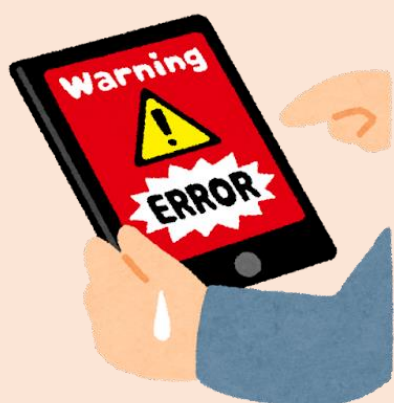


はじめてのスマホ 安心教室



PASSWORD...



2024年

はじめに

スマートフォンは、仕事や生活で欠かせない存在になりつつあります。社会のデジタル化が地球規模で加速しており、インターネットやデジタル技術を使うことで、豊かな社会が実現します。

スマートフォンの場合は、だれでも、安心して安全に操作できることが理想ですが、実際は、基本操作やアプリなどの使い方、どのようなアプリを使ったら良いか、怪しいメールやメッセージなどが氾濫しています。その中で、正しい情報を見つけることは難しい場合が多いです。特に、インターネット検索で調べていると、正しいことでも営利行為による表現が多く、本当の知りたいことがわかりにくいのが現状です。

本書は、スマホを使うっているとさまざま危ないことに経験することを説明し、安心して使えるための資料として作成しました。

今後、このような事例や対処方法などを掲載・紹介して欲しいなどのご要望やご意見は、下記の連絡先までご一報ください。皆様のご意見・ご要望を反映した、なるべく実用的でわかりやすいスマホ操作入門書として公開をしていきます。

ご意見・ご要望の連絡先

〒210-0844 神奈川県川崎市川崎区渡田新町 1-4-9-201

特定非営利活動法人 NPO 福祉支援ゆうやけネット

デジタルボランティア・スマホ講座担当

電話: 044-220-1588 Fax: 044-272-9523

ホームページ <https://yuuyake.or.jp>

電子メール hodota@yuuyake.or.jp



本書の使い方

主に Android 版に対応したスマホ向け教材です。使用したスマホの環境は

- Android 版

Android バージョン 11 使用機種 (モトローラ moto g10)

Android バージョン 13 使用機種 (モトローラ moto g13)



- iOS 版

iOS バージョン 17.2.1 使用機種 (iPhone 11)



目次

はじめに	1
本書の使い方.....	2
用語の説明.....	4
アプリ.....	4
アイコン	4
アラーム.....	4
ホーム画面	4
ロック画面	4
スリープ.....	4
マナー	4
キーパット	5
インストール	5
アンインストール.....	5
ダウンロード	5
デフォルト	5
フォント.....	5
Wi-Fi (ワイファイ)	5
QR コード.....	5
バーコード	5
ホームページ	6
Web サイト.....	6
ブラウザ	6
Bluetooth(ブルートゥース)	6
スクリーンショット.....	6
タップ.....	6
ログイン・サインイン	7
二段階認証	7
SMS (ショートメッセージ)	7
クラウド	7
クラウドサービス.....	7
用語の説明をわかりやすい日本語で	8
アイコンの説明.....	9
動画やサウンド機能などで使うアイコン.....	10
SNS の使い方.....	13
なりすまし、プライバシー、位置情報 (GPS) などに注意しよう	13
SNS でのアカウントなりすまし事例	13
アプリの導入方法.....	14
アプリの導入	14
アプリの削除	14
セキュリティ設定.....	15
LINE の安全な設定	16
QR コードで友達追加.....	16
安全に使う	17
友だちの削除	18
プライバシー管理.....	18

ネットを安心・安全に	20
安心・安全にネット検索するには	20
安心できる情報の見分け方	20
ホームページを見るときに	21
ホームページを見るときのコッキーとは	21
Google アカウントの個人情報の収集	22
2 段階認証について	23
2 段階認証とは	23
Google の 2 段階認証の方法として	23
自分の Google アカウントで他のシステムと連携するために口 グインした場合	24
Yahoo の SMS 認証	25
Dropbox で初めて使うブラウザからログインした場合	25
被害事例	26
迷惑メールとフィルター	26
フィッシング詐欺メール	26
実際に詐欺や被害にあった場合の対処方法	27
「Windows のアップデート」を装う詐欺	27
「ウイルスが見つかりました」を装う詐欺	27
迷惑・詐欺メール	28
詐欺・迷惑メールの事例サンプル	28
ショッピングサイトなどからの詐欺メール	32
Amazon の場合	32
困った時の相談窓口	33
警察	33
迷惑メールや詐欺メールで困ったら	33
消費者相談センター	34

用語の説明

アプリ

スマホで使えるサービスや追加できる機能です。スマホ画面上のアイコンを押すと使えます。地図、ゲーム、カメラ、LINEなどもアプリの1つです

アイコン

アプリや基本設定などの内容を図や絵などでわかりやすく表した、マーク（電話、カメラ、メールなど）を指します。1つ1つがアプリというサービス・機能になっていて、押すと開いて利用できる状態になります

アラーム

特定の時間に音やバイブレータで通知を行う機能のこと

ホーム画面

スマホの待受画面です。ロック解除後に最初に表示される、スマホのベースとなる画面

ロック画面

画面にロックがかかっている状態です。

スマホには、誤動作を防ぐため、およびセキュリティのために、一定時間以上経過するか画面点灯をオフにすると、画面にロックがかかる機能があります

スリープ

画面が消灯している状態です。電源キーを押すと、ロック画面になります

マナー

電車内などで着信音を鳴らさないようにバイブレータの通知にする設定

キーパット

通話中に数字や記号を入力する画面

インストール

スマホにアプリを取り込んで機能を使用できる状態にすること。

アンインストール

アプリを削除して機能を使用できない状態にすることです。

ダウンロード

スマホにアプリやファイル、写真などのデータを取り込んで保存すること。

デフォルト

スマホやパソコンの用語としては、初期設定値になります。

フォント

パソコンやスマホで使う文字の書体デザインのこと。

Wi-Fi (ワイファイ)

自宅や店舗・施設などのインターネット回線（無線 LAN）に接続する機能です。

QRコード

四角い図形のバーコード。カメラや専用アプリで読み込むとサイトにアクセスできる。「QR」は Quick Response の頭字語、高速読み取りを目的の一つとした、バーコードよりも多くの情報（数字だと最大 7,089 文字）を盛り込めるコードです。



Wikipedia

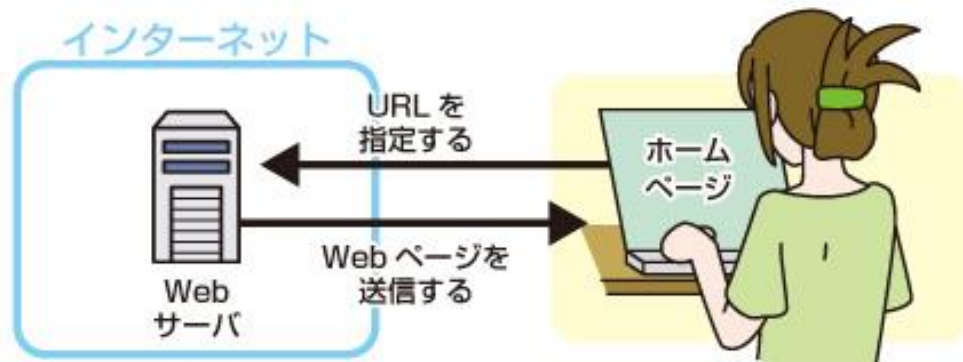
バーコード

縞模様状の線の太さによって数値や文字を表すコードです。



ホームページ

インターネット上で情報を公開する仕組みを、ホームページと言います。ホームページのコンテンツ（内容）は、インターネット上に点在する、Webサーバというホームページ公開専用のコンピュータのなかに保存されています。スマホから、そのスマホに命令を出し、情報を送ってもらうことで、ホームページを見ることができます。



Web サイト

ホームページやそれに類する情報を公開する仕組みを Web サイトともいいます。

ブラウザ

インターネットの情報（ホームページなど）を表示するソフトウェアです。

Bluetooth(ブルートゥース)

無線通信の規格の一つで、スマホや PC などとデジタル機器を繋げるときに使用します。有効範囲は10m以内です。イヤホン、スピーカーなどと接続するとき、接続認識させる方法を「ペアリング」といいます。

スクリーンショット

画面のコピーを撮影する。一般的には PNG ファイルや JPG ファイルの画像データとなります。画面キャプチャーとも言います。

タップ

指先でスマホの画面に触れて操作すること。

ログイン・サインイン

サービスなどを利用するときに、ID 番号とパスワードを使って本人確認すること。

二段階認証

本人確認を2回行う方法です。最初にパスワードなどによって認証し、次に紹介するログイン種類でもう一度認証します。2回目の認証方法は、パスワード、電話番号（携帯の場合はSMS）やメールアドレスに送られるコード、トークン（自動作成システム Google Authenticator やワンタイムパスワードなど）による発行番号、顔や指紋などの生体認証、など多種多様です。

SMS（ショートメッセージ）

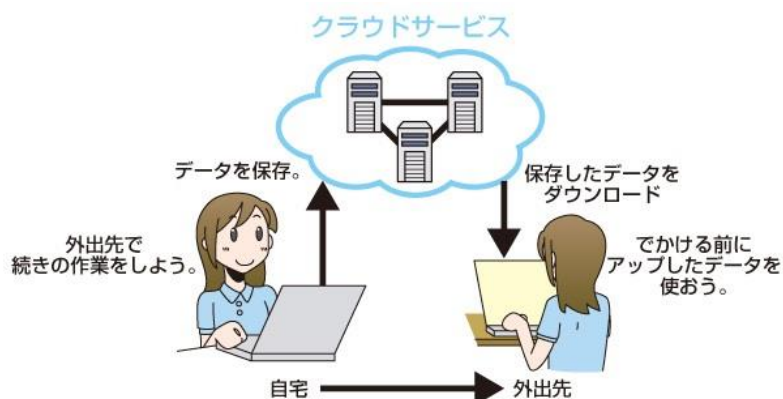
SMS(Short Message Service)は、電話回線を使って携帯の電話番号宛に文字のメッセージを送信するサービスです。全角 670 文字まで送信でき、電話と同じで送信料金がかかります。ドコモはSMS、au はCメール、ソフトバンクはSMS と呼びます。

クラウド

Cloud という英語の雲を意味し、一般的には従来からあるコンピュータデータセンターの機能に、最新の技術により、システム開発者がより使いやすい環境をクラウドと表現しています。

クラウドサービス

従来は利用者が手元のコンピュータで利用していたデータやソフトウェアを、ネットワーク経由で、サービスとして利用者に提供するものです。



用語の説明をわかりやすい日本語で

スマホ初心者で一番多い回答が、説明に英語が多いので理解できない、という話が大変多いです。

IT 専門用語などは、なるべく日本語で説明するようにしましょう。

参考資料 シニア向け IT用語集



https://clasec.sono-sys.net/it_words/

例えば

アップデート 更新 インストール 導入 ドラッグ 指で押したまま移動

バージョンアップ 新しい内容に更新 デフォルト 初期状態

シニア向け 「覚えておきたいスマホに関わる用語とは？」



https://www.soumu.go.jp/use_the_internet_wisely/senior/kisochishiki/4/

上手にネットと付き合おう!
安心・安全なインターネット利用が中心

大 中 小

Google 検索

総務省

未就学児・未就学児の保護者 青少年(U18) 保護者・教職員 シニア インターネットトラブル事例集 特集ページ 動画コンテンツ集 リンク集

第1章
4

覚えておきたいスマホに関わる用語とは？

曖昧なまま使うのはトラブルの原因。このページの用語を再確認しておきましょう。

SMS
「ショートメールサービス」。電話番号を使ってやりとりできる短文メール。

キャリア

無線LAN (Wi-Fi)

SIMカード
電話番号などの契約者情報が記録された小さなカード。

SDカード
写真、動画の他、さまざまなデータが保存できるカード。

アップロード
スマホ → ネット

ダウンロード
ネット → スマホ

アプリ
電話
カメラ
メール
ブラウザ
ゲーム
地図情報
ウイルス対策

OS
iPhoneは「iOS」
それ以外のスマホは「Android OS」

アイコン
画面に並ぶ絵のボタン。タップする(軽たたたく)とそのアプリが起動する。

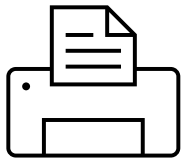
アップデート
スマホのOSや各種アプリを、最新の状態に更新すること。

インストール
アプリなどをスマホに導入すること。

アンインストール
アプリなどをスマホから消去すること。

ホーム画面
スマホのベースとなる画面。この画面に戻すボタンを「ホームボタン」と呼ぶ。

アイコンの説明



プリンター



USB 接続



USB メモリー



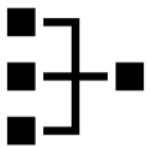
震える状態 シェイク



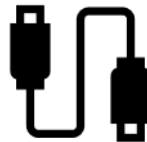
マウス



カメラ



ネットワーク LAN



ケーブル接続



Wi-Fi



Wi-Fi



Wi-Fi



Wi-Fi



クラウド データセンター



クラウドの利用



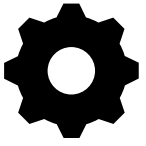
アップロード



ダウンロード



ダウンロード



設定



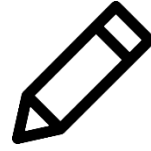
イヤホン



マイク

🔍 アプリを検索

検索



編集



トリミング



iOS



Android

共有

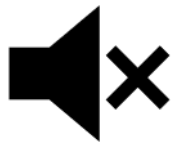


Bluetooth (ブルートゥース)

動画やサウンド機能などで使うアイコン



音あり



音ナシ (ミュート)



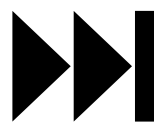
音ナシ (ミュート)



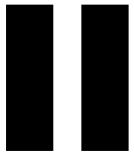
早戻し



再生



早送り



一時停止 (ポーズ)



停止



取り出し



記録



ハンバーガーボタン (選択メニュー)



縦三点リーダー (選択メニュー)



充電中



充電完了 100%



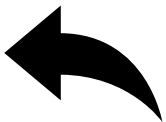
バッテリーが少ない



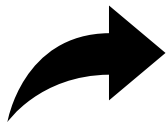
警告



アラーム 警告



戻る



次へ



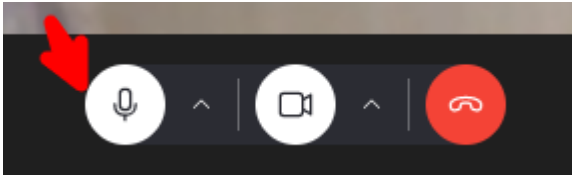
電源



セキュリティ対策のロック



セキュリティ対策のオフ



マイク ビデオカメラ 会議・電話終了 (赤)

なりすまし、プライバシー、位置情報（GPS）などに注意しよう

機種ごとに異なります。詳細はインターネットなどで調べてください。

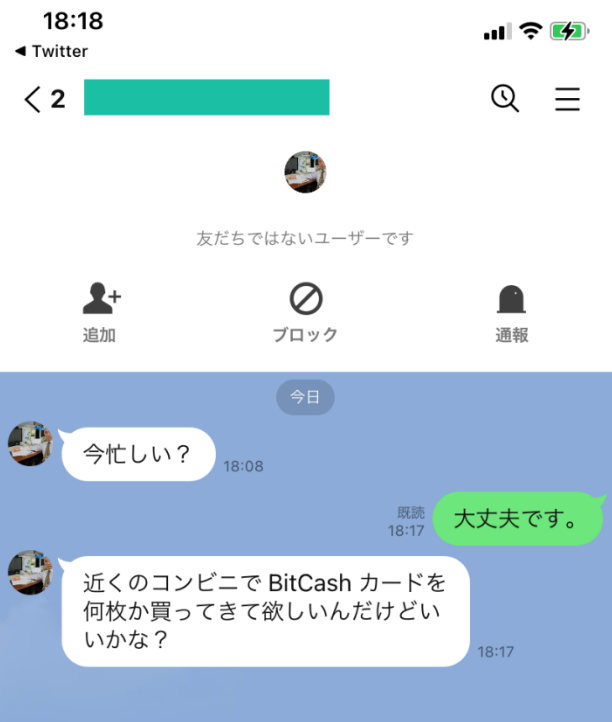
- 世界中が繋がる
- 個人情報を意識する
- 他を意識する
- 相手が見えない
- 新しいことを学ぶ

SNS でのアカウントなりすまし事例

Facebook の友達承認で添付ファイルをクリックして
感染

感染先のパソコンの SNS での友達記録や電話番号を
盗まれて他の SNS で友達になりすまし

LINE での事例



アプリの導入方法

アプリの導入

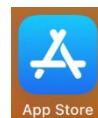
「Paly ストア」や「App Store」でアプリ導入します。インターネットの検索でアプリを探すと、本当のアプリではない別のアプリやアプリの説明などがたくさん出てきます。間違えて別のアプリや記事を見てしまう可能性があるため、必ず、「Paly ストア」や「App Store」でインストールしましょう。



Play スト...

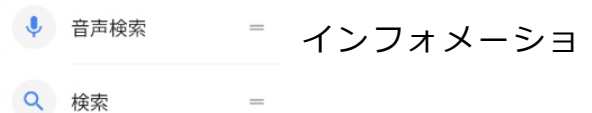
Android に標準でインストールされている「Play ストア」でアプリをダウンロードしてインストールします。

iPhone に標準でインストールされている「App Store」でアプリをダウンロードしてインストールします。



アプリの削除

アプリのアイコンを長押しすると、「アプリ情報」や他のアイコンをクリックします。

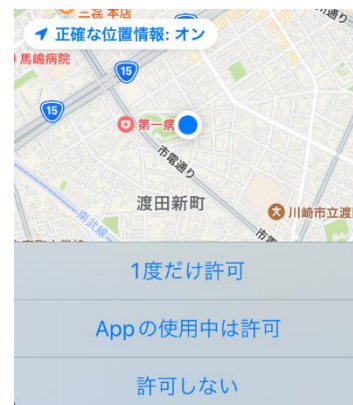


アプリを削除「アンインストール」します。



セキュリティ設定

アプリで使用する GPS、マイク、写真などへのアクセス許可は、「今回限り」「このアプリを使っている時は許可」などを選択します。



アプリの「トラッキング」とは、アプリを使っている時に、ユーザーの行動を追跡して興味のある広告を表示するような仕組みです。

「App にトラッキングしないように要求」を選択しましょう。



LINE の安全な設定

QR コードで友達追加

「LINE ホーム」 > 「友だち追加」をクリック（タップ）



QR コードをクリック



自分の QR コードを友達の LINE でスキャンして友達になります。

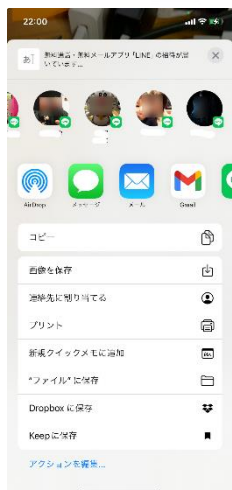
スキャン後は、お互いに友達追加でトーク画面にてメッセージを送信して確認しましょう。



QRコードやリンクを使って、友だち追加しよう。

リンクをコピー シェア 保存

更新



離れた人と友達になるためには、「シェア」をクリックして、自分の QR コードをメールなどで添付送信して、友達になれます。



QRコードやリンクを使って、友だち追加しよう。

リンクをコピー シェア 保存

更新



QRコードやリンクを使って、友だち追加しよう。

リンクをコピー シェア 保存

更新

送信後、友達になれた場合は、自分の QR コードを更新します。送信した QR コードで誰かが友達申請することを防ぐために。

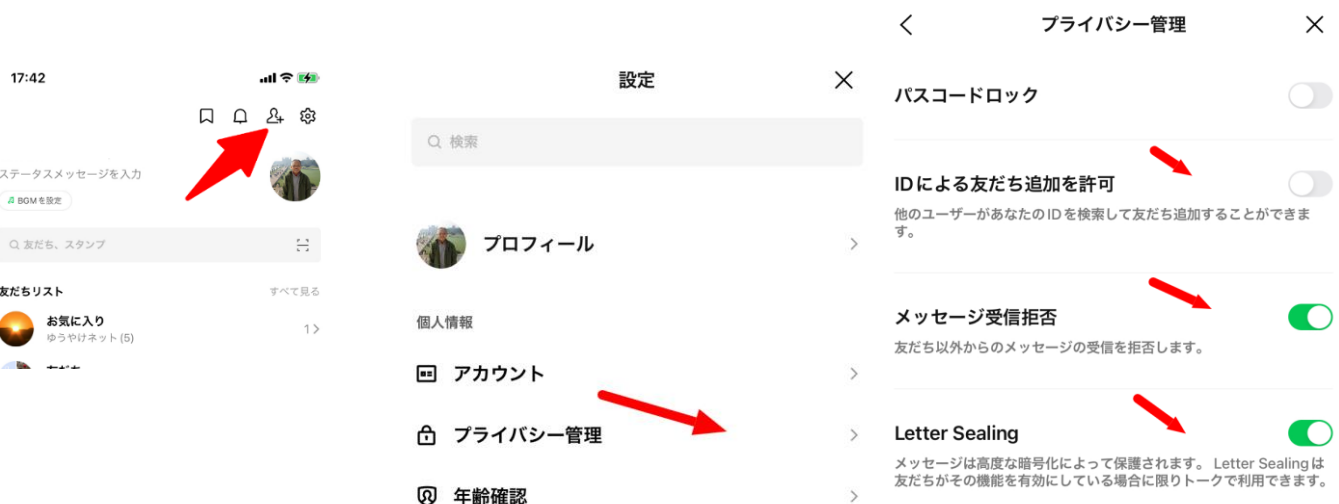
安全に使う

友だちの自動追加はしない 「許可」しない

「LINE ホーム」 → 「友だち追加」



「LINE ホーム」 → 「設定」 → 「プライバシー管理」



友だちの削除

削除したい友達をブロック、または非表示にしてから削除します。

「トーク画面」 -> 「友達アイコン」を長押し -> 「ブロック」または「非表示」を選択



「LINE ホーム画面」 -> 「設定のギアマーク」 -> 「友だち」 -> 「非表示リスト」または「ブロックリスト」を選択 友だちを削除



プライバシー管理

「LINE ホーム」 -> 「設定のギアマーク」 -> 「プライバシー管理」



「プライバシー管理」 → 「アプリからの情報アクセス」

< アプリからの情報アクセス ×

常に許可

お互いに友だちの場合は許可

拒否



あなたを友だちに追加している人が、外部アプリに自身の友だち情報へのアクセスを許可した場合、そのアプリがあなたのプロフィール情報にアクセスすることを許可するかどうかを選択できます。

「プライバシー管理」 → 「情報の提供」

< 情報の提供 ×

コミュニケーション関連情報



オンにすると、LINEでのコミュニケーションに関する情報の一部を取得して、不正利用の防止やサービスの改善などに利用します。友だちとのトーク内容(画像や動画を含む)、通話内容を取得することはありません。
[利用する情報の詳細はこちら](#)

位置情報の取得を許可



オフの場合でも、端末の位置情報を利用した各サービスの機能は利用できます。

[詳細はこちら](#)

「プライバシー管理」 → 「広告の設定」

< 広告の設定 ×

ウェブ行動履歴を利用した追跡型広告の受信



LINE内部識別子を利用した追跡型広告の受信



これらの設定は、お客様の興味関心や属性に基づき最適化された広告を配信するためのものです。設定をオフにすると、お客様に関連性の低い広告が配信されます。

オフにすると、本アカウントで利用している全ての端末に対して最適化された広告の配信を停止しますが、停止の反映に時間がかかる場合があります。

なお、広告識別子を利用した追跡型広告の設定は、OSの設定画面から

ネットを安心・安全に

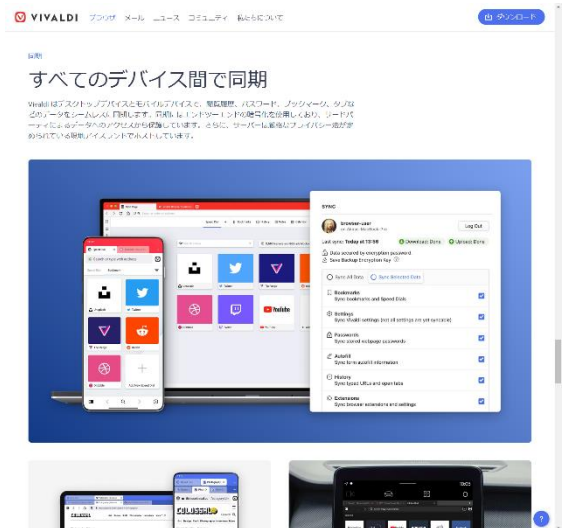
安心・安全にネット検索するには

なるべく安全・安心なスマホアプリを使いましょう。

例えば、インターネット検索では、サイト利用者履歴・追跡管理や広告や宣伝などを拒否できるブラウザを推奨しましょう。

一例として

Vivaldi <https://vivaldi.com/ja/>



安心できる情報の見分け方

スマホ初心者向けには、アプリの紹介やスマホ操作などは、書店で販売している書籍を推奨しています。書籍は出版社側で内容を精査しているのので、安心して正確です。

The screenshot shows the Amazon.co.jp product page for the book "Androidアプリ 厳選 BESTセクション [スマートフォン&タブレット対応] 単行本 (ソフトカバー) - 2020/4/20" by Hiroshi Tanaka and Kenji Asahi. The page includes the Amazon header, navigation menu, and product details. The book is priced at ¥1,848 for the soft cover edition. A promotional banner at the bottom offers a 10% point gift on the first book purchase.

Kindle版 (電子書籍)	単行本 (ソフトカバー)
¥1,811	¥1,848
獲得ポイント: 55pt	獲得ポイント: 56pt

今すぐお読みいただけます: 無料アプリ

プロモーション情報 【クリスマス おもちゃ大セール】 1件

はじめての本の購入で10%ポイントプレゼント、エントリーはこちら

この1冊で最新のAndroidアプリがわかる!

Androidスマートフォン/タブレットの「使える」アプリをまとめて紹介した書籍です。話題のアプリや定番のアプリなど、目的別に、数多くのアプリを用意しています。Androidアプリを使いこなしたい人、アプリの数が多すぎて何をインストールしたらよいかかわからないという人にオススメです。A5サイズにリニューアルして、文字や画面が見やすくなりました。アプリもより厳選したものを紹介しています。

ホームページを見るときに

ホームページを見るときのコッキーとは

EU 一般データ保護規則（GDPR : General Data Protection Regulation）とは

個人データ保護やその取り扱いについて詳細に定められた EU 域内の各国に適用される法令のことで、2018 年 5 月 25 日に施行されました。

主な内容

- ・個人データの処理、移転（別のサービスでの再利用など）に関する原則
- ・本人が自身の個人データに関して有する権利
- ・個人データの管理者や処理者が負う義務
- ・監督機関設置の規定
- ・障害発生時のデータの救済と管理者および処理者への罰則
- ・個人データの保護と表現の自由 など

Cookie(クッキー)などで得られる個人データの処理も対象

例えば <https://www.nikkei.com>



The screenshot shows the homepage of the Nikkei website. At the top, there is a navigation bar with the title "日本経済新聞" and several icons for different sections like "朝刊・夕刊", "LIVE", "Myニュース", "日経会社情報", and "人事ウォッチ". Below the navigation bar, there is a main content area with a large article titled "日本の防衛産業「土俵際」受注数半減、選択と集中問う". A red arrow points to a cookie consent banner at the bottom of the page. The banner contains the following text: "利便性向上、利用分析および広告配信等のためにクッキーを利用してアクセスデータを取得しています。詳しくは「データ利用について」をご覧ください。オプトアウトもこちらから可能です。" and has two buttons: "データ利用について" and "閉じる".

Google アカウントの個人情報の収集

Google が把握している個人の情報

検索や地図検索などで個人の行動傾向や趣味、仕事などが蓄積されてビッグデータに活用される。そのビッグデータは広告配信の基礎データとして再利用。

右の QR コード自分の情報が確認可能です

<https://adssettings.google.com/authenticated>



2 段階認証について

2 段階認証とは

2 段階認証とは、Google や Apple のユーザー管理やホームページなどにログインするときに ID とパスワードの入力以外に、アプリやセキュリティコードでの追加認証を行い、本人確認することでセキュリティを強化する仕組みです。

実際の 2 段階認証の方法や手順はさまざまです。現在、以下のような方法がありますが、新しい技術により常に改善されます。

Google の 2 段階認証の方法として

- Google からのメッセージを使う
- セキュリティキーを使用する
- Google 認証システムなどの確認コードアプリを使う
- テキストメッセージや音声通話で受け取った確認コードを使う
- バックアップコードを使用する

自分の Google アカウントで他のシステムと連携するためにログインした場合

自分のアカウントで連携を始める



連携することを許可する

許可した後に自分の G メールへ他のシステムとの連携が許可された通知が届きます。これは、自分が行ったことであれば、そのまま OK です。もし、自分でこの連携をした覚えがない場合は、他の人がこの連携を行ったことになり、セキュリティ上、危ないこととなります。



Yahoo の SMS 認証

Yahoo の本人認証方法の一つに、「SMS 認証」でログインする方法があります。携帯電話へ SMS (ショートメッセージ) で確認コードを送り、その 4 桁の数字を入力することで本人確認します。

Dropbox で初めて使うブラウザからログインした場合

Dropbox はインターネットで簡単に使えるストレージサービスです。ユーザー登録後にいつもと違うブラウザでログインする場合は 2 段階認証が必要になります。

別の認証が必要です

このアカウントにリンク済みのデバイス宛にコードを送信しました。続けるには、送信されたコードを入力してください。

6 桁のコード

このパソコンを信頼する

続行

[コードを再送](#)

6 桁の認証コードはスマホのショートメッセージ(SMS)で送ってきます。

閉じる

通知

未読



628246 がお客様のセキュリティコードです
このコードを使用してログインしてください
31秒前・個人用

6 桁の認証コードが登録したメールアドレスへ送ってきた場合

様

次のワンタイム セキュリティ コードで Dropbox へのログインを完了してください。

628246

お客様の Dropbox アカウントにログインが試行されました。

ログインの詳細：

デバイス：Windows 上の Chrome

時間：Feb 15, 2024 at 4:57 pm (JST)

場所：Yokohama, Kanagawa, Japan 付近

IP：106.178.187.99

ワンタイム セキュリティコードを安全かつ便利に受け取れるよう、最新の Dropbox モバイル アプリや Dropbox デスクトップ アプリのダウンロードをおすすめします。

ログインしていない場合は、[このリンク](#)をクリックして、不審なログインを報告してください。

様

お客様の Dropbox アカウントで、これまでにご利用いただいたことのないウェブ ブラウザからのログインがありました。アカウントの安全を保つため、このログインがご本人によるものかをお知らせください。

こちらのログインはあなたによるものですか？

日時： Feb 15, 2024 at 5:02 pm (JST)

デバイス： Windows 上の Chrome

はい

いいえ

[わからない](#)

[アカウント保護の詳細についてはこちらをご覧ください。](#)

Dropbox をご利用いただきありがとうございます。
- Dropbox スタッパー同

認証コードを入力し、ログイン完了後に、登録したメールアドレスへ本人確認のメールが届きます。このままで OK です。

もし、ログインした覚えがない場合は、他の人がログインを行ったことになり、セキュリティ上、危ないこととなります。

詐欺は電子メール、ホームページ、電話などから連絡があります。また、QRコードを読むと詐欺サイトへ転送される事例もあります。

迷惑メールとフィルター

迷惑メール

利用者が送信を要求していないのにも関わらず、勝手に送りつけてくる商品広告などの電子メールのこと。スパムメールとも呼ばれています。

迷惑メールフィルター

迷惑メールを取り除く機能のこと。受信した電子メールの内容を分析して、迷惑メールと判断された場合に、件名に「SPAM」や「MEIWAKU」などの文字列を追加するという仕組み。

フィッシング詐欺メール

実在の金融機関、ショッピングサイトを装った電子メールを送付し、これらのホームページとそっくりの偽のサイトに誘導して、住所、氏名、銀行口座番号、クレジットカード番号などの情報を入力させて詐取する行為。

対策： 不用意に Web サイトにアクセスせずに、電子メールや SNS の文面をきちんと読んで、利用しましょう。

実際に詐欺や被害にあった場合の対処方法

- ご家族か友人へ連絡しましょう。
- 一人で対応しない
- 危ない操作した時は、スマホやパソコンの電源を切る
- スマホやパソコンをインターネットに接続しない、Wi-Fiなどを切る
- 電話番号やメールアドレスなどを教えた場合は、新しい電話番号やメールアドレスへ変更する

「Windowsのアップデート」を装う詐欺

詳しくは <https://cs.myicom.jp/knowledgeDetail?an=000477497>



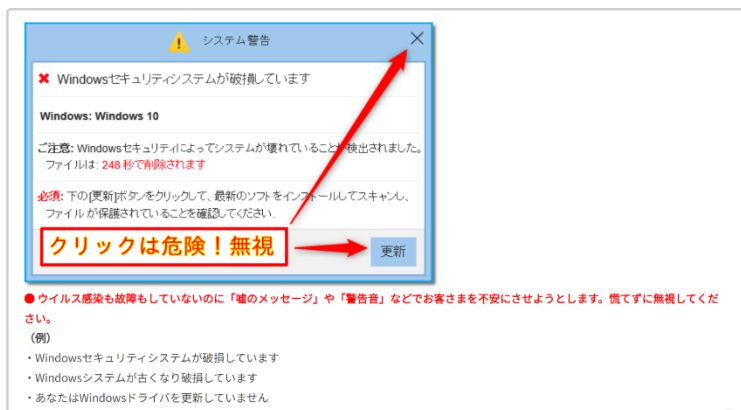
インターネットで「システム警告（詐欺警告）」の対応方法

Windowsパソコンで、突然「システム警告」「システム破損」と表示。ブラウザを閉じられないトラブルが増えています。これは「詐欺警告（警告を装った詐欺）」で、ウイルス感染や故障ではないのでご安心ください。以下に、様々な代表例と解決方法（無視して再発を防ぐ）を紹介します。

動画で確認したい方はこちら

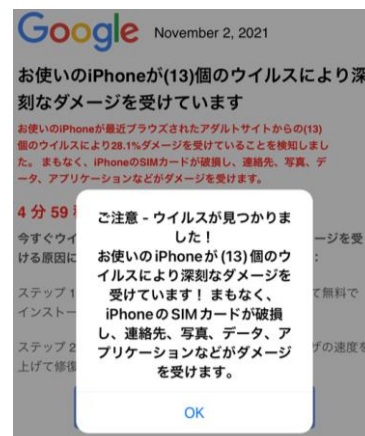


よくある警告表示（代表例）



「ウイルスが見つかりました」を装う詐欺

自分でウイルスチェックをしていないので、これは偽物です。無視してください



詐欺・迷惑メールの事例サンプル

1. メールでは添付ファイルがありますので、**絶対に添付ファイルはクリックしないでください。**このメールはすぐに削除してください。

Subject: **TT-057887564 支払われた 7/12/2023 10:47:27 p.m.
From: d3.dion.ne.jp <info@ieeeinconference.org>
Date: 2023/07/13 7:47
To: _____@d3.dion.ne.jp

_____ -l _____@d3.dion.ne.jp-_____

支払い転送アドバイスが完了しました 7/12/2023 10:47:27 p.m...

この電子メール通信および電子メールで送信されるファイルには機密情報や専有情報が含まれる場合があります。対象の受信者のみが使用するために提供されます。意図された受信者以外によるこの情報のレビュー、再送信、または配布は禁止されています。この電子メールを誤って受信した場合は、送信者に連絡し、この通信とコピーを直ちに削除してください。ありがとうございます。

—添付ファイル:—

@d3.dion.ne.jp.htm

3.9 KB

2. 非常に巧妙にできている詐欺メールです。メールのメッセージの「ソースを表示」させると、このメールの返信先に、JR えきねっととは違うメールアドレスになっています。**メール本文の「ログイン」ボタンは絶対に押さないでください。**メールは削除してください。

From - Thu Sep 21 17:25:18 2023

X-Mozilla-Status: 0001

X-Mozilla-Status2: 00000000

X-Mozilla-Keys:

Return-Path: <eki-update@obqjy.com> ←——！ JRのえきねっとではない

Subject: [SPAM] 【ご注意】会員情報変更および退会に関するお知らせ

From: えきねっと <info@eki-net.co.jp>

Date: 2023/08/28 7:07

To: hodota <[redacted]@[redacted].com>



日頃より「えきねっと」をご利用いただきありがとうございます。

8月21日にセキュリティシステムを全面的にリニューアルしましたため、7日以上にログインしていない方は、今後の利用に支障が出ないよう、このメールを受信後、早急にログインをして個人情報を更新してください。

ログイン

9月29日までにご記入ください。ご記入がない場合は、退会手続きをとらせていただきます。

お客さまにはご不便をおかけいたしますが、何卒ご理解を賜りますようお願い申し上げます。

※このメールは「えきねっと」より自動配信されています。
返信いただきましても対応致しかねますので、あらかじめご了承ください。

※本メールは、「えきねっと」重要なお知らせとしてメールの配信を希望されていないお客様にもお送りさせていただきます。

© 2023 JR East Net Station Co. A8990, Ltd.

3. 銀行のメールを装う詐欺メールです。

非常に似ています。送信元の From 欄にある、メールアドレスが mufg.jp1@mpnionk.cn となっており、.cn は中国です。リンクなどにはクリックしないで、すぐに、削除してください。

Subject: [SPAM] 【MUFG】1月お支払金額確定のお知らせ
From: 三菱UFJニコス株式会社 <mufg.jp1@mpnionk.cn>
Date: 2023/12/27 21:47
To: hodota@

メールが正しく表示されない方はこちらをご覧ください。

MUFG 三菱UFJニコス

MUFGカード

いつもMUFGカードをご利用いただき
誠にありがとうございます。
今月のお引落日をご案内いたします。
お支払金額のご確認はこちら

WEBサービスにログインのうえ、「ご請求額・利用明細照会」を選択してください。
※ショッピング1回払いご利用分は、事前返済を受付していません。

()

お申込期限 (WEB) 1月6日 (土) 12:00まで 2024年1月10日 (水) お支払分のお申込期限は、通常月より早まります。1月4日 (木) 12:00まで

お引落口座にゆうちょ銀行を設定されているお客さまやお電話でお申し込みされる場合は、お申込期限が異なります。詳細はこちら

15,000円を分割払い (3回払い) に変更した場合のお支払いイメージ 12月 15,000円
変更したご利用分は今月のお支払いをスキップ! 2024年1月 お支払いは来月から
5,102円* 1回目 2月 5,102円* 2回目 3月 手数料は284円 5,080円* 3回目 *3回払いに変更した場合の元金+手数料

お申し込みはこちら

WEBサービスにログインのうえ、「お支払方法の変更」からお申し込みください。

※「分割払い」「リボ払い」は、ご利用金額に対して所定の手数料がかかります。
※ご利用状況により、変更いただけない場合がございます。
※一部、対象外のカードやご利用分がございます。

シミュレーションできます

ご利用金額等をご入力いただくと、分割払いやリボ払いを利用した際の手数料や月々のお支払金額をご確認いただけます。

シミュレーションはこちら

[分割払いお支払いシミュレーション](#)

[リボ払いお支払いシミュレーション](#)

インターネットからのお申し込みで口座にお振り込み 秒速振込みサービス「借りまくん」

スマートフォンやパソコンでカードローンのご利用ができるサービスです。
平日9:00~14:30までのお申し込みなら、最短数十秒で必要な金額をカードご利用代金お支払口座にお振り込みいたします。
※一部、ご利用いただけない場合がございます。

詳細はこちら

本メールはご契約に関する大切なお知らせのため、弊社からのメール配信を希望されていないお客さまも含め、皆さまにお送りしておりますのでご了承ください。

MUFGカードからのお知らせ

カード番号やID・パスワードなどお客さま情報の入力を求める「偽画面の表示」や「フィッシングメール」が発生しています。ご注意ください。
[セキュリティに関するお知らせ](#)

※本メールは、DC Webサービスの登録情報をもとにお送りしています。
※メールアドレス変更・ご退会などの最新情報を反映していない場合や、通信環境等により弊社からお送りしたメールが届けられない場合があります。

■メールアドレスの変更方法

- 1) WEBサービスにログイン
- 2) 「WEBサービストップ」→メニューの「各種お手続き」から「Eメールアドレス登録・変更」
- 3) パスワードを入力→「登録・変更」にチェック
- 4) 変更後のEメールアドレスを入力→「確定」

■ご不明な点・お問い合わせ

発行元: 三菱UFJニコス株式会社
〒113-8411 東京都文京区本郷3丁目33番5号
※本メールへの返信には回答を差しあげておりません。

4. 東京電力のメールを装う詐欺メールです。

非常に似ています。未払い金額で小数点以下があり、海外からの詐欺メールです。リンクやボタンなどにはクリックしないで、すぐに、削除してください。

Subject: [SPAM] ※東京電力エナジーパートナー※よりご利用料金のご請求です【9月6日重要なお知らせ】 (自動配信メール)
From: 【東京電力エナジーパートナー】くらしTEPCO web <no-reply@tepcoco.jp>
Date: 2023/09/06 7:47
To: hodota. @gennai3.co.jp>

■□■ TEPCOよりご利用料金のご請求です。 ■□■

- 下記内容をご確認の上、至急お支払いください。万一、支払期日を過ぎると、

- サービスのご供給を【停止】致します。

▼ 支払いの詳細リンクエント

<未払い金額: 19,695.71 円 (税込)>

支払期日: 2023年9月6日 (支払期日の延長不可)

※ 本メールは、TEPCO にメールアドレスを登録いただいた方へ配信しております。

以上、ご不明な点に関しましては、お気軽にお問い合わせください。

東京電力では、SMS（ショートメッセージ）の詐欺メール確認方法を説明しています。



<https://www.tepco.co.jp/ep/support/sms/phishing/index-j.html>

東京電力（TEPCO）を装った SMSフィッシング詐欺※にご注意ください！

東京電力（TEPCO）からのSMS選択払いとは、所定の送信元電話番号（docomo, au : 0120-659-436 SoftBank : 249024）から発信いたします。心当たりのないSMSを受信した際は、本文に書かれているURLのクリックには細心の注意を払い、真偽が不明の場合はアクセスしないようにご注意ください。
※フィッシング詐欺とは銀行やクレジット会社などを装い、認証番号やクレジット番号を盗み、お金を引き出す詐欺のことです。



5. 横浜銀行のメールを装う詐欺メールです。

非常に似ています。パスワードがロックされた場合は、銀行のコールセンターや窓口で手続きが必要になる場合が一般的など思います。「ご本人確認のために、口座から1円を差し引く…」も日本では一般的ではないと思います。海外からの詐欺メールです。リンクなどにはクリックしないで、すぐに、削除してください。

Subject: [SPAM] 【緊急情報】横浜銀行一時的利用制限のお知らせ
From: 横浜銀行 <contact@boy.co.jp>
Date: 2023/09/06 8:03
To: hodota, @gennai3.co.jp>

いつも横浜銀行をご利用いただき、誠にありがとうございます。
お客さまの当ウェブサイトのご利用につきまして、パスワードの誤入力が続いたため、9月6日（金）午前2時38分より横浜銀行ウェブサイトおよびスマートフォンアプリのご利用を一時的に制限させていただきます。
お客様にはご不便をおかけし、誠に申し訳ございません。何卒ご理解のほどよろしくお願い申し上げます。
◆本人確認が完了次第、制限を解除いたします。以下のボタンより本人確認を行ってください。
[本人確認を行う](#)
ご本人様確認のため、口座から1円を差し引かせていただく場合がございます。
※本人確認が完了すると、通常通りログイン後のお手続きが可能になります。
※24時間以内に本人確認が取れない場合、アカウントの取引を制限させていただきます。

株式会社横浜銀行
金融機関コード：0138
登録金融機関：関東財務局長（登金）第36号
加入協会：日本証券業協会、一般社団法人金融先物取引業協会
Copyright (C) 2023 The Bank of Yokohama, Ltd. All rights reserved.

6. Apple のメールを装う詐欺メールです。

From 欄では xxxx@amazon.co.jp となっており、Apple のメールではありません。文章の最後に、「敬具、」日本語では敬具のあとにカンマを付けないので海外からの詐欺メールだと思います。「Apple サービスチーム」の連絡先がないのも怪しいです。リンクなどにはクリックしないで、すぐに、削除してください。

Subject: [SPAM] あなたのAppleアカウント：確認と安全対策をお願いします
From: Apple <glass_1@amazon.co.jp>
Date: 2023/09/07 11:40
To: @gennai3.co.jp

Appleサービスチームからのお知らせです。
最近、一部のAppleアカウントにおける不審な動きを検出いたしました。これを受けて、ユーザーの皆様にはアカウントの安全確認をお願いすることとなりました。
推奨する対応手順は以下の通りです：

[Apple IDサインイン](#)
まず、Appleアカウントから一時的にログアウトしてください。Apple ID管理ページを訪れ、パスワードを変更してください。新設定されたパスワードで、アカウントへのログインを試みてください。何か疑問や不安がございましたら、公式サポートへお気軽にお問い合わせください。我々は常にユーザーの皆様と安全性と利便性を考えております。
ご注意とご協力、心より感謝いたします。
敬具、
Appleサービスチーム

ショッピングサイトなどからの詐欺メール

Amazon や楽天などのショッピングサイトから、たくさんの連絡がきます。自分が利用している場合は、連絡は確認しますが、詐欺メールがほとんどです。自分がショッピングサイトを利用した場合の連絡メールは本物ですが、それ以外は詐欺メールがほとんどです。一般的にショッピングサイトでは、利用者へ送った連絡メールは利用者がホームページへログインして確認できます。

Amazon の場合

アカウントサービスに「メッセージセンター」があります。



https://www.amazon.co.jp/gp/css/homepage.html?ref_=nav_AccountFlyout_ya

アカウントサービス>メッセージセンター

受信トレイ	すべてのメッセージ	購買依頼者/出品者のメッセージ
送信メッセージ	Amazon.co.jpのご注文(#249-8173768-1338214)の商品 1 点が発送されました	2024/2/13 10:4...
	注文249-8173768-1338214を完了するために必要な出品者からの追加情報	2024/2/12 18:3...
	Amazon.co.jpお支払いの確認 【メールでお届け】 簡単解除マニュアル付き EPSON (エプソン...	2024/2/12 16:2...
	Amazon.co.jpでのご注文249-8173768-1338214 (1点)	2024/2/12 12:1...
	Amazon.co.jp お支払い番号のお知らせ 【メールでお届け】 簡単解除マニュアル付き EPSON ...	2024/2/12 12:1...

警察

神奈川県警察のサイバー犯罪について



https://www.police.pref.kanagawa.jp/kurashi/cyber_hanzai/mesd7017.html

サイバーセキュリティに関する相談について

警察機関への相談

- ※ インターネット上の掲示板などに「殺害予告」や「爆破予告」等の急を要する書き込みを発見した場合には、**110番通報**又は**最寄りの警察署に速やかに通報**していただくようお願いいたします。
- ※ 事件化に関する相談については**最寄りの警察署**にご相談ください。
- ※ 神奈川県以外に在住の方は、お住いの都道府県警察本部にあるサイバー犯罪相談窓口をご利用ください。

各都道府県警察のサイバー犯罪相談窓口

<https://www.npa.go.jp/bureau/cyber/soudan.html> (外部サイト)

他の機関の相談窓口等

- インターネット上の書き込みなどに関する相談・通報窓口のご案内



(PDFファイル：294KB/テキストファイル：6KB)

迷惑メールや詐欺メールで困ったら

国の相談窓口： 内閣府(一般財団法人 日本データ通信協会) 電気通信消費者相談センター

迷惑メール相談センター 03-5974-0068

消費者相談センター

川崎市の相談窓口 「消費者生活センター」 へ電話 **044-200-3030**

2024年2月5日から下記へ移転しました。

〒210-0006 川崎市川崎区砂子 1-8-9
川崎御幸ビル 5階



Google 提供

検索

検索の使い方

トップ

くらし・手続き

お知らせ
イベント・募集

市の施設

川崎の魅力
みどころ

現在位置：[トップページ](#) > [くらし・手続き](#) > [届出・手続き・相談](#) > [相談窓口](#) > [川崎市消費者
電話・来所による相談](#) > [電話・来所による相談](#)

電話・来所による相談

ツイッターへのリンクは別ウィンドウで開きます

ツイート

2021年8月12日

コンテンツ番号31351

電話・来所による相談

相談時間：月～金曜日（祝日除く） 9:00～16:00

土曜日（祝日除く） 10:00～16:00

※金曜日は電話相談のみ19:00まで受付

※土曜日は電話相談のみ受付

住所：川崎区駅前本町11-2 川崎フロンティアビル10階

（JR川崎駅北口から徒歩2分）

相談電話番号：044-200-3030 ※「ご相談いただく前に」もお読みください。

はじめてのスマホ 安心教室



2024年

本テキストは令和5年度「はじめてのスマホ安心教室」(後援 川崎市教育委員会)でも使われました。

本書のご意見・ご要望の連絡先

〒210-0844 神奈川県川崎市川崎区渡田新町1-4-9-201

特定非営利活動法人NPO福祉支援ゆうやけネット

デジタルボランティア・スマホ講座担当

電話:044-220-1588 Fax:044-272-9523

ホームページ <https://yuuyake.or.jp>



本書は2023年度かわさき市民公益活動助成金事業により作成しました。