

個人情報漏えいから自分を守る チェックリスト v1.0

2026年10月版 株式会社スターストリーム・スタジオ

このチェックリストの使い方

個人情報漏えいは、もう「起きるもの」と考えたほうが安全です。会社のサーバーの守りは私たちには変えられませんが、ログインの入力口を固めておけば、情報が漏れても乗っ取りは防げます。

このチェックリストは、上から順に印（□ → ㊞）を付けながら進める形にしています。全部を1日でやる必要はありません。

1. 今日やること（1章）だけは、今日のうちに済ませる
2. 残りは、2章の表を1日2～3個ずつ埋めていく
3. 漏えいのお知らせが届いたら、5章をそのまま上から進める

印刷するか、スマホのスクリーンショットに残しておくと、何度でも使えます。

1. 今日やること（15分）

☐ メールアカウントで、二段階認証をオンにした

ふだん使っているメール（Gmail、Yahoo!メール、iCloudメール、プロバイダのメールなど）すべて。ほかのサービスのパスワード再設定はメールで行われるので、ここが最優先です。

☐ スマホのアカウント（Apple Account または Googleアカウント）の二段階認証がオンになっているか確かめた

iPhoneは多くの場合、最初からオンになっています。「オン」と表示されていれば大丈夫です。

☐ いちばん多く使い回しているパスワードを思い浮かべ、それを使っているサービスを書き出した 思い出せる範囲で構いません。2章の表で、その行から先に片づけます。

2. サービス別チェック表

上から「乗っ取られたときの被害が大きい順」に並んでいます。使っていないサービスは飛ばしてください。

それぞれのサービスで、次の3つに印を付けていきます。

- ・A：二段階認証をオンにした
- ・B：パスワードを、ほかのサービスと別のものにした
- ・C：パスキーを設定した（使えるサービスだけ。できなくても大丈夫です）

メール

- ☐A ☐B ☐C Gmail
- ☐A ☐B ☐C Yahoo!メール
- ☐A ☐B ☐C iCloudメール
- ☐A ☐B ☐C プロバイダのメール（ ）
- ☐A ☐B ☐C 会社のメール（会社の決まりに従う）

スマホのアカウント

- ☐A ☐B ☐C Apple Account（iPhone）
- ☐A ☐B ☐C Googleアカウント（Android・Gmail）

お金に関わるもの

- ☐A ☐B ☐C ネット銀行・銀行アプリ（ ）
- ☐A ☐B ☐C 証券会社（ ）
- ☐A ☐B ☐C クレジットカードの会員サイト（ ）
- ☐A ☐B ☐C PayPay・楽天ペイなどの決済アプリ（ ）

買い物

- ☐A ☐B ☐C Amazon
- ☐A ☐B ☐C 楽天
- ☐A ☐B ☐C その他のネットショップ（ ）

SNS・連絡

- ☐A ☐B ☐C LINE
- ☐A ☐B ☐C Instagram
- ☐A ☐B ☐C X
- ☐A ☐B ☐C Facebook

二段階認証の設定が見つからないとき

設定の場所は、サービスごと・時期ごとによります。迷ったら次の順で探します。

1. 設定（歯車のマーク）を開き、上の検索欄に「二段階」「2段階」「認証」のどれかを入れる
2. 見つからなければ「セキュリティ」「ログイン」「アカウント」の項目の中を見る
3. 名前は「二段階認証プロセス」「2ファクタ認証」「多要素認証」「ログイン認証」など、サービスによって違います
4. それでも見つからなければ、検索エンジンで「サービス名 二段階認証 設定」と調べる（公式のヘルプページを開く）

3. 番号の受け取り方を選ぶ

二段階認証をオンにすると、ログインのたびに番号の受け取り方を聞かれます。

☐ まずはSMS（ショートメッセージ）でオンにした

いちばん手軽です。オフのままにしておくより、はるかに安全です。

☐ 慣れたら、認証アプリに切り替えた

Google AuthenticatorやMicrosoft Authenticatorなどのアプリに、30秒ごとに変わる番号が出ます。SMSより乗っ取られにくい方法です。

☐ バックアップコードを保存した

スマホをなくしたときにログインするための予備の番号です。設定の途中で表示されたら、紙に書いて家の中の決まった場所にしまえます。スマホの中だけに置かないこと。

☐ 機種変更の前に、認証アプリの引っ越し方法を確認した

認証アプリは、引っ越しをしないまま古いスマホを初期化すると番号が出なくなります。機種変更の前に、アプリ内の「エクスポート」「引き継ぎ」の項目を確認します。

4. 偽のログイン画面にだまされないためのチェック

二段階認証の番号も、偽の画面に自分で入力してしまうと使われてしまいます。次の7つを習慣にします。

- メールやSMSのリンクから、ログインしない
- 銀行・証券・カードは、ブックマークか公式アプリから開く
- 「アカウントが停止されます」「不正利用を確認しました」など、急がせる連絡ほど疑う
- 宅配の不在通知のSMSのリンクは押さない（配送業者の公式アプリかサイトで確かめる）
- ログイン画面のアドレス（URL）が、いつもと同じかを見る
- 頼んでいないのに届いた「確認番号」は、誰にも教えない（電話で聞かれても答えない）
- 迷ったら、その会社の公式サイトに自分でアクセスし、お知らせを確かめる

5. 漏えいのお知らせが届いたら

「あなたの情報が漏れました」というメールや手紙が届いたときの手順を、上から順に並べました。

当日

- お知らせが本物かを確かめた（メールのリンクではなく、**会社の公式サイトのお知らせ**で確認する）
- 漏れた項目を書き出した（名前・住所・電話・メール・パスワード・生年月日・免許証などの画像）
- 漏れたサービスのパスワードを変えた
- **同じパスワードを使っていたほかのサービスも、全部パスワードを変えた**
- それらのサービスで二段階認証をオンにした

免許証・保険証などの画像が漏れたとき

- 信用情報機関に「**本人確認書類が漏れた**」と申告した

信用情報機関は、カード会社や銀行、消費者金融がお金を貸す前に申込者の情報を確かめる先です。申告しておく、誰かがあなたの書類で申し込んできたときに、審査する会社に注意をうながせます。3つあり、それぞれの公式サイトに申告の案内があります。

- ・CIC（クレジットカード・信販会社など）
- ・JICC（消費者金融・カード会社など）
- ・全国銀行個人信用情報センター（銀行など）

手数料や必要な書類は機関ごとに違うので、各公式サイトの案内を確かめてください。

その後の1〜3か月

- ☐ その会社を名乗る「お詫び」「補償の手続き」のメールやSMSのリンクを押さない
- ☐ クレジットカードの利用明細を、毎月1回見る
- ☐ 身に覚えのないログインのお知らせが来たら、すぐパスワードを変える
- ☐ 身に覚えのない郵便（カードの申込完了・ローンの案内など）が届いたら、その会社に連絡する

6. 家族にも伝える

高齢の親や、スマホに慣れていない家族ほど、狙われやすくなります。

- ☐ 家族のメールとスマホのアカウントの二段階認証を、一緒にオンにした
- ☐ 「リンクからログインしない」「確認番号は誰にも教えない」の2つだけ伝えた
- ☐ 困ったときに、まず自分に連絡してもらう約束をした

7. 月に1回の見直し（5分）

- ☐ 新しく登録したサービスがあれば、2章の表に書き足した
- ☐ 使っていないサービスは退会した（登録している数が少ないほど、漏れる先も減ります）
- ☐ 登録するときは、必要のない項目（生年月日・住所など）を入れないようにしている

株式会社スターストリーム・スタジオ

このチェックリストは、公式LINEでお受け取りいただいた方向けの資料です。