」をタップ
3. Apple IDのパスワードを入力して「OK」をタップ





「Chrome」と入力

「Playストア」をクリック

・「Chrome」でヒットしたアプリが表示される。
・今回、下側の「Google Chrome」を選択して、「インストール」する

目次へ戻る

※　QRコード や カメラ読み取り時のトラブル対処　（Android 端末）

●専用サイトにて、「QRコード読み取り」を押したがカメラが起動しない

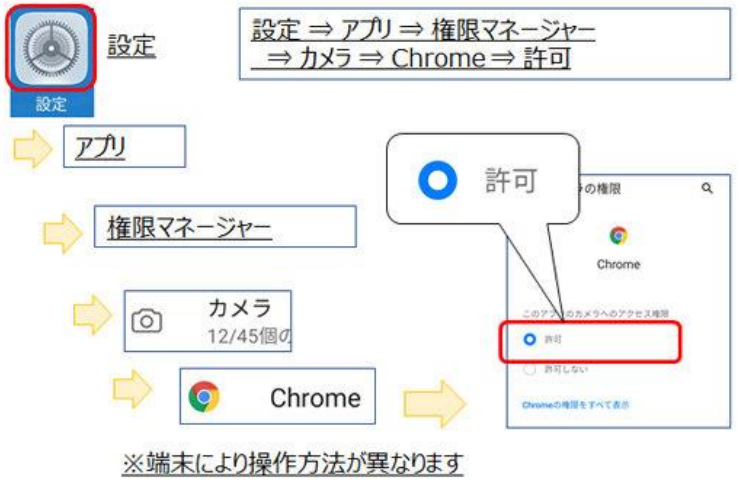
＜Android端末＞
「このサイトを利用するには、Chromeでカメラとマイクの使用を許可する必要があります」→「続行」
→「Chromeに写真の撮影と動画の記録を許可しますか？」
→「許可」

※OSやブラウザのバージョンにより動作が異なる場合があります。
ブラウザからカメラの利用が許可されていない場合、または上記メッセージで許可をしなかった場合（Androidでは「ブロック」とした場合）は設定の以下の変更が必要です。

■「Chrome起動」→「設定」→「サイトの設定」→「カメラ」
※OSやブラウザのバージョンにより動作が異なる場合があります。

＜Android端末のイメージ＞

▽設定を変更してもカメラが起動しない
⇒権限マネージャでカメラの許可を設定してください



※端末により操作方法が異なります

目次へ戻る

※　QRコード や カメラ読み取り時のトラブル対処　（ＩＯＳ端末）

●専用サイトにて「QRコード読み取り」を押したが、カメラが起動しない
→
ご利用のブラウザがカメラアプリ利用の設定ができていない可能性があります。

「コード（ID）の登録」をタップした後に表示される**カメラアプリへのアクセス許可**を設定してください。

＜iOS端末（iPhone、iPad等）＞
「omakase-emoney.jpがカメラへのアクセスを求めています→「許可」

■「設定」→「Safari」→「カメラ」もしくは「カメラとマイクのアクセス」

＜iOS端末のイメージ＞

目次へ戻る

※ブラウザからカメラの利用許可に関する設定変更

＜Android端末＞

・「Chrome起動」→「設定」→「サイトの設定」→「カメラ」

※OSやブラウザのバージョンにより動作が異なる場合があります。

●ブラウザでのカメラアプリ設定で、利用が許可されていない可能性があります。
カメラアプリへのアクセス許可を設定してください。

●サイトにカメラの使用を許可する前に確認するをON（右側）

Chrome起動

Chrome 内の 設定画面

サイトの設定 – カメラ 設定

※　QRコード や カメラ読み取り時のトラブル対処

●らくらくスマホ で カメラが起動しない

→

・「らくらくスマホ」の「インターネット」から起動する標準ブラウザでは、QRコード読取の際にカメラが起動しないケースがあります。

メニューの「Google」から「Chrome」でご利用をお願いいたします。

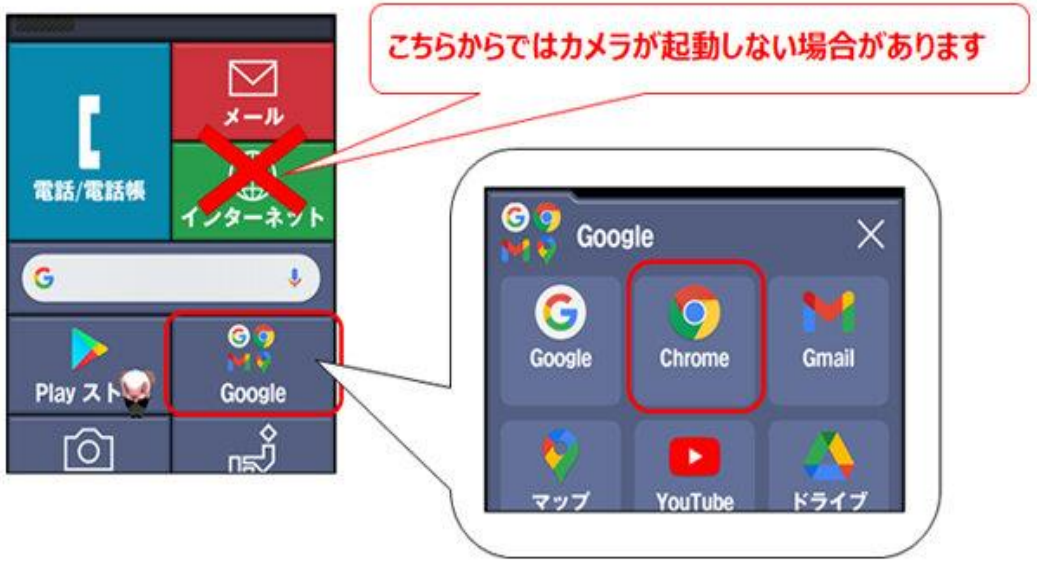
なおChromeでは、Chromeにカメラの使用許可設定が必要になります。

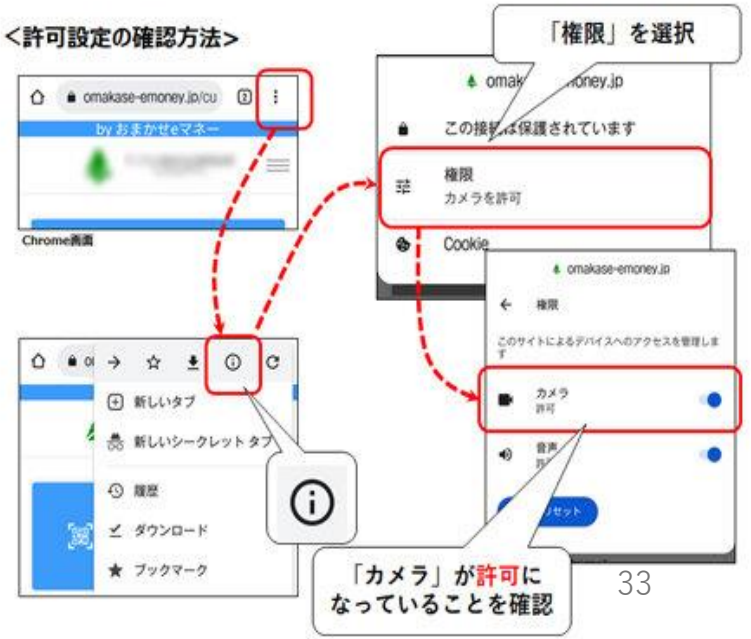
・最初にカメラを利用する際に確認メッセージが表示されますので、必ず「許可」を選択してください。

許可設定後はChromeの画面から確認ができます。

※また「保存領域不足」「バッテリー不足」の際は動作が不安定になり、正常に設定されたChromeでもカメラが起動しない場合があります。

＜iOS端末（iPhone、iPad等）＞
「omakase-emoney.jpがカメラへのアクセスを求めています→　「許可」





●QRコードを読み取ると再生のマーク（黒い三角）が表示される

→

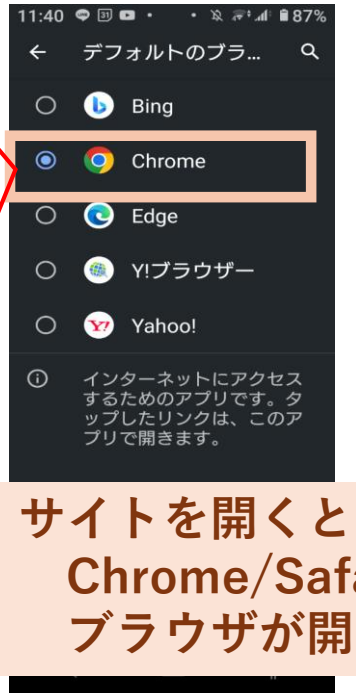
・Android 端末では、「Chrome」以外のブラウザを利用している場合、（IOS では Safari 以外）、機種によっては、QRコード読み取り時にカメラが起動しない場合があります。

・スマホの設定で、「デフォルトのブラウザ」を「Chrome」または「Safari」に設定してご利用下さい。

<Yahooブラウザご利用イメージ：ご利用者サイト例>

カメラが起動されず、黒い▲が表示

・「設定」-「詳細設定」-「標準のアプリ」-「ブラウザアプリ」-「デフォルトのブラウザ」から「Chrome」を選択する



サイトを開くと Chrome/Safari以外のブラウザが開いてしまう

●QRコードにピントが合わず読み取れない

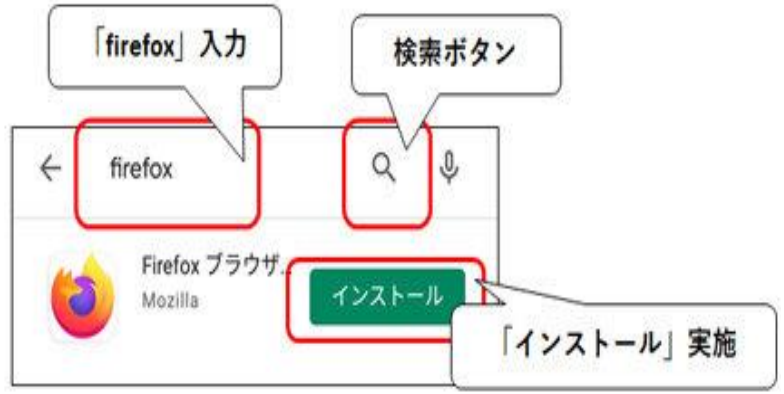
→

「Xperia5」や、OSに「Android GoEdition」を使用している**一部のスマートフォンで、Chromeを使ったQRコード読取ができない事象**が確認されています。

・ブラウザ「Firefox」を利用する事で対処できるケースが多くみられるため、当該のスマートフォンをご利用の方は「Firefox」でのご利用をお試しください。

<Firefoxのインストール>

①「Playストア」を起動



②「firefox」を検索　②「Firefox」をインストール

目次へ戻る

● QRコードが読み取れない （ iPhone13 Pro/Pro Max）

・iPhoneの自動マクロ撮影の設定により、QRコードが読み取れない場合があります。

→

・iOSを15.1以上にアップデートし、自動マクロ撮影の機能をOFF（無効）にしてください。

目次へ戻る

6. 安心して利用するために

1.アカウントの乗っ取りに注意

・ ネット上の生活を便利にするさまざまなサービス
SNSやWebメール、ネットショッピング・・・

・万一、ID／パスワードが何らかの理由で流出した場合、なりすましで勝手にサービスにログインされ、被害を被る可能性があります。

2.アカウントを乗っ取る代表的な手口

■ フィッシング詐欺■　　アカウントリスト攻撃
■ スパムアプリ

3.ＩＤ、パスワードの 危険性と対策

■他人に知られた場合の危険
- □ 銀行口座からの勝手な引き出し
- □ プライバシー情報の漏洩
- □ ネット犯罪への片棒

■対策
- □他の人に教えない　□ 忘れないようメモ
- 安易に、不審なアプリをインストールしない

4. 5つの有効なアカウント管理術

- □ 複雑なID／パスワードを設定する
- □ パスワードを使い回さない
- □ ネットでの情報入力は慎重に
- □ 二段階認証を利用する
- □ 安易にアプリ連携しない

5.パスワードを作るコツ

- □ 自分の名前や電話番号、誕生日などは使わない。
- □ 英大文字小文字、数字、記号交じりで10桁以上
- □ パスワード使い回しはしない
- □ パスワードは半年に1回くらいで変える

6.高齢者が陥りやすい典型的なフィッシング詐欺の手口

- □オレオレ詐欺
- □ 還付金詐欺
- □ 架空請求詐欺
- □ 宅配便を使った詐欺

目次へ戻る

6. 安心して利用するために

7.だまされないための10のポイント

1. 自信過剰は危険
2. 手口は「不安をあおってパニックを引き起こす…そして救済するふり」
3. 詐欺師は失敗しても反省せず、さらに巧妙な手口で出てくる
4. 「詐欺師は良い人に見える」
5. 「お金の話」が出たら、相手が誰であろうと、冷静に判断
6. 動揺や不安に注意
7. 家族で電話の対策を話し合い、訓練を行う
8. 迷惑電話防止機能付きの電話機、アプリを活用
9. 「気を付けて」、具体的な対策を実行
10. 家族で合言葉を決めて、詐欺をブロック

8.自分のスマホがマルウエアに汚染されていないか？

- □ スマホの挙動をチェック
- □ アプリ一覧を確認
- □ セキュリティアプリを利用
- □ OSを最新バージョンにアップデート
- □ 怪しいサイトにアクセスしない

9.ＱＲコードとセキュリティリスク

QRコードの使用には常に注意を払うこと

- ■偽装QRコード
- ■マルウェアのダウンロード
- ■不正な支払いリクエスト
- ■プライバシー侵害
- ■無許可のURLリダイレクト
- ■公共の場での使用リスク
- ■セキュリティ対策の不十分なアプリ
- ■ユーザーの過信

6.1 アカウントの乗っ取りに注意

- SNSやWebメール、オンラインストレージなど、ネット上には私たちの生活を便利にするさまざまなサービスがあります。

  これらのサービスを利用するにあたっては、

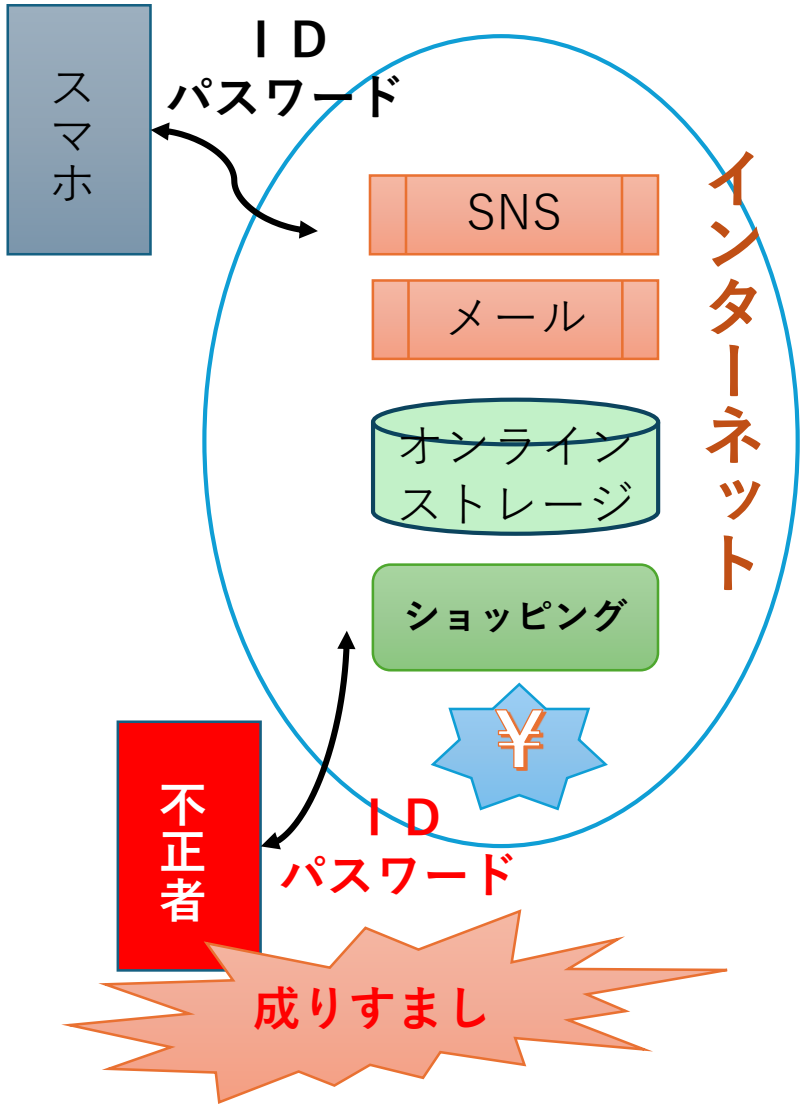
第三者による不正利用を防止する手段として、一般に

ID／パスワードの登録が求められます。

- **ID／パスワードは完璧な認証方法ではありません。**

  万一、ID／パスワードが何らかの理由で流出した場合、ユーザ本人の知らない所で勝手にサービスにログインされ、アカウント（サービスを利用する権利）を不正使用される可能性があります。

- いったんアカウントを乗っ取ると、**本人になりすまして**SNS上で詐欺サイトへ誘導する　投稿をしたり、ネットショッピングで勝手に買い物をしたり、メールを盗み見たりといった**様々なネット犯罪が可能になる**のです。



6.2 アカウントを乗っ取る代表的な手口

●フィッシング詐欺

✓サイバー犯罪者がID／パスワードを盗み出す際によく用いる

✓実在するサービスをかたって**本物そっくりの不正サイトにユーザを誘い込み**、そこで入力させたID／パスワードを盗み出す

●アカウントリスト攻撃

✓ネット上の複数のサービスで**同じID／パスワードを使い回し**ていると、アカウント乗っ取りの被害を広げてしまう可能性あり

✓何らかの方法で不正に入手したあるサービスのID／パスワードの組み合わせで他の複数のサービスへの不正ログインも試みる

●スパムアプリ

✓SNS上の投稿の多くは、アプリ連携の承認ページへ誘い込み、**承認ボタンを押したユーザのアカウントを乗っ取る**

✓**悪質なメッセージの送信や投稿を行われたりする可能性がある**

目次へ戻る

6.3 ＩＤ、パスワードの 危険性と対策

- **他人に知られた場合、こんな危険が想定されます。**
  - 本人のなりすましで、銀行口座からの勝手な引き出し
  - （例：　プロ野球の大谷選手の口座から、側近者が勝手にギャンブル用に引き出し）
  - プライバシー情報の漏洩
  - ネット犯罪への片棒

●多段階認証とは

・サービスへのログイン時にID／パスワードの入力に加え、利用者本人しか知り得ない情報の入力を追加で求めることにより、認証の精度を高める。

例：☐ PINコード　☐ 指紋や顔認証
　　☐ 秘密の質問

- **対策**
  - 他の人に教えない
  - アプリごとにＩＤやパスワードを使い分ける
  - 自分でも、忘れないようにメモしておく
  - 2段階認証で、もし他人に漏れたとしても、実害が少なくなるようにする
  - 自分の端末が乗っ取られないように、セキュリティ対策用のアプリを入れておく。
  - 安易に、不審なアプリをインストールしない。

6.4 5つの有効なアカウント管理術

1. **複雑なID／パスワードを設定する**
   - 英大文字小文字、数字、記号交じりで10桁以上が理想的
   - 自分の名前や電話番号などは類推されるので使わない
   - パスワードは知らぬ間に漏れていることもあるので、半年に1回くらいで変える

2. **パスワードを使い回さない**
   - サービスごとに異なるID／パスワードを設定する
   - ID／パスワードの組み合わせをいくつも覚えられない方は、パスワード管理ソフトを使うか、手帳に記録する

3. **ネットでの情報入力は慎重に**
   - ネットでの情報入力、特に「アカウント情報の更新をしてください」といった要求　や、いつもより多くの情報入力を求められたときは、フィッシング詐欺の可能性あり。少しでも不安を覚えたら入力をやめ、電話など別の手段で確認する

目次へ戻る

4. 多段階認証を利用する

- サービスへのログイン時にID／パスワードの入力に加え、利用者本人しか知り得ない情報の入力を追加で求めることにより、認証の精度を高める

5. 安易にアプリ連携しない

- アプリ連携の承認ページでは、アプリに許可する権限の一覧を必ず確認し、危険を冒してもそのアプリを利用する必要があるかどうか慎重になる

※多段階認証

・パスワードとワンタイムパスワードを使う方法がよく採用され ている。
（他、 PINコード、 指紋や顔認証、 秘密の質問　など）

①　あるサービスにログイン　→　ユーザーIDとパスワードを入力
②　あらかじめ登録されている電話番号に対して、一定時間だけ有効な数字列（ワンタイムパスワード）がサービスからSMS（ショートメッセージサービス）などで送られる。
③　このワンタイムパスワードを入力すると、サービスにログインできる。
★パスワードを知っていて、なおかつ電話番号を登録したスマートフォンなどを所持しているユーザーだけがログインできることになる。パスワードを知っているだけでは不十分。

目次へ戻る

6.5 パスワードを作るコツ

- 自分の名前や電話番号、誕生日などは類推されるので使わない。
- 英大文字小文字、数字、記号交じりで10桁以上
- 複数のサービスでのパスワード使い回しはしない
- パスワードは半年に1回くらいで変える

●パスワードの弱体化に注意
　定期的なパスワード更新の際に、パスワードの数字をインクリメントするなどの単純な変換をしない

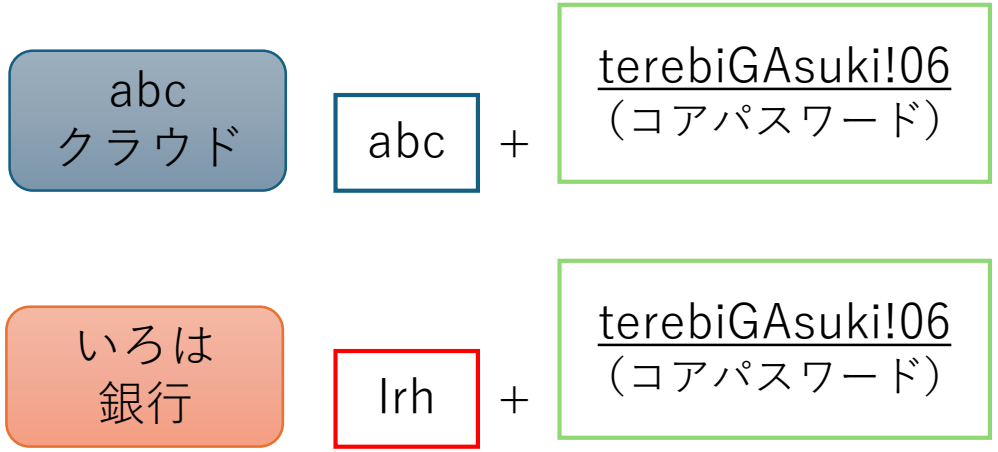
★パスワードをサービスごとに効率よく作り、管理する方法（情報処理推進機構（IPA）が推奨する方法）

1.コアパスワードを作成

① 短い日本語のフレーズ　例）「テレビが好き」
② ローマ字返還「terebigasuki」
③ 一部を大文字にし、末尾に記号・数字を追加
「terebiGAsuki!06」

2.利用サービスごとの識別子をつける

例：
・abcクラウド　→　abc ＋ terebiGAsuki!06
・いろは銀行　→　irh ＋ terebiGAsuki!06



6.6 高齢者が陥りやすい典型的なフィッシング詐欺の手口

1. オレオレ詐欺

- 詐欺師が家族を装い、「トラブルに巻き込まれた」「急にお金が必要になった」と偽って電話をかけ、現金を要求します。

2. 還付金詐欺

- 「過払い金がある」「還付金を受け取れる」と偽り、手数料名目でお金を振り込ませる手口

3. 架空請求詐欺

- 心当たりのないサービス料や商品代金を請求し、支払いを迫る詐欺

4. 宅配便を使った詐欺

- 宅配便のドライバーを装い、現金やキャッシュカードの受け取りを試みる手口

6.7 だまされないための10のポイント

1. 自信過剰は危険

- 「自分に電話なんてかかって来ない」という非現実的楽観主義は注意が必要です。誰でも被害に遭う可能性があります。
- 根拠のない自信過剰は被害に遭うきっかけになります。

2. 手口は「不安をあおってパニックを引き起こす…そして救済するふり」

- 詐欺師は不安を煽り、パニックを引き起こす手法を用います。動揺しているときには相手を信頼しやすくなります。

3. 詐欺師は常に考え「アップデート」

- 詐欺師は失敗しても反省せず、さらに巧妙な手口で出てきます。ずっと人をだますことを考えている詐欺のプロです。

4. 注意点は「詐欺師は良い人に見える」

- 詐欺師は「良い人」に見えることが多いです。外見だけで判断せず、冷静に対応しましょう

目次へ戻る

5. 「お金の話」が出たら意識「全集中」を

- お金に関する話が出たら頭をフル回転させましょう。相手が誰であろうと、冷静に判断することが重要です。

6. 動揺や不安に注意

- 自分がドキドキする、動揺していると感じたら、冷静になりましょう。

7. 「だまされない訓練」を行う

- 家族で電話の対策を話し合い、訓練を行うことが効果的です。

8. 頼れるテクノロジーを活用

- 迷惑電話防止機能付きの電話機を使いましょう。テレビ電話も有効です。

9. 「気を付けて」は意味がない

- 過信は油断となります。具体的な対策を実行しましょう。

10. 家族の絆でSTOP!オレオレ詐欺

- 家族で合言葉を決めて、詐欺をブロックしましょう

目次へ戻る

6.8 自分のスマホがマルウエアに汚染されていないか？

1. **スマホの挙動をチェック**
   - スマホの動作が普段と異なる場合、マルウェア感染を疑うべきです。
2. **アプリ一覧を確認**
   - スマホの設定から「アプリと通知」を選び、「アプリ情報」をタップします。
   - インストールした覚えのないアプリや不審なアプリがないか確認してください。
3. **セキュリティアプリを利用**
   - スマホにセキュリティアプリをインストールしてスキャンを実行することで、マルウェア感染を検出できます。
   - セキュリティアプリは定期的にアップデートし、スマホのセキュリティを強化しましょう。
4. **OSを最新バージョンにアップデート**
   - スマホのOSを最新バージョンにアップデートすることで、セキュリティの脆弱性を修正できます。
5. **怪しいサイトにアクセスしない**
   - 不明なリンクや怪しいサイトにアクセスしないように注意しましょう。

● 具体的な症状

- 動作が重くなる
- バッテリー消費が激しくなる
- データ使用量が増える
- 予期しない動作が頻繁に起こる
- 広告や警告のポップアップが消えない
- 見覚えのないアプリがインストールされている

目次へ戻る

6.9 ＱＲコード　と　セキュリティリスク（1/2）

以下のポイントを理解し、QRコードの使用には常に注意を払うことが重要です。

●偽装QRコード：

悪意のある第三者が正規のQRコードに見せかけた偽のQRコードを作成し、ユーザーをフィッシングサイトに誘導する可能性がある。

●マルウェアのダウンロード：

QRコードをスキャンすることで、ユーザーのデバイスにマルウェアやウイルスがダウンロードされるリスクがある。

●不正な支払いリクエスト：

支払い用のQRコードが改ざんされ、ユーザーが知らないうちに不正な口座にお金を送金してしまうリスクがある。

●プライバシーの侵害：

QRコードに埋め込まれた情報が個人データを含む場合、不正に取得されたり悪用されたりするリスクがある。

6.9 ＱＲコード　と　セキュリティリスク（2/2）

●無許可のURLリダイレクト：

QRコードをスキャンすることで、ユーザーが意図しないURLにリダイレクトされ、セキュリティの脆弱なサイトに誘導される可能性がある。

●公共の場での使用リスク：

公共の場に掲示されたQRコードが改ざんされているリスクがあるため、信頼できるソースからのQRコード以外はスキャンしないことが重要。

●セキュリティ対策の不十分なアプリ：

QRコードリーダーアプリ自体にセキュリティホールがある場合、デバイスが危険にさらされる可能性がある。

●ユーザーの過信：

QRコードは信頼できるものと思い込んでしまい、注意を怠ることでセキュリティリスクが増大する。

目次へ戻る

7.　技術的な参考情報

目次へ戻る

【最新のOS・ファームウェアへの　アップデート方法】

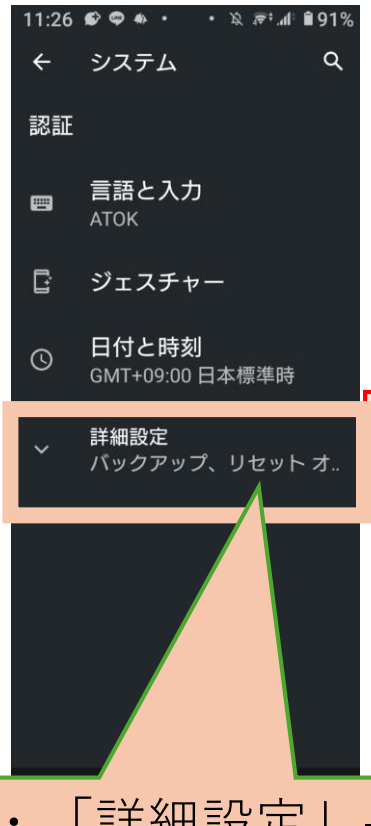
＜Android端末＞

1. スマートフォンの設定アプリをタップします。

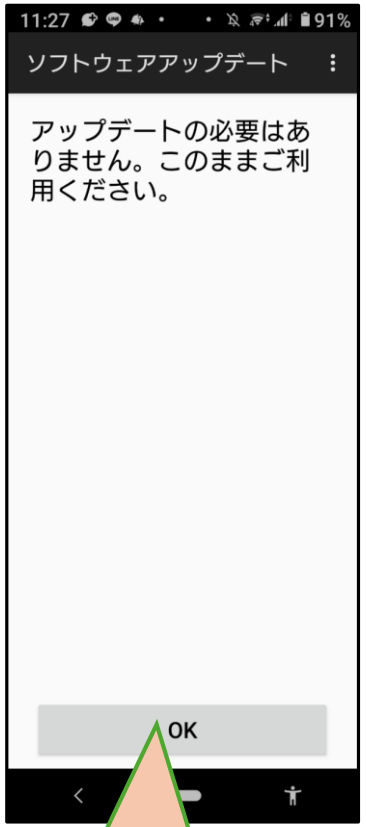
2. 画面下部にある「システム」＞「詳細設定」＞「ソウフトウェア アップデート」をタップします。

3. アップデートのステータスが表示されます。
　画面に表示される手順に沿って操作します。

・「設定」-「システム」



・「詳細設定」-「ソフトウェアアップデート」



・アップデートがある場合には、更新手続きを行う

目次へ戻る

【最新のOS・ファームウェアへの　アップデート方法】

＜iOS端末（iPhone、iPad）＞

1.　デバイスを電源に接続し、
Wi-Fiでインターネットに接続します。

２.「設定」＞「一般」の順に選択し、「ソフトウェア・アップデート」をタップします。

※画面イメージは機種等により異なります。

最新版へのアップデートが必要な通知

・アップデート対象となっていれば、更新されます。

・アップデート対象外の時は、ただ単に、現在のＯＳバージョンを表示するのみ

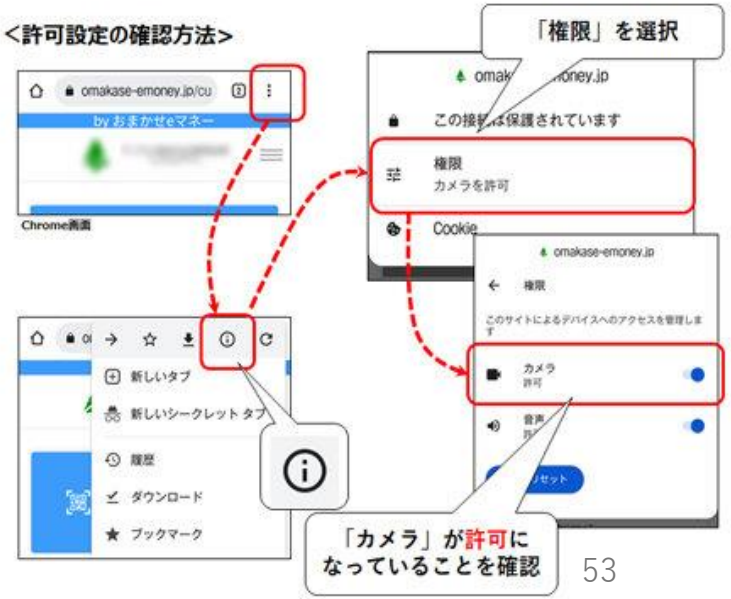
目次へ戻る

保存領域の確認方法（らくらくスマホの場合）

・保存領域については
メニューの「本体設定→その他→保存領域」から「空き容量」から確認が可能です。

少ない場合は空き容量を増やすよう、下記をご検討下さい。

・不要なアプリケーションをアンインストールする
・不要な写真、メール等のデータを削除する



目次へ戻る

保存領域の確認方法（らくらくスマホ以外）

・保存領域については
メニューの「設定→ ストレージ→内部共有ストレージ→ストレージを管理」
から「空き容量」から確認が可能です。

少ない場合は空き容量を増やすよう、下記をご検討下さい。

・不要なアプリケーションをアンインストールする
・不要な写真、メール等のデータを削除する

目次へ戻る

なとりコイン　不正利用の可能性　と対策

なとりコイン 会員情報

■ なとりコインID

□ なとりコイン パスワード

□ 電子メールアドレス
（ワンタイム・パスワード 通知）

・一度登録したログインIDは変更できない
・他の方が既に使用しているものは登録できない
・架空の人物を作り上げて、何人分でも会員IDを生成可能

・フリーメールアドレスを含めて、一人でいくらでも生成可能

電子メール
なとりコイン（実証モニター）
当選のお知らせ
https://omakase-emoney.jp/customer/ap/……

・登録している電子メールアドレスが、フリーメールアドレス（例： Gmail、Yahoo！メール、Outlookメールなど） や、既定値などで「迷惑メール受信拒否」設定されている場合には、
■ メールそのものが届かない か
■ 「迷惑メール フォルダー」に届いている可能性がある。

なとりコイン 会員情報

正常

チャージ用URLコード処理済み または 会員登録異常

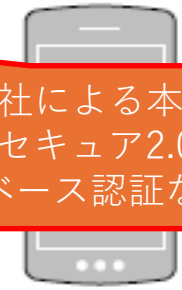
（スマホ上で）
チャージ処理 / コイン利用

チャージ機能

クレジットカードを紛失したら、すぐにカード会社に通報

自分で作り上げた「架空人物のID、パスワード」

カード会社による本人認証
{3Dセキュア2.0、リスクベース認証など}



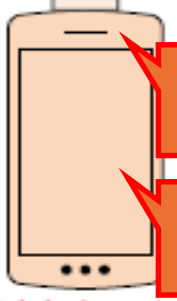
犯人のスマホ

他人のID、パスワード入力による なりすまし

ID、パスワードを漏らさない

犯人のスマホ

盗難



ロック設定

リモートロック

盗まれたスマホ

SIMスワッピング による なりすまし

犯人のスマホ

販売店側で、新機種乗換時に、本人確認を厳しくする

目次へ戻る

スマホの不正利用を防ぐために

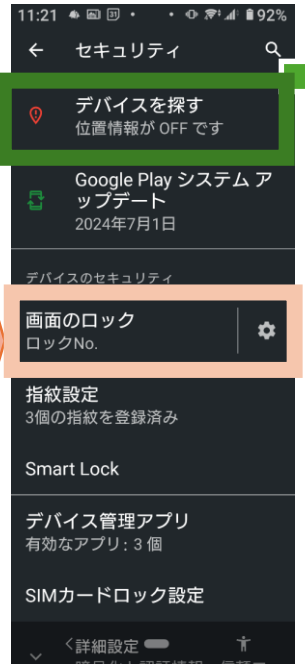
●盗難にあっても、実害を少なくするために

□　スマホ本体のセキュリティ設定で、本人固有の情報や、秘密のパスワード設定で、ロックがかかるようにしておく

□　「デバイスを探す」機能をＯＮにする。
（ただし、バッテリーの消費が早くなる）

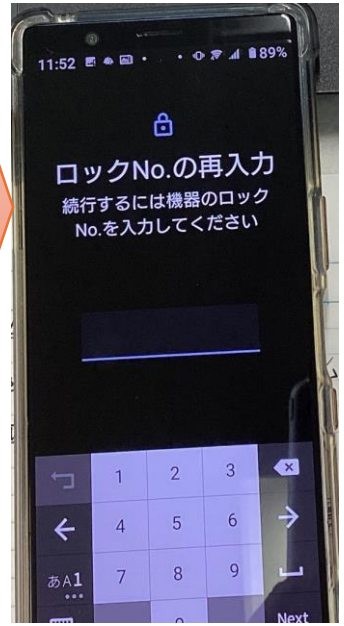
［設定］をクリック

［セキュリティ］をクリック



［画面のロック］

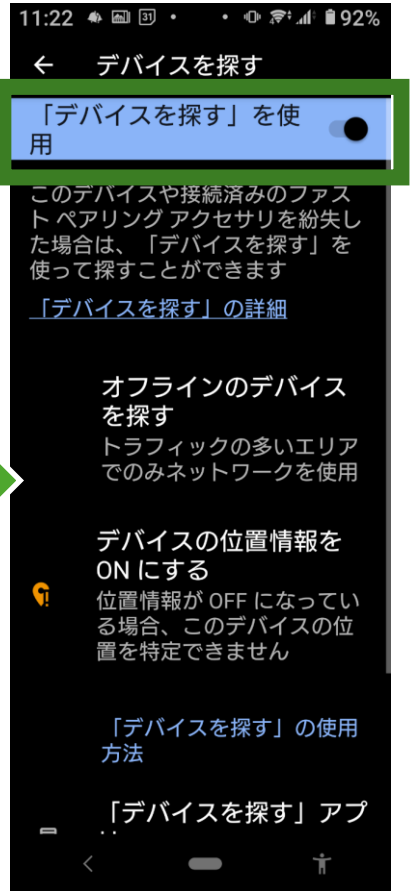
デバイスを探す設定



ロック用数字4桁を入力

画面消灯

画面にロックがかかっている状態



・例えば、パソコンやタブレット等の他のデバイスから、紛失したAndroidデバイスとの通信により、紛失したスマホの位置を確認したり、リモートでロックすることが出来る。

・画面消灯や電源オフなどで、画面がロックされた場合には、先に指定した数字4桁を正しく入力することで、ロック解除される

目次へ戻る

クレジットカードからチャージできない場合の対応について

クレジットカードからなとりコインをチャージする際に「お支払い手続きに失敗しました。」というエラー画面が表示され、チャージできない事象が発生することがあります。

※**各クレジットカード会社のセキュリティ上の理由**等により
決済が完了しないために発生
（カード所有者の成りすまし防止のため、本人確認を求める）

●エラー画面が表示された際は、大変お手数ですが、
ご利用されているクレジットカード会社に
ご本人からお問い合わせをお願いいたします。

また、お問い合わせの際には以下の事項をお伝えください。

1. **利用した店舗等→「おまかせeマネー」※**
2. **利用日時**
3. **利用金額（チャージしようとした金額）**

※**「なとりコイン」ではなく、「おまかせeマネー」と**
お伝えください。

目次へ戻る

3D セキュア Ver.2.0 について

●3D セキュア Ver.2.0 （正式名称：EMV 3Dセキュア）とは

・オンラインショッピングにおけるクレジットカードの不正利用を防ぐための本人認証システムです。

・3Dセキュア2.0は、従来のバージョンに比べて以下の点で優れています

■　**ユーザー体験の向上**
認証方法が多様化し、よりスムーズな認証が可能です。

■　**リスクベース認証**
トランザクションの**リスクレベルに応じて認証の厳しさを調整**するため、低リスクの取引では簡単な認証、高リスクの取引では厳格な認証が行われます。

■　**高度なセキュリティ**
生体認証（指紋や顔認証）やワンタイムパスワード（OTP）を使用することで、不正利用のリスクを大幅に減少させます。

■　**柔軟性**
モバイルデバイスやアプリを利用した認証が可能です。

■　**コンプライアンス**
3Dセキュア2.0は、**最新の規制や業界標準に準拠**しており、将来的な規制変更にも対応しやすいです。

3Dセキュア Ver.2.0 の留意点

●日本では、3Dセキュア Ver.2.0の導入が**2025年4月1日までに義務化**されている。
（すべてのＥＣ加盟店が対象）

● 事業者は、ネットショップで3Dセキュアに対応する必要がある。

●**カード名義人もクレジットカード会社の専用ページなどで設定手続きをしなければいけない。**
（設定が済んでいるクレジットカードによる決済だけが3Dセキュアの対象となる。）

各カード会社の取組状況（令和6年 状況）

■VISA：　2021年10月から3Dセキュア2.0を導入

■ Mastercard：　2022年10月から対応開始

■JCB：　2022年後半から2023年にかけて移行

■American Express:　2022年10月から対応

■SAISON：
・3Dセキュアの自動登録～2021年頃から開始
・ワンタイムパスワード認証～2022年から本格的に導入
・対応ブランド: 各カードブランド（VISA、Mastercard、JCB、American Express）に対する対応は、2022年から2023年にかけて順次進行

目次へ戻る

3Dセキュア2.0 の動作の仕組み

●なとりコインに、クレジットカードからチャージ（入金）することは、オンライン上でクレジットカード決済を利用し、物品を購入することと同義とみなされます。

●**カード名義人は、クレジットカード会社の専用ページなどで設定手続きをしておかないと、本人認証でエラーとなる**ことが予想されます。（Ver.2 になって、モバイルデバイスやアプリを利用した認証が可能となった。）

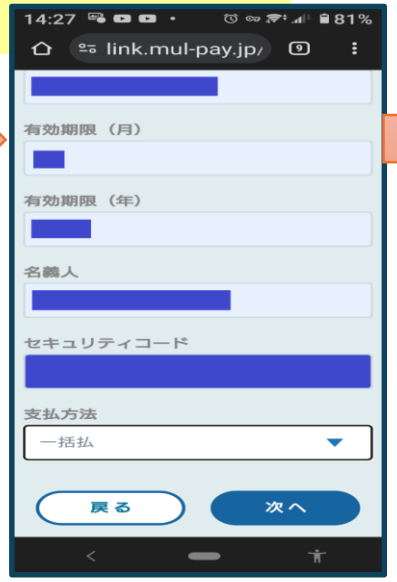
●カード情報を入力すると、カード会社により、自動でリスクベース認証が行われます。

●3Dセキュア2.0では、使っているデバイスの情報、アクセスしている時間や地域、お客様の行動パターンなどを確認し、直近で高額な決済はされていないか、短期間で複数回決済が行われていないかなどで、リスクレベルを判断しています。

●認証リクエスト:
購入情報がカード発行会社に送信され、認証が必要かどうか判断されます。

チャージの指示

クレジットカード情報の登録



決済のリスクを検出

リスク低
追加認証なし

リスク（中・高）
追加認証
（ワンタイムパスワードまたは生体認証）

認証成功

認証失敗

※認証エラーで、どうしてもらちが開かない時には、本人が直接クレジットカード会社に電話で確認をする等が必要となります。

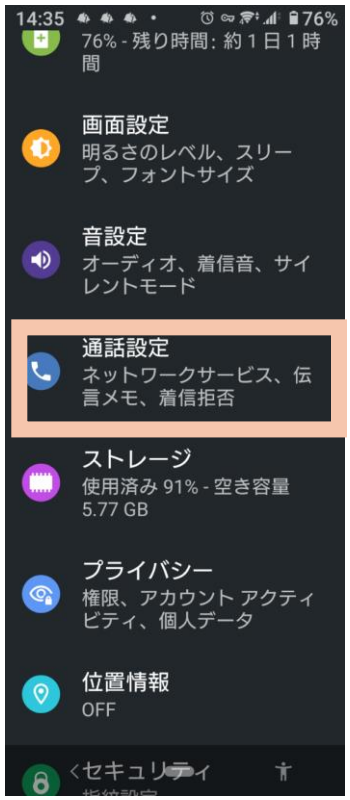
目次へ戻る

迷惑電話解消の方法

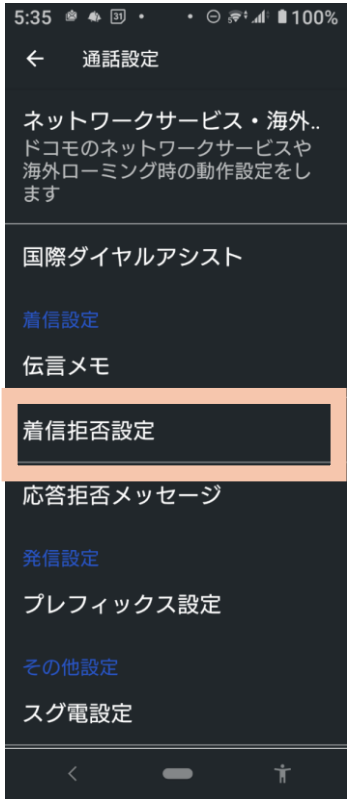
●スマホ側の設定で、着信拒否設定を行うことができます。

- □ **電話帳登録外**
  - **・電話帳に登録していない番号からの着信を拒否**
- □ **非通知**
- □ **公衆電話**
- □ **通知不可能**
  - **・電話番号を通知不可能な着信を拒否**
- □ **番号を追加**

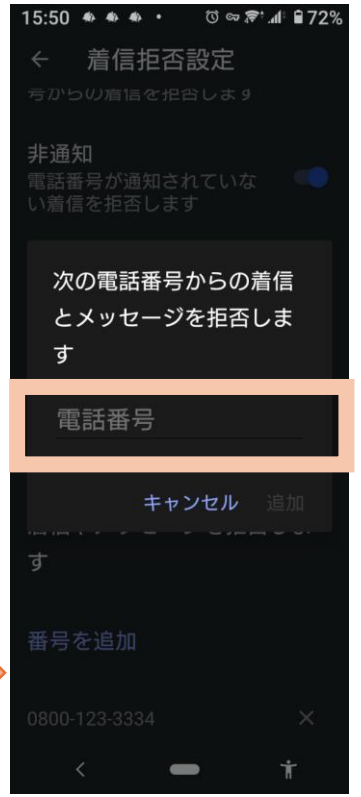
［設定］をクリック



［通話設定］をクリック



「着信拒否設定」をクリック



「番号を追加」の場合、拒否する電話番号を登録

●機種固有の設定以外に、迷惑電話を拒否するアプリはいろいろと出回っています。

例：
□ Whoscall
□ 電話帳ナビ
□ Call Blocker など

どのアプリが自分に合っているか調べてみると良いと思います。

目次へ戻る

スマートフォンのサービス期間について

・スマートフォンのサービス期間とは、
主にOS（オペレーティングシステム）や
アプリのサポート期間を指します。

・サポートが終了したOSを使い続けると、セキュリティリスクが高まるため、新しいスマホへの買い替えを検討することが推奨されます。

・最新OSがサポートされる期間は、メーカーによって異なります。
iPhoneのOSサポート期間は約5年間、
Androidスマホのサポート期間は約2～4年間です。

・**Android 9** はリリース日 が**2018年8月** ▶ **2022年1月**サポート終了
・**Android 10** はリリース日が**2019年9月** ▶ **2023年2月** サポート終了
・**Android 11** はリリース日が**2020年9月** ▶ **2024年2月** サポート終了

●よく「バッテリー」がスマホの寿命だということが挙げられますが、**OS サポートの有無もスマホの寿命を決める重要な要因**です。

【 サポート期間終了によるディメリット】

■　最新機能が使えなくなる
■　非対応アプリが増える
■　セキュリティリスクが高まる

※参考：　代表的なスマホアプリの動作環境

アプリ	iOS	Android
なとりコイン	12.0 以上	6.0 以上
LINE	15.0 以上	8.0 以上
インスタ	14.0 以上	9.0 以上

【 現在の最新ＯＳ（R6.8.20 現在）】

・iOS 17（他 18ベータ版）
・Android 14

終了