個人編・小さな会社編

情報漏えいから身を守る対応ガイド

流出した情報の種類別に、被害を防ぐ・被害にあったら

2026年10月版



著作　株式会社アルファテック

目次

はじめに 3

■ 共通

第1章 いま何が起きているのか 7
- 数字で見る2026年 7
- 2026年の主な事案 8
- 10月に相次いだ注意喚起 13

第2章 なぜ漏えいが相次ぐのか 14
- 集計で見る漏えいの原因 14
- ランサムウェアと VPN 機器 15
- 1か所の侵害が広がる 16
- 弱点を突く速さ 17
- 設定の誤りで見える状態に 19
- 持つ情報・残す期間 19

第3章 漏れた情報はどう悪用されるのか 21
- 漏えいから被害までの流れ 21
- 本物の情報を使った偽の連絡 22
- 使い回したパスワードでの不正ログイン 25
- 本人確認書類を使ったなりすまし 25
- 数字で見る詐欺の被害 26

■ 個人編

第4章 被害にあわないために 28
- パスワードを使い回さない 29
- パスワードを安全に保管する 29
- パスキー・2段階認証を使う 31
- 連絡のリンクを開かない 32
- カード・口座の通知を受け取る 33
- 渡す情報・残す情報を減らす 33
- 電話・SMS の詐欺に備える 33
- スマホが使えなくなったときに備える 34
- 家族で決めておくこと 40

第5章 漏えいの通知が届いたら 42
- 5つのステップ 43
- 通知が届く前に気づいたら 45
- 会社から届く通知とは 46
- お詫び・返金をかたる偽の連絡 48
- 脅しや「削除」を持ちかける連絡 49
- 役所・学校・病院から届いたとき 52
- その後、何を確かめ続けるか 53

第6章 流出した情報の種類別の対応 54
- 6-1 メールアドレス 55
- 6-2 電話番号 57
- 6-3 氏名・住所・生年月日 58
- 6-4 クレジットカード 59
- 6-5 ID・パスワード 64
- 6-6 マイナンバー 73
- 6-7 銀行口座 75
- 6-8 健康・医療の情報 78
- 6-9 本人確認書類・顔写真 78
- 6-10 購買履歴・会員情報 84

第7章 救済と相談窓口 86
- 会社の窓口・補填・お詫び 86
- 口座が不正に使われたときの補償 89
- 賠償と裁判の例 93
- 改正個人情報保護法 95
- 相談窓口 96

■ 小さな会社編

第8章 小さな会社の担当者へ 98
- 8-1 小さな会社でも起きる 98
- 8-2 漏えいが起きたら 99
- 8-3 委託先・委託元のとき 106
- 8-4 まずやる対策 107
- 8-5 送金をねらう詐欺に備える 109
- 8-6 Web のシステムが止まったときに備える 113
- 8-7 公的な支援を使う 116

■ 共通

第9章 これからの見通し 118
- 9-1 予測の読み方 118
- 9-2 いま進行中(2026年10月) 119
- 9-3 数か月以内(～2027年1月ごろ) 119
- 9-4 半年後(2027年3～4月ごろ) 120
- 9-5 1年後(2027年9～11月ごろ) 120

第10章 本書の見解 122
- 「漏れる前提」で守る 122
- 強い認証に効果の兆し 122
- 被害者の手間と費用 123
- 本人確認は画像から IC チップへ 123
- 救済の仕組みの限界 123
- 会社に求めたいこと 123

■ 付録

付録 125
- 付録A 個人のチェックリスト 125
- 付録B 会社のチェックリスト 128
- 付録C 相談窓口の一覧 129
- 付録D 用語集 133
- 付録E 出典について 137

はじめに

2026年は、会社や団体からの大規模な情報漏えいの公表が相次いでいます。とくに9月中旬からは、毎週のように新しい発表が続きました（第1章）。漏えいの通知を受け取って、何をすればよいか迷った人もいるでしょう。

制度・公式情報 2026年10月には、国の機関などが事業者向けの注意喚起を相次いで出しました。国家サイバー統括室は10月14日に、各機関の注意喚起の一覧を載せています。

本書は、漏れた情報の種類ごとに、被害を防ぐ方法と、被害にあったときにすることをまとめた手引きです。主な読者は、専門知識のない個人・家族と、小さな会社やお店の担当者です。

本書は、株式会社アルファテックが、公開された情報をもとにまとめました。特定の会社を責めるためのものではありません。法律の判断はしないので、自分の場合は付録Cの窓口に相談してください。詐欺の手口は見分けるのに必要な範囲にとどめ、確かめる手順は、自分のアカウントと自分の情報に限ります。

漏えいした会社や団体も、攻撃を受けた被害者です。そこで本書では、本文や図に会社・団体の名前を書かず、「カーシェアの件」のように業種と仕組みで呼びます。似た事案は、狙われた仕組みの型ごとにまとめました。同じ型の事案から、自分が使うサービスにも当てはまる備えを読み取れるようにするためです。もとの発表は、別冊の「出典一覧」で確かめられます。

この本の使い方

立場ごとの入口

図0-1で自分に近い立場を探し、その章から読んでください。



図0-1　立場別の早見表

図0-1にない困りごとは、次の節から読めます。

- **パスワードの控え方**: 第4章「パスワードを安全に保管する」
- **パソコンがランサムウェアに感染したおそれがある**: 6-5「パソコンがランサムウェアに感染したおそれがあるとき」。会社は 8-2
- **スマホをなくした・不正なアプリを入れてしまった**: 6-5「スマホをなくしたとき」「スマホに不正なアプリを入れてしまったとき」

- **スマホ・認証のアプリ・支払いが使えなくなったときに備える**: 第4章「スマホが使えなくなったときに備える」。カードの番号を変える再発行のあいだは 6-4
- **家族で決めておくこと**: 第4章「家族で決めておくこと」
- **通知が届く前に、覚えのない請求やログインに気づいた**: 第5章「通知が届く前に気づいたら」
- **パスワードや、写真・家族のことを示して脅された**: 第5章「脅しや『削除』を持ちかける連絡」
- **口座から不正にお金を引き出された**: 6-7「身に覚えのない送金に気づいたら」。補償の制度は第7章「口座が不正に使われたときの補償」
- **予約サイトや店の Web のシステムが止まった**: 6-10「予約サイトや決済が止まったとき」。会社の担当者は 8-6

本文の要所では、図0-2の人物が、手口や手順を吹き出しで説明します。

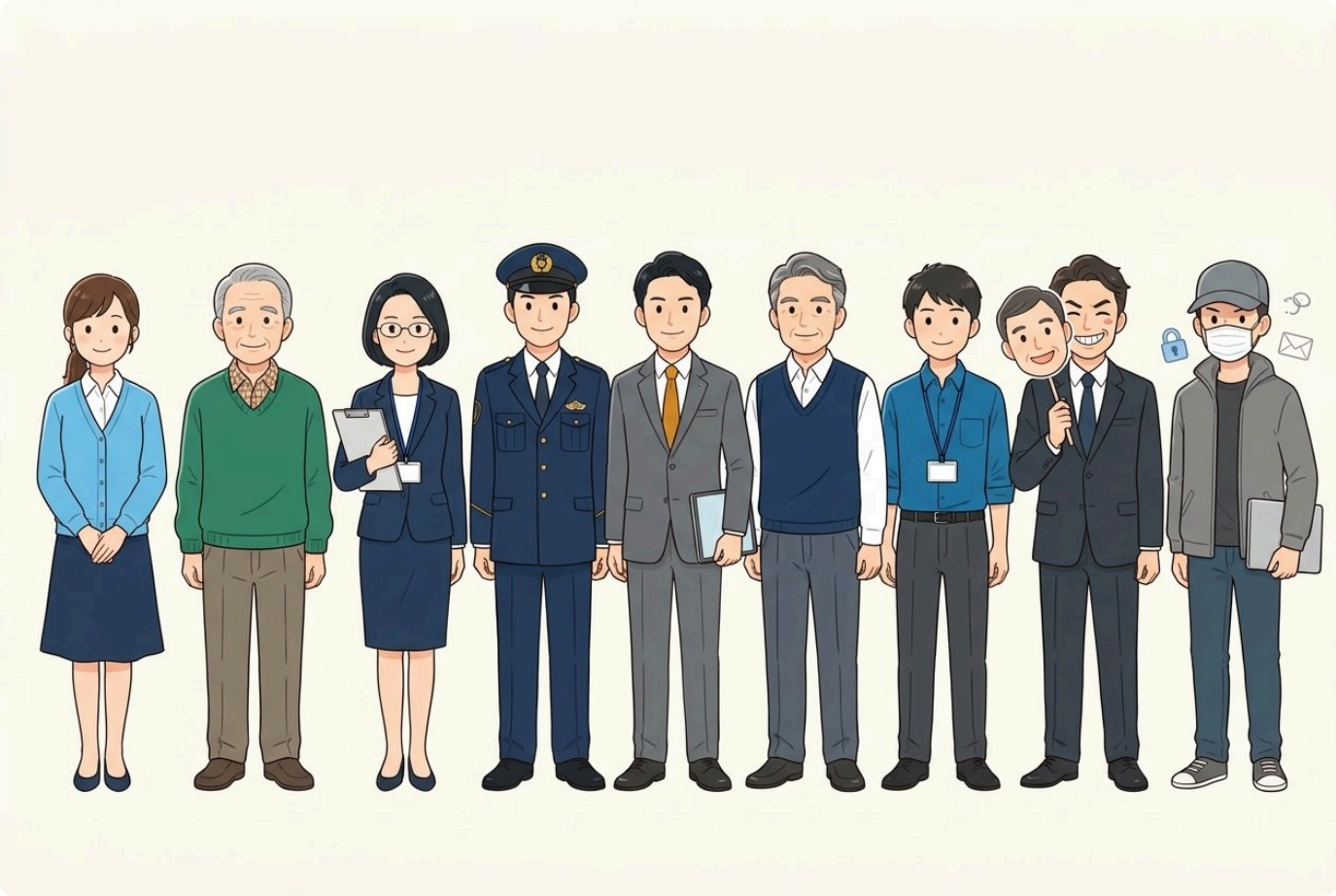


図0-2　この本の登場人物（人物は架空です）

確度の札と「本書の推奨」

事実や意見を述べる段落の先頭には、次の5種類の札を付けています。

札	意味
実際に起きた事例	公式発表や信頼できる報道で確かめた、実際に起きた事案とその集計
制度・公式情報	法律・制度や、公的機関・会社・団体の公式の説明
専門家の予測・懸念	公的機関・企業・専門家の見通しや懸念。起きると決まったわけではありません
予測（本書の推論）	本書が事実から考えた見通し。根拠と外れる条件を添えます（第9章）
本書の見解	株式会社アルファテックとしての意見。事実とは分けて書きます（第10章）

手順や助言の段落には札を付けていません。文末の「（本書の推奨）」は、出典にそのままの記載はなく、調べた内容をもとに本書が勧める手順や目安です。人物の吹き出しでも、出典のある内容には出典の番号を、本書が勧めることには「（本書の推奨）」を付けています。

色帯と出典

各章の初めの帯と目次で、「共通」（紺・本の印）、「個人編」（青・家の印）、「小さな会社編」（茶色・盾の印）、「付録」（灰色）を見分けられます。

事実を述べた文には小さな番号を付け、その出典（発行元・題名・公開日・リンク〔URL〕）を、別冊の「出典一覧」に章ごとに載せています。番号は章ごとに1から数えます。はじめにで述べる事実の出典は、同じ事実を書いた各章の出典にあります。スマホの操作の手順と、相談窓口の番号・受付時間は、2026年10月に各社・各機関の公式サイトで確かめました。ページを減らすため、これらの出典の注は省いています。調査の基準日は2026年10月22日です。主な事案の続報と新しい事案は、10月27日まで確かめました。窓口の番号や受付時間、制度は変わることがあるので、使う前に公式サイトで確かめてください。

3分でわかる要点

いま起きていることを3点にまとめ、今日やることを5つ挙げます。

1　大規模な漏えいの公表が相次いでいます

実際に起きた事例 東京商工リサーチ（調査会社）の集計では、上場企業とその子会社が公表した個人情報の漏えい・紛失事故のうち、1回で100万件以上のものが、2026年は10月5日時点で10件ありました。2025年の1年間の6件をすでに上回り、同社は「過去最悪ペース」としています。

実際に起きた事例 同社の10月23日の集計では、宅配便の会社の最大約5,323万件（重複を含む）が、2012年からの集計で過去最多になりました。1回で1,000万件以上の漏えいは、2025年までの14年間で3件でしたが、2026年は10月23日までに8件（速報値）あります。

主な事案は第1章に、狙われた仕組みの型ごとにまとめました。漏えいが相次ぐ背景と原因は第2章にあります。

2　怖いのは、漏れた「その後」です

実際に起きた事例 衣料品の通販の件では、注文情報と一致する不審な返金案内のメールを受け取ったと顧客から問い合わせがあり、調べると不正アクセス（許可なく他人のシステムに入ること）の痕跡が見つかりました（2026年10月3日公表）。モニター（覆面調査）サイトの件では2026年8月、リスト型攻撃（ほかで漏れた ID・パスワードの組を、次々に試す手口）を受け、会員59,389名が不正にログインされました。カーシェアの件（2026年9月公表）では、運転免許証などの画像のデータ約146万件に、外部へ送られた痕跡がありました（10月23日の第5報。画像は暗号化して保管されていました）。

ただし、特定の漏えいと、その後のなりすましの被害との因果関係を確かめた公的資料や具体例は、本書の調査では見つかりませんでした（2026年10月22日時点）。

制度・公式情報 警察庁は、メールの中のリンクを安易に押さないよう呼びかけています。「情報流出元の企業をかたる偽メールの可能性があります」というのが理由です。悪用のされ方の全体は第3章で説明します。

3　何が漏れたかで、やることが変わります

漏れた（または漏れたおそれがある）項目によって、悪用のされ方と今日やることが変わります（第6章）。情報が漏れても、ふだんの備えがあれば、被害を防いだり小さくしたりできます（第4章）。

制度・公式情報 IPA（情報処理推進機構）も2026年10月26日、漏れた情報の種類をまず確かめ、種類ごとに対処するよう勧めています。

通知が届く前でも、覚えのない請求やログインに気づいたら、通知を待たずに、サービスの会社やカード会社・銀行に連絡します（第5章。本書の推奨）。口座が不正に使われたときの手順は 6-7、補償の制度は第7章にあります。

制度・公式情報 IPA は、パスキー（パスワードの代わりに、スマホなどの機器と指紋・顔・PIN〔暗証番号〕で本人を確かめる仕組み）はパスワードや確認コードを入力しないため、フィッシング（本物そっくりの偽のメールやサイトで、情報をだまし取る手口）に強いとしています。これからの見通しは第9章、本書の意見は第10章にまとめました。

今日やること5つ

1. メールと銀行のパスワードを、ほかと違うものにします（第4章）。
2. よく使うサービスを1つ選び、パスキーか2段階認証（パスワードのほかに、確認コードなどでも本人かを確かめる仕組み）を設定します（第4章）。
3. カードの利用通知を有効にします（第4章）。
4. よく使う銀行・カード・通販は、公式アプリを入れるか、公式サイトをブックマーク（よく見るページを登録しておく機能）しておきます（第4章）。
5. 漏えいの通知が届いていたら、第5・6章の手順で確かめます。

会社の担当者は、第8章と付録Bのチェックリストから始めます（本書の推奨）。

■ 共通

第1章　いま何が起きているのか



2026年は、会社や団体からの大規模な情報漏えいの公表が相次いでいます。とくに9月中旬からは、表と図1-1のとおり、毎週のように新しい発表が続きました。この章では、数字、型ごとの主な事案、10月の注意喚起の順に見ていきます。事案は、会社・団体の名前ではなく、業種と狙われた仕組みで呼びます（はじめに）。

数字で見る2026年

実際に起きた事例 東京商工リサーチ（調査会社）の集計では、上場企業とその子会社が公表した個人情報の漏えい・紛失事故のうち、1回で100万件以上のものが、2026年は10月5日時点で10件ありました。2025年の1年間の6件をすでに上回り、同社は「過去最悪ペース」としています。1回で1,000万件以上の漏えいは、2012～2025年の14年間で計3件でしたが、2026年は10月5日までに3件ありました[1]。

実際に起きた事例 同社の10月23日の集計では、宅配便の会社の最大約5,323万件（重複を含む）が、2012年からの集計で過去最多になりました。1回で1,000万件以上の漏えいは、2026年は10月23日までに8件（速報値）に増えています[2]。

実際に起きた事例 その前の2025年も、同社の集計では、上場企業とその子会社が公表した漏えい・紛失事故は180件（過去2番目）で、社数は158社と過去最多でした。漏えい・紛失した可能性のある個人情報は3,063万6,910人分で、2024年の約2倍です。180件のうち70件は、人数が開示されていません[3]。

実際に起きた事例 個人情報保護委員会（個人情報の扱いを監督する国の機関）が2026年4～6月に処理した漏えい等の報告は6,101件で、前年度の四半期あたりの件数（4,854件）を上回りました。民間事業者の報告5,451件のうち、不正アクセス（許可なく他人のシステムに入ること）などの「不正の目的」の類型は1,450件（26.6%）で、委員会の表にある直近5四半期で最も高い割合でした[4]。これは報告を処理した件数で、その期間に起きた事故の数や、漏えいした人数ではありません。

実際に起きた事例 トレンドマイクロ（セキュリティ企業）の集計では、国内の組織が公表したセキュリティインシデント（サイバー攻撃による被害。紛失や誤送信は数えない）は、2026年1～9月で607件でした。9月末の時点で2025年の

1年分(594件)を超え、10月9日時点では659件です[5]。

実際に起きた事例 MM総研(調査会社)は、公表・報道された事案を独自に集計しています(漏えいの可能性があるものを含む)。サイバー攻撃による国内の漏えい事案は、2026年1～9月で454件(9月分は暫定値)でした。前年同期(304件)より49%多く、比べた5年間(2022年から)で最多です。10月13日時点では485件で、2025年の1年分(432件)を超えています[6]。

数字の読み方

4つの集計は、数える範囲も単位も違います(上場企業とその子会社の分だけ、委員会への報告の件数、サイバー攻撃による事案だけ)。足したり互いに比べたりせず、同じ集計の前の年と比べて読みます。

専門家の予測・懸念 一方で、ラックの CTO(技術の責任者)は、2026年秋に公表が集中したことについて、こう述べています(企業の解説記事による)。「攻撃が短期間に急増したというよりも、各社の調査や情報開示の時期が9月末に重なった面が大きい」。同じ攻撃者によると判断する材料はない、ともしています[7]。



専門家

数字の大きさに驚くより、自分が使っているサービスが含まれていないかを確かめることが大切です。使っている店やサービスからのお知らせを見てみましょう(本書の推奨)。

2026年の主な事案

実際に起きた事例 2026年4月以降に公表された主な事案を、狙われた仕組みの型ごとに、次の4つの表にまとめます(各社・各団体の公式発表による)。同じ型の事案は、起き方も、使っていた人が確かめることも似ています。このうち10件の公表の時期を、図1-1に示しました。

「公表」は最初の発表の日(2026年)、規模は2026年10月27日の時点で確かめた最新の発表の値です。規模の表し方(人・件・アカウント・レコード〔データの1行分〕・延べ〔重なりを含めて数えた数〕)は、発表ごとに違います。同じ人が重なることもあるので、足したり比べたりはできません。「おそれ」「可能性」「最大」は発表の言い方のままです。名寄せは同じ人の重複をまとめること、ハッシュ値は元に戻しにくい形に変換した値です。

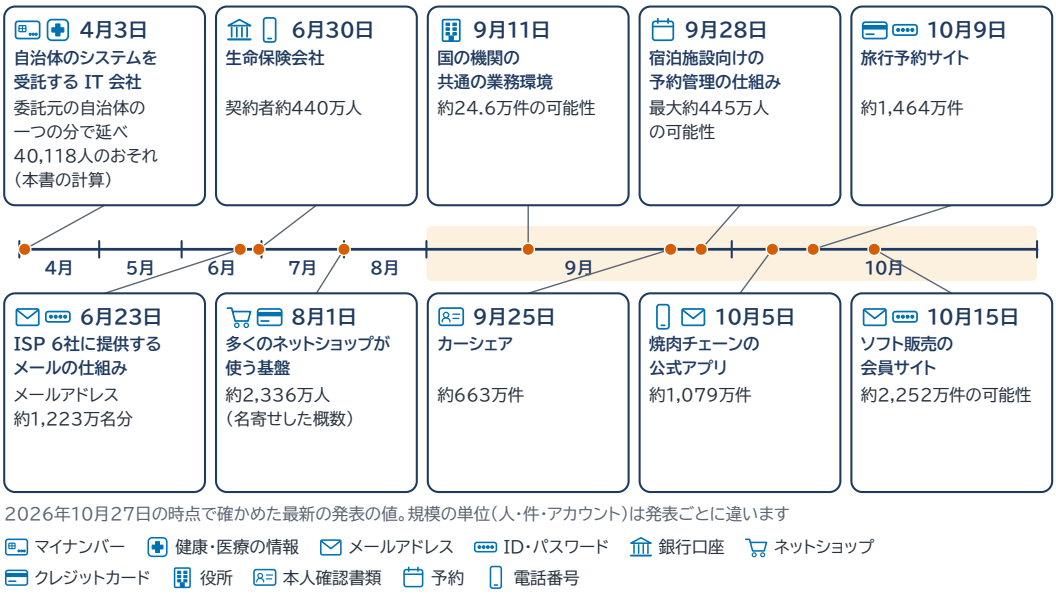


図1-1 2026年4～10月の主な事案の公表時期

型1　多くの会社や店が使う共通の仕組み

1つの仕組みが破られると、それを使う多くの会社や店の利用者に広がります（第2章「1か所の侵害が広がる」）。

公表	事案（狙われた仕組み）	規模	漏れた（おそれを含む）主な情報
6/23	ISP（インターネット接続事業者）6社に提供するメールの仕組み[8]	メールアドレス約1,223万名分（うちパスワード約762万名分）	メールアドレス、ID・パスワード
7/31	リラクゼーションの店の予約・顧客管理の仕組み[9]	約2,218万レコード（人数ではない）	氏名・住所・生年月日、電話番号、メールアドレス、健康・医療の情報（施術の備考欄の一部）
8/1	多くのネットショップが使う基盤[10]	約2,336万人（名寄せした概数）、7,858店	氏名・住所、電話番号、メールアドレス、クレジットカード（番号の一部など）、ID・パスワード（暗号化したもの）
9/11	国の機関の共通の業務環境[11]	約24.6万件の可能性（職員など。一般の人の情報は含まない）	氏名、メールアドレス、電話番号など
9/28	宿泊施設向けの予約管理の仕組み[12]	最大約445万人の可能性	氏名、電話番号、メールアドレス、購買履歴・会員情報（宿泊の予約）
10/19	企業が顧客にメールを送るための配信サービス[13]	49システムで延べ51,628,280件（調べている最中のシステムがあり、増える可能性）	メールアドレスなど（利用する会社ごとに違う）
10/21	別のメール配信サービス[14]	全契約者の情報と、345契約の配信先のリストなど（10/27 の12時30分の時点）	メールアドレスなど（利用する会社ごとに違う）
10/21	仮想のパソコンを貸すクラウド[15]	サーバー26,739件（影響の可能性がある数。取得が確認された数ではない）	ID・パスワード（サーバーに保存された取引口座のログイン情報など）
10/23	別のネットショップの基盤[16]	利用する1店舗の会員情報3,147,469件	氏名・住所・生年月日、電話番号、メールアドレス、ID・パスワード（ハッシュ化したもの）

型2　仕事を任された会社（委託先）

自分が使っていた会社ではなく、その会社が仕事を任せた先から漏れることがあります。

公表	事案（狙われた仕組み）	規模	漏れた（おそれを含む）主な情報
4/3	自治体のシステムを受託する IT 会社[17]	委託元の自治体の一つの分で、3つのシステムの延べ40,118人（本書の計算）のおそれ[18]	氏名・住所・生年月日、マイナンバー、健康・医療の情報
10/8	カラオケ店（委託先のパソコン1台が感染）[19]	約872万件のおそれ（顧客約863.1万件、従業員約9.3万件）	氏名（登録名）・生年月日、電話番号、メールアドレス

型3　公式アプリ・共通の会員 ID

スマホの公式アプリや、1つの ID で複数のサービスに入る仕組みが狙われました。

公表	事案(狙われた仕組み)	規模	漏れた(おそれを含む)主な情報
10/5	焼肉チェーンの公式アプリ[20]	約1,079万件	氏名(登録名)、電話番号、メールアドレス、会員情報(会員番号)
10/6	ディスカウントストアのアプリと通販[21]	流出の可能性がある対象は最大1,735,154人(10/3 時点の会員)	氏名、電話番号、メールアドレス、会員情報(会員 ID)
10/8	コンビニのアプリ(アプリに本人の情報を表示する仕組み)[22]	会員 ID の2,155,345件、アプリ予約の26件	氏名、生年月日(可能性)、性別・電話番号・住所(入力していた人)、クレジットカード(予約の26件。番号の一部)
10/15	ハンバーガーチェーンの公式アプリ[23]	約1,118万件	氏名・生年月日・都道府県、電話番号、メールアドレス、会員情報(会員 ID など)
10/19	百貨店グループの共通の会員 ID(予約サイトから顧客管理の仕組みへ)[24]	約126万件の個人情報の一部(共通の会員 ID のほぼすべての会員)	氏名・住所・生年月日、電話番号、メールアドレス、会員情報(利用サービス)
10/22	ゲーム会社の共通の会員ID[25]	メールアドレスなど11,774,247件(全世界の合計)。うち196件はパスワードを不正に変えられた	メールアドレスと識別情報、連携する通販サイトの氏名・住所・購入履歴など(19件)[26]

型4　会員サイト・通販・予約などのサービス

会社が自分で運営するサイトや、その裏の仕組みが狙われました。

公表	事案(狙われた仕組み)	規模	漏れた(おそれを含む)主な情報
6/30	生命保険会社(契約者向けのサイトなど)[27]	契約者約440万人(うち口座の情報は約22万人)	氏名・住所・生年月日、電話番号、銀行口座、保険の保障内容
7/24	家電などの通販サイト[28]	約772万件(外部に持ち出し)	氏名・住所・生年月日、電話番号、メールアドレス
8/28	カー用品店の作業予約[29]	会員1,797,124名(10/15 の最終報で流出が確定。第一報は最大1,801,499名の可能性)	氏名・住所・生年月日、電話番号、メールアドレス、ID・パスワード(「復元できない状態」とされる)、会員情報(会員番号)
9/16	画像共有サービス[30]	約2,362万件(アカウント数で、人数ではない)、画像の付帯情報約4.9億件。133名の画像432件は閲覧・取得	メールアドレス、ID・パスワード(ハッシュ値)
9/25	カーシェア[31]	約663万件(うち本人確認書類の画像は、外部へ送られた痕跡が約146万件)	氏名・住所・生年月日、電話番号、メールアドレス、本人確認書類・顔写真
9/30	宅配便の荷物問い合わせのサービス[32]	流出した可能性がある情報が最大約5,323万件(重複を含む件数。人数ではない)	氏名・住所、電話番号(送り状の依頼主・届け先)、メールアドレス(会員サービスの会員)
10/5	アンケートサイト[33]	会員の個人情報894,082件(外部に持ち出し。10/14 の第2報で確定)	氏名・住所・生年月日、電話番号、メールアドレス、ID・パスワード(暗号化したもの)、会員情報(保有ポイント数など)

公表	事案(狙われた仕組み)	規模	漏れた(おそれを含む)主な情報
10/9	旅行予約サイト[34]	約1,464万件(うちハッシュ化したパスワード約413万件)	氏名など、ID・パスワード、クレジットカード(最大6,140名)
10/15	ソフト販売の会員サイト(会員情報を取り出す仕組み)[35]	約2,252万件の可能性	メールアドレス、ID・パスワード、氏名・住所・生年月日、電話番号
10/23	リユース店の出張買取などの案件管理[36]	顧客の情報746,277件(うち11件は氏名・住所も)	メールアドレス
10/23	ホビー用品の公式の通販サイト[37]	件数の記載なし(すべての会員に個別に案内)	氏名・住所、電話番号、メールアドレス、注文情報、クレジットカード(番号の下4桁と有効期限)。どれも閲覧された可能性

型ごとに、使っていた人が確かめること

実際に起きた事例 表のうち次の8件は、それぞれの発表の時点で、不正利用などは確認されていないとしています。家電などの通販サイト[28]・カーシェア[31]・焼肉チェーン[20]・カラオケ店[19]・コンビニ[22]・百貨店グループ[24]・宅配便[32]・リユース店[36]の件です。一方、仮想のパソコン(ネットの向こうのサーバーで動き、手元の端末から使うパソコン)を貸すクラウドの件では10月22日、利用者から、取引口座で第三者による不正な操作が行われたとの報告がありました[15]。10月24日の第4報では、利用者の情報が外部に持ち出された事実を確認したとし、攻撃者とみられる者からの金銭の要求には応じないとしています[38]。その後の続報は 6-5 で紹介します。数字や項目は、続報で変わることがあります。ネットショップの基盤の件では、8月の「最大で延べ約885万件」が、最終報で約2,336万人になりました[10]。

実際に起きた事例 各社の発表のうち、使っていた人が確かめるときに役立つ点を、型ごとに挙げます。

型1 共通の仕組み

- **お知らせは、使っていた店やプロバイダーから届きます。** 基盤や配信サービスの会社の名前を知らなくても、店からのお知らせを確かめます(本書の推奨)。
- **同じ基盤でも、店ごとに漏れた項目が違うことがあります。** 8月公表のネットショップの基盤の件では、基盤の最終報の項目にカード情報とパスワードがありました。一方、利用店の中には、自店の客の分は対象外と知らせた店もあります[39,40]。自分が使った店のお知らせで、項目を確かめます(本書の推奨)。
- **ISP 向けのメールの件:** 対象は6つの ISP のメールです。各 ISP がパスワードの強制変更を進めていて、同じ会社の携帯電話のメールなどは、別の設備のため影響はないとされています[8]。
- **メール配信サービスの件(10月19日公表):** 鉄道の予約サービス・銀行・ソフト会社は、最初は影響がない、または対象外と知らされていました。10月26日になって、漏えいした、または漏えいの可能性が高いと知らされています[41,42,43]。最初のお知らせで対象外とあっても、続報を確かめます(第5章)。配信サービスの会社のドメイン(メールアドレスの @ より後ろの部分)を使い、カード会社を名乗る迷惑メールも確認されています[13]。
- **別のメール配信サービスの件(10月21日公表):** マンガ配信アプリの会社では、メールマガジンの宛先1,002,404件のメールアドレスが流出しました。パスワード・氏名・カード情報は含まれていません[44]。

型2 委託先

- **カラオケ店の件:** パスワードは含まれないと明記しています。10月26日には、影響を受けた可能性のある人に、SMS などで順次連絡していると追記しました。新たな漏えいが確認されたわけではないとしています[19]。届いた連絡が本物か迷うときは、連絡にあるリンクを使わず、公式サイトで確かめます(第5章。本書の推奨)。

型3　公式アプリ・共通の会員 ID

- **ゲーム会社の件**: パスワードを不正に変えられた196件のうち19件では、連携する通販サイトのマイページで、氏名・住所・購入履歴などが見られました[26]。1つの ID で複数のサービスに入る仕組みでは、1か所の乗っ取りが広がります。パスキーか2段階認証を設定します（第4章。本書の推奨）。パスキーは、パスワードの代わりに、スマホなどの機器と指紋・顔・PIN（暗証番号）で本人を確かめる仕組みです。2段階認証は、パスワードのほかに、確認コードなどでも本人かを確かめる仕組みです。
- **ディスカウントストアの件**: 住所・生年月日・クレジットカードの情報・パスワード・購入履歴は流出していないとしています[21]。
- **コンビニのアプリの件**: 10月24日に、メールアドレスは漏えいしておらず、生年月日の漏えいの可能性がある、と項目を訂正しました[22]。
- **ハンバーガーチェーンの件**: カード番号は持っておらず、ログインのパスワードの漏えいは確認されていないとしています[23]。
- **百貨店グループの件**: 通販の2つのサイトでも10月17日に不正アクセスが確認され、両サイトのシステム全体を止めました。持っている情報が漏えいした可能性は、調べている最中です（10月19日の発表）[24]。

型4　会員サイト・通販・予約

- **生命保険会社の件**: マイナンバー、クレジットカードの情報、メールアドレスは含まれていません[27]。
- **カー用品店の件**: パスワードは「復元できない形式で保管」していたので、漏れた情報でアカウントが不正に使われるおそれはない、としています[29]。それでも、そのサービスのパスワードを変え、同じパスワードをほかで使っていれば、そちらも変えます（本書の推奨）。
- **画像共有サービスの件**: 会社は、データベースの情報が外部に流出したとしています。ただ、送られた通信の内容そのものの記録はなく、送られた項目や件数は直接確かめられていません。外部の専門機関は「データ流出のおそれは相応に高い」と評価しています。流出したとする付帯情報には、撮影場所の位置情報（画像に含まれる場合）や、画像の中の文字を読み取ったテキストなども含まれます。会社は、ログインに関わる情報の一部と、外部サービスとの連携の情報を無効にしました。そのうえで、まだパスワードを変えていない人には変更を求め、同じか似たパスワードをほかで使っていれば、そちらも変えるよう呼びかけています[30]。
- **宅配便の件**: 荷物を送った人は依頼主として、通販で受け取っただけの人も届け先として、対象になる可能性があります。カード情報・パスワード・口座の情報は含まれていません[32,45]。会社を装った不審なメール・SMS・電話に注意します（第5章）。
- **アンケートサイトの件**: 10月7日に、全会員のパスワードを無効にしました[33]。ポイントの不正な交換と補填は、第7章で紹介します。
- **旅行予約サイトの件**: 表の約1,464万件とは別の2つの経路でも、返金先の口座の情報を含む17,780件と、バス予約の情報約12,000件が出ました。表の数とは足し合わせません[34]。
- **ソフト販売の件**: パスワードを順に無効にし、ログインのときに再設定を求めています。同じメールアドレスとパスワードの組み合わせをほかで使っていれば、そちらも変えるよう呼びかけています[35]。
- **リユース店の件**: 不審な電話を受けたら、相手が名乗った組織の公式の連絡先を自分で確かめて問い合わせるよう呼びかけています[36]。
- **ホビー用品の通販の件**: すべての会員に、個別のメールで案内するとしています。会社や公的機関・金融機関を名乗る不審な連絡に注意するよう呼びかけています[37]。

スクリーンショット（画面を写した画像）には、パスワードや個人情報が写りこみやすいものです。画像共有サービスに置いた画像も見直します（本書の推奨）。

漏れた情報の種類によって、やることは変わります。種類ごとの「今日やること」は第6章にまとめました。

10月に相次いだ注意喚起

制度・公式情報 2026年10月には、国の機関などが事業者向けの注意喚起を相次いで出しました。7〜13日に出したのは、個人情報保護委員会、JPCERT/CC（国内のセキュリティの事故の情報を集め、対応を調整する組織）、国家サイバー統括室、IPA（情報処理推進機構）などです。同じ期間に、金融庁、総務省、経済産業省、情報通信研究機構（NICT）も続きました。国家サイバー統括室は10月14日に、各機関の注意喚起の一覧を載せています[46]。

制度・公式情報 JPCERT/CC は、9月前後に国内の組織で、不正アクセスによる個人情報などの漏えいが相次いでいるとしています。ふだん散発的に起きるランサムウェア（データを暗号化して身代金を求める不正なプログラム）の攻撃とは別に、大量の漏えいにつながる攻撃の型が増えているおそれがある、としています[47]。

制度・公式情報 10月21〜22日には、IPA と JPCERT/CC が、Web サイトなどで広く使われているプログラムの言語 PHP の深刻な脆弱性（ソフトや機器の弱点）について、注意喚起を出しました[48]。止めたサービスの例は第2章、会社の対応は第8章で説明します。

制度・公式情報 個人に向けては、警察庁が「サイバー警察局便り」Vol.19（10月8日）で、「様々な事業者、団体、企業を狙って様々な手口でサイバー攻撃が行われ情報流出事案が続発しています」と書いています。そのうえで、「情報流出元の企業をかたる偽メールの可能性があります」として、メールの中のリンクを安易に押さないよう呼びかけています[49]。



警察官

情報が漏れた会社をかたる、偽のメールの可能性があります。メールの中のリンクは、安易に押さないでください[49]。

制度・公式情報 IPA は10月26日、自分の個人情報が漏えいしたときの「対処」と「日頃の対策」をまとめました。まず、漏れた情報の種類を、サービスの会社からの連絡や案内で確かめます。そのうえで、種類ごとに対処するよう勧めています[50]。本書の第6章も、同じ考え方で、漏れた情報の種類ごとにまとめています。

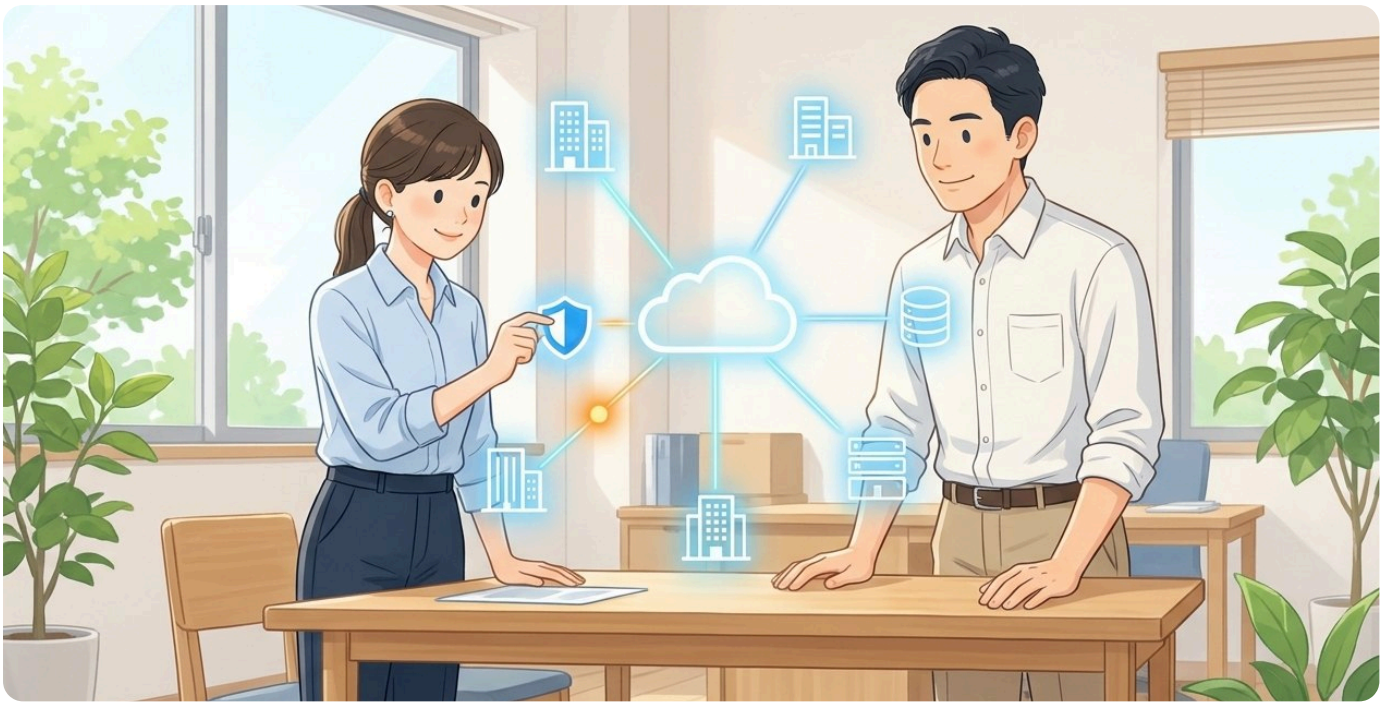
会社の担当者がすべきことは、第8章で説明します。

今日やること

1. 使っているサービスや店から、漏えいのお知らせが届いていないか確かめます。気になるときは、その会社の公式サイトを自分で開いて、お知らせを確かめます。最初のお知らせで対象外とされても、続報を確かめます（本書の推奨）。
2. メールや SMS（携帯電話の番号あてに届く短いメッセージ）のリンクは安易に押さず、パスワードの使い回しをやめます（第4章）[49]。
3. 漏れた、または漏れたおそれがあると知らされたら、第5章の手順に進みます。

■ 共通

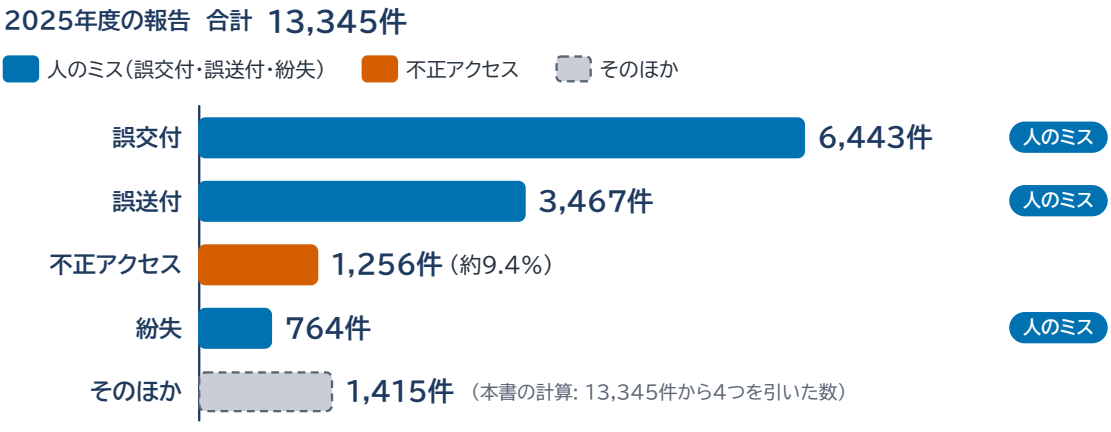
第2章　なぜ漏えいが相次ぐのか



第1章で見た漏えいの背景と原因を、公的機関や調査会社の資料から整理します。原因が分かると、備え方も見えてきます。

集計で見る漏えいの原因

実際に起きた事例 個人情報保護委員会（個人情報の扱いを監督する国の機関）が民間の事業者などから直接受け付けて処理した報告は、2025年度に13,345件ありました。原因別では、誤交付（書類などを別の人に渡すこと）が6,443件、誤送付（別の宛先に送ること）が3,467件、紛失が764件と、人のミスが多くを占めました。不正アクセス（許可なく他人のシステムに入ること）は1,256件（約9.4%）です。ほかの省庁を通じて届いた分も含む民間の報告17,139件では、1件あたりの本人の数が1,000人以下のものが93.6%でした[1]。



個人情報保護委員会が直接受け付けて処理した報告。

図2-1　個人情報保護委員会に直接届いた漏えいの報告の原因（2025年度）

実際に起きた事例 一方、東京商工リサーチ（調査会社）の2025年の集計では、上場企業とその子会社が公表した漏えい・紛失事故180件のうち、原因は「ウイルス感染・不正アクセス」が116件（64.4%）で最多でした。同社が示した人数の平均も、この原因が最多の563,637人分でした（平均の計算の対象は示されていません）[2]。

2つの集計は、主体も範囲も違うので比べられません。委員会への直接の報告では人のミスが多く、上場企業とその子会社が公表した事故では「ウイルス感染・不正アクセス」が目立つ、ということです。人のミスへの備えは第8章で扱い、この章では不正アクセスの原因を見ていきます。

専門家の予測・懸念 IPA（情報処理推進機構）の「情報セキュリティ10大脅威 2026」の組織編では、1位がランサムウェア（データを暗号化して身代金を求める不正なプログラム）などによる攻撃の被害（11年連続）でした。2位は、サプライチェーン（委託先や取引先のつながり）や委託先を狙った攻撃です。3位には、AI（人工知能）の利用をめぐるサイバーリスクが初めて選ばれました。4位は、システムの脆弱性（ソフトや機器の弱点）を悪用した攻撃です[3]。前の年に社会に影響があった脅威を、有識者が審議・投票して選んだもので、起きた件数の順位ではありません。

この章では、これらの脅威に沿って、ランサムウェア、委託先、脆弱性と AI、設定の誤り、持つ情報の順に見ていきます。

ランサムウェアと VPN 機器

実際に起きた事例 警察庁によると、企業・団体などのランサムウェアの被害の報告は、2026年上半期（1～6月）に123件でした。統計を取り始めた2020年下半期以降、半期で最多です。規模別では、中小企業が約6割です[4]。警察に報告された件数で、すべての被害の数ではありません。

制度・公式情報 警察庁は、背景に RaaS（ランサムウェアを、攻撃に必要な道具や場所ごと貸し出す犯罪の分業）による「攻撃者の裾野の広がり」があるとしています。被害の多くは、データを盗んだうえで、払わなければ公開すると要求する二重恐喝です[4]。ランサムウェアの被害では、データの暗号化だけでなく、情報の漏えいを伴うことが多いのです。

実際に起きた事例 これとは別に、データを暗号化せずに盗み、公開をほのめかして金銭を求める「ノーウェアランサム」も、2026年上半期に9件ありました（2025年の1年間は17件）[4]。

実際に起きた事例 侵入の入口で多いのは VPN 機器（社外から社内のネットワークにつなぐための機器）です。警察庁が被害組織に聞くと、2026年上半期に感染経路の回答があった36件のうち、VPN 機器が18件、リモートデスクトップ（離れた場所からパソコンを操作する仕組み）が9件でした。過去5年（2021～2025年）の485件でも、VPN 機器が293件、リモートデスクトップが105件で、不審なメールやその添付ファイルは24件です[4]。どちらも回答の数で、すべての被害ではありません。

制度・公式情報 警察庁は、インターネットに露出した箇所から、攻撃者が遠隔操作で中に入る手口が多くを占めるとしています。特定の相手を狙ったメールの添付ファイルによる感染は、少なくなっているといいます。攻撃者は、修正していない脆弱性や、漏えいした認証情報（ID・パスワードなど）を悪用して入る、とも説明しています[4]。



攻撃者

インターネットにつながった VPN 機器などの弱点や、漏れた ID・パスワードを使って、遠隔操作で入り込みます[4]。

実際に起きた事例 自治体のシステムを受託する IT 会社は、ネットワーク機器の管理者アカウントの認証情報が「攻撃者による認証試行等により推測または取得され」、内部に入られたと推定しています[5]。国の機関の共通の業務環境でも、第三者が VPN 機器の脆弱性を使って侵入したと公表されました（9月11日）[6]。

VPN 機器の更新など、会社がすべきことは第8章で説明します。

1か所の侵害が広がる

実際に起きた事例 2026年は、多くの会社が使う仕組みや、仕事を任された会社（委託先）が狙われる事案が続きました。1か所の侵害が、多くの会社と利用者に広がります（図2-3）。プロバイダー（ISP。インターネット接続事業者）6社向けのメールの仕組みの件では、メールアドレス約1,223万名分が漏えいしました[7]。多くのネットショップが使う基盤の件では、対象の店舗が7,858店、対象者が約2,336万人（名寄せした概数）です[8]。



図2-2　1か所の仕組みが狙われると、多くの店や利用者に広がる

実際に起きた事例 メール配信サービス（企業が顧客にメールを送るためのサービス）の件（10月19日公表）でも、専用プランの5つのシステムが狙われました。プログラムの脆弱性を突かれ、担当者の認証情報（ログインに使う情報）を取られています。メールアドレスを含む情報が、延べ約900万件出力されたと試算されました（10月19日）[9]。10月26日の第二報では、漏えいは49システムで起き、延べ51,628,280件としています。漏えいの件数を調べている最中のシステムが16あり、延べ件数は増える可能性があります[10]。このサービスを使っていた鉄道の予約サービス・銀行・ソフト会社は、最初は影響がない、または対象外と知らされていました。10月26日になって、漏えいした、または漏えいの可能性が高いと知らされています[11,12,13]。

実際に起きた事例 別のメール配信サービスの件（10月21日公表）では、運営会社のサーバーに侵入され、全契約者の情報が持ち出されました。配信先のリストなど、契約者の情報以外の漏えいが確認された契約は、345件です（10月27日12時30分の時点。契約の数で、人数ではありません）[14]。このサービスでメールマガジンを送っていたマンガ配信アプリの会社では、1回分の配信の宛先1,002,404件のメールアドレスが流出しました[15]。自治体の事業の委託先・再委託先が使っていた分でも、漏えいやその可能性が公表されました（10月23日）。ある自治体の関係団体が仕事を任せた事業者の分では、最大約16,000件（氏名・メールアドレス・属性）です[16]。別の自治体も、再委託先を含む受託事業者の3つのサイトで、漏えいの可能性があるとしています[17]。自治体の事業に登録した人の情報が、委託先・再委託先が使う外部のサービスをたどって漏れた例です。

実際に起きた事例 委託先や外部の会社が狙われた件もあります。自治体のシステムを受託する IT 会社の件では、委託元の自治体の一つの分だけで、3つのシステムの延べ40,118人（本書の計算）に、漏えいのおそれがありました[18]。カラオケ店の件では、委託先の従業員のパソコン1台がマルウェア（不正なプログラム）に感染し、約872万件に漏えいのおそれがあると公表されました[19]。国の機関も10月22日、不正アクセスがあったと公表しました。狙われたのは、

ホームページの運営に使っていた、外部の会社のクラウド（ネット上で使うソフトや保存場所）の環境です。Web サイトを作るためのものです。問い合わせフォームの情報などに、漏えいの可能性があるとしています[20]。

制度・公式情報 国家サイバー統括室は10月9日、サプライチェーンを通じた侵害などで、個人情報を含むデータが盗まれる事案を「複数確認」したと発表しました。攻撃者は「比較的防御が弱い委託先企業等を足掛かりとして侵入」することがある、としています[21]。

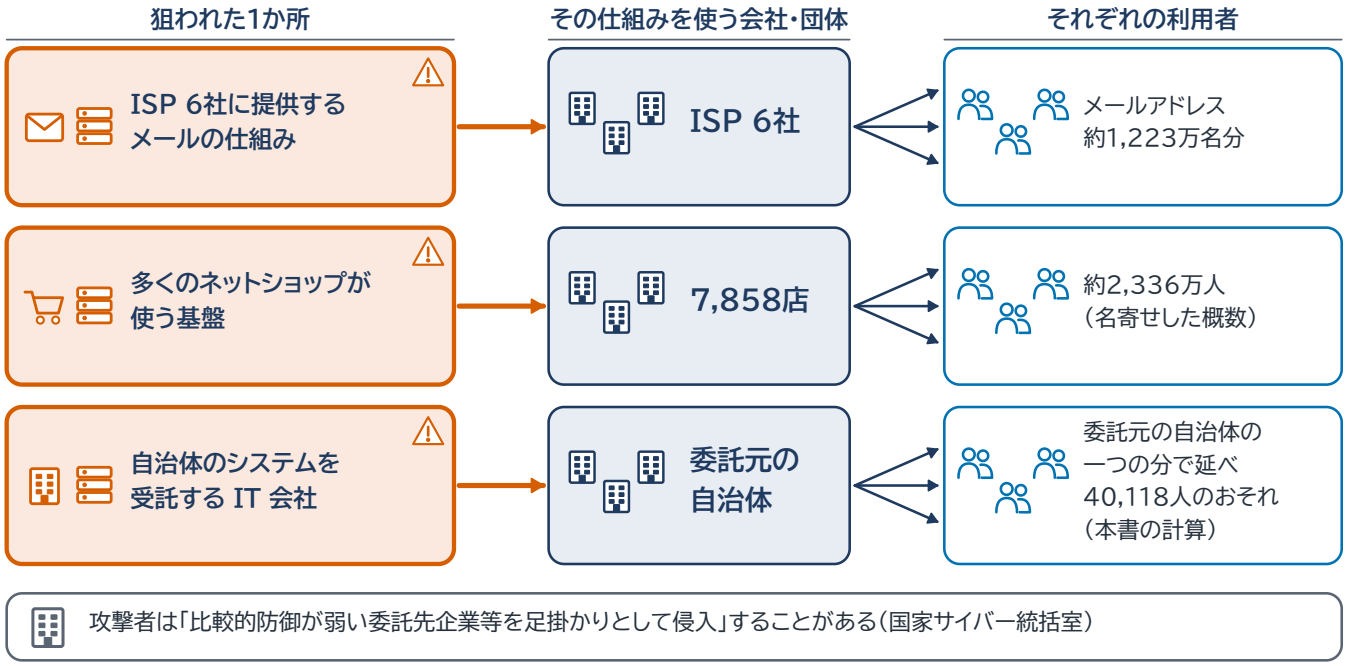


図2-3　1か所の侵害が多くの会社と利用者に広がるしくみ

実際に起きた事例 数字にも表れています。個人情報保護委員会が直接受け付けた報告（2025年度）では、漏えい元が委託先のものが1,292件（9.7%）で、そのうち不正アクセスは328件でした[1]。トレンドマイクロ（セキュリティ企業）の集計では、国内の組織が2026年1～9月に公表したサイバー攻撃の被害は607件でした。そのうち、委託先などでの被害（データサプライチェーン被害）は62件（10.2%）です[22]。



専門家

使っている会社が、どの委託先やサービスを使っているかは、利用者からは見えにくいものです。知らない会社から「漏れたおそれがある」と知らされても、捨てたりリンクを開いたりせず、第5章の手順で確かめましょう。使っている会社のお知らせも、ときどき確かめます（本書の推奨）。

弱点を突く速さ

修正が追いつかない

実際に起きた事例 Verizon（米国の通信会社）の2026年の報告は、世界145か国の確定した侵害2万2,000件超を集計しています。そのうち、侵入の入口が分かった約2万件（人のミスや内部の者の不正を除く）では、「脆弱性の悪用」が31%で、初めて首位になりました。米国の政府機関（CISA）の一覧で悪用が確認されている重大な脆弱性のうち、組織が2025年に完全に修正したのは26%（前年38%）でした。完全に修正するまでの日数は、中央値で43日（前年32日）です[23]。

専門家の予測・懸念 Microsoft の報告（世界）は、公開された脆弱性が悪用されるまでの期間が「数日程度」に縮まっているとしています[24]。

実際に起きた事例 国内でも、トレンドマイクロの集計では、攻撃された場所が分かる375件のうち38.7%が、Web サーバーなどの公開システムでした。前年同期の30.3%から上がっています[22]。

実際に起きた事例 2026年10月21～22日には、Web サイトで広く使われるプログラムの言語 PHP の深刻な脆弱性が公表され、IPA が注意喚起を出しました[25]。保育・教育施設向けのサービスの会社は、修正版が出る前に予防のため全サービスを止めました。修正を当てて22日3時22分に主なサービスを再開し、23日にはすべての機能を再開しました。本件による不正アクセスや情報漏えいは確認されていないとしています[26]。ネットショップ作成サービス・イラスト投稿サービス・関西の鉄道会社なども、サービスを一時止めたと報じられています[27]。国税を扱う国の機関も22日、ホームページなどの公開を午前10時20分ごろから一時止め、点検と修正プログラムの適用のあと、午後4時10分ごろに再開しました[28]。

実際に起きた事例 同じ週の10月23日には、8月の件とは別のネットショップの基盤、リユース店の出張買取などの案件管理、ホビー用品の公式の通販サイトの漏えいや、そのおそれが公表されました。3社とも、PHP の脆弱性によるものではないとしています[29,30,31]。予防のためのサービスの停止と、同じ時期に公表された漏えいは、分けて読みます（本書の推奨）。

業務のシステムとアプリの窓口

制度・公式情報 JPCERT/CC（国内のセキュリティの事故の情報を集め、対応を調整する組織）によると、被害は利用者向けのアプリだけでなく、業務用のシステムにも及んでいます。BI ツール（データを集計・分析する業務ソフト）や、従業員向けの管理システムなどです。画面の操作ではできない内部の API（ソフト同士がやりとりする窓口）への不正な要求も、手口の型に挙げています[32]。

実際に起きた事例 ある会社は、社内で使っていた BI ツールの脆弱性が、修正プログラムを当てる前に悪用され、約17万件の個人情報が漏えいしたと公表しました（9月30日の第四報）。購買履歴や決済金額の記録も含まれます。この会社は、スクリーンショットやデータを SNS で転載・拡散しないよう呼びかけています[33]。漏れた情報を見かけても、広めないようにします（本書の推奨）。

専門家の予測・懸念 情報通信研究機構（NICT）は10月13日、サーバーを狙う手口の一つを「A2B攻撃」と名付けました。公開されているスマホのアプリ（Android 版）を解析し、アプリが通信するサーバーの接続先や仕組みを調べて狙うものです。NICT は、これを「国内で相次ぐ情報漏えい事案の原因の一つ」としています[34]。

推測されやすいパスワードと保存のしかた

制度・公式情報 個人情報保護委員会は、指導した不正アクセスの原因を挙げています。①公表され対応の方法も出ていた VPN 機器などの脆弱性の放置、②推測されやすい ID・パスワード、③設定ミスによるデータベースへのアクセスの制限の不備などです。個人データ（会社などが、名簿やデータベースのように探しやすく整理して持っている個人情報）を守る対策（安全管理措置）に「不備があったケースが多くみられた」ともしています[1]。プロバイダー向けのメールの仕組みの件では、パスワードが平文（そのまま読める形）で保存されていた、と委員会は説明しています[35]。

実際に起きた事例 あるクラウド事業者は9月10日、顧客の契約情報を管理する販売管理システムへの不正アクセスが、2023年4月～2026年3月の間に起きていたと公表しました。閲覧・取得された可能性がある会員情報は1,360,563アカウントです。外部へ持ち出されたことを裏付ける明確な事実は確認されていない、としています。このシステムには、一部の初期パスワードが、ハッシュ化（元に戻しにくい形への変換）をされずに保存されていました。使われ続けていたものは、会社が変えました[36]。

実際に起きた事例 Microsoft の報告の要約版では、侵入の63%でデータが盗まれていました（何件の侵入を対象にした数かは示されていません）。侵入の半数超では、入ったあとにさらに認証情報が盗まれていました。同社は、1つの乗っ取りが多くの乗っ取りを生む、と書いています[24]。

AI の悪用

専門家の予測・懸念 AI の悪用も懸念されています。警察庁は、生成 AI で攻撃のハードルが下がり、高度な技術を持たない者でもサイバー攻撃を実行しやすくなると考えられる、としています[4]。

実際に起きた事例 警察庁は、AI を悪用した事件の検挙例も挙げています。2026年6月には、AI を悪用して作ったコードを組み合わせてランサムウェアを作った19歳の会社員が、千葉県警察に逮捕されました[4]。

実際に起きた事例 Verizon の報告では、AI の助けを借りた不正なプログラムの開発の多くは、よく知られた手口と同じ機能のものでした。知られた類例が1つ以下の珍しい手口は、同報告が観測した中の2.5%未満です[23]。

専門家の予測・懸念 トレンドマイクロは10月23日、日本を狙う3つの攻撃の基盤（攻撃に使う道具や仕組み）を解析した結果を公表しました。AI が変えたのは、並行して扱える標的の数や、試す速さなどだとしています。悪用される脆弱性の種類や、侵入口の性質は変えていないといいます。同社は「攻撃者が入り込む侵入口そのものは、いまも昔と変わらず、公開された旧式のシステムや設定の不備です」と述べています[37]。

対策の基本は、修正プログラムを速やかに当てることと、推測されにくいパスワードや多要素認証（パスワード・スマホ・指紋など、種類の違う確かめ方を2つ以上組み合わせる仕組み）を使うことです[21]。個人の備えは第4章、会社の対策は第8章で説明します。

設定の誤りで見える状態に

実際に起きた事例 侵入されなくても、設定の誤りで、情報が外から見える状態になることがあります。宿泊のチェックインの仕組みを提供する会社は、本人確認書類の画像などを保存していたクラウドの保存場所に、設定の不備があったと公表しました（6月30日）。2020年1月20日～2026年5月14日に取得した1,060,338人分の顔写真・署名・パスポートや運転免許証などの画像が、外部から第三者がアクセスできる状態でした[38]。

実際に起きた事例 この会社の9月17日の続報では、第三者機関の調査で、画像データが外部へ流出した事実は確認されていません。二次被害（漏れた情報が使われて、あとから起きる被害）も確認されていないとしています。再発防止策には、権限の設定の棚卸しや、クラウドの設定を自動で点検する仕組みの導入を挙げています[38]。

制度・公式情報 JIPDEC（日本情報経済社会推進協会）のプライバシーマーク推進センターは2026年4月、アクセス権限の設定ミスで、意図せず第三者に情報を公開してしまうことがあると注意を呼びかけました。クラウドの保存サービスや業務ツールで、共有リンクが「リンクを知っている全員が閲覧可」になっている例などです。対策として、アクセス制御の徹底、多要素認証などの認証の強化、ログ（操作の記録）の監視を勧めています[39]。

個人も、Google Drive・OneDrive・Dropbox などで写真や書類を共有しているなら、共有の設定を見直します。「リンクを知っている全員」になっているもののうち、もう要らないものは共有をやめ、要るものは相手を指定する設定に変えます（本書の推奨）。会社の対策は第8章で説明します。

持つ情報・残す期間

実際に起きた事例 漏れた情報には、退会した人や、契約が終わったシステムの情報も含まれていました。カーシェアの件では、退会した人（退会後7年分）や、入会の手続きを終えなかった人のアカウントも含まれました。氏名・住所・生年月日は、法人税法などにもとづいて7年間保管していたと、この会社は説明しています[40]。自治体のシステムを受託する IT 会社の件でも、委託元の自治体では、契約が終わったシステムのデータが、漏えいのおそれの対象でした[18]。

実際に起きた事例 カーシェアの会社は、本人確認書類の画像を「会員期間中および退会後7年間」持っていました。これを、確認が済んだらすぐ削除するルールに改め、持っている画像は2026年10月末までにすべて削除するとしていま

す[40]。焼肉チェーンの会社は、グループの公式アプリ11本を、氏名と電話番号を持たない新しいシステムに変える予定です（2027年上半期）[41]。

制度・公式情報 国家サイバー統括室は、持つ情報の最小化や、パスワードを平文で保存しないことを事業者に求めています[21]。JPCERT/CC も、保存期間を過ぎたデータや、利用目的を終えたデータを残さないよう求めています[32]。

使っていないサービスは退会し、登録したカード情報を消しておきましょう。ただし、退会してもデータがすぐに消えるとは限りません。退会のときに、本人確認書類の画像などの削除も頼みます（本書の推奨）。「持たない・残さない」についての本書の見解は、第10章で述べます。

この章をふまえて

1. 個人: 漏れても被害が広がらないよう、パスワードを使い回さない、強い認証を使う、使わない会員を退会する、の3つを第4章で確かめます。クラウドの保存サービスを使っていれば、共有の設定も見直します（本書の推奨）。
2. 会社: VPN 機器の更新、多要素認証、委託先の確認、クラウドの共有の設定の点検を、第8章で確かめます。データは、法令で保存が求められていないか、業務に必要かを確かめてから、要らなくなったものを消します。

■ 共通

第3章　漏れた情報はどう悪用されるのか



情報が漏れると、知られたくないことを他人に知られるうえ、詐欺や不正なログインなどの二次被害（漏れた情報が使われて、あとから起きる被害）につながる場合があります。この章では、その流れと実例を紹介します。漏れた情報ごとの対応は、第6章で種類別に説明します。

漏えいから被害までの流れ

本書では、漏えいから被害までの代表的な流れを、図3-1の4つの段階で整理します。段階が重なることもあります。各段階に、被害の可能性や広がりを小さくする「止めどころ」があります。

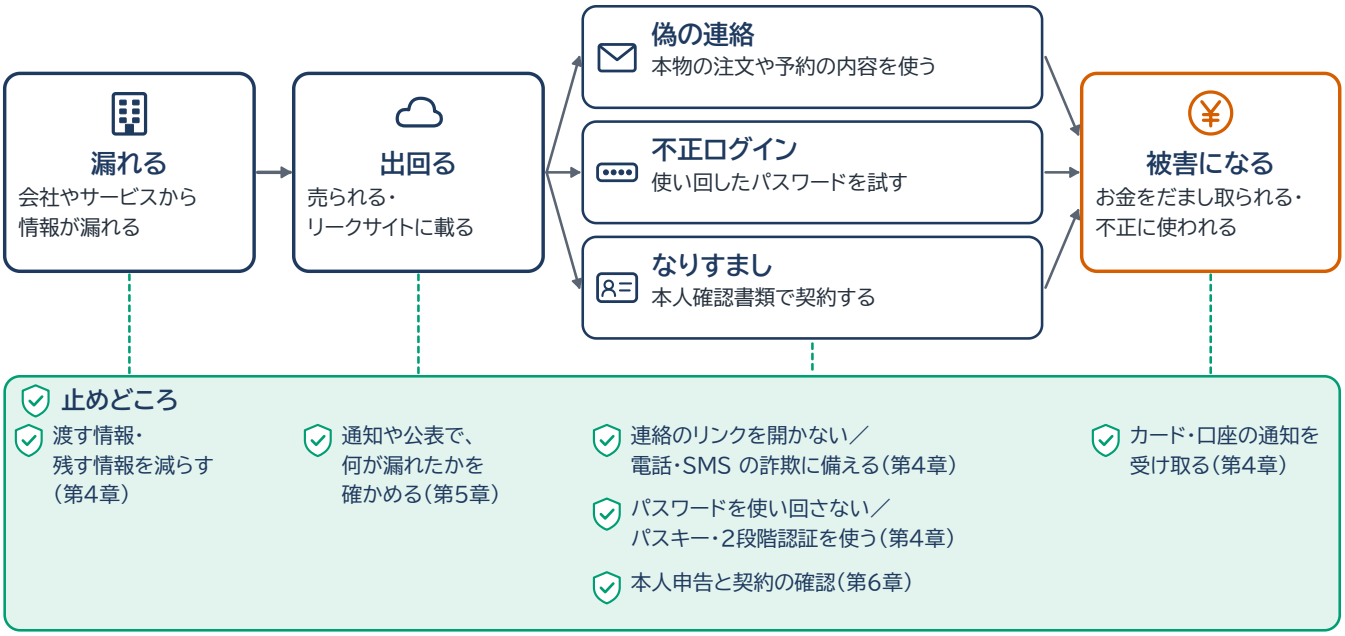


図3-1　漏えいから被害までの流れと止めどころ

制度・公式情報 警察庁によると、ランサムウェア（データを暗号化して身代金を求める不正なプログラム）の被害では、「二重恐喝」が多くを占めます。盗んだデータを公開すると脅す手口です。個人情報などが、ダークウェブ（一般の方法では見られない闇サイト）のリークサイト（盗んだデータをさらすサイト）に載る例も、多数確認されています[1]。

実際に起きた事例 不動産会社が使うクラウド（ネット上で使うソフトや保存場所）の件です。その一部の機能で、2026年4月に不正アクセス（許可なく他人のシステムに入ること）とデータの取得が確認されました。このクラウドを使う不動産会社の親会社は、運営会社からの報告として次のように公表しています。流出した可能性のあるデータが、外部の特定のサイトで販売されている事実が確認されている、という内容です。この親会社は、自社や公的機関を名乗って口座の情報やパスワードを求める連絡に、応じないよう呼びかけています[2]。

実際に起きた事例 仮想のパソコンを貸すクラウドの件（2026年10月公表）では、運営会社が10月27日に公表しました。攻撃者とみられる者が、会社と利用者に関する情報と称するものを公開したのを確認した、という内容です。会社は、事実と異なる内容が含まれるおそれがあるとしています。公開された情報と称するものにはアクセスしたり拡散したりしないよう呼びかけ、アクセスした人の情報は攻撃者に取得されるとしています[3]。同じ日の第11報では、見かけても転載・再投稿・リンクの共有をしないよう求め、公開された情報に利用者の情報があると確認したら、対象の人に個別に連絡するとしています[4]。

公開されたとされる情報は、見に行かず、広めません。自分の情報が含まれているかは、会社からの個別の連絡やお知らせで確かめます。脅されたときは、第5章「写真や家族のことを持ち出して脅されたとき」の手順に従います（本書の推奨）。

専門家の予測・懸念 セキュリティ企業の2026年の調査では、ダークウェブの市場で、日本のカード情報が1件27ドル（約4,000円。中央値とされる）程度で出品されていたと報じられています。個人のメールアカウントは、約1ドルだったとされます。売買が成立したかは、確かめられていません[5]。

実際に起きた事例 2026年10月には、詐欺に関わった疑いなどで逮捕された男のスマホから、名簿が見つかったと報じられました。北九州市の75歳以上の市民7,000人以上の、氏名・住所・電話番号が書かれていたとされます。名簿の入手元は特定されておらず、企業からの漏えいとの関係も確認されていません[6]。

専門家の予測・懸念 IPA（情報処理推進機構）の「情報セキュリティ10大脅威 2026」の個人編は、順位を付けずに10の脅威を挙げています。そこには、ネット上のサービスから個人情報を盗まれることや、サービスへの不正ログインが入っています。クレジットカード情報の不正利用や、フィッシング（本物そっくりの偽のメールやサイトで、情報をだまし取る手口）で個人情報などをだまし取られることも入っています。ネットバンキング（ネットで振込などができる銀行のサービス）の不正利用は、4年ぶりに選ばれました[7]。

本書では、悪用のされ方を「偽の連絡」「不正ログイン」「なりすまし」に分けて説明します。止めどころ（図3-1の下の段）は、第4～6章で説明します。

本物の情報を使った偽の連絡

実際に起きた事例 衣料品の通販の件です。2026年9月28日、複数の顧客から会社に「注文情報と一致する不審な返金案内メールを受け取った」と問い合わせがありました。調べると、会員情報と受注情報の一部に、不正アクセスの痕跡が見つかりました（10月3日公表）。漏えいした可能性があるのは、氏名・住所・電話番号・メールアドレス・生年月日や、注文日時・商品名・金額・届け先などです。カード情報は持っていませんでした[8]。10月9日の続報の時点で、お金の被害の申し出は確認されていません[9]。

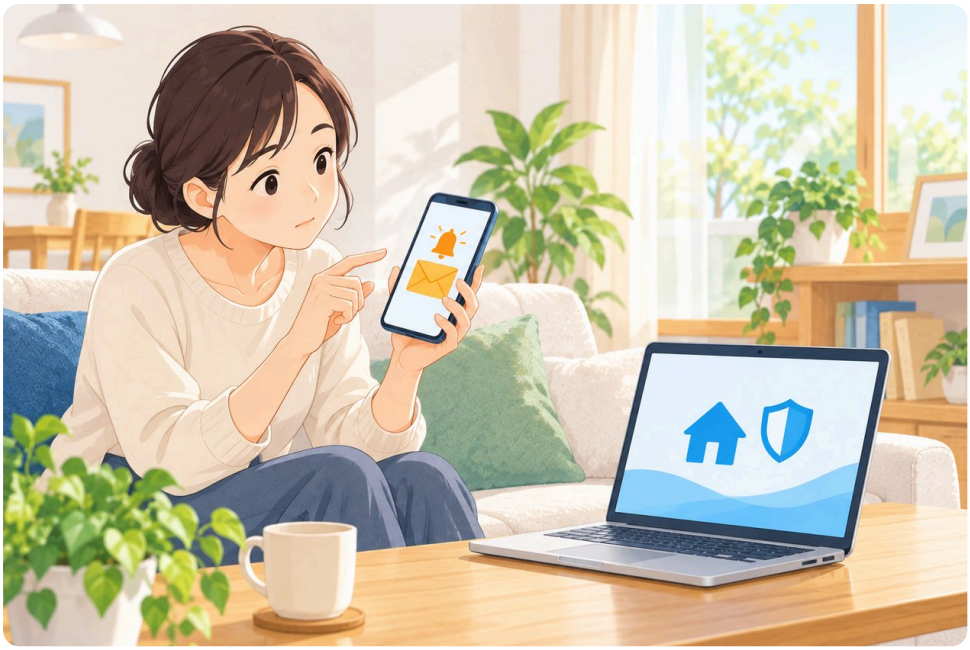


図3-2　本物そっくりの連絡でも、すぐには押さずに立ち止まる

実際に起きた事例 この会社は、関係のないフリーメールのアドレスから届くメール、LINE（メッセージアプリ）への連絡を促す内容、返金の期限で急がせる内容に、特に注意するよう呼びかけたと報じられています[10]。

実際に起きた事例 宿泊施設向けの予約管理の件では、予約した人に不審なメッセージが届きました。予約の情報を知っているらしいもので、メッセージアプリ・メール・SMS（携帯電話の番号あてに届く短いメッセージ）で届いています。事前のチェックインなどを口実に外部のサイトへ誘い、カード情報の入力や支払いを求めるもので、運営会社はフィッシング詐欺とみています[11]。この件では、予約した人の氏名・連絡先・宿泊日などが閲覧または取得された可能性があり、対象は最大で約445万人です（10月9日時点）[12]。

実際に起きた事例 大阪のホテルの件も、予約の情報が漏れた似た例です。ホテルは2026年5月、予約した546名の情報が漏えいしたと公表しました。これに関連して、キャンセルや支払いを促すフィッシングメールが送られた、または送られた可能性が高いとしています。5月29日時点で、具体的な被害は確認されていません[13]。



詐欺師

本物の会社を名乗り、注文や予約と同じ内容で連絡して信用させます。そのうえで、カードの情報やお金をねらいます[8,11]。

実際に起きた事例 フィッシング対策協議会は、2026年9月は情報漏えいの公表が相次いだとしています。「各漏えい事故との関連性については不明」としたうえで、受信者の氏名が本文に書かれたフィッシングメールを確認しています。同じ報告では、AI（人工知能）への指示文が本文に残った「不自然すぎる」メールも見られました[14]。一方で警察庁は、AI 技術の発達で、見抜きにくいフィッシングが増えているとしています[1]。

実際に起きた事例 同じ9月の報告を分野別に見ると、EC（通販）系が47.9%、クレジット・信販系が35.0%でした。かたられたブランドは、Amazon が約33.2%、Apple が約11.1%です。これはかたられた名前で、その会社から情報が漏れたという意味ではありません[14]。

実際に起きた事例 メール配信サービス（企業が顧客にメールを送るためのサービス）の件（10月19日公表）です。配信サービスの会社のドメイン（メールアドレスの @ より後ろの部分）を使い、カード会社を名乗る迷惑メールが複数確認されました。会社は、漏れた情報が公開された事実や、不正に使われた事実は確認されていないとしています[15]。

制度・公式情報 IPA は2026年10月26日、自分の情報が漏えいしたときの対処をまとめました。その中で、「偽メール等の文面に漏えいした自分の氏名が記載されているといった状況も考えられます」としています[16]。



図3-3　詐欺師は、本物の会社や警察になりすまして連絡してくる

制度・公式情報 警察庁も2026年10月、情報が流出した企業をかたる偽メールに注意するよう呼びかけています（第1章）[17]。

実際に起きた事例 警察庁は10月15日、マイクロソフトや日本サイバー犯罪対策センター（JC3）と連携して、フィッシングに使われていた犯罪のインフラ（攻撃の基盤）の実態を調べてきたと発表しました。マイクロソフトなどが米国で起こした民事訴訟の結果、そのテイクダウン（停止させること）に至ったとしています[18]。

対策は進んでいますが、偽の連絡がなくなるわけではありません。



相談者

注文した商品や予約の日まで書いてあると、本物のお知らせかもしれないと迷ってしまいます。

自分しか知らないはずの注文や予約の内容が書かれていても、お金・カード番号・ログインを求める連絡は疑います。通販やカード会社を名乗る連絡は、とくに気をつけます（本書の推奨）。突然届いたメールや SMS のリンクは開かず、自分で開いた会社の公式サイトのお知らせや、アプリの注文履歴で確かめます[17]。通知が届いたときの確かめ方は第5章、公的機関や「被害金を取り戻せる」とかたる連絡は第7章で説明します。

漏れたパスワードを示して脅すメール

制度・公式情報 IPA は2018年10月から、「性的な映像をばらまく」と脅して、暗号資産（ビットコインなど）でお金を求める迷惑メールに注意を呼びかけています。件名や本文には、受け取った人が実際に設定したことのあるパスワードが書かれている場合があります。IPA は、このパスワードについて「外部のサービスから何らかの原因でデータが漏えいし、それをもとに記載されていると考えられる」としています。送信元が自分のメールアドレスになっていても、差出人を偽ることは技術的にできます。撮影したとされる映像がメールにあった例も、払わなかったためにばらまかれた例も、相談の中で「1件も確認されていません」としています（2021年3月の追記）[19]。

実際に起きた事例 2026年も、IPA の相談窓口には、暗号資産でお金を求める迷惑メールの相談が寄せられています。4～6月は30件、7～9月は19件でした（相談の数で、被害の数ではありません）。IPA は、どちらの期間も「暗号資産で金銭を支払ってしまったという相談は確認していません」としています[20,21]。



専門家

パスワードが書かれていても、脅しの中身が本当だという根拠にはなりません。お金は払わず、第5章の手順で対応しましょう（本書の推奨）。

使い回したパスワードでの不正ログイン

実際に起きた事例 モニター（覆面調査）サイトの件です。このサイトは2026年8月20～24日、リスト型攻撃（ほかで漏れた ID・パスワードの組を、次々に試す手口）を受けました。試行は5,060,270回で、会員59,389名が不正にログインされました。2アカウントでは、第三者によるポイントの不正な交換も確認されています[22]。



図3-4　使い回したパスワードは次々に試されるが、2段階認証やパスキーが守る

実際に起きた事例 IPA の相談窓口には、2026年4～6月に「不正ログイン」の相談が423件寄せられました。Facebook や Instagram に不正ログインされ、自分でログインできなくなったという相談が多くありました[20]。

同じパスワードを使い回していると、1つのサービスから漏れた ID・パスワードで、ほかのサービスにも入られるおそれがあります。IPA は、被害のあとは、同じパスワードを使うほかのサービスも確かめるよう呼びかけています[20]。パスワードは、サービスごとに変えましょう。パスキー（パスワードの代わりに、スマホなどの機器と指紋・顔・PIN〔暗証番号〕で本人を確かめる仕組み）も使います。2段階認証（パスワードのほかに、確認コードなどでも本人かを確かめる仕組み）も、使えるサービスでは設定します（第4章）。漏れた、または漏れたおそれがあるときの手順は第6章です。

本人確認書類を使ったなりすまし

運転免許証などの本人確認書類の情報が、他人になりすました携帯電話や口座の契約に使われるおそれについて、警察庁・総務省・金融庁の資料と報道から見ていきます。

実際に起きた事例 カーシェアの件（2026年9月公表）では、運転免許証などの画像のデータ約146万件に、外部へ送られた痕跡がありました（10月23日の第5報。画像は暗号化して保管されていました）[23]。

実際に起きた事例 警察庁によると、データ通信専用の SIM（スマホなどで通信するためのカード）は、契約のときの本人確認が義務ではありませんでした。警察庁は、近年、本人確認書類や ID・パスワードを使った不正な契約などの悪用が「数多く発生」しているとしています[1]。報道によると、2025年4月ごろに他人の免許証でオンラインの口座を開き、ローンで80万円をだまし取った疑いで、男が逮捕されました[24]。

ただし、特定の漏えいと、その後のなりすましの被害との因果関係を確かめた公的資料や具体例は、本書の調査では見つかりませんでした（2026年10月22日時点）。

制度・公式情報 総務省によると、書類の偽造による「なりすまし契約」（他人の名前で結ぶ契約）が問題になっています。そのため、携帯電話の契約では、IC チップ（カードに埋め込まれた、情報を記録する部品）の読み取りが原則必須になります。オンラインの契約は2026年4月1日から、対面の契約も2027年4月以降です[25]。

制度・公式情報 データ通信専用の SIM も、今後は契約の本人確認の対象になります。総務省は、本人確認をしていない既存の回線には、通信事業者から順に案内が届くとしています。この案内を装って詐欺に誘うメールや SMS が届くおそれもあります。総務省は、届いたリンクから開かず、自分で通信事業者のマイページなどを開くよう呼びかけています[25]。

制度・公式情報 携帯電話不正利用防止法（携帯電話の契約者の本人確認などを定めた法律）の改正法も、2026年5月に成立しました。総務省は7月29日、携帯電話の業界団体に、対面の契約での IC チップの読み取りを、2027年4月の施行を待たずに速やかに始めるよう努めることを要請しました。2026年4月から義務になっている、追加の回線の契約のときの多要素認証も、さらに厳しくするよう求めています。多要素認証は、パスワード・スマホ・指紋など、種類の違う確かめ方を2つ以上組み合わせる仕組みです。パスキーを使う方式を原則にする、といった内容です[26]。

制度・公式情報 金融機関の口座開設などをオンライン（非対面）で申し込むときの本人確認も変わります。金融庁によると、犯罪収益移転防止法（犯罪で得たお金の受け渡しを防ぐための法律）の施行規則の改正で、2027年4月1日から、本人確認書類の画像を送る方式は廃止されます。IC チップの読み取りに、原則として一本化されます。金融庁は金融機関に、書類や顔の画像に不自然な点がないかの確認の徹底と、施行を待たない対応も求めています[27]。店頭（対面）での手続きや、使える書類は、第6章 6-9 で説明します。

本人確認書類の画像が漏れた、または漏れたおそれがあると知らされたら、信用情報機関（ローンやクレジットの契約の情報を集める機関）への本人申告や、ローン・クレジットと携帯電話の契約の確認を考えます。本人申告は、書類の紛失や漏えいを登録して、会員の会社へ注意をうながす手続きです。手順は第6章です。携帯電話会社のアカウントにも、パスキーや2段階認証を設定しておきます（本書の推奨。第4章）。

数字で見る詐欺の被害

次の数字は、詐欺やフィッシング全体のものです。漏えいが原因と確認された数ではありません。集計した機関も範囲も違うので、足したり比べたりはできません。

実際に起きた事例 おもな数字は次のとおりです。特殊詐欺は、電話や SNS などで、会わずに相手を信じさせ、振込や現金・カードの受け渡しなどでお金をだまし取る犯罪の総称です[28]。2026年からは SNS 型投資・ロマンス詐欺も含み、数は暫定値です。

何の数か（期間）	数	集計
フィッシングの報告（2026年9月）	94,661件（前月比15.0%増）	フィッシング対策協議会[14]

何の数か(期間)	数	集計
特殊詐欺(2026年1〜8月)	29,687件・2,360.7億円(被害額は前年同期比33.2%増。前年も SNS 型投資・ロマンス詐欺を含めて比べた値)	警察庁[29]
うちニセ警察詐欺(警察官などをかたる詐欺)	6,346件・728.6億円	警察庁[29]
カードの不正利用(2025年)	510.5億円(前年比8.0%減)	日本クレジット協会[30]
証券会社のネット取引への不正アクセス(2025年1月〜2026年9月)	19,252件(うち不正な取引10,642件。発生日で集計した暫定値で、あとから増える可能性あり)	金融庁[31]

実際に起きた事例 フィッシングの報告の数は、被害者の数ではありません。警察庁は、フィッシングで盗まれた情報が、ネットバンキングの不正送金やカードの不正利用に使われているとしています[1]。カードの不正利用の被害額の93.1%(475.4億円)は、番号盗用(カードの番号などを盗んで使う手口)です[30]。

実際に起きた事例 警察庁は、2026年上半期の時点で、特殊詐欺の被害額が「過去最悪となった令和7年の被害額を上回るペースで推移している」としています[1]。同じ期間のニセ警察詐欺では、最初の接触の98.2%が電話でした(暫定値)。住所・氏名・資産などを探る「予兆電話」(特殊詐欺が疑われる電話)は、119,778件でした(前年同期比27.1%減)[28]。

実際に起きた事例 2026年上半期に、振込でだまし取る型の特殊詐欺は12,263件・1,033.4億円でした(暫定値)。そのうちネットバンキングを使ったものが6,727件・745.7億円で、振込型の被害額の72.2%です。暗号資産で送らせる型も、3,498件・409.6億円(前年同期比74.6%増)に増えています[28]。口座の情報が漏れていなくても、だまされて自分で送金してしまう被害が大きいということです。

連絡のリンクを開かないこと、知らない番号からの電話への備えは、第4章の「連絡のリンクを開かない」「電話・SMSの詐欺に備える」で説明します。振込や暗号資産での送金を求められたら、その場では応じず、家族や警察に相談します(本書の推奨)。

個人編

第4章　被害にあわないために



情報が漏れても、ふだんの備えがあれば、被害を防いだり小さくしたりできます。この章では、今日からできる8つの備えと、家族で決めておくことを紹介します。

この章の使い方

まずは、次の3つから始めましょう。一度に全部しなくてかまいません（本書の推奨）。

1. メールと銀行のパスワードを、ほかと違うものにします（図4-1の1）。
2. よく使うサービスを1つ選び、パスキー（パスワードの代わりに、スマホなどの機器と指紋・顔・PIN〔暗証番号〕で本人を確かめる仕組み）か2段階認証（パスワードのほかに、確認コードなどでも本人かを確かめる仕組み）を設定します（図4-1の3）。
3. カードの利用通知（カードが使われたことを知らせる通知）を有効にします（図4-1の5）。

図4-1は8つの備えの一覧で、この章の節も同じ順に並べました。できたものから印を付けましょう。スマホをなくしたときや、不正なアプリを入れてしまったときの手順は 6-5 に、漏えいを知らされたときの手順は第5章にあります。



図4-1　今日からの備えチェックリスト

パスワードを使い回さない

1. 先に、パスワードの控え方を1つ決めます。迷うときは、紙のノートで足ります（決め方は次の節）。覚えられないからと、同じパスワードに戻さないためです（本書の推奨）。
2. 大事なサービス（メール・銀行・証券・通販など）から順に、パスワードをサービスごとに別のものに変えます。英数字と記号を含めて10文字以上にします[1]。
3. 最初に変えるのはメールです。メールが乗っ取られると、ほかのサービスのパスワードの再設定に悪用されるおそれがあるためです（本書の推奨）。

制度・公式情報 IPA（情報処理推進機構）は、パスワードを英数字と記号を含めて10文字以上にし、使い回さないよう勧めています[1]。警察庁も、安全なパスワードを設定して使いまわさないよう呼びかけています[2]。

今日は、メールと銀行のパスワードが、ほかと同じでないか確かめましょう。

パスワードを安全に保管する

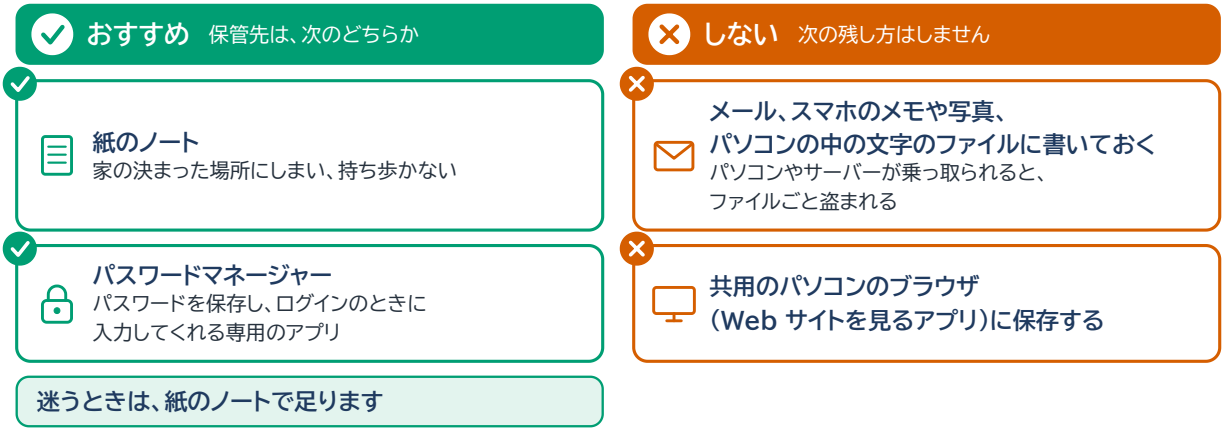


図4-2　パスワードの控え方（する・しない）

保管先は、次のどちらかにします。迷うときは、紙のノートで足ります（本書の推奨。2つの方法は、内閣官房 国家サイバー統括室の「インターネットの安全・安心ハンドブック」の例によります[3]）。

- **紙のノート**: 家の決まった場所にしまい、持ち歩きません。ハンドブックは、一見して内容が分からないようにできる専用のパスワードノートも紹介しています[3]。
- **パスワードマネージャー**(パスワードを保存し、ログインのときに入力してくれる専用のアプリ)[4]: 始めるときは、次の順にします。

1. アプリは、スマホの設定や公式ストア(App Store・Google Play)から入れます。メールのリンクからは入れません[4]。パソコンに入れるときは、提供元の公式サイトから入れます(本書の推奨)。本書は、特定の製品を勧めません。
2. アプリを開くための主パスワード(マスターパスワード)を決めます。これだけは長く強いものにして、覚えます(本書の推奨)。
3. アプリの2段階認証も設定します(本書の推奨)。
4. データを複数の機器で共有する「クラウド連携」は安易に使わず、スマホの中だけで管理できるものを優先します。その場合は、スマホをなくしたときのために、アプリの案内に沿ってバックアップをとります(ハンドブックの勧め[3])。
5. 大事なサービスから順に、パスワードを登録します(前の節の手順2・3と一緒に進めます。本書の推奨)。

いまブラウザ(Web サイトを見るアプリ。Chrome や Safari など)にパスワードを保存しているときは、次の順に移します(本書の推奨)。

1. パスワードマネージャーか紙のノートに控え直します。
2. 控え直した先でログインできることを確かめます。
3. 控え直した先が、ブラウザの保存とは別の保管場所かも確かめます。同じアカウントの同期(複数の機器で同じ中身にそろえる仕組み)で1つにつながっていると、ブラウザから消したときに、両方から消えてしまうためです。別の場所でないとき、または分からないときは、手順4に進みません。手順1に戻り、ブラウザとは別のパスワードマネージャーか紙のノートに控え直します。
4. ブラウザの設定で、保存したパスワードを消します。設定の場所が分からないときは、ブラウザの「ヘルプ」で「パスワード」と探します。

次の残し方はしません(本書の推奨)。

- メール、スマホのメモや写真、パソコンの中の文字のファイルに、パスワードを書いておく。パソコンやサーバーが乗っ取られると、ファイルごと盗まれます(6-5 の、仮想のパソコンを貸すクラウドの件)。
- 共用のパソコンのブラウザに保存する。



警察官

パソコンやスマホに保存した ID・パスワードを盗む、不正なプログラムに注意してください。ブラウザに保存する使い方を見直し、パスワードマネージャーでの管理も考えてください[5]。

制度・公式情報 このハンドブックは、ブラウザにはパスワードを保存しないよう勧めています。保存すると、席を離れたすきに勝手に使われるおそれがあるためです。パソコンを乗っ取られたときに、まとめて盗まれるおそれもあるとしています[3]。栃木県警察も2026年9月、パソコンやスマホに保存された ID・パスワードなどを盗む不正なプログラム(インフォスティーラー)に注意を呼びかけました。ブラウザに保存する使い方を見直し、パスワード管理専用のパスワードマネージャーでの管理を検討するよう勧めています[5]。

パスワードマネージャーの中には、漏れたパスワードや使い回しを知らせる機能を持つものもあります(例: Google の「パスワード チェックアップ」[6])。

今日は、パスワードの控え方を1つに決めましょう。

パスキー・2段階認証を使う

1. 銀行・証券・メール・通販など、大事なサービスから設定します[1]。パスキーが選べるならパスキーを、選べなければ2段階認証を使います（本書の推奨）。
2. 設定の場所や名前はサービスごとに違います（例:「設定」の中の「セキュリティ」にある「2段階認証」）。見つからないときは、アプリやサイトの「ヘルプ」「よくある質問」で、「パスキー」「2段階認証」と探します（本書の推奨）。
3. 設定の案内がメールや SMS（携帯電話の番号あてに届く短いメッセージ）で届いても、そのリンクからは設定しません。自分で開いた公式アプリやサイトから設定します（本書の推奨）。
4. SMS で届く確認コードやワンタイムパスワード（1回だけ使えるパスワード）は、誰にも教えません（本書の推奨）。



図4-3　パスキーや2段階認証は、家族で一緒に設定する

制度・公式情報 IPA は、できれば多要素認証（パスワード・スマホ・指紋など、種類の違う確かめ方を2つ以上組み合わせる仕組み）やパスキーを使うよう勧めています。SMS で届く確認コードを盗もうとするフィッシング（本物そっくりの偽のメールやサイトで、情報をだまし取る手口）も確認されています。パスキーは、パスワードや確認コードを入力しません。そのため、フィッシングに強いとされます[1]。

スマホに届く確認コードを使う2段階認証は、パスワードとスマホという種類の違う確かめ方を組み合わせるので、多要素認証の身近な形です（本書の整理）。

制度・公式情報 金融庁によると、証券口座の乗っ取りの被害をふまえ、証券会社では、パスキーなど「フィッシングに耐性のある」認証を必須にする動きが進んでいます[7]。偽のサイトにだまされても破られにくい認証のことです。金融庁は銀行などにも2026年2月、ログインや出金のときに、こうした認証を初期設定で必須にする（最初から必ず使う設定にする）よう求めました。この改正の意見募集では、認証の切り替えを装う詐欺を心配する意見も寄せられました[8]。

実際に起きた事例 金融庁が報告を受けた証券会社のネット取引への不正アクセス（許可なく他人のシステムに入ること）は、2025年4月の5,490件が最も多く、2026年9月は37件でした。発生日で集計した暫定値で、まだ判明していないものがある可能性も示されています。この変化と必須化の関係を、金融庁は述べていません[7]。

今日は、よく使うサービスを1つ選んで設定してみましょう。

連絡のリンクを開かない

1. よく使う銀行・カード・通販は、公式アプリを入れるか、公式サイトをブックマーク(よく見るページを登録しておく機能)しておきます[7]。登録するページは、契約の書類や請求書に載っているアドレス、公式アプリの中のリンクなど、確かな所から開きます(本書の推奨)。
2. 「お知らせ」「本人確認」「返金」などの連絡が突然来ても、リンクは押しません。ふだん使っている公式アプリや、登録済みの公式サイトから確かめます[9]。自分で公式サイトから始めた手続き(パスワードの再設定など)で、すぐに届く確認のメールは別です。手続きの内容と合っていれば、そのサービスの案内に沿って使います(本書の推奨)。
3. アプリは、スマホの設定や公式ストアから入れます。メールのリンクからは入れません[4]。
4. スマホやパソコンの OS(基本のソフト)やブラウザ、パソコンに入れたソフトに更新の知らせが来たら、早めに更新します[1]。iPhone の更新を自動にする設定と、Android の更新を確かめる方法は、節「スマホが使えなくなったときに備える」で説明します。

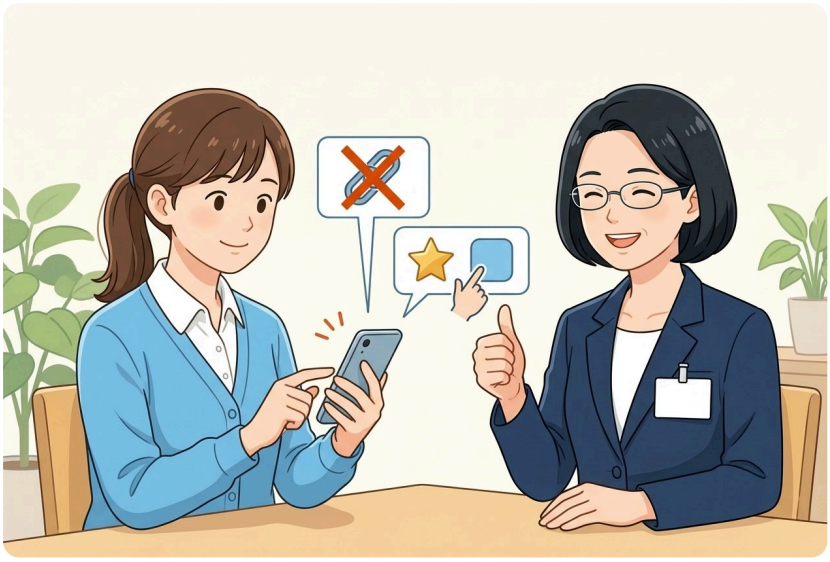


図4-4　届いたリンクは開かず、ブックマークや公式アプリから開く

制度・公式情報 警察庁は、フィッシングの被害を防ぐには、技術的な対策だけでは十分ではないとしています。「メール等に記載のリンクを安易にクリックしない」「公式サイトや公式アプリからアクセスする」といった、日ごろの意識が重要だという説明です。AI(人工知能)技術の発達で、見抜きにくいフィッシングが増えているとも述べています[10]。

制度・公式情報 SMS の送信元が「0005」で始まる番号は、携帯電話会社が企業ごとに審査して出す番号(共通ショートコード)です[11]。ただし、それだけで本物と決めず、手順2のとおり公式アプリやサイトで確かめます(本書の推奨)。

制度・公式情報 IPA の「情報セキュリティ6か条」は、1つめに「OSやソフトウェアは常に最新の状態にしよう！」を挙げています[1]。IPA は10月21日にも、Oracle の Java(パソコンなどで使われるソフト)の早急な更新を呼びかけました[12]。

実際に起きた事例 2026年10月には、海外の認証局の鍵に欠陥が見つかりました。認証局は、Web サイトとの暗号化した通信などに使う証明書を出す会社です。悪用の証拠はないものの、主なブラウザの会社が、この認証局を信頼しない対応をとりました[12]。こうした対応を早く受け取るためにも、更新は後回しにしません(本書の推奨)。

今日は、よく使うサービスのブックマークを作っておきましょう。

カード・口座の通知を受け取る

1. カードの利用通知（カードが使われたことを知らせる通知）を有効にします。例: カード会社の公式アプリの通知の設定。名前や場所、何が通知されるかは会社ごとに違うので、公式の案内で確かめます。通知だけに頼らず、手順3の明細の確認も続けます（本書の推奨）。
2. ネットの買い物の本人認証（3D セキュア。買い物のときに、カード会社がもう一度本人かを確かめる仕組み）を有効にします。例: カード会社の会員サイトやアプリの「本人認証」の設定（本書の推奨）。
3. 電子の明細は「定期的（できれば利用したらその日）に」確かめます。覚えのない請求があれば、「速やかに契約しているクレジットカード会社に連絡」します[13]。
4. ネットバンキング（ネットで振込などができる銀行のサービス）を使っている人は、振込の上限額を、ふだん必要な額まで下げておきます。例: 銀行のアプリや会員サイトの「限度額」の画面（本書の推奨）。警察庁は、上限額を簡単に引き上げられる点などが、犯罪に悪用されているとしています[10]。
5. ログインの通知を有効にし、ログインの履歴もときどき確かめます[14]。

制度・公式情報 日本クレジット協会は、不正利用の被害を小さくするには「できるだけ早くその被害に気付くこと」が必要だとしています。そのための対策が、利用明細の確認です[13]。

今日は、カードの利用通知がオンになっているか確かめましょう。

渡す情報・残す情報を減らす

1. 使っていないサービスやアプリを探します。思い出せないときは、メールで「会員登録」などの言葉を検索すると見つかることがあります（本書の推奨）。
2. 退会の前に、終わっていない注文・返金やポイントの残りを確かめ、必要な記録を残します。有料の契約や自動更新があれば、退会とは別に解約が要らないかも確かめます。そのアカウントで、ほかのサービスにログインしていたり、復旧の連絡先にしていたりしないかも見ます。使っていたら、先にログインの方法や復旧の連絡先を別のものに変え、使えることを確かめます。登録したカード情報など消せる情報を消し、本人確認書類を出していたら、その削除も頼めるか確かめます。そのうえで退会します（本書の推奨）。
3. 会員登録では、任意の項目（生年月日・性別・電話番号など）を必要以上に入れません（本書の推奨）。
4. メールアドレスを用途で分けます（例: お金や大事な手続き用、買い物用、メルマガ用）。1つが漏れても、ほかへの影響を小さくできます（本書の推奨）。
5. ホテルや店で本人確認書類を出したら、どこに出したかを手帳やスマホのメモに控えておきます。漏えいの通知が来たとき、自分が対象かを判断しやすくなります（本書の推奨）。

実際に起きた事例 退会しても、データがすぐに消えるとは限りません（第2章のカーシェアの件）[15]。

今日は、使っていない会員サービスを1つ退会してみましょう。

電話・SMS の詐欺に備える

1. スマホに「警察庁推奨アプリ」を入れます[2]。2026年3月に認定されたのは、「詐欺対策 by NTTタウンページ」と「詐欺バスター Lite」の2つです[16,17]。App Store や Google Play で名前を検索して入れます（本書の推奨）。
2. 固定電話は留守番電話にしておきます。知らない番号には出ず、留守番電話で用件を聞きます。かけ直すときは、着信の番号や録音で言われた番号ではなく、公式サイトなどで自分で調べた番号にかけます（本書の推奨）。
3. 「警察」を名乗る電話は、いったん切ります。都道府県警察の公式サイトなどで自分で調べた警察署の代表番号か、警察相談専用電話（＃9110。受付時間は都道府県で異なる）にかけて確かめます。緊急のときは110番です（本書

の推奨)。

4. 離れて暮らす家族とは、電話やビデオ通話で本人かを確かめる「合言葉」を決めておきます。顔や声が本人に見えても、合言葉で確かめます(本書の推奨)。
5. 家族で「役所や銀行が電話や SMS で暗証番号を聞くことはない」と話し合っておきます(本書の推奨)。全国銀行協会は「銀行協会職員や銀行員が暗証番号を尋ねることは一切ない」としています[18]。
6. 固定電話・ひかり電話(光回線を使う固定電話)で国際電話を使わないなら、国際電話の発信と着信の休止を申し込みます。「国際電話不取扱受付センター」に申し込むと、無償で休止できます[16]。NTT東日本・西日本の電話なら、NTT の窓口でもまとめて申し込めます[19]。申し込み先は付録Cに載せました。

制度・公式情報 特殊詐欺は、電話や SNS などで、会わずに相手を信じさせ、振込や現金・カードの受け渡しなどでお金をだまし取る犯罪の総称です。警察庁によると、2023年7月以降、国際電話番号を使った特殊詐欺が急増しました[16]。

実際に起きた事例 警察庁は、警察官役の顔を AI で作った偽の映像で、ビデオ通話をしてだました特殊詐欺の事件(2025年8月に逮捕)も紹介しています[10]。



警察官などのふりをして近づきます。AI で作った顔の映像で、ビデオ通話をかけたこともあります[10]。

詐欺師



顔や声が本人に見えても、それだけで決めないでください。手順4の、家族で決めた合言葉で確かめましょう(本書の推奨)。

専門家

今日は、家族と合言葉を決めておきましょう。

スマホが使えなくなったときに備える

スマホには、パスキー、認証のアプリ、パスワードマネージャー、支払いや銀行のアプリが集まっています。なくした・壊れた・機種を変えた・乗っ取られたおそれがある、といったときには、これらがまとめて使えなくなることがあります(本書の整理)。

ここでは、そうなる前にしておく備えを、小見出しに分けて説明します。なくしたときや、不正なアプリを入れてしまったときの手順は、6-5 にあります。

こんなとき	前もってする備え	小見出し
壊れた・機種を変えた	予備のコードを印刷し、本人の確かめ方を2つ以上登録する。写真や連絡先はバックアップ	予備のコードとバックアップ
弱点を突かれないように	iPhone は更新を自動に、Android は更新が止まっていないか確かめる	更新を自動にする
更新の期間が終わった	買い替えを計画する。手放す前にカードの削除、ログアウト、初期化	更新が終わったスマホ

こんなとき	前もってする備え	小見出し
なくした	画面ロックと、「探す」(Android は Find Hub)をオンにしておく	なくしたときに備える
不正なアプリ	公式ストアなどから入れ、強い権限は許可しない	不正なアプリを入れない
通信が止まった	家族の連絡の方法を決め、171 を試す。公衆電話・ラジオも	通信が止まったとき
支払いができない	もう1つの支払いの手段と、少しの現金を持つ	支払いの手段を1つに頼らない

予備のコードとバックアップ

1. バックアップ コード(確認コードを受け取れないときに使う、予備のコード)を出せるサービスでは発行し、印刷して大事な書類と同じ場所にしまいます。誰にも教えません。
2. 本人の確かめ方を2つ以上登録しておきます。そのうち少なくとも1つは、いつものスマホが使えなくても使えるものにします。例えば、2台目の機器に登録したパスキー、印刷したバックアップ コード、iPhone の復旧用連絡先(下の説明)に登録した家族です。認証のアプリと電話番号が同じスマホにあると、そのスマホをなくしたときに両方使えなくなります(本書の推奨)。
3. 機種を変えるときは、古いスマホを初期化(買ったときの状態に戻すこと)したり下取りに出したりする前に、認証のアプリの引き継ぎや、新しいスマホでのパスキーの登録を済ませます。手順はサービスごとに違うので、公式の案内で確かめます(本書の推奨)。スマホの決済(Apple Pay・Google Pay・おサイフケータイなど)や一部の SNS にも、前もって移す手続きが要るものがあります[20]。
4. 写真や連絡先は、自動のバックアップ(クラウド〔ネット上で使うソフトや保存場所〕など)を有効にしておきます。スマホを初期化しなければならないときや、データを消されたときにも戻しやすくなります[21]。クラウドの「同期」(スマホと同じ中身にそろえる仕組み)では、スマホで消したものがクラウドからも消えることがあります。消したものを戻せる期間や方法も、各サービスの案内で確かめておきます(本書の推奨)。
5. カード会社・銀行・携帯電話会社の連絡先を、紙にも控えておきます。スマホが使えないときでも、自分で調べた番号ですぐに止められます(本書の推奨)。
6. それでもログインできないときは、サービスの公式の窓口に連絡し、本人確認を受けて手続きします(本書の推奨)。
7. 家族や取引先との連絡が、ふだんのアプリでつながらないときの代わり(電話・メールなど)を決めておきます(本書の推奨)。
8. パソコンの大事なファイルは、外付けの記憶装置や USB メモリにも定期的に取ります[22]。記憶装置は、バックアップのときだけつなぎます。つないだままだと、ランサムウェア(データを暗号化して身代金を求める不正なプログラム)に感染したとき、バックアップまで暗号化されるおそれがあるためです。バックアップは2つ以上の記憶装置に、それぞれ取ります。取っている最中は、ほかの操作をしません(IPA の2017年の資料)[23]。

制度・公式情報 Google は、2段階認証のバックアップ コード(10個あり、1回ずつ使える予備のコード)を、確認コードを受け取れないときに使えるとしています。スマホをなくしたときや、電話番号を変えたときなどです。印刷して、パスポートなどの大事な書類をしまう場所に保管し、誰とも共有しないよう求めています。

制度・公式情報 iPhone では、Apple の「復旧用連絡先」も使えます。パスワードやパスコード(iPhone の画面のロックを解く暗証番号)を忘れて、アカウントに入れなくなったときの備えです。自分が指定した家族などが、復旧用のコードを伝えてくれます。指定した人は、アカウントには入れません。「設定」→自分の名前→「サインインとセキュリティ」→「復旧用連絡先」で、最大5人まで指定できます。

制度・公式情報 松井証券は、パスキーを設定したスマホの機種を変えるときの扱いを案内しています（2026年7月）。iPhone と Android の間の乗り換えでは、登録し直しが必要です。同じ OS で同じ Apple ID（いまの名前は Apple Account）・Google アカウントを使うなら、要りません。古い端末がないときは ID・パスワードと SMS の認証でログインでき、「パスキーでのみログイン」に設定している場合は顧客サポートに連絡します。扱いは会社ごとに違います。

制度・公式情報 国家サイバー統括室と IPA の「サイバーセキュリティ対策9か条」は、「大切な情報は失う前にバックアップ（複製）しよう」としています。大切な情報を失っても、バックアップから戻せば被害を軽くできるという説明です[21]。

専門家の予測・懸念 ホワイトハッカー（攻撃の技術を、守る側で使う専門家）の田中悠斗氏（デジタルハリウッド大学特任教授）は、2026年10月14日のテレビ番組で話しました。トラブルのときの代わりの手段を、場面ごとに用意しておくよう勧めています。例えば、ふだんの連絡アプリがつながらなければ電話に、電話もつながらなければメールに切り替える、と決めておくことです。安全と便利さは引き換えの関係にある、という考えからです[24]。手順7は、この勧めにならったものです。

更新を自動にする

「連絡のリンクを開かない」の手順4の更新は、自動にしておくと、知らせが届いたときに忘れずに入ります（本書の推奨）。Android は、更新の時期や設定の画面が機種で違います（下の Google の説明）。手順3・4で、更新が止まっていないかをときどき確かめます（本書の推奨）。

1. iPhone は、「設定」→「一般」→「ソフトウェアアップデート」→「自動アップデート」で、「自動インストール」をオンにします。充電中で Wi-Fi につながっている夜間に更新が入り、入る前には通知が届きます。
2. iPhone は、「設定」→「プライバシーとセキュリティ」→「バックグラウンドでのセキュリティ改善」でも、「自動インストール」をオンにします。
3. Android は、例えば「設定」→「システム」→「ソフトウェア アップデート」で更新を確かめます。更新の前に Wi-Fi につなぎ、75%以上充電します。
4. Android は、「設定」→「デバイス情報」→「Android バージョン」で、「Android セキュリティ アップデート」の日付も見ます。古いまま止まっていないかを確かめます（本書の推奨）。
5. 寝る前に、充電器と Wi-Fi につないでおきます。夜のうちに更新が入りやすくなります（本書の推奨）。
6. 画面の名前は、OS の版や機種で変わることがあります。見つからないときは、Apple・Google やメーカーのサポートのページで「アップデート」と探します（本書の推奨）。

実際に起きた事例 Apple は2026年に少なくとも2回、悪用された可能性がある脆弱性（ソフトや機器の弱点）を直したと公表しました。9月28日の iOS 26.7.1（iPhone 11 以降が対象）の説明には、次の一文があります。「標的となった特定の個人に対するきわめて巧妙な攻撃において、この脆弱性が悪用された可能性があるという報告を把握しています」。2月11日の iOS 26.3 にも、同じ趣旨の項目があります[25]。特定の個人をねらった攻撃についての報告です。こうした修正を早く受け取るためにも、自動更新をオンにしておきます（本書の推奨）。

制度・公式情報 Apple は「ソフトウェアを常に最新の状態にしておくことは、Apple製品を安全にお使いいただくための最も重要な方策の1つです」としています。また、調査が終わって修正が公開されるまでは、問題を公開・説明しないとしています[26]。初期設定のときに自動アップデートをオンにするのが「最善の方法」ともしています。iOS 26.1 以降には、通常の更新とは別に、Safari などの部品に小さなセキュリティの修正を届ける「バックグラウンドセキュリティ改善」もあります。オフにすると、次の通常の更新まで届きません。

制度・公式情報 Google によると、Android の更新の時期は、機種・メーカー・携帯電話会社で違います。

更新が終わったスマホ

1. 自分の機種の更新の期間を確かめます。メーカーの公式の「サポート」のページで、機種名と「アップデート」で探します（本書の推奨）。
2. 最新の OS に上げられない機種でも、更新が出ていれば入れます。ただし、いつまで出るかを、メーカーが定めていないことがあります（本書の推奨）。
3. 銀行・決済など大事なアプリの「動作環境」（使える機種や OS の条件）を、各社の公式ページで確かめておきます（本書の推奨）。
4. 更新が終わったら、更新の期間が残っている機種への買い替えを計画します（本書の推奨）。
5. スマホに入れたマイナンバーカードは、手放す前にスマホから削除します[27]。Android の場合、電子証明書（スマホに入れたマイナンバーカードの機能）は「スマートフォンの端末初期化では削除されません」。デジタル庁は、使うのをやめるときにマイナアプリで失効（証明書を使えなくすること）の手続きをすることを、法律上の義務としています[28]。初期化するとマイナアプリも消えるので、この手続きは初期化より先にします（本書の推奨）。
6. そのうえで、古いスマホを手放す前に、ログアウトしてから初期化します[20]。

制度・公式情報 更新の期間の示し方は、メーカーによって違います。例えば、次のとおりです（2026年10月23日時点）。

メーカー	更新の期間
Google（Pixel）	Pixel 8 以降は、米国の Google Store での販売開始日から7年間、OS とセキュリティの更新が提供される。Pixel 6・6a・7・7a・7 Pro・Fold は5年間。Pixel 5a（5G）以前は提供が終わっている
Apple（iPhone）	何年まで更新を出すかの定めは、公式の案内に見当たらない。2026年も、最新の iOS 27（iPhone 11 以降が対象）に上げられない古い iPhone に、セキュリティの更新を出した（例: iPhone XS・XR など向けの iOS 18.7.10〔8月17日〕、iPhone 6s・7 など向けの iOS 15.8.8〔5月11日〕）[26]

制度・公式情報 総務省は、更新の配布などのサポートには期間が決まっているものがあり、「サポート期間が切れたソフトウェアは脆弱性が発見された場合も修正されない」としています。サポートが終わる時期を前もって知り、計画的に更新するよう求めています[29]。

制度・公式情報 国家サイバー統括室のハンドブックは、とくにスマホは個人情報などが集まっているので、「よほどの理由がない場合以外は、サポート切れのものを使うのは避けましょう」としています[20]。Google も、「古いデバイスでは新しいバージョンの Android を実行できない可能性があります」としています。

制度・公式情報 OS が古いと、使えないサービスもあります。例えば、デジタル庁の「iPhone のマイナンバーカード」は、iPhone XS 以降で、iOS 18.5 以上の機種で使えます[27]。

なくしたときに備える

スマホをなくしたときに、遠くからロックや位置の確認ができるよう、前もって次を済ませておきます。

1. 画面ロックを必ず有効にし、ロックまでの時間を短めにします[22]。
2. iPhone は「探す」（Apple の、端末を探す機能）、Android は Find Hub（Google の、端末を探す機能。以前の名前は「デバイスを探す」）がオンになっているかを確かめます。Android は、Google アカウントを追加した端末では自動でオンになります。パソコンや家族のスマホから一度開き、自分のスマホが出るかを試しておきます[20]。
3. iPhone は、「設定」→「Face IDとパスコード」→「盗難デバイスの保護」をオンにします。iOS 17.3 以降で使え、最初からオンの場合もあります。

4. 携帯電話会社の紛失の窓口の番号を、紙に控えておきます(「予備のコードとバックアップ」の手順5。本書の推奨)。

制度・公式情報 国家サイバー統括室のハンドブックは、遠隔でのロック・位置の確認・消去を使える状態にし、試しておくよう勧めています。スマホをなくしたときに備えるためです[20]。

制度・公式情報 iPhone の「盗難デバイスの保護」をオンにすると、よく知っている場所(自宅や職場など)の外では、顔か指紋での確認(Face ID か Touch ID)が要る操作が増えます。保存したパスワード・パスキーの使用や、すべての消去などです。パスコードでは代えられません。Apple Account のパスワードの変更などは、1時間待ってから、もう一度、顔か指紋での確認が要ります。その間に、紛失としてマークできます。

なくしたときは、まず別の機器から「探す」か Find Hub を開き、「紛失としてマーク」でロックします[20]。見つからなければ、携帯電話会社に連絡して回線を止め、警察に届け出ます。マイナンバーカードの機能やスマホの決済を止めることなど、続きの手順は 6-5 の「スマホをなくしたとき」にあります。

不正なアプリを入れない

1. アプリは、スマホの設定や公式ストアから入れます。メールや SMS のリンクからは入れません(「連絡のリンクを開かない」の手順3)。
2. 入れたアプリが、ユーザー補助(アクセシビリティ機能。画面の読み上げなど、操作を助ける機能)などの強い権限(アプリに許す操作)を求めてきたら、すぐに許可せず、本当に必要かを考えます。怪しければ許可せず、そのアプリを削除します(本書の推奨)。
3. 国税庁などを名乗る連絡で、アプリを入れるよう求められても入れません(本書の推奨)。2026年10月1日現在、Android 向けの公式の e-Tax(国税の申告などをネットで行う仕組み)のアプリはありません。

制度・公式情報 日本サイバー犯罪対策センター(JC3。サイバー犯罪の対策に取り組む一般財団法人)は、偽のアプリは、ユーザー補助などの強い権限を求める傾向があるとしています[30]。国税庁などをかたって偽のアプリを入れさせる手口と被害の例は、6-5 の「スマホに不正なアプリを入れてしまったとき」で説明します。

実際に起きた事例 2026年9月には、Android 版の認証アプリ「Microsoft Authenticator」の脆弱性が修正されました。同じスマホに不正なアプリが入っていると、トークン(ログインした状態を保つための、一時的な鍵)を取られ、本人として使われるおそれがありました。開発元は修正した版(6.2606.4246)を配っていて、悪用は確認されていないとしています[31]。見つけたセキュリティ企業は10月23日に詳しい内容を公表しました。自社の検証で、不正なアプリが正規のアプリになりすましてトークンを受け取れたこと、業務用のアカウントのメールやファイルにアクセスできたことを示しています[32]。

こうした弱点は、不正なアプリが同じスマホに入っていることが前提です。次のように備えます(本書の推奨)。

- アプリは公式ストアから入れ、提供元の分からないアプリは入れません(上の手順1)。
- アプリも自動で更新されるようにし、認証アプリなど大事なアプリは、ストアで最新になっているか確かめます。Google も、アプリを最新にすると、アプリのセキュリティも向上するとしています。
- Google アカウントにつながったアプリは、「リンク済みアプリ」のページで確かめ、心当たりのないものはアクセス権を削除します。削除すると、そのアプリは Google アカウントにアクセスできなくなります。
- 会社から渡されたスマホや、会社のアカウントを入れたスマホは、会社の担当者の案内に従います。

Android のスマホに不正なアプリを入れてしまったら、まず機内モード(スマホの通信をまとめて止める設定)をオンにし、Wi-Fi もオフにして、通信を止めます[33]。お金の被害が疑われるときは、家族のスマホや固定電話など別の安全な電話から、すぐに銀行・カード会社に連絡します(本書の推奨)。記録・削除・初期化などの続きの手順は、6-5 の「スマホに不正なアプリを入れてしまったとき」にあります。

通信が止まったとき

1. スマホのネットワークの設定は、「自動選択」をオンのままにします。自分の機種が JAPANローミング（大きな災害や障害のとき、ほかの会社の回線を一時的に使える仕組み）に対応しているかは、携帯電話会社のページで確かめます（本書の推奨）。
2. 次の1日か15日に、家族で災害用伝言ダイヤル（171。声の伝言を残せるサービス）を試してみます（本書の推奨）。体験利用日は、毎月1日・15日などです[34]。
3. 家族で、安否確認の方法と集合場所を決めておきます[35]。ふだんの連絡アプリがつながらないときの代わりも決めます（「予備のコードとバックアップ」の手順7）。
4. 家族の電話番号を、紙にも控えておきます（本書の推奨）。
5. 自宅・職場・学校の近くの公衆電話の場所を確かめ、小銭を用意しておきます（本書の推奨）。
6. ラジオなど、スマホ以外で情報を得る手段も用意しておきます[36]。

実際に起きた事例 総務省の検証報告（2026年7月17日）によると、2025年4月～2026年3月の電気通信の重大な事故は6件でした。ある携帯電話会社では2026年1月27日から約6時間24分、1都5県の一部で影響が出ました（音声で約9.1万人）。別の携帯電話会社の件（2025年10月21日）では、その会社のメールが Wi-Fi の環境などで使えることを周知できなかったことが、代わりの手段の周知の不足として挙げられています[37]。

制度・公式情報 JAPANローミング™（非常時事業者間ローミング）は、2026年4月1日に、NTTドコモ・KDDI（沖縄セルラーを含む）・ソフトバンク・楽天モバイルの4社が始めました。一定の条件のもとで、データ通信（送受信最大300kbps。ふだんより遅い通信）・SMS・音声通話（緊急通報を含む）が使えます。それができない場合も、緊急通報だけは使える場合があります[38]。

制度・公式情報 ただし、平常時や小規模な障害では使われません。受け入れる側の容量の範囲で運用するので、全員の通信を保証するものではありません。緊急通報では、番号や位置が送られない、警察・海上保安庁・消防からかけ直せない、という場合があります。対応する端末は「おおむね令和8年春モデル以降」とされ、それより前の機種も、更新で対応している場合があります[38]。

制度・公式情報 災害用伝言ダイヤル（171）は、1伝言30秒以内の声の伝言です。携帯電話会社の「災害用伝言板」（文字。100文字以内）や、「災害用伝言板（web171）」（文字。100文字まで）もあります。171 は、公衆電話・携帯電話・IP 電話（インターネットを使う電話）などからも使え、前もっての登録は要りません。総務省は、体験利用日に家族などと使い方を確かめ、安否確認の方法を決めておくよう勧めています。体験利用日は、毎月1日・15日、正月三が日（1月1～3日）、防災とボランティア週間（1月15～21日）、防災週間（8月30日～9月5日）です[34]。

制度・公式情報 首相官邸も、「災害時には、携帯電話の回線がつながりにくくなり、連絡がとれない場合もあります」としています。家族が別々の場所で災害にあっても安否を確かめられるよう、日ごろから安否確認の方法や集合場所を話し合っておくよう勧めています[35]。

制度・公式情報 総務省の対応ガイド（2023年3月時点の情報）は、災害時には、役場や避難所などに無料の「特設公衆電話」が置かれることがあるとしています。「00000JAPAN」という名前の Wi-Fi が、無料で開放されることもあります。情報の入手は、スマホのインターネットだけでなく、「ラジオや防災行政無線等の手段も予め用意し、平時から利用しておくことが重要」としています[36]。

制度・公式情報 NTT東日本・西日本の「公衆電話インフォメーション」では、公衆電話と災害時用公衆電話の設置場所を調べられます。大きな災害のときに、公衆電話を無料にしたこともあります（北海道全域〔2018年9月〕、千葉県全域〔2019年9～10月〕）。

支払いの手段を1つに頼らない

いつもの支払いができなくなるのは、スマホをなくしたときだけではありません。カードの番号を変える再発行のあいだ（第6章 6-4）や、災害・障害のときにも起こりえます（本書の整理）。次の3つは、下の首相官邸のチェックリストの「現金」と、キャッシュレス（現金を使わない支払い）の現状をふまえた本書の推奨です。

1. ふだん使うカードのほかに、もう1つ支払いの手段を持っておきます。例えば、別の会社・別の国際ブランド（Visa・JCB など、カードの支払いの仕組みの名前）のカードです。デビットカード（使うとすぐに口座から代金が引き落とされるカード）でもかまいません。
2. スマホの決済とは別に、少しの現金（小銭を含む）を持っておきます。非常用持ち出し袋と一緒に持ち出す貴重品にも、現金を加えておきます。
3. カードで払っている継続払い（公共料金・携帯電話料金・定額のサービスなどの決まった支払い）の登録先を、一覧にしておきます。カードの番号が変わったとき、登録を変える先がすぐ分かります（変え方は第6章 6-4）。

制度・公式情報 首相官邸の「災害の『備え』チェックリスト」は、内閣府の防災担当などが監修したものです。非常用持ち出し袋と一緒に持ち出す貴重品として、通帳・現金・パスポート・運転免許証・病院の診察券・マイナンバーカードなどを挙げています[35]。

制度・公式情報 キャッシュレス推進協議会（キャッシュレスの普及に取り組む業界団体）は、2024年12月に報告をまとめました。災害時でも使い続けられるキャッシュレスの環境は、「実際に継続利用可能な状況には至っていない」としています。同じ報告は、「非常時における現金の利便性」にも触れています[39]。

制度・公式情報 大きな災害では、通帳や印鑑をなくしても預金を引き出せるよう、公的な要請が出たことがあります。2026年7月29日、九州財務局と日本銀行は、令和8年熊本地震で災害救助法が適用された熊本県の金融機関に要請しました。通帳や届出の印鑑などをなくした場合でも、被災の状況をふまえた方法で本人と確かめて、払い戻しに応じることなどです[40]。

今日は、いちばん大事なサービスのバックアップ コードを印刷しておきましょう。あわせて、iPhone は自動アップデートがオンか、Android は更新が止まっていないかを確かめます。「探す」（Android は Find Hub）がオンかも確かめましょう。

家族で決めておくこと

困ったことが起きたとき、家族の誰もが一人で抱えずに、すぐ話せるようにしておくことも備えの一つです。高齢の親や子どもと、次の6つを前もって決めておきます。下の公的な案内をふまえた本書の推奨です。

1. **責めない約束**: 「変な連絡が来た」「入力してしまった」と打ち明けられても責めずに、まず受け止める、と家族で約束しておきます。早く話してもらえれば、カードや口座を早く止められます。
2. **消さずに残す**: 困ったメッセージや画面は、消したり相手をブロックしたりする前に、スクリーンショット（画面をそのまま画像で保存すること）で残してもらいます。ブロックやアカウントの削除で、証拠が消えることもあるためです。
3. **お金の依頼は文字以外で確かめる**: メッセージで家族や友人からお金や確認コード（LINE では「認証番号」）を頼まれたら、返事をする前に、電話か対面で本人に確かめます。電話やビデオ通話でも、合言葉で確かめます（「電話・SMS の詐欺に備える」の手順4）。確認コードは、家族を名乗る相手にも教えません（理由は第6章 6-5）。
4. **手続きは本人と一緒に**: サービスによっては、家族が代わりに問い合わせられません（下の LINE の例）。高齢の親のアカウントは、本人が自分で手続きできるかを前もって一緒に確かめ、困ったときは隣で手伝います。どうするかは、本人の気持ちを聞いて決めます。

5. **写真を載せる決まり**: 子どもや家族の顔、学校名や制服、自宅の場所が分かる写真を、SNS などに載せるかどうかを家族で決めておきます。
6. **相談先を控える**: 家族の誰でもかけられるよう、相談先(消費者ホットライン 188、警察相談専用電話 #9110 など。第7章)を、家族の電話番号と一緒に紙に控えます(「通信が止まったとき」の手順4)。

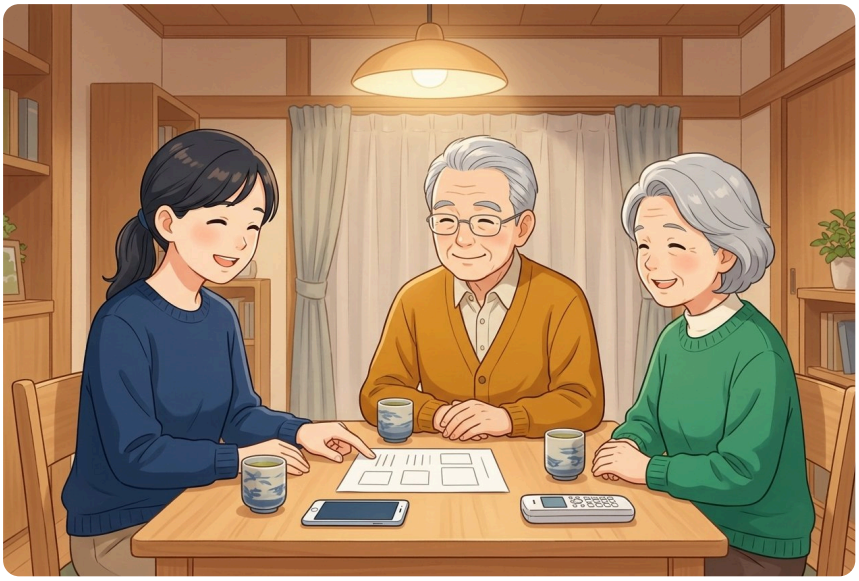


図4-5　困ったときの連絡のしかたを、家族で決めておく

制度・公式情報 LINE ヘルプセンター(2026年5月20日更新)は、乗っ取ったアカウントを使う手口を確認しているとしています。家族・友人・知人から、PayPay で送金させようとするものです。突然送金を求められたら、「対面やビデオ通話など、テキストメッセージ以外の手段で必ず本人に確認」するよう求めています。乗っ取りの問い合わせは本人からだけで、家族や友人などの代理は原則として受け付けていません[41]。

お子さんがいる家庭では

制度・公式情報 総務省は「インターネットトラブル事例集(2026年版)」で、子どもに呼びかけています。トラブルに遭ったら、保護者や先生など信頼できる大人に相談します。言いにくければ、国や自治体の相談窓口(匿名でもよい)を使うよう勧めています。メッセージや履歴はスクリーンショットなどで残し、お金や顔・体の画像を求められても応じないとしています。保護者には、相談を受けたら「批判をする・責めるのではなく、まずは受け止める」よう求めています。自分だけで判断せず、子どもと一緒に相談窓口に相談することも求めています[42]。

制度・公式情報 同じ事例集は、卒業アルバムなどの写真を、生成 AI(文章や画像を作る AI)などで性的な画像に加工される被害が「急増しています」としています。消すことと引き換えにお金を求められても、「絶対にお金を払わずに」相談するよう呼びかけています。大人には、否定せずに味方になり、証拠を残して、削除の依頼や被害届に進むよう求めています[42]。脅されたときの対応は、第5章の「『消してあげる』という持ちかけ」にもあります。

制度・公式情報 個人情報保護委員会も、写真には顔や住所、画像の位置情報(撮った場所の情報)などが映り込むことがあるとしています。そのうえで、「一度ネット上に出てしまった画像等を完全に削除することは極めて困難です」と説明しています[43]。子ども向けには、同委員会の資料「みんなの大切な個人情報」(2022年4月)があります。困ったときは一人で何とかしようとせず、早く家の人や学校の先生に相談するよう呼びかけています[44]。

今日は、家族と「責めない約束」をして、お金の依頼を確かめる方法を話し合っておきましょう。

漏れた、または漏れたおそれがあると知らされたら、第5章の手順に進みます。

個人編

第5章　漏えいの通知が届いたら



会社から「情報が漏えいしたおそれがあります」という通知が届いたら、あわてずに順番に進めます。この章の手順は、どの情報が漏れた場合にも共通です（種類ごとの手順は第6章）。手順は公的機関の資料をもとに本書がまとめたもので、多くは本書の推奨です。

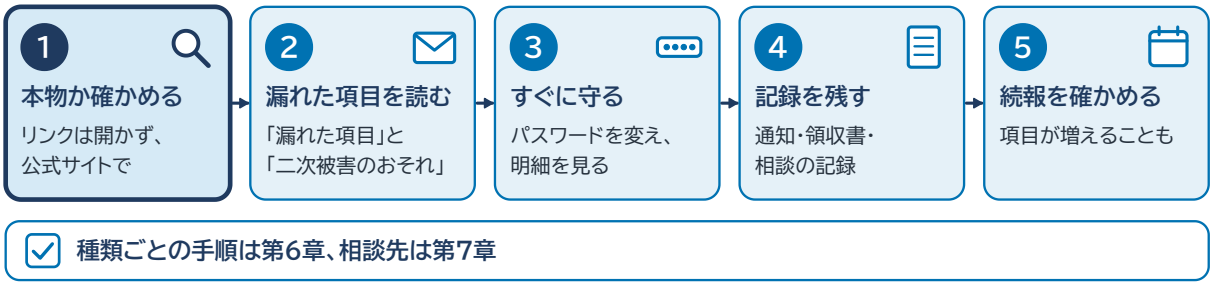


図5-1　通知が届いたら5つのステップ

この章の使い方

- **会社から漏えいの通知が届いた:**「5つのステップ」（図5-1の順に進めます）
- **通知はまだ届いていないが、覚えのない請求やログインなどの異変がある:**「通知が届く前に気づいたら」
- **お詫び・返金の連絡や、脅し・「削除」の持ちかけが届いた:**「お詫び・返金をかたる偽の連絡」「脅しや『削除』を持ちかける連絡」
- **役所・学校・病院から通知が届いた:**「5つのステップ」に加えて、「役所・学校・病院から届いたとき」
- **初動が済んだ・通知が届く決まりを知りたい:**「その後、何を確かめ続けるか」「会社から届く通知とは」

5つのステップ

通知が届いたら、図5-1の順に進めます。次の手順は、公的機関の資料をもとにした本書の推奨です（札の付いた段落が、その根拠です）。



図5-2　お知らせが届いたら、公式サイトを自分で開いて確かめる



相談者

「漏えいしたおそれがあります」という通知が届きました。でも、この通知が本物かどうか分かりません。

1. **本物か確かめる**（リンクは開かず、公式サイトで）

   通知のメールや SMS（携帯電話の番号あてに届く短いメッセージ）のリンクは開きません。自分で開いた公式サイトのお知らせや、会社が公表した送信元のアドレス（@ の後ろまで）と見比べます。送信元の表示はまねされることがあるので、同じでもリンクは開きません。郵送や電話で知らされたときも、書かれた番号や言われた番号ではなく、公式サイトなどで自分で調べた番号にかけます。

   制度・公式情報　国民生活センターも、メッセージの中のリンクではなく、ふだん使っている公式アプリや登録済みの公式サイト（ブックマークなど）から確かめるよう案内しています[1]。

   実際に起きた事例　漏えいを公表した会社も、同じように呼びかけています。8月公表のネットショップの基盤の件では、利用店の一つが、連絡の真偽に不安があるときは、連絡に書かれたリンクや電話番号を使わないよう呼びかけました。各社の公式サイトの窓口で確かめる、という内容です[2]。リユース店の件（2026年10月公表）では、会社が不審な電話に注意するよう呼びかけています。相手が名乗った組織の公式の連絡先を自分で確かめて、問い合わせるように、という内容です[3]。

2. **漏れた項目を読む**（「漏れた項目」と「二次被害のおそれ」）

   通知に書かれた「漏れた（または漏れたおそれがある）項目」と「二次被害（漏れた情報が使われて、あとから起きる被害）のおそれ」を読みます。どの項目かで、するべきことが変わります（第6章）。書かれていなければ、会社の公式の窓口に聞きます。通知に書かれる事項は、この章の「会社から届く通知とは」にあります。会社が自分のどんな情報を持っているかは、開示を求めて確かめる制度もあります（第7章）。

制度・公式情報 IPA(情報処理推進機構)も2026年10月26日、まず漏れた情報の種類を、サービスの会社からの連絡や案内で確かめるよう勧めています[4]。

3. **すぐに守る**(パスワードを変え、明細を見る)

ID(ログインに使う名前)とパスワードが漏れた、または漏れたおそれがあると知らされたら、確定を待たずに変えます。対象は、そのサービスと、同じパスワードを使うほかのサービスです。変えるのは、ステップ1で確かめた公式のアプリかサイトからです。メールのパスワードも漏れたときや、メールと同じパスワードだったときは、メールを最優先にします。乗っ取られると、ほかのサービスの再設定に悪用されるおそれがあるためです。

制度・公式情報 IPA は、サービスから個人情報が盗まれることへの備えを挙げています。カードの利用明細を定期的に確かめる、ログインの通知を有効にする、ログインの履歴を確かめる、などです[5]。

履歴に覚えのないログインがあれば、その画面を保存するか印刷して残します[6]。そのうえで、公式の案内に従って、覚えのないスマホやパソコンのログインを解除(ログアウト)します。画面の名前は、サービスごとに違います。再設定用のメールアドレスや電話番号が変えられていないかも確かめます。ログインできないときは、公式の復旧の手続きか窓口を使います(6-5)。

4. **記録を残す**(通知・領収書・相談の記録)

会社からの通知、手続きの手数料の領収書、相談した記録(日時・相手・内容)をとっておきます。あとで窓口に相談するときに、経緯を説明しやすくなります。残し方の例です。

- メールの通知は消さずに残し、郵送の通知は封筒ごとしまいます。
- 会社のお知らせのページは、続報で書き足されることがあります。読んだ日の画面を保存(スクリーンショット)するか印刷します。
- 電話で相談したら、その場で日時・相手・内容をメモします。
- お金の被害が出たときは、被害の日時、サービスの名前、取引の記録、相手とのやりとりも残します。

5. **続報を確かめる**(項目が増えることも)

最初の発表だけで安心せず、会社のお知らせの続報を確かめます。最終報が出るまでは、お知らせのページを週に1回ほど見ます。

実際に起きた事例 カー用品店の作業予約の件では、第一報の項目が、氏名・電話番号・メールアドレス・会員番号でした。2026年10月15日の最終報では、住所・生年月日・性別・ログイン ID・パスワードの流出も分かりました。パスワードは「復元できない形式」(そのままでは元の文字に戻せない形)で保管していたので、漏れた情報でアカウントが不正に使われるおそれはない、と会社は説明しています[7]。それでも、そのサービスのパスワードを変え、同じパスワードをほかで使っていれば、そちらも変えます(本書の推奨)。

実際に起きた事例 最初は対象外とされていても、あとから対象になることがあります。メール配信サービス(企業が顧客にメールを送るためのサービス)の件(10月19日公表)です。このサービスを使っていた鉄道の予約サービス・銀行・ソフト会社は、最初は影響がない、または対象外と知らされていました。10月26日になって、漏えいした、または漏えいの可能性が高いと知らされています[8,9,10]。

最初のお知らせで対象外とあっても、続報を確かめます(本書の推奨)。件数が続報で大きく変わることもあります(第1章のネットショップの基盤の件)。

漏えいを調べるサービス

制度・公式情報 メールアドレスを入れて、漏えいした記録に含まれるかを調べられるサービスがあります。IPA の2025年版の解説書も、こうしたサービスで定期的に確かめることを、備えの一つに挙げています[5]。

制度・公式情報 その一つ、海外の Have I Been Pwned は、多くの漏えいはデータが公開されず、まったく見つからないものも多いと説明しています。収録しているのは、漏えいしたすべての記録の「一部にすぎない」としています。

調べるのは、自分のメールアドレスだけにします。パスワードは、こうしたサービスに入れません。見つからなくても安心せず、会社からの通知や公表を優先します。漏れたパスワードや使い回しは、パスワードマネージャーの点検の機能で知らせてくれるものがあります（第4章の「パスワードを安全に保管する」。本書の推奨）。

通知が届く前に気づいたら

漏えいの通知より先に、異変に気づくこともあります。

制度・公式情報 警察庁は、ネットのサービスの乗っ取りなどの相談の例として、次のようなものを挙げています[6]。

- ウェブメール（インターネットのサイトで読み書きするメール）で、見た覚えのないメールが既読になり、送信済みのメールが消されていた
- SNS のパスワードが変えられ、自分の名前で投稿されていた
- カードの請求に、覚えのない買い物があった

こうした異変や、身に覚えのない引き落とし、自分ではしていないログインやパスワード変更の通知に気づいたら、会社からの漏えいの通知を待たずに動きます。送った覚えのないメッセージのことを、知人から言われたときも同じです（本書の推奨）。

制度・公式情報 警察庁は、被害にあったら次のようにするよう案内しています[6]。

1. サービスの会社に、すぐに連絡・相談します。カードを登録していればカード会社にも連絡します。ネットバンキング（ネットで振込などができる銀行のサービス）なら、不正な送金がないかを確かめて、銀行にも連絡します。
2. ログインできれば、すぐにパスワードを変えます。同じパスワードを使っているほかのサービスも変えます。
3. ログインの履歴が見られれば、その画面を保存するか印刷して、証拠を残します。会社とのやりとりも記録します。
4. 保存した記録を持って、最寄りの警察署か、都道府県警察のサイバー犯罪相談窓口に相談します。前もって電話で、行く日時と持っていく資料を相談しておくとよい、としています。

記録を集めるために、1の連絡を遅らせません。止めるのが先です。異変ごとに、まずすることと、続きを読む所は次のとおりです。この表は本書の推奨です。

気づいた異変	まずすること	続きを読む所
カードの覚えのない請求	カードの裏面の番号で、カード会社に連絡する	6-4
身に覚えのない送金	銀行の緊急の連絡先に連絡する	6-7
ログインできない	公式の復旧の手続きか窓口を使う	6-5
メールのアカウントの異変	ログインできれば、すぐにパスワードを変える（上の2）	6-1・6-5
スマホのアプリが怪しい	スマホの通信を止める	6-5

スマホのアプリの手順は、6-5 の「スマホに不正なアプリを入れてしまったとき」にあります。あとから漏えいの通知が届いたら、この章の最初の「5つのステップ」に進みます。

会社から届く通知とは

どんなときに通知が届くか

制度・公式情報 会社などが持つ個人データ（名簿やデータベースのように整理して持っている個人情報）が漏えいし（おそれを含む）、次のどれかに当たるときは、会社は原則として個人情報保護委員会（個人情報の扱いを監督する国の機関）に報告し、情報が漏れた人に通知します[11]。

- ① 病歴など、とくに配慮が必要な情報が含まれる
- ② カード番号など、不正に使われるとお金の被害が出るおそれがある
- ③ 不正アクセス（許可なく他人のシステムに入ること）など、不正の目的で行われたおそれがある
- ④ 1つの漏えいの事案で、情報が漏れた（またはそのおそれがある）人が1,000人を超える。漏れた情報の種類は問いません

④は、法律の言葉では「本人の数が1,000人を超える」と書かれています。「本人」は、漏れた情報が指している人のことです。お客様や会員など、その情報の持ち主です。通知を受け取った自分ひとりの数ではありません。その事案で情報が漏れた人が、合わせて1,000人より多いことをいいます。

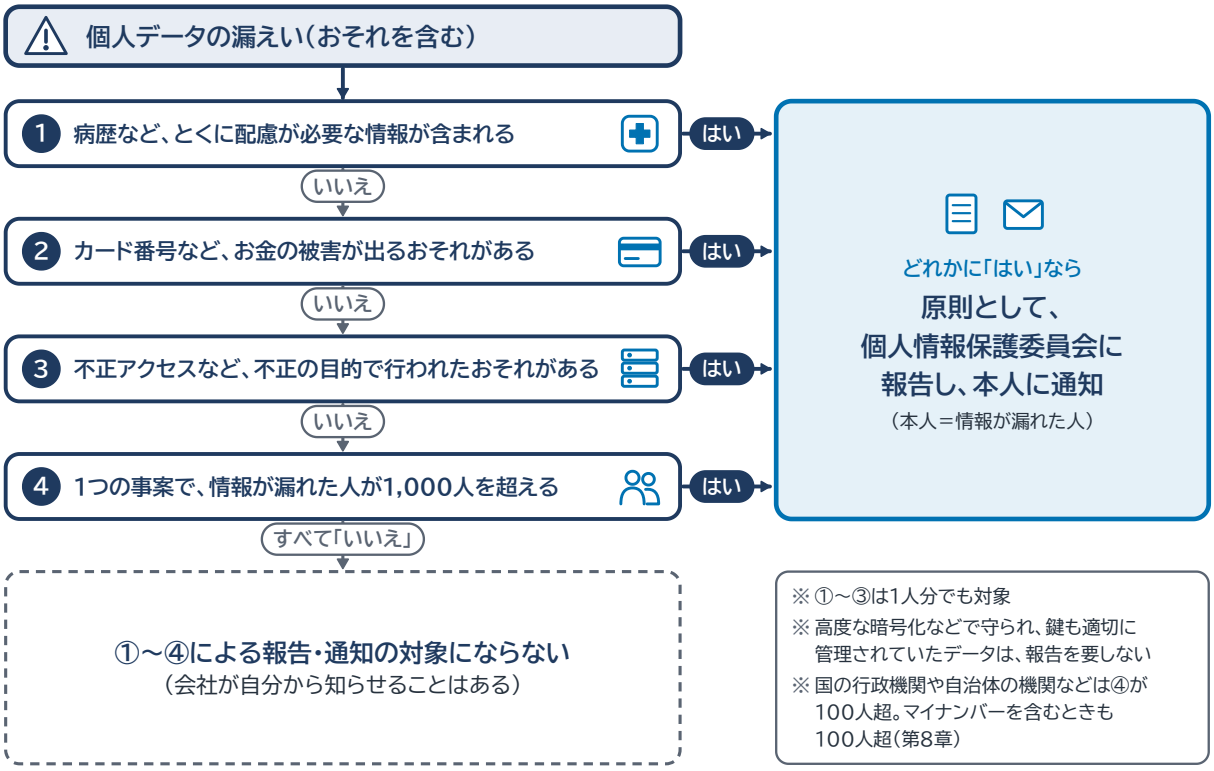


図5-3　会社が報告・通知をする漏えいか（①～④）

制度・公式情報 ①～③は、1人分でも対象です。人数の条件があるのは④だけです。高度な暗号化などで守られ、元に戻すための鍵なども適切に管理されていたデータは、どれに当たっても報告を要しないとされています。暗号化してあるだけでは足りません（詳しくは第8章）[11]。

人数は、データの件数ではなく人で数えます。確定できないときの考え方や委員会の例は、第8章 8-2 の囲み「『1,000人を超える』の数え方」にあります。

制度・公式情報 人数の基準が違う場合もあります。国の行政機関や自治体の機関など（法律では「行政機関等」）では、④の人数が「100人を超える」です[11]。ただし、自治体の病院や大学などの業務では、扱いが違う場合があります（この章の「役所・学校・病院から届いたとき」）。マイナンバーを含む情報の漏えいは別の決まり（番号法）で、人数の基準は会社でも「100人を超える」です。人数のほかに、不正の目的で行われたおそれがあるときや、ネット上などで不特定多数の人に見られる（おそれがある）ときなども対象です（第8章）[12]。

具体的な例に当てはめると、次のようになります（委員会の基準に当てはめた本書の例）[11]。

例	報告・通知の対象か
健康診断の結果1人分を、別の人に渡してしまった	対象（①）。1人分でも対象
会員1,200人へのメールを、全員のアドレスが見える CC の欄に入れて送ってしまった	対象（④）。1,000人を超える
不正アクセスで、会員10人分のメールアドレスが漏れたおそれがある	対象（③）。1人分でも対象
会員300人へのメールを、CC の欄に入れて送ってしまった（漏れたのはメールアドレスだけ）	対象にならないと考えられる（メールアドレスだけでは、直ちに②には当たらないとされる。会社が自分から知らせることはある）

3行目と4行目は、どちらも漏れたのはメールアドレスだけです。分かれ目は、不正アクセスによるもの（③）かどうかです。

通知に書かれること

制度・公式情報 通知は、郵送やメールなどで本人に直接知らせるものです。書かれるのは、次の事項です[11]。

- 概要
- 漏えいした（またはそのおそれがある）項目
- 原因
- 二次被害やそのおそれの有無
- その他の参考になること

このうち「項目」と「二次被害」が、ステップ2で読む所です。

通知が届かないこともある

制度・公式情報 連絡先が分からないなど、通知が難しいときは、公表や問い合わせ窓口などの「代わりの措置」で対応できます[11]。

実際に起きた事例 ネットショップの基盤の件では、会社が、漏えいの対象者への個別の連絡を終えたと公表しました。連絡先が分からない人には、公表と問い合わせ窓口で代えるとしています（2026年10月16日の最終報）[13]。

制度・公式情報 改正個人情報保護法（2026年7月に公布〔国が法律を広く知らせること〕。2026年10月22日時点では施行〔実際に始まること〕の前。第7章）が施行されると、本人の権利利益の保護に欠けるおそれが少ない場合（それだけではほぼ意味を持たない社内の ID だけが漏れた場合など）に、通知の代わりに、公表などの「代わりの措置」で対応できるようになります（第7章）[14]。

①～④のどれにも当たらない漏えいや、代わりの措置で済ませた場合には、通知が届かないことがあります。通知が届かなくても、漏れていないとは限りません。通知だけに頼らず、使っているサービスの公式サイトやアプリの「お知らせ」を、月に1回ほど見ます（本書の推奨）。

実際に起きた事例 自分が会員になっていない会社の漏えいで、対象になることもあります。宅配便の荷物問い合わせのサービスの件では、会社のよくある質問（FAQ）が、通販で商品を受け取っただけでも、届け先として対象になる可能性があるとしています[15]。

会員でなくても、荷物の受け取りなどで関わった会社の漏えいが報じられたら、公式サイトのお知らせを確かめます（本書の推奨）。

通知をまねた偽のメール

実際に起きた事例 本物の案内の送信元を公表する会社もあります。コンビニのアプリの件では、会社が対象者にメールで個別に案内し、送信元のアドレスをお知らせのページで公表しました[16]。カラオケ店の件でも、会社は影響を受けた可能性のある人に、SMS などで順次個別に連絡しています。送信元の番号も、公式サイトに示しています。新たな漏えいが確認されたわけではない、としています（2026年10月26日の追記）[17]。

制度・公式情報 一方で警察庁は、情報が流出した企業をかたる偽メールに注意するよう呼びかけています（第1章）[18]。10月15日の号でも、流出したメールアドレスに偽のメールが届くおそれがあるとして、サービスの利用者に次の3つを呼びかけました[19]。

- メールの中のリンクを安易に押さない
- ID・パスワードを使い回さない
- パスキーなどの多要素認証を使う

多要素認証は、パスワード・スマホ・指紋など、種類の違う確かめ方を2つ以上組み合わせる仕組みです。パスキーは、パスワードの代わりに、スマホなどの機器と指紋・顔・PIN（暗証番号）で本人を確かめる仕組みです。設定の仕方は第4章にあります。届いた通知が本物かは、ステップ1のやり方で確かめます。

お詫び・返金をかたる偽の連絡



図5-4　届いた連絡は、自分で開いた公式のページで確かめる

実際に起きた事例 漏えいのあとには、本物の情報を使った偽の連絡が届くことがあります。第3章で紹介した衣料品の通販の件では、注文情報と一致する返金案内のメールが顧客に届いていました[20]。



詐欺師

会社になりすまして、本物の注文の情報と同じ内容で、返金の案内を送ります[20]。

注文や予約の内容、氏名が正しくても、本物の証拠にはなりません。次のような連絡は偽物を疑います（本書の推奨）。

- お金の振込、カード番号、ログインを求める
- 返金やお詫びを口実に、連絡の中のリンクから手続きさせようとする
- 送信元が、会社の公表したものと違う

制度・公式情報 会社のお知らせに、会社から聞かないことが書かれている場合もあります。その例が、焼肉チェーンの公式アプリの件です。会社は、漏えいした情報が、なりすましのメールや、偽のサイトで情報をだまし取る詐欺に悪用されるおそれがあるとしました。そのうえで、会社からパスワードやカード情報を聞くことはないと明記しています[21]。

お知らせに、こうした「会社から聞かないこと」が書かれていないかも読んでおきます。それを求める連絡は、偽物を疑います。迷ったら、書かれた番号やリンクは使わず、自分で調べた公式の連絡先やアプリの注文履歴で確かめます（本書の推奨）。

もし偽の連絡に入力・返事をしてしまったら

気づいたら、すぐに次のように動きます（本書の推奨）。

- パスワード: 公式のアプリかサイトから変えます。同じパスワードのほかのサービスも変えます。
- カード番号: カード会社に連絡します（6-4）。
- お金を払った: すぐに、払うのに使ったカード会社・銀行・決済のサービスに連絡し、そのうえで警察署に相談します（6-4・6-7）。自分で振り込んだときは、振り込んだ先の口座がある銀行と警察に、直ちに連絡します。振り込みを頼んだ自分の銀行にも相談します（6-7）。
- 電話で話した: 警察署か警察相談専用電話（＃9110）に、契約や請求のトラブルは 188 に相談します（第7章）。

制度・公式情報 総務省の FAQ（よくある質問）は、偽サイトや電話で個人情報を伝えてしまった場合について、「身に覚えのない契約や請求がないか確認しましょう」としています。

脅しや「削除」を持ちかける連絡

この節では、漏れたパスワードを示して脅すメール、写真や家族のことを持ち出す脅し、情報の「削除」を持ちかける連絡への対応をまとめます。

制度・公式情報 攻撃者を名乗る者からの連絡にも注意します。仮想のパソコンを貸すクラウドの件では、運営会社が2026年10月24日、利用者に呼びかけました。攻撃者を名乗る者からメールやメッセージが届いたら、URL やファイルを開かず、返信もしない、という内容です。攻撃者が公開するとする情報には、事実と異なる内容が含まれるおそれがあるともしています[22]。

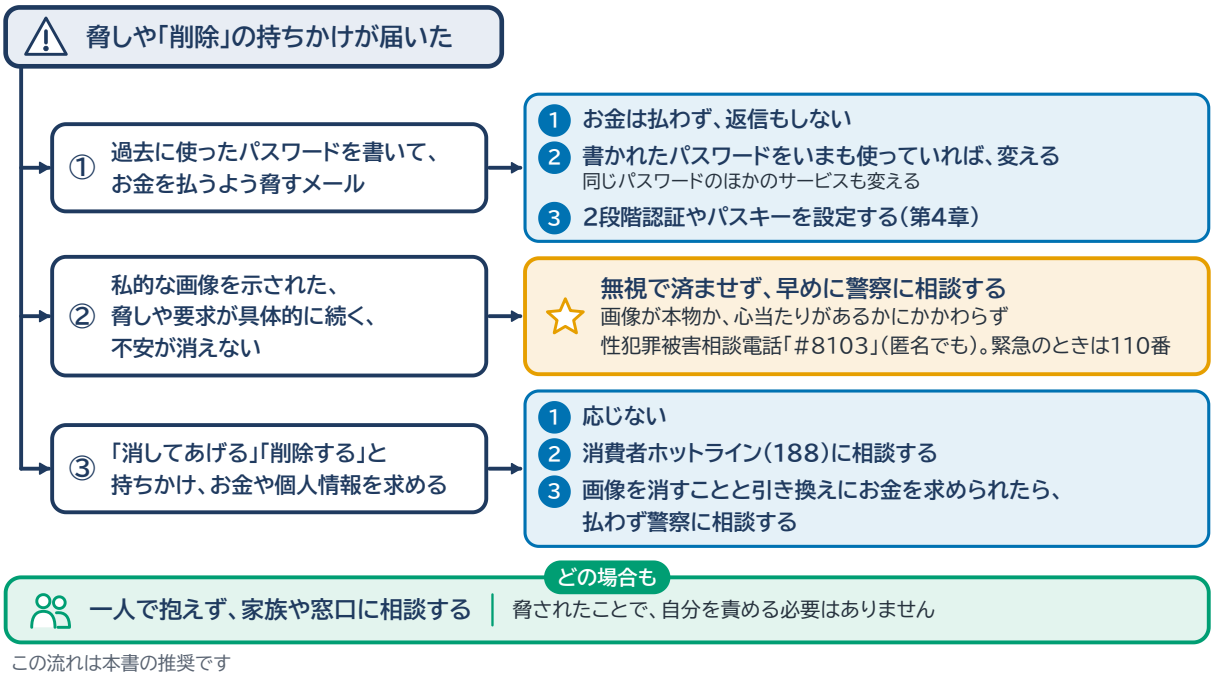


図5-5　脅しや「削除」の持ちかけが届いたとき

パスワードを示して脅すメール

第3章で紹介したように、過去に使ったパスワードを書いて、お金を払うよう脅すメールがあります。届いたら、次のようにします。この手順は本書の推奨です。

1. お金は払わず、返信もしません。
2. 書かれたパスワードをいまも使っていれば、公式のアプリかサイトから変えます。同じパスワードのほかのサービスも変えます。
3. 2段階認証（パスワードのほかに、確認コードなどでも本人かを確かめる仕組み）やパスキーを設定します（第4章）。
4. 送信元が自分のメールアドレスでも、それだけで乗っ取られたとは限りません（第3章）。気になるときは、メールのログインの履歴を確かめます（6-1・6-5）。

制度・公式情報 IPA も、このメールは無視して、支払わないよう勧めています。書かれたパスワードをいまも使っていれば変え、できれば2段階認証にすることも勧めています。パスワードの出どころと、IPA が確かめた相談の例は、第3章にあります[23]。

パスワードを知られていることと、脅しの中身が本当かは、別のことです。パスワードを知っていることだけでは、「撮影した」「乗っ取った」という脅しが本当だという根拠にはなりません（本書の推奨）。

制度・公式情報 一方で警察庁は、性的な画像について不安にさせる言動があれば、まだ公表されていなくても、すぐに警察などに相談するよう呼びかけています[24]。

画像が本物か、心当たりがあるかにかかわらず、私的な画像を示された、脅しや要求が具体的に続く、不安が消えない、といったときは、無視で済ませません。早めに警察に相談します（本書の推奨）。性的な画像の被害や脅しは、警察の性犯罪被害相談電話「#8103」に匿名でも相談できます（詳しくは第7章）。緊急のときは110番です。

脅されたことで、自分を責める必要はありません。一人で抱えず、家族や窓口に相談します（本書の推奨）。

写真や家族のことを持ち出して脅されたとき

パソコンやスマホの中には、写真や家族の情報、よく行く場所の記録なども入っています。こうした情報を示して、「公開する」「家族や勤め先に知らせる」と脅されたときも、次のようにします。出典の番号が付いていない手順は、本書の推奨です。

1. お金は払わず、返信もしません。
2. 届いたメールやメッセージは消さずに残します。画面を写真に撮り、届いた日時と送り主を書き留めます。
3. 命にかかわる脅しは、最寄りの警察署に通報します。急ぐときは110番です。それ以外の脅しも、早めに警察に相談します。どこに相談するか迷うときは、警察相談ダイヤル ＃9110 にかけます。
4. 家族に知らせると言われたら、相手より先に、家族など信頼できる人に事情を話しておきます。
5. 攻撃者が情報を公開したとされる場所は、自分で確かめに行きません。記録は、会社や警察に任せます。



図5-6　脅されたら、一人で抱えずに警察に相談する

実際に起きた事例 仮想のパソコンを貸すクラウドの件で、会社は10月27日に公表しました。公開された情報と称するものの掲載先にアクセスした人の情報は、攻撃者に取得されていることを確認した、という内容です。公開された情報に利用者の情報があると確認したら、対象の人に個別に連絡するとしています。要求に応じない理由は、応じても、取得された情報の削除や不正利用の防止が保証されるものではないため、と説明しています[25]。



攻撃者

情報を「公開した」と称するサイトを見に来た人の情報まで、取っていた例があります[25]。

制度・公式情報 自分の名前・住所・写真などが SNS や掲示板に載せられたときについて、警察庁は、ページを印字し、サイトの名前・URL・書き込んだ人・書き込みの日時・内容などを記録するよう案内しています。削除の方法は、法務省の人権相談などで相談できます。法務局が、事案に応じてプロバイダなどに削除を依頼することもあるとしています[26]。これは、ふつうの SNS や掲示板に載せられたときの案内です。攻撃者が公開したとされる場所は、開くと自分の情報を取られるおそれがあるので、上の5のとおり自分では開きません（本書の推奨）。

「消してあげる」という持ちかけ

「漏れた個人情報を消してあげる」「ネットから削除する」などと持ちかけて、お金や個人情報を求める連絡には応じません。消費者ホットライン(188)に相談します。画像を消すことと引き換えにお金を求められたときも払わず、警察に相談します(本書の推奨)。

制度・公式情報 国民生活センターを名乗って「個人情報が漏れているので削除してあげる」と持ちかける電話について、同センターは、個人情報の削除はしないとしています(6-3)[27]。

制度・公式情報 総務省の「インターネットトラブル事例集」(2026年版)は、自分の写真を性的な画像に加工されるなどの被害で、加工した画像を消すことと引き換えにお金を求めて脅す手口もあるとしています。そのうえで、「絶対にお金を払わずに」相談するよう呼びかけています[28]。

ネットに出た自分の情報を消したいときは、削除を持ちかけてくる相手ではなく、自分で調べた公的な窓口に相談します。サイトに自分で削除を頼む方法と、法務局などの相談先は 6-9 に、窓口の番号は第7章にあります(本書の推奨)。「被害金を取り戻せる」「代わりに訴える」という連絡は、第7章の囲みを見てください。

役所・学校・病院から届いたとき

公立の学校や病院、役所から通知が届くと、どこに問い合わせればよいか迷うことがあります。施設の種類だけで、どの決まりで扱われるかを決めつけず、次の順に確かめます。この手順は本書の推奨です。

1. 通知を出した機関と、施設を運営している主体(市区町村、教育委員会、病院を運営する法人など)を確かめます。
2. その機関の、個人情報の問い合わせの窓口を、公式サイトで調べます。
3. 電話で知らされたら、内容を書面かメールでも送ってもらうよう頼みます。電話が本物かは、自分で調べた代表番号にかけ直して確かめます。

運営する主体を確かめるのは、施設によって、使われる決まりや請求先が違うためです。

制度・公式情報 個人情報保護委員会の Q&A(行政機関等編。2026年4月更新)は、次のように説明しています[29]。

- 自治体の機関が運営する病院や大学の業務には、開示の請求(自分の情報を見せるよう求めること)などの決まりを除いて、民間の会社と同じ決まりが使われます。
- 公立学校では、個々の学校ではなく、その学校を受け持つ教育委員会が自治体の機関にあたります。
- 自治体の病院や大学などが持つ自分の情報の開示を求めるときの請求先は、運営する自治体の機関(市長など)とされています。地方独立行政法人(自治体が設立した法人)が運営するときは、その法人です。

制度・公式情報 同じ Q&A は、役所などが本人に電話で知らせることも妨げられないとしています。そのうえで、知らせた日時などを記録し、本人があとで内容を確かめられるよう、必要に応じて書面やメールを併用するのが望ましいとしています[29]。

制度・公式情報 苦情の扱いについても、同じ Q&A は次のように説明しています。個人情報保護法は、自治体の機関に、個人情報の扱いへの苦情を「適切かつ迅速」に処理するよう努めることを求めています。個人情報保護委員会の相談ダイヤルは、役所などの扱いへの苦情も受けます。ただし、委員会が間に入って歩み寄りを促す「あっせん」は、役所など(行政機関等)への苦情を対象にしていません[29]。

通知を出した機関の対応に納得できないときは、個人情報保護法相談ダイヤルで助言を受けられます。国の行政機関の対応なら、総務省の行政相談(担当の機関とは別の立場で、行政への苦情を受ける窓口)も使えます。窓口の番号は第7章にあります(本書の推奨)。

その後、何を確かめ続けるか

初動が済んだあとも、しばらくは次の6つを続けます。公的機関などの呼びかけをもとにした、本書の推奨です。

いつ	何をするか	くわしく
少なくとも毎月（漏えいの直後はこまめに）	カードの明細と口座の入出金を確かめる	1
通知が届くたび	利用やログインの通知を確かめ、覚えがなければすぐ連絡する	2
最終報が出るまで	会社のお知らせの続報を確かめる	3
連絡が届いたとき	届いたリンクや番号は使わず、公式の窓口で確かめる	4
相談・手続きのたび	記録をとっておく	5
使わなくなったとき	退会して、持たれている情報を減らす	6

1. カードの明細と口座の入出金を、少なくとも毎月確かめます。漏えいの直後は、もっとこまめに見ます（ステップ3）。口座の補償は、被害から30日を過ぎて銀行に知らせると受けられないことがあるので（6-7）、入出金の通知も有効にしておきます。
2. カードの利用通知や、ログインの通知を有効にしておきます（第4章）。通知が届いたら、その都度確かめます。覚えのない利用やログインは、次の確認の日を待たずに、カード会社・銀行・そのサービスに連絡します。
3. 漏えいした会社の続報を確かめます（ステップ5）。
4. 自分のことを知っているような電話・メール・SMS が届いても、届いたリンクや番号は使わず、公式の窓口で確かめます。
5. 相談や手続きの記録をとっておきます（ステップ4）。
6. 使わなくなったサービスは退会して、持たれている情報を減らします（第4章）。

制度・公式情報 IPA は2026年10月23日、偽のサイトに個人情報を入力してしまった人に向けて呼びかけました。さらに被害につながる不審なメールや SMS が届くおそれがある、というものです。「相手があたかもあなた自身のことを知っているかのような文面を作成することも可能であるため」としています。

制度・公式情報 個人情報保護委員会は、使わなくなったサービスは、退会の手続きなどで登録した個人情報を削除してから、利用をやめるよう勧めています[30]。

「何か月たてば安全」という決まった終わりはありません。明細の確認は毎月の習慣にし、通知はその都度見ます。習慣になれば、続ける手間は小さくなります（本書の推奨）。社会全体のこれからの見通しは、第9章で述べます。

個人編

第6章　流出した情報の種類別の対応



お知らせに書かれた、漏れた（または漏れたおそれがある）項目によって、悪用のされ方と今日やることが変わります。10種類の情報ごとに、今日やること・悪用のされ方と実例・相談先を同じ順に並べました。共通の手順は第5章、悪用の全体像は第3章、救済の制度は第7章にあります。図6-1で漏れた項目のマスを探し、その節を読んでください。

6-1 メールアドレス
悪用　流出元の企業をかたる偽メール
まず　**リンクを押さず公式アプリで確認**

6-2 電話番号
悪用　偽の SMS・警察をかたる電話
まず　**いったん切り、自分で確かめる**

6-3 氏名・住所・生年月日
悪用　削除をもちかける電話・送り付け
まず　**払わずに188に相談**

6-4 クレジットカード　お金に直結
悪用　番号を盗んで使う不正利用
まず　**裏面の番号でカード会社へ連絡**

6-5 ID・パスワード　お金に直結
悪用　ほかのサービスで試される
まず　**パスワードを変え使い回しをやめる**

6-6 マイナンバー
悪用　番号だけでは直ちに悪用できない
まず　**市区町村に番号の変更を相談**

6-7 銀行口座　お金に直結
悪用　暗証番号を聞き出す詐欺
まず　**取引している銀行に連絡**

6-8 健康・医療の情報
悪用　悪用の公表例は見つかっていない
まず　**対象かを公式サイトで確かめる**

6-9 本人確認書類・顔写真
悪用　書類を偽造したなりすまし契約
まず　**書類の画像なら本人申告を検討**

6-10 購買履歴・会員情報
悪用　注文内容と一致する偽の連絡
まず　**お金を求める連絡は疑う**

詳しい手順と相談先は各節（6-1〜6-10）へ

図6-1　流出した情報の種類別の早見図

この章の使い方

- 待ち伏せやつきまといなど、身の危険を感じたら、最寄りの警察署に相談し、緊急のときは110番です。安全の確保を最優先にします(6-3)。そのうえで、複数の種類が漏れたときは、お金に直結するクレジットカード・銀行口座・ID・パスワードから手を打ちます(本書の推奨)。
- 起きたことから探すときは、次の節を読みます。メールの乗っ取りは 6-1 です。SNS(X・Instagram・Facebook など、人とつながって投稿や連絡をするサービス)の乗っ取り、不正なアプリ、スマホをなくしたときは 6-5 です。覚えのない利用・送金は 6-4・6-7、写真や住所がネットに出たときは 6-9 です。
- 覚えのない設定・端末・アプリは、できれば画面を保存してから消します。ただし、カード会社・銀行への停止の連絡やパスワードの変更は、記録のために遅らせません(第5章。本書の推奨)。
- 連絡先は、届いたメールや SMS(携帯電話の番号あてに届く短いメッセージ)に書かれたものを使わず、カードの裏面や公式サイトで確かめます(本書の推奨)。
- 確かめる手順は、自分のアカウントと自分の情報に限ります。窓口の番号と受付時間は2026年10月22〜23日時点のものです。かける前に公式サイトで確かめます。

6-1 メールアドレス

制度・公式情報 警察庁も、情報が流出した企業をかたる偽メールに注意するよう呼びかけています(第1章)[1]。

今日やること

1. 漏えいした会社の名前で届くメールのリンクは押しません。公式アプリか、ブックマークした公式サイトから確かめます[1]。
2. メールのパスワードも漏れたときや、同じパスワードをほかで使っていたときは、メールのパスワードを最優先で変えます(第5章。本書の推奨)。覚えのない既読や送信済みのメールに気づいたら、下の「メールのアカウントが乗っ取られたとき」に進みます。
3. 偽のメールが増えて困るときは、迷惑メールへの対策の強いメールサービスで新しいアドレスを作り、登録先を少しずつ移すことも考えます[2]。

どう悪用されるか・実例

実際に起きた事例 プロバイダー(ISP。インターネット接続事業者)向けのメールの仕組みの件です。6つのプロバイダーに提供されていた仕組みが、不正アクセス(許可なく他人のシステムに入ること)を受けました。メールアドレス約1,223万名分の漏えいが確認されています(第1章)[3]。

メールのアカウントが乗っ取られたとき

「メールアドレスが漏れた」だけなら、注意するのは、迷惑なメールや偽のメールが増えることです。「メールのアカウントが乗っ取られた」ときは違います。受信箱を読まれたり、メールを転送・削除されたりするおそれがあります。そのアドレスで登録したほかのサービスのパスワードを、再設定されるおそれもあります(本書の整理)。

制度・公式情報 警察庁は、ウェブメール(Web のサイトで読み書きするメール)の相談の例を挙げています。見た覚えのないメールが既読になり、送信済みのメールが消されていた、というものです[4]。Google のヘルプも、乗っ取りの兆しを挙げています。メールが届かなくなる、友人に自分からの迷惑メールが届いている、送信済みに覚えのないメールがある、受信トレイのメールが消えてゴミ箱にもない、などです。

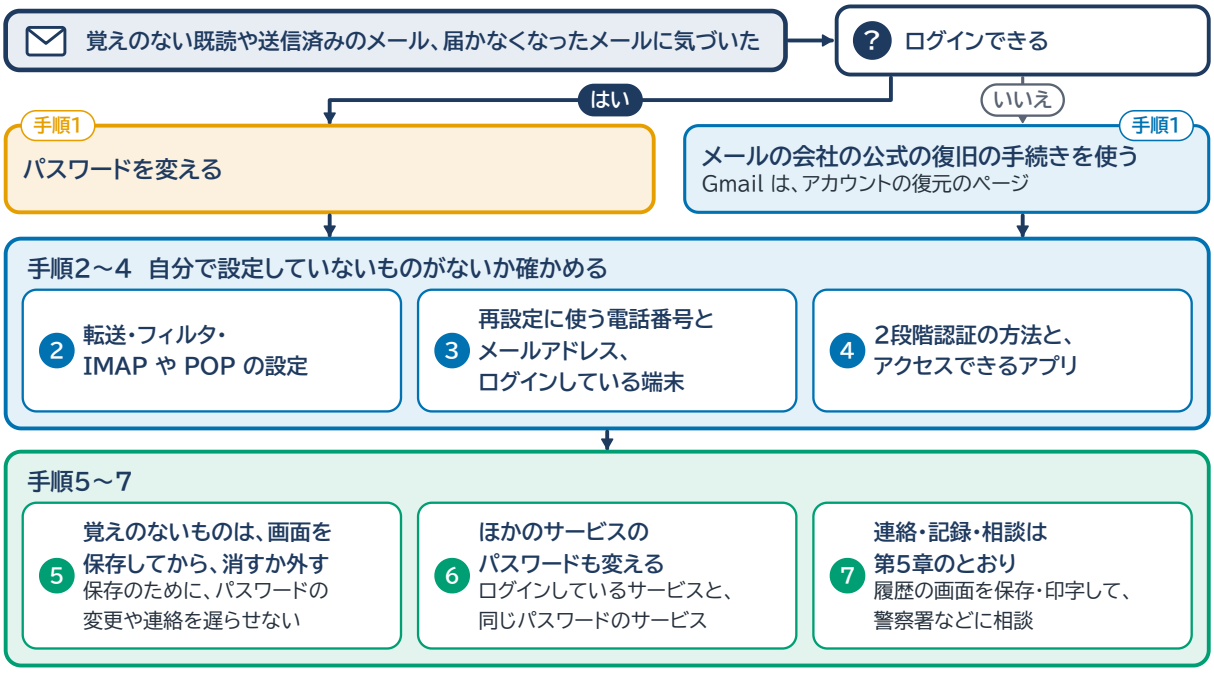


図6-2 メールのアカウントが乗っ取られたとき

メールのアカウントが乗っ取られたとき

1. 覚えのない既読や送信済みのメール、届かなくなったメールに気づいたら、パスワードを変えます。ログインできなければ、メールの会社の公式の復旧の手続きを使います(Gmail はアカウントの復元のページ)。
2. 自分で設定していない転送(届いたメールを、別のアドレスへ自動で送る設定)・フィルタ(振り分け)・IMAP や POP(ほかのメールソフトでメールを読むための設定)の設定がないかを確かめます。
3. パスワードの再設定に使う電話番号とメールアドレス、ログインしている端末に、覚えのないものがないかを確かめます。
4. 2段階認証の方法(覚えのない電話番号や認証のアプリ)と、アカウントにアクセスできるアプリを確かめます。
5. 2〜4で覚えのないものは、画面を保存してから、消すかアクセスを外します。保存のために、パスワードの変更や停止の連絡を遅らせません(第5章のステップ3。本書の推奨)。
6. そのメールアドレスでログインしているほかのサービスと、同じパスワードを使っていたサービスのパスワードも変えます。
7. 連絡・記録・相談の順は、第5章のとおりです。警察庁も、ログインの履歴の画面を保存・印字して、警察署などに相談するよう案内しています[4]。
8. 画面の名前や手順は、メールの会社で違います。携帯電話会社や ISP のメールは、各社の公式の案内で確かめます(本書の推奨)。

制度・公式情報 上の手順2〜4・6は、Google の Gmail の案内にもとづきます。Gmail では、自分で設定していないラベル(メールに付ける分類の名前)も消すよう案内しています。

相談先

- 偽のメール・サイトの報告: フィッシング対策協議会(メール info@antiphishing.jp か Web のフォーム)[2]
- 困ったとき: 警察相談専用電話(＃9110。受付時間は都道府県で異なる)

- メールのアカウントの乗っ取り: メールの会社の公式の窓口・ヘルプ。技術的な相談は IPA 情報セキュリティ安心相談窓口(6-5)

6-2 電話番号

実際に起きた事例 フィッシング(本物そっくりの偽のメールやサイトで、情報をだまし取る手口)のうち SMS を使うもの(スミッシング)では、電力会社・水道局・カード会社・宅配業者などをかたるものが確認されています(2026年8〜9月の報告)[2,5]。

実際に起きた事例 警察庁によると、警察官などをかたるニセ警察詐欺では、2026年上半期(暫定値〔確定前の数字〕)の最初の接触の98.2%が電話でした(第3章)[6]。漏えいが原因と確認された数ではありません。



図6-3 「警察」を名乗る電話は、いったん切って自分で確かめる



父

「警察です」と言われると、切ってはいけない気がしてしまいます。



専門家

いったん切って大丈夫です。かけ直すときは、自分で調べた番号にかけて確かめましょう(本書の推奨)。

今日やること

出典の番号が付いていない手順は、本書の推奨です。

1. 「警察」を名乗る電話は、いったん切ります。自分で調べた警察署の代表番号か、警察相談専用電話(#9110)にかけて確かめます。役所を名乗るときは、その役所の公式サイトなどで調べた番号にかけます。

2. 電話番号を変えるのは負担が大きいので、まず、かかってくる電話を減らします。知らない番号には出ず、かけ直すときは自分で調べた番号にかけます(第4章)。
3. 電話会社の番号表示・非通知拒否のサービスや、防犯機能付き電話も使えます(本書の推奨)。防犯機能付き電話は、通話を自動で録音したり、鳴る前に録音することを伝える警告を流したりする電話です。特殊詐欺(電話などで相手を信じさせ、会わずにお金をだまし取る詐欺)の対策について、警察庁は「何よりも『犯人と話をしない』ことが大切」とし、こうした対策を挙げています[7]。
4. スマホに「警察庁推奨アプリ」を入れ[8]、国際電話を使わない固定電話・ひかり電話(光回線を使う固定電話)は、発信と着信の休止を申し込みます(無償)[9]。くわしくは第4章の「電話・SMS の詐欺に備える」です。

家族と合言葉を決めておくなど、ふだんの電話の備えは、第4章の「電話・SMS の詐欺に備える」にあります。

どう悪用されるか・実例

実際に起きた事例 焼肉チェーンの公式アプリの件では、会員情報約1,079万件の漏えいに、電話番号も含まれていました(10月5日公表)[10]。

相談先

- 国際電話の休止: 国際電話不取扱受付センター 0120-210-364(通話料無料)。オペレーターは平日9時～17時、自動音声は24時間。Web でも申し込め、手続きが難しいときは最寄りの警察署に相談できます[9]。NTT東日本・西日本の電話は、NTT の窓口でも申し込めます(第4章)
- 不安なとき: 警察相談専用電話(＃9110)。緊急のときは110番

6-3 氏名・住所・生年月日

制度・公式情報 国民生活センターを名乗って「削除してあげる」と持ちかける電話もあります。同センターは、個人情報の削除はしないとしています[11]。対応は第5章の「『消してあげる』という持ちかけ」です。

制度・公式情報 消費者庁によると、注文や契約をしていないのに、お金を得る目的で一方的に送り付けられた商品は、2021年7月6日以降、すぐに処分できます。代金を払う義務はなく、誤って払ったときは、返すよう求めることができるとされています[12]。

今日やること

次の手順は本書の推奨です。

1. 頼んでいない商品や覚えのない請求のはがきが届いたら、払わずに消費者ホットライン(188)に相談します。
2. 「個人情報を削除してあげる」という電話には応じません。費用を払わず、本人確認の情報も渡しません。
3. 住所を知られていても、点検や配達を名乗る突然の訪問には、ドアを開ける前にインターホン越しで確かめます。

どう悪用されるか・実例

実際に起きた事例 家電などの通販サイトの件では、顧客の情報約772万件(氏名・住所・電話番号など)が外部に持ち出されたと公表されました(第二報9月15日)[13]。

住所が知られて不安なとき

住所が漏れて、つきまといなどの身の危険を感じたときの手順です。パスワードを変えても解決しないので、ためらわずに相談します（本書の推奨）。

> **住所が知られて不安なとき**
>
> 次の手順は、警察庁の案内をもとにした本書の推奨です。
>
> 1. つきまといや待ち伏せなど、身の危険を感じたら、ためらわずに最寄りの警察署に相談します。緊急のときは110番です。
> 2. ストーカーや DV（配偶者などからの暴力）の被害を受けていて、加害者に住所を知られたくないときは、市区町村の支援措置（下の警察庁の案内）などを使えるかを、警察と住んでいる市区町村に相談します。
> 3. 職場や学校にも、伝える範囲を決めて事情を話しておくことを考えます。
> 4. 住所や写真がネットに書き込まれたときは、6-9 の「写真や住所がネットに出たとき」に進みます。

制度・公式情報 警察庁のストーカー被害の「相談窓口・支援制度」のページは、「まずは警察に相談してみてください」としています。支援の制度として挙げているのは、市区町村の「支援措置」などです。ストーカーや DV の加害者からの、住民票の写しなどの交付の請求を制限する仕組みです。警察が費用を負担して、一時的な避難場所を確保できる場合があるともしています。

相談先

- 消費者ホットライン（188）: 近くの消費生活センターなどを案内します。相談は無料で、通話料がかかります
- 警察相談専用電話（＃9110）
- 身の危険を感じるとき: 最寄りの警察署（緊急は110番）。支援措置は、住んでいる市区町村の窓口

6-4 クレジットカード

実際に起きた事例 日本クレジット協会の集計では、カードの不正利用の被害額は2025年に510.5億円で、その93.1%が番号盗用（カードの番号などを盗んで使う手口）でした（第3章）[14]。



図6-4　カードの明細を確かめ、覚えのない利用はカード会社へ

今日やること

出典の番号が付いていない手順は、本書の推奨です。

1. カードの裏面の番号など、自分で確かめた番号でカード会社に連絡し、番号を変える再発行（差し替え）が必要かを相談します。不正利用の補償を受けるには、いつまでに連絡が要るかも聞きます。カードをなくした・盗まれた、覚えのない利用がある、というときは、支払いの予定の確認や差し替えの段取りより先に、すぐ連絡して止めます。
2. 番号の一部だけが漏れたときも、利用明細を確かめます。協会は、電子の明細は「定期的（できれば利用したらその日）に」見て、覚えのない請求は「速やかに」カード会社に連絡するよう勧めています[15]。
3. 利用通知（カードが使われたことを知らせる通知）と、3D セキュア（ネットの買い物のときに、カード会社がもう一度本人かを確かめる仕組み）を有効にします。何が通知されるかは会社ごとに違うので、通知だけに頼らず、手順2の明細の確認も続けます（第4章）。
4. カード会社から差し替えの案内が来たら、本物かを確かめます。連絡に書かれた方法ではなく、カードの裏面の番号や公式アプリを使います。

番号を変える再発行を頼むとき、ビューカードを使っているとき、スマホの決済を止めるときは、下の小見出しの手順も見ます。

どう悪用されるか・実例

制度・公式情報 協会は、カード会社が利用の確認の連絡で「クレジットカード番号等の入力を促すことはない」としています[15]。

実際に起きた事例 ネットショップの基盤（多くのネットショップが使う仕組み）の件では、約210万人分のカード情報の一部が対象でした。名義、番号の先頭6桁と下4桁、有効期限です。これだけでは決済に使えないと、基盤を運営する会社は説明しています[16]。

補償の期間の数え方と条件は会社ごとに違う

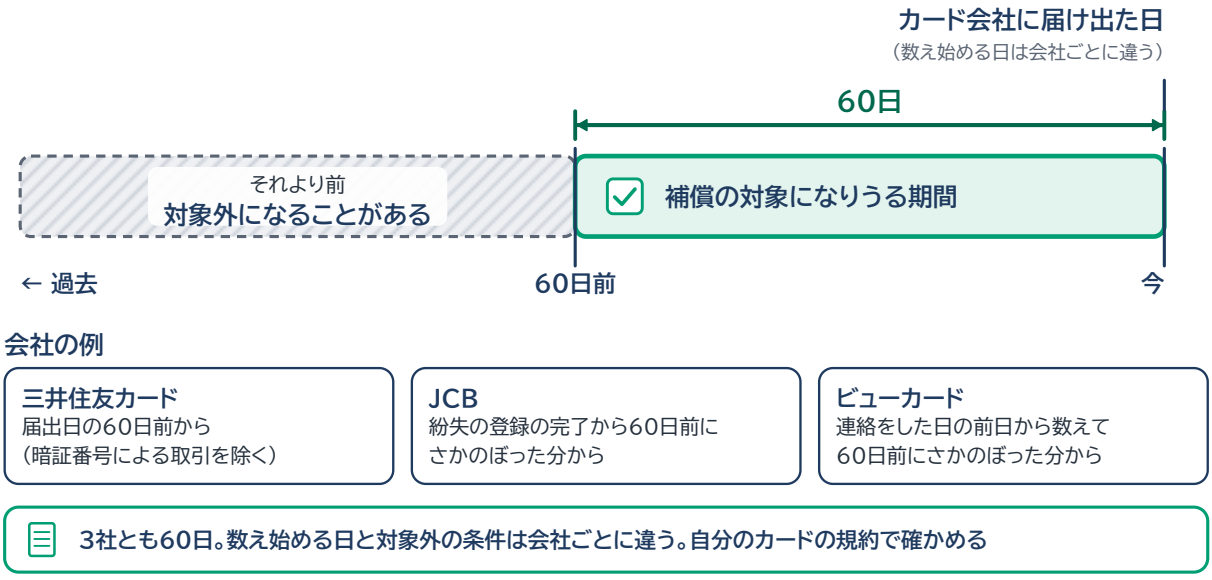


図6-5　カードの不正利用の補償の期間（会社の例）

制度・公式情報 補償の期間は、カード会社の規約で決まります。鹿児島県の相談事例では、明細の確認が郵送からアプリに変わり、うまく操作できずに確かめないまま、2か月にわたって不正利用が続いていました。カード会社からは「既

に補償期間の60日を経過しており補償できない」と言われました[17]。早く気づけば、期間のうちに連絡できます（本書の推奨）。

制度・公式情報 会社の例を挙げます。三井住友カードは、不正利用の補償を「暗証番号による取引を除き、届出日の60日前から」としています。JCB は、紛失の登録の完了から60日前にさかのぼった分からで、家族・同居人などの利用や、暗証番号が入力された利用などは対象外です。ビューカードは、紛失・盗難の連絡をした日の前日から数えて、60日前にさかのぼった分からで、登録した暗証番号が使われた場合など特別な場合は対象外です。JCB とビューカードは、詳しくは会員規約を見るよう案内しています。3社とも60日ですが、いつから数えるかと、対象外の条件が違います。数え方や対象外の条件は会社ごとに違うので、自分のカードの規約で確かめます。暗証番号が使われた利用でも、自分で対象外と決めつけず、補償の対象になるかをカード会社に確かめます（本書の推奨）。

番号を変える再発行のあいだ

番号が漏れたときは、番号を変える再発行（差し替え）を頼むことがあります。カード会社のほうから、差し替えの案内が来ることもあります。そのあいだに困らないための情報です。

番号を変える再発行のあいだ

次の手順は本書の推奨です。

1. 紛失・盗難や覚えのない利用がなく、漏えいの懸念で差し替えるときは、頼む前に、近いうちの大きな支払いと、カードで払っている継続払い（公共料金・携帯電話料金・定額のサービスなどの決まった支払い）を確かめます。古いカードがいつ止まるかも聞きます。
2. あわせて、新しいカードがいつ届くかと、スマホのウォレット（カードを登録して、スマホで払う機能）やカードに付いた電子マネーの扱いを、カード会社に聞きます。
3. 新しいカードが届いたら、利用制限の設定、スマホのウォレットへの登録、継続払いの登録先の変更の3つを確かめます。
4. カードで払っている継続払いの登録先を、ふだんから一覧にしておきます（第4章）。どこに登録したかは、カード会社でも分からないためです。

制度・公式情報 楽天カードは、加盟店（カードで払えるお店）でカードの情報が流出した可能性があるなどの連絡を受けることがあります。そのときは、漏えいの可能性がある会員に、メールや SMS で差し替えを案内することがあります。案内を受けた会員は、第三者に不正に使われる可能性が非常に高くなっているとして、早めの差し替えを勧めています。2026年7月29日のお知らせでは、手数料はかからず、楽天カードが「クレジットカード番号（16桁）やポイントカード番号を聞き取ることはございません」としています[18]。

制度・公式情報 番号を変える再発行では、新しいカードが届くまで、古いカードは使えないのが基本です。各社の案内の例は次のとおりです[18]。

会社と手続き（例）	古いカード	新しいカードの発送・到着（目安）
楽天カードの差し替え	止めてから新しいカードを送る。届くまで使えない	通常1週間から10日
三井住友カードの停止・再発行（紛失・盗難・不正利用）	完全に止める。止めたカードは使えない	1週間から10日ほどで発送。交通系 IC つきは、さらに1〜2週間ほど
JCB の紛失・盗難	手続きのあと、すぐ止まる	1〜2週間

会社と手続き(例)	古いカード	新しいカードの発送・到着(目安)
ビューカードの番号の変更(不正利用・悪用の懸念)	手元のカードの機能を止める	通常2〜4週間ほど。手続きの種類や時期で前後する

古いカードがいつ止まるかは、会社や再発行の理由で違うことがあります。手続きの前にカード会社に確かめます(本書の推奨)。

制度・公式情報 楽天カードは、漏えいの懸念による差し替えの案内について、カードを使う予定があるときは「カードご利用後に差し替えのお手続きをお願いいたします」と答えています。一方で、差し替えをしないと、第三者の利用が疑われるときに利用を制限することがあり、カードが使えない頻度が増える可能性があるとしています[18]。なお、カードが見当たらないだけのときは、番号を変えずに一時的に止める仕組みもあります(楽天カード・三井住友カードなど)[18]。

制度・公式情報 番号が変わると、カードで払っている継続払いは、自分で登録を変えるのが原則です。三井住友カードは、各契約会社に自分で問い合わせて変えるよう求めています。契約会社によっては、自動で新しいカードの情報に変わる場合もあります。JCB は、大手の電力・ガス会社や携帯電話3社などを、手続きが要らない場合の例に挙げています。一方、App Store などの Apple のサービスや、国民年金保険料は、手続きが要る例です。楽天カードは、自動で更新される場合も1〜2か月ほどかかることがあり、「加盟店ごとの契約状況は弊社では確認できません」としています[18]。

制度・公式情報 スマホのウォレットや、カードに付いたサービスの扱いも、会社や再発行の理由で違います。ビューカードによると、不正利用や流出の懸念で再発行したときの Apple Pay(iPhone で支払う機能)は、Visa ブランド(ブランドは、Visa・JCB など、カードの支払いの仕組みの名前)なら登録し直しが要ります。JCB・Mastercard ブランドは、手続きが要りません。JCB は、悪用の疑いで再発行したときなど、Apple Pay・Google Pay などは一部引き継げない場合があるとしています。カードに付いた楽天 Edy の残高は新しいカードに引き継がれないので、使い切ってから古いカードを捨てるよう案内しています。なくした・盗まれたなどで手元にカードがないときの残高の扱いは、カード会社に確かめます(本書の推奨)。三井住友カードの Olive フレキシブルペイは、紛失や悪用の懸念で再発行すると「利用制限が設定された状態」で届くので、アプリで「制限しない」に変えます。

ふだんから支払いの手段を複数持っておく備えは、第4章の「支払いの手段を1つに頼らない」で説明しています。

ビューカード(Suica・定期券つき)

ビューカードのとき

次の手順は本書の推奨です。

1. なくしたときや覚えのない利用があるときは、予定の確認より先に、紛失・盗難デスク(番号は下の相談先)に連絡して止めます。
2. 紛失・盗難や覚えのない利用がないまま番号だけ変えるときは、変える前に、電車・買い物・オートチャージ(残高が減ると、登録したカードから自動で入金する機能)などの予定を確かめます。この場合に Suica の残額や定期券がどうなるかも、電話で確かめます。

制度・公式情報 ビューカードを紛失・盗難で止めると、Suica の機能(定期券の機能を含む)もあわせて止まります。一度止めたカードは、あとで見つかっても使えません。連絡先は「ビューカード紛失・盗難デスク」(24時間・年中無休。番号は下の相談先)で、警察にも届け出ます。

制度・公式情報 定期券つきのカードを紛失・盗難で再発行するとき、定期券は新しいカードに自動では引き継がれません。デスクに連絡した翌日以降に、JR東日本のみどりの窓口へ行きます。持ち物は、整理番号（17桁）・公的証明書・1,020円（うち500円は預り金で、実質の負担は520円）です。Suica の残額と定期の情報を引き継いだ、新しい Suica カードを受け取れます。新しいビューカードが届くまでは、それを使います。届いたら、多機能券売機で「発行替え」をして1枚に戻します。

制度・公式情報 番号が変わったら、毎月の支払いに使っていた各事業者に、番号の変更を申し出ます。モバイル Suica は「カード番号などのお客さま情報の変更手続き」が、えきねっとの新幹線eチケットサービスは IC カードの情報の変更の手続きも要ります。不正利用や悪用の懸念で番号を変えるときは、名義人の本人が、カードを手元に用意して「ビューカードセンター（再発行受付デスク）」に電話します。手数料がかかる場合があります。

制度・公式情報 ビューカードは、Suica の機能の不正使用は、停止の手続きが完了するまでの分を補償の対象外としています。覚えのない請求も、利用日から長く経ってからの申し出には対応できない場合がある、としています。

電子決済・コード決済

スマホのアプリで払う電子決済や、スマホの画面のバーコードなどで払うコード決済も、スマホをなくしたときや、乗っ取られたおそれがあるときには止めます。

電子決済・コード決済

先に確かめること: 不正なアプリを入れたおそれがあるときは、先に通信を止めます（6-5）。手順2・3の連絡や操作は、別の安全な電話や端末からします（本書の推奨）。

1. スマホをなくしたら、携帯電話の回線とは別に、モバイル Suica やコード決済のサービスにも、それぞれ連絡して止めます。なくしたときの全体の手順は、6-5 の「スマホをなくしたとき」です（本書の推奨）。
2. 覚えのない利用に気づいたら、すぐ申し出ます。残高や銀行口座から払った分は、サービスの窓口へ申し出ます。登録したクレジットカードで払った分は、まずカード会社に連絡します。PayPay・楽天ペイも、カードへの請求はカード会社へ、と案内しています（下の表）。補償の申請の期限はサービスごとに違うので、早く申し出ます（本書の推奨）。
3. 覚えのない端末のログインを外します。例: PayPay は、アプリの[アカウント]→[セキュリティとプライバシー]→[端末の管理]で操作します。心当たりのない端末を削除したり、すべての端末からログアウトしたりできます。
4. 決済のアプリは、公式のアプリストアでも提供元や内容をよく確かめてから入れます。SNS の広告や、メール・SMS のリンクからは入れません（本書の推奨）。
5. 警察庁は、不正なアプリを入れてしまったら、直ちに削除して警察に相談するよう求めています[19]。アプリの名前などを控えてから削除します。順番は、6-5 の「スマホに不正なアプリを入れてしまったとき」です（本書の推奨）。

実際に起きた事例 警察庁は2026年9月、キャッシュレス決済（現金を使わない支払い）の不正な送金の被害に、注意を呼びかけました。不正なアプリを入れたことで、決済のサービスが遠隔操作（離れた所から端末を操作すること）されたものです。入口は SNS の広告、メール・SMS のリンク、SNS で知り合った相手などで、有名な SNS やアプリを装っているとしています[19]。

制度・公式情報 モバイル Suica を入れたスマホをなくしたときは、すみやかに会員メニューサイト（パソコン）で「利用停止手続き（再発行登録）」をします。オートチャージを設定していると、停止が完了するまでに第三者に使われ、登録

したカードに請求が来るおそれがあります。JR東日本の決済アプリ teppay も、モバイル Suica の利用停止で一時的に止まります。

制度・公式情報 止める窓口と、不正利用の補償の主な条件は、サービスごとに違います。各社の案内の例です[20]。

サービス（例）	スマホをなくしたとき	覚えのない利用・補償（例）
PayPay	「PayPay 携帯電話紛失・盗難専用窓口」0120-990-633（24時間受付、土日祝日を含む365日）に連絡する	補償の条件は、損害発生日から60日以内の申請、警察への被害の届出、家族などの利用でないことなど。自分で「送る・受け取る」を使った取引は対象外
楽天ペイ	楽天 ID のパスワードを変え、利用停止の申請フォームで申請する	カードへの請求はカード会社へ。楽天ポイント・楽天ペイ残高（楽天キャッシュ）・楽天銀行口座の利用は「楽天ペイ カスタマーデスク」0570-000-348（9時30分～23時）へ
d払い	「d払いお問い合わせダイヤル」（ドコモの携帯から ＃9785〔無料〕、ほかから 0570-018-360〔有料〕）。ドコモの回線を契約している人の利用停止は24時間受け付け	紛失・盗難はただちに申告して警察に相談し、損害を知った日から30日以内に書類を出す。申告した日から遡って90日より前の利用は対象外

制度・公式情報 PayPay は、登録したクレジットカードでの被害は、カード会社を通じて補償される場合があるので、まずカード会社に連絡するよう案内しています。d払いは、家族・同居人などの利用や、地震などの混乱に乗じた紛失・盗難なども、補償の対象外としています[20]。

相談先

- まず、カード会社（カードの裏面の番号）
- ビューカード: 紛失・盗難デスク 03-6685-4800（24時間・年中無休）、再発行受付デスク 03-6685-5851（9時～17時30分）、ご利用覚えなし相談デスク 03-6685-5861（9時～17時30分）
- 電子決済: 上の表の窓口（番号は、アプリや公式サイトでも確かめる）
- 話が進まないとき: 日本クレジット協会 消費者相談室 03-5645-3361（月～金曜日の10時～12時と13時～16時、祝日・年末年始を除く）

6-5 ID・パスワード

実際に起きた事例 モニター（覆面調査）サイトの件では2026年8月、リスト型攻撃（ほかで漏れた ID・パスワードの組を、次々に試す手口）を受け、59,389名の会員がログインされました。2アカウントでは、ポイントが不正に交換されました（第3章）[21]。



攻撃者

ほかで漏れた ID とパスワードの組を、別のサービスで次々に試します。パスワードを使い回していると、ログインできてしまいます[21]。

今日やること

出典の番号が付いていない手順は、本書の推奨です。

先に確かめること: スマホに不正なアプリを入れてしまったおそれがあるときは、そのスマホでパスワードを変えたり、ログインしたりしません。下の手順1～7より先に、この節の「スマホに不正なアプリを入れてしまったとき」の手順で進めます。

1. ID・パスワードが漏れた、または漏れたおそれがあると知らされたら、そのサービスと、同じパスワードを使うほかのサービスのパスワードを、すべて別のものに変えます[21]。メールのパスワードと同じだったときは、メールを最優先で変えます(6-1。本書の推奨)。パスワードを保存していたパソコンやサーバーが乗っ取られたおそれがあるときは、別の端末から変えます[22]。
2. 使えるサービスでは、多要素認証(パスワード・スマホ・指紋など、種類の違う確かめ方を2つ以上組み合わせる仕組み)やパスキー(パスワードの代わりに、スマホなどの機器と指紋・顔・PIN〔暗証番号〕で本人を確かめる仕組み)を設定します(第4章)[23]。
3. ログインの履歴(覚えのない端末・場所)を確かめます。覚えのないログインがあれば、その画面を保存します(第5章のステップ3)。そのうえで、サービスの公式の案内に沿って、その端末をログアウトさせます。
4. パスワードの再設定に使うメールアドレスや電話番号が、書き換えられていないかを確かめます。
5. 連携しているアプリ(そのアカウントでログインできるようにした、ほかのサービス)を確かめ、使っていない連携は外します。
6. 自分でログインできなくなったら、公式の窓口に相談します。メールのアカウントは 6-1、SNS・メッセージアプリは下の「SNS・メッセージアプリが乗っ取られたとき」で確かめます。
7. ポイントやマイルの残高と交換の履歴を確かめ、覚えのない交換はすぐ運営会社に連絡します。

SNS・メッセージアプリの乗っ取り、不正なアプリ、スマホをなくしたときの手順は、この節の小見出しにあります。

どう悪用されるか・実例

実際に起きた事例 プロバイダー向けのメールの仕組みの件では、6-1の人数のうち約762万名分のパスワードが、暗号化されず、そのまま読める形で保存されていて、漏えいしました。メールボックスの中まで見られる状態だった、と個人情報保護委員会(個人情報の扱いを監督する国の機関)は説明しています[24]。

実際に起きた事例 仮想のパソコンを貸すクラウドの件(2026年10月)では、サービスへの不正アクセスが公表されました。運営する会社は10月22日の第2報で、サーバー内に保存されていた取引口座のログイン情報などが取られ、不正に使われた可能性があるとしています。利用者から、取引口座で第三者による不正な操作が行われたとの報告もあったとしています[22]。報道によると、このサービスは FX(外国為替証拠金取引)の自動売買のソフトを24時間動かすのに使われていました[25]。

その会社は10月23日の第3報で、FX の取引に使っていない端末(スマホや別のパソコン)から、パスワードを変えるよう求めています。ログイン中の接続も、すべて切るよう求めています。パスワードを変えても、取引先の会社(証券会社・FX 会社など)の仕組みによっては、しばらく接続が残り、第三者が取引を続けられる場合があるためです。接続を切ることは、取引先の会社にも頼むよう案内しています。あわせて、取引の履歴と残高を確かめ、2段階認証を設定するよう求めています[22]。

SNS・メッセージアプリが乗っ取られたとき

乗っ取られたと気づいたら、取り戻す手続きと、家族や友人への知らせを並行して進めます。

SNS・メッセージアプリが乗っ取られたとき

出典の番号が付いていない手順は、本書の推奨です。

1. ログインできるうちに、パスワードを変えます。登録のメールアドレス・電話番号を確かめて自分のものでない情報を消し、多要素認証を設定します[26]。
2. ログインできなければ、運営者の公式の手順(再ログイン・引き継ぎ・「パスワードを忘れた」など)を試します。だめなら、公式のアプリやサイトから開いた問い合わせフォームで連絡します[27,26]。
3. 取り戻す手続きと並行して、家族や友人に知らせます。電話や対面、別の SNS など、乗っ取られたアカウント以外の方法で、「私を名乗る送金や確認コードの依頼には応じないで」と伝えます(確認コードは、ログインなどのときに SMS などで届く確認用の番号です)。
4. 取り戻せたら、覚えのない端末がログインしていないかと、登録の連絡先が書き換えられていないかを確かめます。メールのアカウントも心配なときは、6-1 の手順で確かめます。
5. アカウントが削除され、作り直しになることもあります(下の LINE の例)。友人や家族の連絡先は、ふだんから別にも控えておきます(第4章の「予備のコードとバックアップ」の手順4・7と、「通信が止まったとき」の手順4)。

実際に起きた事例 IPA の2026年4～6月の相談事例です。知り合いの SNS のアカウントから、投票を頼む DM(ほかの人には見えない個別のメッセージ)が届きました。誘導された偽の入力画面に、電話番号・パスワード・確認コードを入れてしまいました。そのため、LINE(メッセージアプリ)のアカウントを乗っ取られたと考えられる例です。乗っ取られたアカウントから、友人や家族に PayPay での送金を求めるメッセージが送られました。IPA は、「LINE上の知り合いに対して注意喚起を行う」よう勧めています[28]。

制度・公式情報 IPA は2025年8月の注意喚起で、次のように説明しています。乗っ取られると、パスワードや登録の電話番号・メールアドレスを変えられ、本人がパスワードを再設定できなくなることがあります。無料のサービスなどでは「電話での受付窓口が存在しないサービスが多い」ので、ウェブのフォームで相談します[26]。警察庁も、SNS のパスワードを変えられ、自分の名前で投稿されていた、という相談の例を挙げています[4]。

家族や友人から突然お金や認証番号を頼まれたときの確かめ方は、第4章の「家族で決めておくこと」です。会社やお店の公式アカウントが乗っ取られたときは、第8章を見てください。

LINE の場合

制度・公式情報 LINE ヘルプセンター(2026年5月20日更新)も、投票ページを装った偽のサイトで、アカウントを乗っ取られる事例が「相次いでいます」としています。LINE は、LINE の登録情報と組み合わせて認証番号(SMS で届く確認用の番号)を聞き出したり、画面に入力させたりする行為は「全て詐欺」だとしています。自分で引き継ぎをするときや、メールアドレス・電話番号を変えるとき以外に、認証番号を使うことはないとしています[27]。認証番号は、誰に聞かれても伝えず、人に教えられた画面には入れません(本書の推奨)。

制度・公式情報 LINE の案内は、いまの端末でメッセージを送受信できれば、アカウントは乗っ取られて(ほかの端末に引き継がれて)いない、としています。ただし同じ案内は、第三者がパソコンや iPad などからログインした可能性もあるとしています。ログインの通知が届いた、覚えのないメッセージが送られていた、というときは、パスワードを変え、「ログイン許可」をオフにし、覚えのない端末をログアウトします。使えなくなったら、再ログインや引き継ぎを試し、できなければ問い合わせフォームから連絡します。乗っ取りが確認されると、LINE は悪用を防ぐためにアカウントを削除し、有料のアイテムやコインを新しいアカウントへ移します。問い合わせは本人からだけで、家族や友人などの代理は原則として受け付けていません[27]。

スマホに不正なアプリを入れてしまったとき



図6-6　まず通信を止めて、別の電話から連絡する

まず、機内モード（スマホの通信をまとめて止める設定）をオンにし、Wi-Fi もオフにして通信を止めます。お金の被害が疑われるときは、別の電話から銀行・カード会社に連絡します。確かめるのは、自分のスマホとアカウントに限ります。

Android のスマホに不正なアプリを入れてしまったときは、次の順に進めます。IPA の手順[29]に、お金の被害を止めることと、記録を残すことを足しました（手順2～4は本書の推奨）。

不正なアプリを入れてしまったとき

1. 機内モードをオンにし、Wi-Fi もオフにして、通信を止めます。初期化が終わるまで、通信は戻しません（本書の推奨）。
2. お金の被害（身に覚えのない送金・引き落とし・決済の知らせなど）が疑われるときは、すぐに銀行・カード会社に連絡します。家族のスマホや固定電話など、別の安全な電話や端末を使い、アプリの削除や初期化（買ったときの状態に戻すこと）を待ちません。
3. お金の被害がなくても、ネットバンキング（ネットで振込などができる銀行のサービス）・メール・Google アカウントなど大事なアカウントのパスワードは、別の安全な端末から先に変えます。
4. 安全にできる範囲で、記録を残します。アプリの名前と、入れた日時・きっかけ（届いたメールや SMS など）を紙に控えます。アプリの一覧などの画面は、別の機器のカメラで撮っておきます。
5. 機内モードのまま、「設定」のアプリの一覧から、そのアプリを削除（アンインストール）します。ホーム画面には出ないことがあります。
6. 携帯電話会社・フリマ（個人どうしで物を売り買いするサービス）・後払い決済（商品を受け取ったあとで代金を払う仕組み）などから、登録や変更の知らせが届いていないかを確かめます。SMS は初期化で消えるので、先に確かめます。写真などは、別の媒体に保存しておきます。
7. 影響の範囲が分からないため、IPA は、アプリの削除だけでなく、スマホの初期化を勧めています。お金の被害が疑われるときは、初期化の前に、銀行・カード会社と警察に相談します。初期化で記録が消えることがあるためです（6-7。本書の推奨）。

8. 初期化の操作は、契約している携帯電話会社などに問い合わせます。初期化のあとで通信を戻し、アプリを入れる前のバックアップから戻します。
9. 初期化のあとで、まだ変えていない各アカウント（Google アカウントなど）のパスワードを変えます。多要素認証も使います（第4章の「パスキー・2段階認証を使う」）。
10. 覚えのないキャリア決済（買い物の代金を携帯電話の料金と一緒に払う仕組み）の請求がないかを、携帯電話会社に確かめます。携帯電話会社の ID・パスワード・暗証番号を入れてしまったときは、変更します。変更できなければ乗っ取られている可能性があるので、携帯電話会社に相談します。

制度・公式情報 IPA は2026年10月23日、国税庁をかたるフィッシングメールの報告を公表しました。2026年9月から、Android のスマホ向けの不正なアプリを入れさせようとするものを確認しているとしています。不正なアプリを入れると、遠隔操作や不正送金の被害にあうおそれがあります。個人情報やカード情報を盗まれたり、勝手に SMS を送られたりするおそれもあります。入れてしまったら、「ただちに通信を遮断（機内モードをオン）」するよう求めています。2026年10月1日現在、Android 向けの公式の e-Tax（国税の申告などをネットで行う仕組み）のアプリはありません。

実際に起きた事例 日本サイバー犯罪対策センター（JC3。サイバー犯罪の対策に取り組む一般財団法人）は10月15日、偽のスマホのアプリによる被害に注意を呼びかけました。「お得」「見たい」という興味につけ込んで、偽のアプリを入れさせる手口です。遠隔操作で、ネットバンキングの不正送金や、不正なキャッシュレス決済をする被害を確認しているとしています。偽のアプリは、アクセシビリティ機能（ユーザー補助。画面の読み上げなど、操作を助ける機能）の権限（アプリに許す操作）など、強い権限を求める傾向があります。スマホの操作を奪われ、操作できなくなる事例も確認しています[30]。

実際に起きた事例 フィッシング対策協議会も9月30日、注意を呼びかけました。国税庁のほかにも、「さまざまなブランドをかたり不正アプリのインストールへ誘導するメールが急増」しているとしています。メールや SMS のリンクを開かず、アプリを入れないよう求めています[31]。

JC3 は、被害を確かめたら警察に通報・相談し、できればすぐに偽のアプリを削除するよう求めています[30]。カードや口座の被害に気づいたときの連絡の順と記録は、6-4・6-7 で説明します（補償の制度は第7章）。iPhone で心配なときや、手順が分からないときは、IPA の情報セキュリティ安心相談窓口（下の相談先）に相談します（本書の推奨）。アプリの入れ方の備えは、第4章の「不正なアプリを入れない」にあります。

スマホをなくしたとき

まず、別の機器から「探す」（Apple の、端末を探す機能）か Find Hub（Google の、端末を探す機能。以前の名前は「デバイスを探す」）を開き、スマホをロックします。

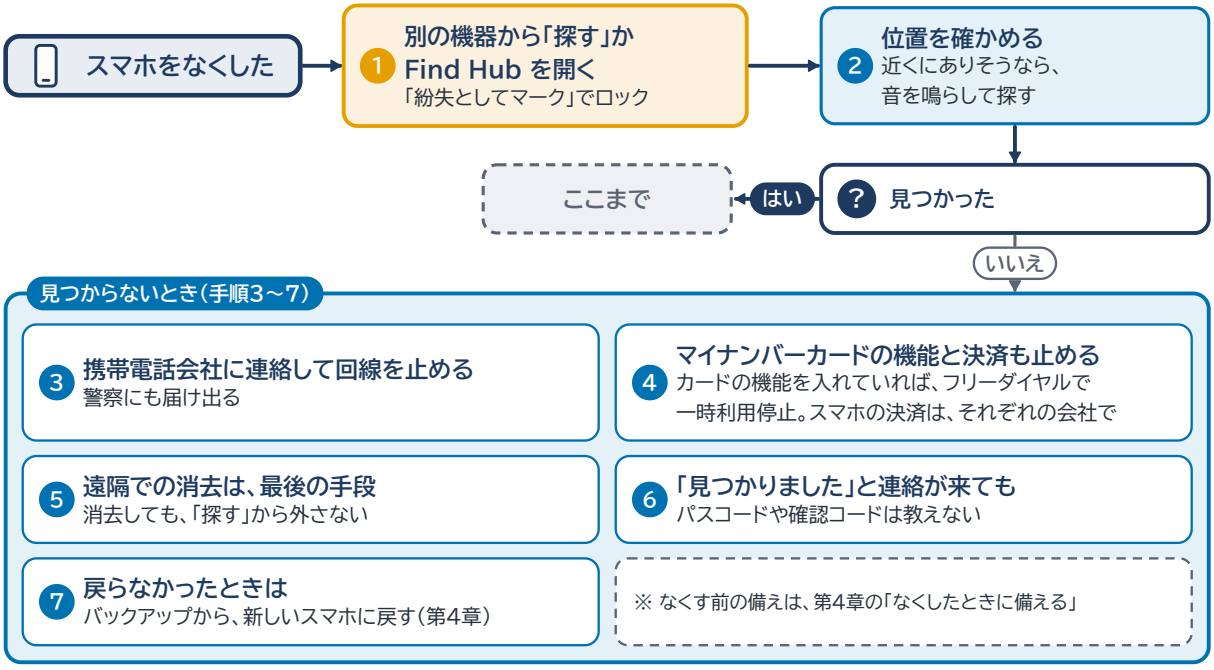


図6-7 スマホをなくしたとき

スマホをなくしたとき

1. 別の機器やパソコンから「探す」か Find Hub を開き、「紛失としてマーク」でロックします[32]。
2. 位置を確かめます。近くにありそうなら、音を鳴らして探します。
3. 見つからなければ、携帯電話会社に連絡して回線を止め、警察に届け出ます。
4. マイナンバーカードの機能を入れたスマホは、マイナンバー総合フリーダイヤルに電話して一時利用停止を頼みます(番号は 6-6)[33]。スマホの決済(モバイル Suica・コード決済など)は、回線とは別に、それぞれの会社で止めます(6-4。本書の推奨)。
5. 遠隔での消去は、最後の手段にします。消去しても、「探す」から外しません[32]。
6. 「見つかりました」という連絡が来ても、パスコード(iPhone の画面のロックを解く暗証番号)や確認コードは教えません。Apple は、Apple から「見つかった」と連絡することはないとしています。
7. 戻らなかったときは、バックアップから新しいスマホに戻します(第4章の「予備のコードとバックアップ」の手順4)[32]。

制度・公式情報 国家サイバー統括室のハンドブックは、スマホが見当たらなくなったら「なによりもまずスマホをロック」し、次に位置を確かめる、としています。遠隔で消去すると位置が分からなくなるとして、危険が少なければロックだけにして、警察に遺失物として相談するよう勧めています[32]。

制度・公式情報 Apple の案内では、iPhone をなくしたときは、ほかの Apple 製品の「探す」アプリを使います。ブラウザで icloud.com/find を開いても使えます。ログインに確認コードは要らないので、コードを受け取る機器をなくしていても使えます。「紛失としてマーク」すると、パスコードでロックされ、Apple Pay のカードも使えなくなります。遠隔での消去は元に戻せないので、最後の手段にします。スマホが通信につながっていないときは、次につながったときに消去が始まります。

制度・公式情報 Android では、Google の Find Hub を使います。別の Android の端末の Find Hub アプリか、ブラウザの Find Hub で、位置の確認、音を鳴らす、「紛失としてマーク」、データの消去ができます。紛失としてマークすると、PIN などでロックし、画面に連絡先を出せます。ロックやデータの消去ができるのは、スマホの電源が入っていて、モバイルデータか Wi-Fi につながり、Google アカウントにログインしているときです。位置は、

Google に保存された最近の位置や、ほかの Android 端末の助けを借りる「Find Hub ネットワーク」で分かる場合もあります。

制度・公式情報 携帯電話会社は、なくしたスマホの回線を止める窓口を設けています。例えば au は、Web（My au）か電話で、24時間365日受け付けています。ソフトバンクは、回線の停止を24時間受け付け、本人が連絡できないときは家族からの電話でも受け付けるとしています。USIM カード（スマホなどで通信するためのカード）は別の端末に差しても使えるので、必ず止めるよう求めています。

なくす前の備え（画面ロック、「探す」・Find Hub をオンにする、iPhone の「盗難デバイスの保護」、窓口の番号を紙に控える）は、第4章の「なくしたときに備える」にあります。

パソコンがランサムウェアに感染したおそれがあるとき

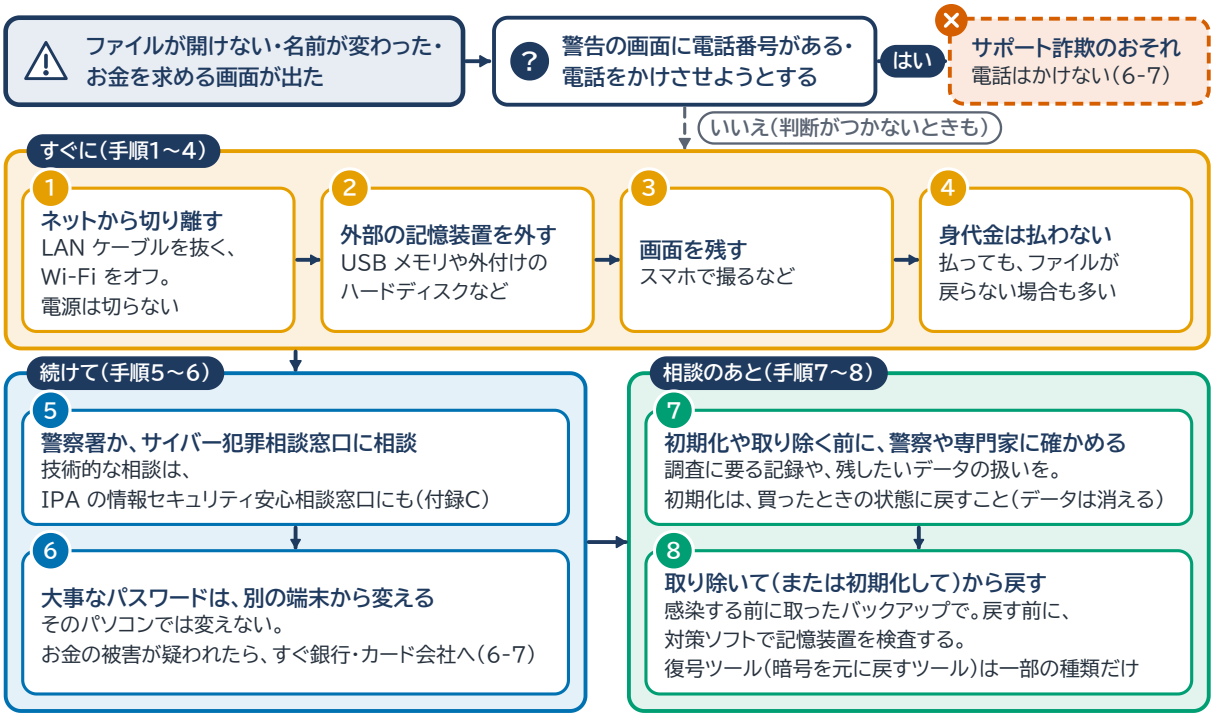


図6-8　パソコンがランサムウェアに感染したおそれがあるとき

ランサムウェア（データを暗号化して身代金を求める不正なプログラム）は、会社だけでなく、個人のパソコンもねらいます。

制度・公式情報 警察庁は、相談の例として、パソコンが操作できなくなり、元に戻すことと引き換えにお金を払うよう求める画面が出た例や、ファイルの名前が書き換えられて暗号化され、お金を求められた例を挙げています[34]。

ファイルが開けない、ファイルの名前が変わっている、お金を求める画面が出る、といったときは、感染を疑います（本書の推奨）。ただし、画面の警告だけで感染と決めつけません。サポート詐欺（ウイルスを見つけたという偽の警告で電話をかけさせ、遠隔操作のソフトなどを入れさせる手口）もあるためです（6-7）。警告に出た電話番号にはかけません。判断がつかないときは、念のため次の手順に進みます（本書の推奨）。

感染したおそれがあるときの手順

出典の番号が付いていない手順と、手順の中の具体的なやり方の例は、本書の推奨です。

1. LAN ケーブルを抜く、Wi-Fi をオフにするなどして、パソコンをネットワークから切り離します。電源は切りません。原因を調べるための記録が消えることがあるためです[34]。
2. USB メモリや外付けのハードディスクなど、つないでいる外部の記憶装置も外します[35]。

3. 画面に出たメッセージを残します(スマホのカメラで撮るなど)。種類を調べる手がかりになります[35]。
4. 身代金は払いません。払ってもファイルが元に戻らない場合も多く、要求に応じることは勧められません[36]。
5. 最寄りの警察署か、サイバー犯罪相談窓口に相談します。初動の支援や、復号ツール(暗号を元に戻すツール)の案内を受けられる場合があります[34]。パソコンの技術的な相談は、IPA の情報セキュリティ安心相談窓口にもできます(付録C)。
6. ネットバンキングやメールなど大事なアカウントのパスワードは、そのパソコンではなく、別の安全な端末から変えます。お金の被害が疑われるときは、すぐ銀行・カード会社に連絡します(6-7)。
7. 初期化(パソコンを買ったときの状態に戻すこと。保存したデータは消えます)や駆除の前に、調査に要る記録や、残したいデータの扱いを、警察や専門家に確かめます。IPA は、ほかのウイルスにも感染している可能性があるとして、初期化をしてから使い直すよう勧めています(2017年の案内)[37]。
8. データは、ランサムウェアを取り除いて(または初期化して)から、感染する前に取ったバックアップで戻します[35]。気づく前でも、不正なプログラムが入り込んだあとに取ったバックアップは、汚染されているおそれがあります。IPA は、汚染された可能性があるバックアップは復旧に使えないとしています[38]。戻す前に、更新した対策ソフトで記憶装置を検査します。IPA も、データを保存していた USB メモリ等は、使う前に検査するよう勧めています(長期休暇の対策)[39]。ただし、検査で何も見つからなくても、安全とは言い切れません。どれが安全か迷うときは、使う前に IPA の相談窓口に聞きます。復号ツールで戻せる場合もありますが、一部の種類にしか使えず、すべてが戻るとは限りません[34,35]。

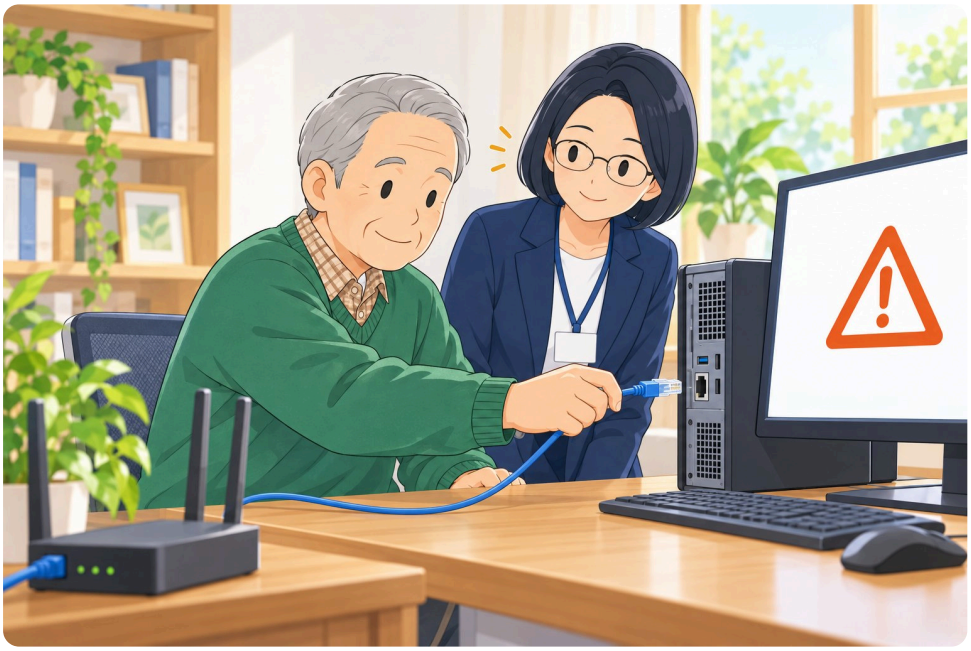


図6-9　警告の画面が出ても番号にはかけず、ネットから切り離して相談する

制度・公式情報 警察庁は、バックアップのデータまで暗号化される例が多いとして、バックアップをこまめに取り、ネットワークから切り離して保管するよう勧めています[34]。ふだんの備えは、第4章の「予備のコードとバックアップ」にあります。

使っていたサービスの攻撃者が、ランサムウェア攻撃を予告しているとき

実際に起きた事例 仮想のパソコンを貸すクラウドの件(2026年10月)では、運営する会社が10月24日に公表しました。攻撃者とみられる者から、要求に応じなければ情報の公開などに及ぶとの連絡を受けている、という内容です。その中に、サービスに接続した利用者のパソコンに関する情報の公開と、ランサムウェア攻撃の実行がありました。会社は要求に応じないとしています[40]。のちの第7報では、その理由を「要求に応じても、取得された情報の削除や不正利用の防止が保証されるものではないため」と説明しています[41]。第5報では、二次被害を防ぐための予防的な対応とし

て、利用者に2つのことを求めました。端末のウイルス対策ソフトでのフルスキャン（すべてのファイルを調べること）と、データのバックアップです。バックアップしたファイルの取り扱いには注意するよう添えています。取引口座については、別の端末からパスワードを変え、ログイン中の接続（セッション）をすべて切るよう求めています[42]。

実際に起きた事例 会社は10月26日の第6報で、利用者へのお願いを4つにまとめ直しました。1つ目は、接続した端末のフルスキャンです。2つ目は、ネットワークから切り離した状態での、外付けの記憶装置へのバックアップです。3つ目は、別の安全な端末から公式サイトで行う、アカウントの保護です。すべての端末・接続からのログアウト、パスワードの変更、多要素認証の設定が含まれます。心当たりのない連携アプリ・転送設定・拡張機能・登録端末の削除も求めています。点検が終わるまで、ブラウザの同期はオンにしないよう求めています。4つ目は、調査への任意の協力です。「被害金を取り戻す」など、費用を求める連絡には応じないよう呼びかけています[43]。

実際に起きた事例 予告の時刻が近づいた10月27日の第8報・第9報では、その時刻の前にバックアップを取ったうえで、ネットワークを切り、電源を落とし、コードを抜くよう求めました[44,45]。第9報では、解析を終えた端末からマルウェアは確認されていないとしました。ただし、すべての端末の安全を確かめたものではないとしています。ランサムウェアの被害にあった利用者には、被害を確かめたうえで、同等の性能の新しいパソコンを渡すとしています[45]。

実際に起きた事例 第10報（10月27日）では、攻撃者とみられる者が、会社と利用者に関する情報と称するものを公開したのを確認したとしました。事実と異なる内容が含まれるおそれがあるとしています。公開された情報と称するものにはアクセスしたり拡散したりしないよう呼びかけ、アクセスした人の情報は攻撃者に取得されるとしています。13時55分の時点で、ランサムウェア攻撃は確認されていません[46]。同じ日の第11報では、アクセスした人の情報が攻撃者に取得されていることを確認したとし、すでにアクセスした人にはフルスキャンを求めました。公開された情報に利用者の情報があると確認したら、対象の人に個別に連絡するとしています[47]。

予告されたときに合わせた公的な手順は、本書の調査では見つかりませんでした（2026年10月27日時点）。サービスの会社の案内に従い、次のように備えます（本書の推奨）。

- 使っているサービスの会社の案内を確かめ、それに従います。
- すでに感染のサインがあるときは、記憶装置をつながずに、上の手順に従います。
- バックアップは外付けの記憶装置などに取り、取り終えたらパソコンから外して保管します。
- いま取るバックアップにも、気づかないうちに不正なプログラムが入っているおそれがあります。取った日付を書いて別にしまい、戻す前に検査します（本書の推奨）。自分が管理していないパソコンにはつなぎません[48]。
- 大事なアカウントのパスワードは、別の安全な端末から変えます。
- 予告の時刻より前に、会社から電源を切るよう求められたら、それに従います。予告された時刻より前に行う、予防のための対応です（本書の推奨）。
- 感染したおそれに気づいたあとは、上の手順のとおり、電源は切らずに相談します。記録を残すためです（本書の推奨）。
- 攻撃者が公開したとされる情報には、アクセスしたり広めたりしません。見かけても、転載・再投稿・リンクの共有はしません。開いてしまったときは、ウイルス対策ソフトでフルスキャンをします[46,47]。
- 写真や家族のことを持ち出して脅されたときは、第5章「写真や家族のことを持ち出して脅されたとき」の手順に従います。
- 攻撃者を名乗る者からのメールやメッセージは開かず、返信もしません（第5章）。

相談先

- 漏れたサービスの公式の窓口（自分で開いた公式サイト・公式アプリのお知らせに載っているもの。届いたメールやSMS に書かれた番号やリンクは使わない）

- 乗っ取りなど技術的な相談: IPA 情報セキュリティ安心相談窓口 03-5978-7509(10時～17時、土日祝日・年末年始を除く)
- SNS・メッセージアプリの乗っ取り: 運営者の公式の問い合わせフォーム(LINE は本人からだけ受け付ける)[27]
- 被害を届けるとき: 最寄りの警察署(相談の流れは第5章)[4]
- スマホをなくしたとき: 契約している携帯電話会社の紛失・盗難の窓口(番号は公式サイトで確かめる)。お金の被害は、カード会社・銀行(6-4・6-7)

6-6 マイナンバー

制度・公式情報 デジタル庁は、マイナンバーだけでは手続きができず、「直ちに悪用したりすることはできません」と説明しています[49]。

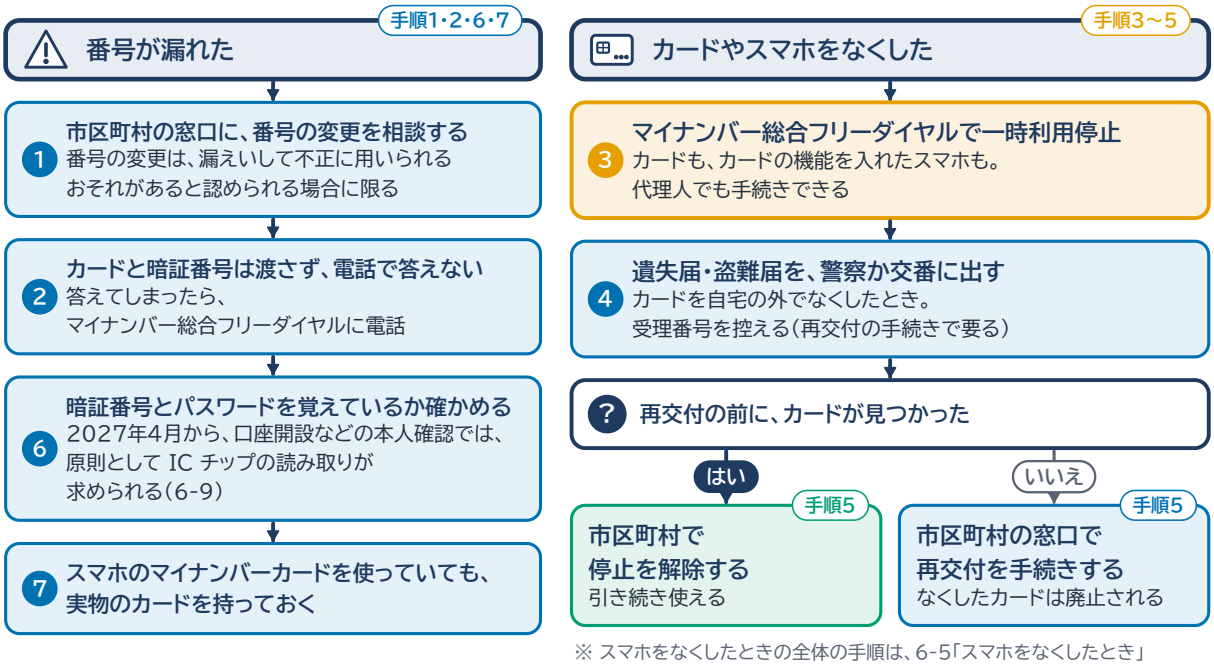


図6-10 マイナンバーが漏れた・カードやスマホをなくしたとき

今日やること

手順3～5は、カードやスマホをなくしたときの手順です。番号が漏れただけのときは、手順1・2・6・7を進めます。

1. 住んでいる市区町村の窓口に、番号の変更の対象になるかを相談します。マイナンバーは原則として変えられませんが、「漏えいして不正に用いられるおそれがあると認められる場合に限り」、本人の申請などで変更できます[49]。
2. カード本体と暗証番号は人に渡さず、電話で番号や暗証番号を答えません。答えてしまったら、マイナンバー総合フリーダイヤルに電話します[49,50]。
3. カードや、マイナンバーカードの機能(電子証明書。ネットの手続きで本人を確かめる機能)を入れたスマホをなくしたときは、マイナンバー総合フリーダイヤルに電話して一時利用停止を頼みます。代理人でも手続きできます[51]。スマホをなくしたときの全体の手順は、6-5 の「スマホをなくしたとき」です。
4. カードを自宅の外でなくしたときは、警察か交番に遺失届・盗難届を出し、受理番号を控えます。再交付の手続きで要ります[49,51]。

5. カードが見つからないときは、市区町村の窓口で、再交付を手続きします(なくしたカードは廃止されます)。再交付の前にカードが見つかったら、市区町村で停止を解除すれば、引き続き使えます[49,51]。
6. カードの暗証番号とパスワードを覚えているか確かめます。2027年4月から、口座開設などの本人確認では、原則として IC チップ(カードに埋め込まれた、情報を記録する部品)の読み取りが求められます(6-9。本書の推奨)。
7. スマホのマイナンバーカードを使っていても、実物のカードを持っておきます[52]。

どう悪用されるか・実例

制度・公式情報 デジタル庁と J-LIS(地方公共団体情報システム機構)によると、マイナンバーカードの券面には、偽造を難しくする工夫があります。見る角度で色が変わるインキや、レーザーで文字を彫る加工などです。顔写真つきなので、なくしても第三者が容易になりすますことはできない、としています。IC チップに記録された情報を読み取るには、「4桁の暗証番号や顔認証が必要」としています。暗証番号は、一定回数まちがえるとロックがかかります[53]。カードには、4桁の暗証番号のほかに署名用パスワード(英数字6〜16文字)もあり、使う機能や手続きで求められるものが違います(下の「カードをなくしたとき・スマホのカード」)。

制度・公式情報 厚生労働省は、同省の職員を装う詐欺の電話に、注意を呼びかけています。マイナ保険証の利用登録を口実に、手続きをうながすものです。同省は、電話の音声案内や SMS で利用登録を求めることは「一切ありません」としています[50]。

実際に起きた事例 自治体の委託先(仕事を任された会社)の IT 会社が、ランサムウェア(データを暗号化して身代金を求める不正なプログラム)の攻撃を受けました。委託元の自治体の発表(7月30日更新)では、マイナンバーを含む人事給与システムの6,167人分に漏えいのおそれがあります[54]。

制度・公式情報 マイナンバーを含む情報の漏えいは、ほかの個人情報より厳しい決まりで扱われます。会社などは、漏れた(おそれを含む)人が100人を超えるときや、不正の目的によるおそれがあるときなどに、個人情報保護委員会に報告し、本人に知らせます(第8章)[55]。

カードをなくしたとき・スマホのカード

制度・公式情報 カードをなくしたときは、自宅の外なら警察か交番に遺失届・盗難届を出し、受理番号を控えます(再交付で要ります)。フリーダイヤルでの一時利用停止と、市区町村での再交付は、別の手続きです。停止のあとカードが見つかったら、市区町村で停止を解除すれば、引き続き使えます。再交付では、なくしたカードを廃止する手続きをします[49,51]。

制度・公式情報 再交付の手数料は、次のとおりです(デジタル庁、2025年3月・12月)。「特急発行・交付制度」は、紛失・盗難・破損などから30日以内に市区町村の窓口で申請すると使え、原則1週間で届きます[51,53]。

申請のしかた	手数料	電子証明書が要らないとき
通常	1,000円	800円
特急発行・交付制度	2,000円	1,800円

制度・公式情報 窓口には、顔写真つきの公的な本人確認書類1点、顔写真、遺失届・盗難届の受理番号の控えなどを持って行きます。顔写真つきの書類がないときは、市区町村からの照会書への回答書と、ほかの書類2点が要ります[51,53]。

制度・公式情報 「スマートフォンのマイナンバーカード」は、カードの機能をスマホに入れ、暗証番号の代わりに顔や指紋などで本人確認ができるサービスです。iPhone 版は2025年6月24日から使え、Android 版は2026年10月

20日から「Androidのマイナンバーカード」になりました。マイナ免許証（運転免許証の機能をマイナンバーカードに入れたもの）としては使えません。デジタル庁は、実物のカードしか使えない場面に備えて、「必ず実物のマイナンバーカードもお持ちください」と案内しています[52]。

制度・公式情報 実物のカードかスマホをなくして一時利用停止をすると、スマホのマイナンバーカードも使えなくなります。利用を再開するには、マイナアプリ、実物のカード、券面事項入力補助用暗証番号（数字4桁）、署名用パスワード（英数字6～16文字）が要ります[52]。

相談先

- 住んでいる市区町村の窓口（番号の変更の相談）
- マイナンバー総合フリーダイヤル 0120-95-0178（音声案内で番号を押す）

用件	番号	受付時間
カード・スマホをなくした	2番	カードの一時利用停止は24時間365日
カード・電子証明書の問い合わせ	1番	毎日9時30分～20時（年末年始も）
そのほかの問い合わせ	3～7番	平日9時30分～20時、土日祝日9時30分～17時30分（年末年始を除く）

6-7 銀行口座

制度・公式情報 口座の情報が漏れた生命保険会社の件（下の実例）では、その会社が、詐欺に注意するよう呼びかけました。金融機関や警察などを装い、暗証番号や認証の情報を聞き出そうとするものです。「今回漏えいした情報のみで、直ちに預金が引き出されるものではございません」とも説明しています[56]。全国銀行協会も「銀行協会職員や銀行員が暗証番号を尋ねることは一切ない」としています[57]。

今日やること

出典の番号が付いていない手順は、本書の推奨です。

1. 取引している銀行に、キャッシュカードや公式サイトで確かめた番号で連絡します。口座の情報が漏れたことを伝え、取れる対策を聞きます。
2. ネットバンキングのパスワードを変え、使い回しをやめます。
3. 振込の上限額を、ふだん必要な額まで下げます。例: 銀行のアプリや会員サイトの「限度額」の画面（第4章）[58,59]。
4. ログインや送金を知らせる通知を有効にし、口座振替を含む入出金明細をこまめに確かめます[60]。
5. 銀行や証券会社がパスキー（6-5）などの強い認証の方式を用意していれば、切り替えます[58,61]。
6. 暗証番号や、ワンタイムパスワード（1回だけ使えるパスワード）などの認証の情報は、誰にも伝えません。

身に覚えのない送金に気づいたときは、下の「身に覚えのない送金に気づいたら」に進みます。

どう悪用されるか・実例

実際に起きた事例 生命保険会社の件では、契約者約440万人のうち約22万人分に、保険料を引き落とす口座の情報（金融機関名・支店・口座番号・名義など）が含まれていました（7月31日の調査結果）[62]。

上限・通知・強い認証で備える

制度・公式情報 金融庁は2026年4月16日、銀行・証券会社などや警察庁と連携した広報を始めました。その「ご自身でできる7つの対策」には、不審なリンクは開かない、パスワードは使いまわさない、などがあります。取引や振込の上限は「取引の実態に合わせて適切な金額を設定する」こと、金融機関から強力な認証方式が提供されている場合は積極的に利用すること、も入っています。金融機関は対策をしていますが、「完全に防ぐことはできません」としています[58]。

制度・公式情報 金融庁は、ネットバンキングの利用状況を知らせる通知の機能を有効にするよう呼びかけています。ログイン・パスワードの変更・送金などの不審な取引に注意するよう求め、「金融機関が、ID・パスワード等をSMS等で問い合わせることはありません」としています[60]。全国銀行協会も、振込などの限度額を「必要な範囲内でできるだけ低く設定すること」を勧めています[59]。

制度・公式情報 証券口座も同じです。日本証券業協会は2026年3月25日、ネット取引を使う人に、2つのことを求めました。パスキーによる認証などが提供されていれば速やかに切り替えることと、メールや SMS のリンクからログインしないことです。覚えのないログイン・取引・出金があれば、速やかに証券会社の窓口に確かめ、警察に相談するよう呼びかけています[61]。

身に覚えのない送金に気づいたら

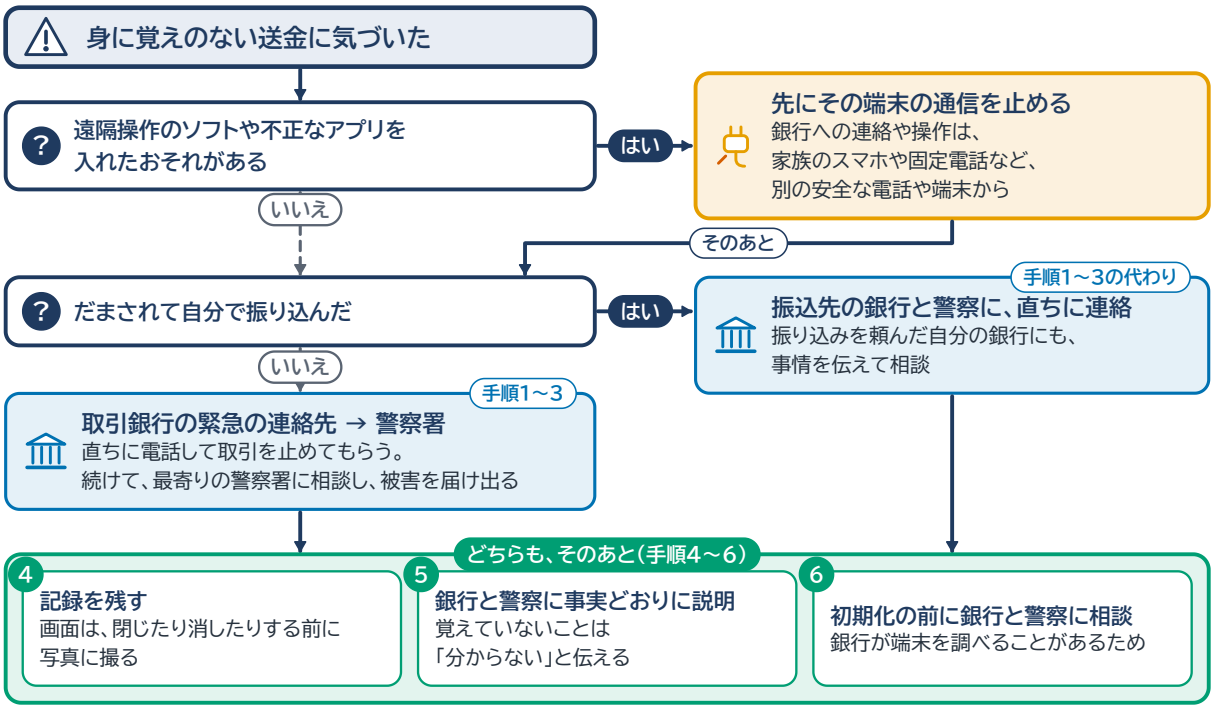


図6-11　身に覚えのない送金に気づいたら（先に確かめる2つ）

身に覚えのない送金に気づいたら

出典の番号が付いていない手順は、本書の推奨です。

先に確かめること:

- 遠隔操作のソフトや不正なアプリを入れたおそれがあるときは、先にその端末の通信を止めます。銀行への連絡や操作は、家族のスマホや固定電話など、別の安全な電話や端末からします（6-5 の「スマホに不正なアプリを入れてしまったとき」）。

- だまされて自分で振り込んでしまったときは、手順1～3の代わりに、振り込んだ先の口座がある銀行に連絡し、必ず警察にも届け出ます[63]。どちらにも直ちに連絡し、振り込みを頼んだ自分の銀行にも、事情を伝えて相談します（本書の推奨）。この場合の制度は第7章です。そのあとは、手順4～6と同じです。

1. 直ちに、取引銀行の緊急の連絡先に電話し、取引を止めてもらいます。番号は、キャッシュカードの裏面や公式サイトで確かめたものを使います。
2. だまされて自分で入力したり操作したりしたときも、まず銀行に連絡し、補償の対象になるかを確かめます（第7章）。
3. 続けて、最寄りの警察署に相談し、被害を届け出ます。迷うときは、警察相談専用電話（＃9110）に相談します。
4. 記録を残します。気づいた日時、送金の日時・金額・相手先、画面の写真（偽の警告画面や入れたアプリが分かるもの）、銀行・警察とのやりとり（日時・相手・内容）です。画面は、閉じたり消したりする前に写真に撮ります。メールの通知などの残し方は、第5章のステップ4と同じです。
5. 銀行と警察には、事実どおりに説明します。覚えていないことは「分からない」と伝えます。
6. パソコンやスマホは、初期化する前に銀行と警察に相談します。警察庁のサポート詐欺（偽の警告で、遠隔操作のソフトなどを入れさせる手口）の案内は、可能であれば初期化するよう求めていますが、銀行が端末を調べることがあるためです（本書の推奨）[64,65]。

制度・公式情報 警察庁は、フィッシングの被害にあったら、まずサービスを提供する会社に相談するよう案内しています。不正送金の被害は、金融機関が補償の制度や相談の窓口を設けている場合がある、としています。そのうえで、最寄りの警察署や、サイバー事案のオンライン受付の窓口に通報・相談するよう求めています[66]。全国銀行協会も、被害にあったら「警察、取引銀行へただちに連絡する」よう求めています[67]。

制度・公式情報 サポート詐欺は、ウイルスを見つけたという偽の警告で、遠隔操作のソフトなどを入れさせる手口です。警察庁は、その被害にあったときは、偽の警告画面や入れたソフトが分かる資料を持って、最寄りの警察署に通報・相談するよう案内しています[64]。ある大手銀行は、手口を調べるために、パソコンやスマホを預かる場合があるとしています[65]。

補償の条件の要点

制度・公式情報 全国銀行協会の申し合わせ（会員の銀行の間で決めた方針。2008年2月19日。個人の顧客が対象）では、ネットバンキングで預金が不正に払い戻されたときの補償の要件を、次の3つとしています[59,68]。

- 「金融機関への速やかな通知」
- 「金融機関への十分な説明」
- 「捜査当局への被害事実等の事情説明（真摯な協力）」

制度・公式情報 同じ申し合わせでは、銀行への通知が被害の発生日の30日後までなかった場合などは、「補償を行わない」とされています[68]。過失（注意を怠ったこと）があるときの扱いは、第7章で説明します。

これは業界の申し合わせの基準で、実際の扱いは各銀行の規定によります。30日を過ぎてから気づいても、自分で決めつけずに、すぐ銀行に連絡して事情を伝えます（本書の推奨）。

ただし、補償を求めるときは、この3つだけで済むとは限りません。銀行が調べるために、経緯を詳しく聞いたり、パソコンやスマホを預かったりすることがあります（上の「身に覚えのない送金に気づいたら」の、ある大手銀行の例）。

そこで、気づいたらすぐ銀行に連絡し、気づいた時点からの記録を残して、事実どおりに説明します。これが、補償を求めるときの備えになります。手順は、この節の「身に覚えのない送金に気づいたら」です。補償を受けられるかの判断

は、銀行の規定と個別の事情によります。迷うときは、全国銀行協会相談室などに相談します（本書の推奨）。

全額補償か個別対応かの基準、補償が減ったり、されなかったりする例、キャッシュカード・通帳・証券口座の場合、補償された割合の統計は、第7章の「口座が不正に使われたときの補償」で説明します。

相談先

- 取引している銀行・証券会社（キャッシュカードの裏面や公式サイトで確かめた番号）
- 被害にあったとき: 最寄りの警察署、警察相談専用電話（#9110）
- 全国銀行協会相談室 0570-017109 または 03-5252-3772（月～金曜日の9時～17時、祝日・銀行の休業日を除く）[69]

6-8 健康・医療の情報

2025～2026年に、健康・医療の情報そのものが悪用された被害（恐喝など）の国内の公表例は、見当たりません（2026年10月22日時点）。ただし、起きないという意味ではないので、次の備えをします。

今日やること

次の手順は本書の推奨です。

1. 通知の内容と、病院や会社の公式サイトで、自分が対象かを確かめます。
2. 病院や保険会社をかたる、電話や郵便でのお金の要求や、健康状態につけこむ勧誘に注意します。自分で調べた番号で確かめます。
3. 医療の情報は変えられません。お店などに体調を伝えるときは、必要なことにとどめます。
4. 病気や体調のことがネットに書き込まれたときの削除の相談は、6-9 の「写真や住所がネットに出たとき」と同じです。

漏えいの実例

実際に起きた事例 首都圏の大学病院では2026年2月、ランサムウェアの攻撃で患者約13万人の氏名・住所・電話番号・生年月日などが漏えいしました。カルテの情報の漏えいは、2月27日の第5報の時点で確認されていません[70]。リラクゼーションの店の予約の仕組みの件では、店が施術の申し送り（引き継ぎ）として書いた備考欄に、健康状態などが含まれていました[71]。

相談先

- 病院・会社の窓口（番号は公式サイトで確かめる）
- お金の要求や勧誘で困ったとき: 消費者ホットライン（188）
- 個人情報の扱いへの苦情・質問: 個人情報保護委員会「個人情報保護法相談ダイヤル」03-6457-9849（9時30分～17時30分、土日祝日・年末年始を除く）
- ネットに書き込まれたとき: 法務局（6-9 の相談先）

6-9 本人確認書類・顔写真

制度・公式情報 総務省によると、書類の偽造による携帯電話の「なりすまし契約」（他人の名前で結ぶ契約）が問題になっています。契約の本人確認では、IC チップ（6-6）の読み取りが原則必須になります（オンラインは2026年4月1日から、対面は2027年4月以降。第3章）[72]。

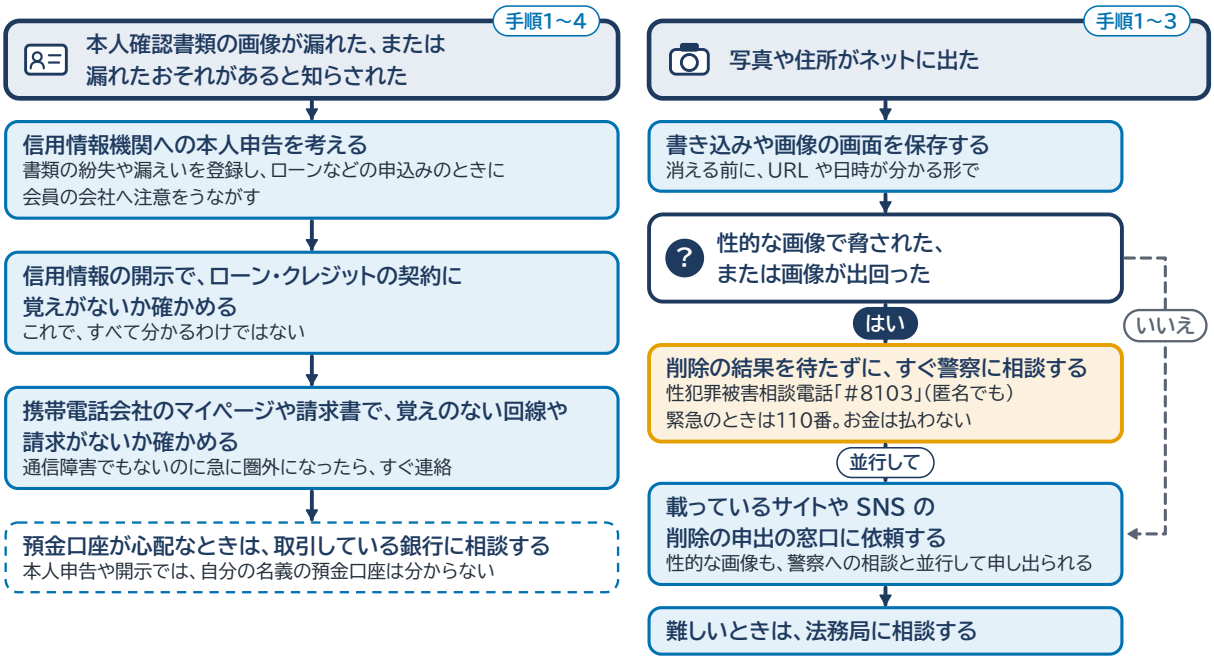


図6-12　本人確認書類の画像が漏れた・写真や住所がネットに出たとき

今日やること

出典の番号が付いていない手順は、本書の推奨です。

1. 本人確認書類の画像が漏れた、または漏れたおそれがあると知らされたら、信用情報機関(ローンやクレジットの契約の情報を集める機関)への本人申告を考えます。本人申告は、書類の紛失や漏えいを登録して、ローンなどの申込みのときに会員の会社へ注意をうながす手続きです。3つの機関とも、画像が漏れたときの申告を受け付けています。方法と費用は、すぐ下の表のとおりです[73,74]。
2. KSC は、本人申告は審査の判断を縛るものではなく、預金口座を開くときには照会されないとしています。そのため、ローン・クレジットと携帯電話の契約の確認(手順3・4)と組み合わせます。自分の名義の預金口座は、これらでは分かりません。口座が心配なときは、取引している銀行に相談します。迷うときは消費者ホットライン(188)に相談します(本書の推奨)。
3. しばらくは信用情報の開示(自分の信用情報を見る手続き)で、ローンやクレジットの申込み・契約に覚えがないか確かめます。これで、なりすまし契約がすべて分かるわけではありません。
4. 携帯電話会社のマイページや請求書で、覚えのない回線や請求がないか確かめます。通信障害でもないのにスマホが急に圏外になったら、すぐ携帯電話会社に連絡します。
5. 運転免許証の再交付は選択肢の一つですが、報道によると、変えられるのは顔写真と番号の末尾だけで、効果は限られるとされます。氏名・住所・生年月日は変わらず、漏れた情報が使えなくなるわけではありません。手続きと持ち物は、住所地の都道府県警察のページで確かめます[75,76]。
6. パスポートの画像が漏れたときも、手順1～4で備えます。画像の漏えいを理由に作り直す公式の手続きは、見当たりません(2026年10月23日時点)。
7. 運転免許証の2つの暗証番号と、マイナンバーカードの暗証番号・パスワードを覚えているか確かめます。控えを残すなら、免許証やカードと一緒に持ち歩きません。
8. 顔写真つきの本人確認書類を2種類持つことを考えます。パスポートを主な書類にしている人は、住所の書かれた書類(住民票の写し、公共料金の領収証など)も出せるようにしておきます(下の「確かめる手段を複数持つ」「本人確認に使える書類」)。
9. IC チップの読み取りを求められたら、相手が正規の事業者か、利用目的が示されているかを確かめます。

本人申告の申込み方と問い合わせ先は、次のとおりです。

機関	本人申告の申込み	問い合わせ
KSC（全国銀行個人信用情報センター）	インターネット（500円。マイナンバーカードが必要）か郵送（利用券2,403円）	0120-540-558（携帯電話などは 03-3214-5020）。月～金曜日の9時～12時と13時～17時[77]
CIC	インターネット（1,000円。8時～21時45分）か郵送	0570-666-414（オペレーターは平日の10時～16時、土日祝日・年末年始を除く）[73]
JICC（日本信用情報機構）	郵送（1種類1,111円）。アプリと QR コード付きの申込書は10月22日から一時停止中	0570-055-955（月～金曜日の10時～16時、祝日・年末年始を除く。通話料がかかる）[74,78]

どう悪用されるか・実例

漏えいによるなりすましの被害と確かめられた例は、公表されたものが見当たりません（2026年10月22日時点）。

実際に起きた事例 カーシェアの件では、運転免許証などの画像のデータのうち、外部へ送られた痕跡があったものは約146万件（1,464,800件）でした（10月23日の第5報）。画像は暗号化して保管されていました。第3報では、約160万件を「漏えいのおそれ」としていました[79]。設定の誤りで、本人確認書類の画像が外から見える状態になっていた例は、第2章で紹介しています。

制度・公式情報 KSC は、本人申告は悪用を防ぐ効果を保証しないとしています。CIC は、信用情報機関ごとに加盟している会社が違うため、必要に応じてほかの機関にも登録するよう勧めています[73]。

本物の書類は使えなくなるのか

偽造に使われても、本物の書類がそのまま使えなくなるわけではありません（本書の調べた範囲）。調べた範囲では、本物の書類が使えなくなるのは、紛失の届け出や再交付など、本人が手続きをしたときでした。ただし、なりすましの疑いがあるときは、事業者が別の書類での確認を求めることがあります（この節の「確かめる手段を複数持つ」）。

制度・公式情報 書類ごとの公式の案内は、次のとおりです（運転免許証の「画像が漏れたとき」の欄は報道による）[80,49,51,52]。

書類	本人の手続きで使えなくなるとき	画像が漏れたとき
パスポート	紛失・盗難の届出をしたとき（届け出たあとに見つかっても使えない）。切替の申請で返納したとき	画像の漏えいを理由に作り直す手続きの記載は見当たらない（2026年10月23日時点）
運転免許証	写真の変更などで再交付を受け、今の免許証を提出したとき	再交付は選択肢の一つ。変えられるのは顔写真と番号の末尾（再交付の回数を示す数字）だけで、効果は限られるとされる（報道による）[76]
マイナンバーカード	再交付で、なくしたカードを廃止したとき。一時利用停止をすると、スマホのマイナンバーカードも使えなくなる（見つかれば市区町村で解除できる）	番号を変えられるのは、不正に使われるおそれがあると認められる場合に限る（6-6）

制度・公式情報 外務省によると、パスポートをなくしたり盗まれたりしたときは、警察署に届けたうえで、都道府県の申請窓口に「紛失一般旅券等届出書」を出します。届け出るときは、運転免許証などの身元確認書類を見せます。「この届出により、紛失等したパスポートは失効します」とされ、紛失届はオンライン（マイナポータル）でもできます[80]。

制度・公式情報 新しいパスポートに、以前と同じ番号は付けられません。紛失・盗難のパスポートの番号は、ICPO（国際刑事警察機構）を通じて各国の出入国管理の当局に提供され、不正な使用を防ぐ手段になっている、と外務省は説

明しています。切替の申請ができるのは、残りの有効期間が1年未満になった人や、査証欄(ビザのページ)の余白が少なくなった人などです[80]。

制度・公式情報 運転免許証は、警視庁の案内では、今の写真を変更したい人も再交付を受けられ、そのときは今の免許証を提出します。なくした・盗まれた人は、住所・氏名・生年月日を確かめる書類(住民票の写し〔マイナンバーの記載がないもの〕、マイナンバーカード、資格確認書、社員証、学生証、パスポートなど)が要ります。マイナ免許証の人は、先に市区町村でマイナンバーカードの再交付を受けてから行きます(警察ではカードの再交付はできません)。東京の例なので、住所地の都道府県警察のページでも確かめます(本書の推奨)。



図6-13　免許証などの再交付は、公式の窓口で手続きする

確かめる手段を複数持つ

制度・公式情報 手続きの中には、別の書類を求めるものがあります。

- マイナンバーカードの再交付には、顔写真つきの書類1点か、照会書への回答書とほかの書類2点が要ります(6-6)[51]。
- 運転免許証をなくしたときの再交付には、住所・氏名・生年月日を確かめる書類が要ります。マイナ免許証の人は、市区町村と警察の両方で手続きをします。
- パスポートの紛失届では、運転免許証などの身元確認書類を見せます[80]。
- なりすましや偽りの疑いがあるとき、口座などの事業者は、契約のときに確かめた書類「以外の書類を少なくとも1つ」確かめることになっています[81]。
- スマホのマイナンバーカードは、実物のカードを止めると一緒に使えなくなります(6-6)[52]。

そこで本書は、顔写真つきの本人確認書類を2種類(例: 運転免許証とマイナンバーカード、またはパスポート)持っておくことを勧めます。1つをなくしたり止めたりしても、もう1つで再交付や本人確認の手続きを進めやすくなります。マイナ免許証にすると、カード1枚に機能が集まる点にも気をつけます。スマホのマイナンバーカードは実物のカードと一緒に止まるので、別の書類の代わりには数えません(本書の推奨)。

本人確認に使える書類

いまの決まり(2027年3月まで)で、窓口で使える書類の区分です。

制度・公式情報 犯罪収益移転防止法(犯罪で得たお金の受け渡しを防ぐための法律)では、口座開設などのときに本人確認を受けます。警察庁の「犯罪収益移転防止法の概要」(2026年8月7日時点)は、使える個人の書類を次のように分けています。有効期限のある書類は有効なもの、期限のない書類は、原則として6か月以内に作られたものに限ります[81]。

区分	主な書類	窓口での使い方(2027年3月まで)
顔写真つき	運転免許証、運転経歴証明書、マイナンバーカード、パスポート、在留カード(顔写真のあるもの)など	見せるだけで足りる(今の住所が書かれていない書類は、下のとおり別の書類も要る)
顔写真なし	資格確認書(健康保険証の代わりの書類)、国民年金手帳、母子健康手帳など	見せたうえで、書類の住所に届く転送不要郵便(ほかの住所へ転送されない郵便)を受け取るか、別の書類も見せる
住民票の写しなど	住民票の写し、戸籍の附票の写しなど	見せたうえで、転送不要郵便を受け取る

制度・公式情報 2020年2月4日以降に申請・発給されたパスポートには、住所を書く欄がありません(外務省)。住所の書かれていない書類のときは、ほかの本人確認書類か、公共料金の領収証書などの補完書類(6か月以内のもの)で、今の住所を確かめます[80,81]。警視庁の免許証の再交付でも、住所が書かれていないパスポートを持って行く人には、住所が確認できるほかの書類も持って行くよう案内しています。

2027年4月からは IC チップの読み取りへ



図6-14　本人確認は、カードの IC チップの読み取りへ

この小見出しで今日することは、暗証番号を覚えているか確かめることです(今日やることの手順7)。変更の中身は、次のとおりです。

制度・公式情報 警察庁は、2027年4月1日から、口座開設などで本人確認を受けるときに、IC チップの情報の読み取りなどが必須になると案内しています(2026年6月作成のチラシ)。対面では、運転免許証やマイナンバーカードなどを見せたうえで、チップの情報を読み取らせます。非対面では、チップの情報を送ります。「原則本人確認書類の画像や写しを用いることはできません」。金融機関などの判断で、先に始める場合もあります[82]。金融庁が金融機関に求めた対応は第3章で説明しています。携帯電話の契約(この節の冒頭)とは別の制度で、時期も一部違います(携帯電話のオンラインの契約は2026年4月から。対面は、どちらも2027年4月から)。

制度・公式情報 業界団体の案内では、2027年4月1日からは、顔写真や IC チップのない書類の一部が、原則として使えなくなるとされています[83]。自分の書類が当たるかは、手続きの前に窓口で確かめます（本書の推奨）。

制度・公式情報 運転免許証の IC チップの情報を読み取らせるには、2つの暗証番号の入力が必要です。警察庁は「設定した暗証番号を覚えておきましょう」と呼びかけ、忘れたときは警察署などで確かめられるとしています[82]。警視庁では、電話では答えず、本人が免許証を持って試験場・運転免許更新センター・都内の警察署に申し出たときだけ答えます。暗証番号は、次の免許証の交付まで変えられません[84]。マイナンバーカードの暗証番号は 6-6 のとおりです。

制度・公式情報 外務省は、IC チップを読み取る装置を持つ民間企業にパスポートを出すと、チップの情報を読み取ってためることは「理論上」できるとしています。空港の出入国の手続きのほかで、IC の読み取りを前提にパスポートを求められたときは「留意が必要」としています[80]。

写真や住所がネットに出たとき

本人確認書類の画像や顔写真、私的な写真、住所などがネットに出てしまったときの相談先です。本人は自分を責めず、打ち明けられた人は本人を責めずに、早く相談につなぎます（本書の推奨）。

写真や住所がネットに出たとき

出典の番号が付いていない手順は、本書の推奨です。

1. 書き込みや画像の画面は、消える前に、URL や日時が分かる形で保存します。
2. 性的な画像で脅されたり、画像が出回ったりしたら、削除の結果を待たずに、すぐ警察に相談します。性犯罪被害相談電話 #8103（ハートさん）は、匿名でも相談できます。緊急のときは110番です[85]。お金は払いません。漏れたパスワードを示して脅すメールへの対応は、第5章です（本書の推奨）。
3. 写真や住所の書き込みの削除は、載っているサイトや SNS の削除の申出の窓口に依頼します。性的な画像も、警察への相談と並行して申し出られます。難しいときは、法務局に相談します[86,87]。
4. 身の危険を感じるときは、6-3 の「住所が知られて不安なとき」も見ます。
5. 家族や友人から打ち明けられたら、責めずに受け止め、一緒に相談先に連絡します（子どもとの約束は第4章の「家族で決めておくこと」）。



警察官

性的な画像のことで不安にさせる言動があれば、まだ公表されていなくても、すぐ警察に相談してください。#8103（ハートさん）は、匿名でも相談できます[85]。

制度・公式情報 警察庁は、撮影された人の同意なく、性的な画像をネットの掲示板などに公表する被害が起きているとしています。一度出回ると世界中に広がり、完全に消すのは困難です。掲載されたら、プロバイダー（ネットの接続やサービスを提供する会社）や掲示板の業者に削除を依頼できます。警察庁の説明では、違法性が明らかな場合などは即時に削除され、判断できない場合は、掲載した人への照会を経て削除されることがあります。警察庁は、広がるのを防ぐため、できるだけ早く相談するよう求め、相手からの着信の履歴やメールなどは消さずに保存するよう呼びかけています[85]。

制度・公式情報 法務省によると、ネット上でプライバシーの侵害などを受けた人は、サイトの管理者などに、自分で削除を依頼できます。難しいときは、最寄りの法務局に相談できます。法務局は、削除依頼の方法を助言し、侵害にあたると認めた情報は、プロバイダーなどに削除を要請します[86]。2025年4月には、情報流通プラットフォーム対処法（SNS などでの権利の侵害への対応を定めた法律）が施行されました。指定された大規模な SNS などの事業者に、

削除の申出への対応を早めることなどを義務付けています。総務省のページに、各社の削除の申出の窓口の一覧があります[87]。

相談先

- パスポートの紛失・盗難: 警察署と、都道府県のパスポートの申請窓口[80]
- 運転免許証の再交付・暗証番号: 住所地の都道府県警察(運転免許センター・警察署など)[75]
- マイナンバーカード: 6-6 の窓口
- 性的な画像の被害・脅し: 性犯罪被害相談電話 #8103(ハートさん。かけた地域の都道府県警察につながる。匿名でもよい)。緊急のときは110番
- ネットに出た情報の削除の相談: 最寄りの法務局(みんなの人権110番 0570-003-110、平日8時30分～17時15分。ネットでは「インターネット人権相談受付窓口」から)。ほかの窓口は第7章
- 信用情報機関の本人申告: 上の「今日やること」のすぐ下の表

6-10 購買履歴・会員情報

実際に起きた事例 衣料品の通販の件では、顧客から「注文情報と一致する不審な返金案内メールを受け取った」と問い合わせがあり、不正アクセスの痕跡が見つかりました(10月3日公表。第3章)[88]。



詐欺師

注文の情報と一致する内容で、返金の案内のメールを送ります[88]。別の手口では、返金を口実に、コード決済のアプリでお金を送らせます[89]。

今日やること

次の手順は本書の推奨です。

1. 注文や予約の内容が正しく書かれた連絡でも、お金・カード番号・ログインを求めるものは疑います。自分で調べた公式の連絡先や、アプリの注文履歴で確かめます。
2. ポイントの残高と交換の履歴を確かめます(6-5の手順7)。
3. 使っていないサービスは、第4章の「渡す情報・残す情報を減らす」の手順2で退会します(終わっていない注文・返金やポイントの残り、有料の契約・自動更新の解約、ほかのサービスのログインや復旧に使っていないかを確かめ、記録を残し、消せる情報を消してから退会)。アドレス帳に残る家族・知人の送り先も消します。

どう悪用されるか・実例

実際に起きた事例 百貨店グループの共通会員 ID の件では、百貨店の予約サイトを通じた不正アクセスが公表されました(10月19日)。グループ共通の会員 ID のほぼすべての会員にあたる約126万件の、個人情報の一部が漏えいしたとしています。グループの通販サイトなどでも、10月17日に不正アクセスが確認されました。注文の履歴やアドレス帳(贈り物の送り先など)を含む情報の、漏えいの可能性を調査中です[90]。

予約サイトや決済が止まったとき

止まったとき・その前後に「予約の取り直し」「返金」「支払いのやり直し」の連絡が届いたら、次のようにします(本書の推奨)。

1. 届いたメールや SMS のリンク、書かれた電話番号は使いません。
2. 予約確認のメール、公式のアプリ、自分で調べた施設の電話番号で、予約と支払いの状態を確かめます。
3. 決済でエラーが出ても、すぐに払い直しません。カードの利用明細や予約確認のメールで、支払いが済んでいないかを先に確かめます。明細やメールに出ていなくても、支払いが済んでいることがあります。分からないときは、自分で調べた施設や予約サイトの公式の窓口に確かめてから払い直します。
4. 返金のために、送金や支払いの操作を求められたら、操作をやめます。
5. 予約番号と施設の電話番号は、予約したときに控えておきます。

制度・公式情報 予約サイトが止まっている間は、予約の確認・変更・取り消しもできないことがあります。じゃらんnetは、メンテナンスの間はサポートデスクに問い合わせても受け付けられないと案内しています[91]。

実際に起きた事例 実際に予約した施設の名前で、偽の連絡が届いた例もあります。京都のホテルの件（2026年5月公表）では、予約サイト経由の一部のお客さまに、偽のサイトへ誘うメッセージが届きました[92]。

制度・公式情報 Booking.com は、メールや電話などでカードの情報を求めることは「決してありません」としています。予約確認書の支払いの条件と違う銀行振込を頼むこともないとしています[93]。国民生活センターは、ふだん使う事業者を名乗るメールでもフィッシングを疑うよう勧めています。書かれた URL ではなく、登録済みの公式サイトや公式アプリから確かめます[94]。

制度・公式情報 返金のはずが、コード決済のアプリで逆にお金を送らされる相談もあります。国民生活センターは、「〇〇ペイで返金します」と言われたら詐欺を疑うよう呼びかけています（2024年7月）[89]。

困ったときは、下の相談先に相談します。

相談先

- 漏れたサービスの公式の窓口（自分で開いた公式サイト・公式アプリのお知らせに載っているもの。届いたメールや SMS に書かれた番号やリンクは使わない）
- 返金や契約のトラブル: 消費者ホットライン（188）
- 詐欺の被害にあったとき: 最寄りの警察署、警察相談専用電話（＃9110）[1]

個人編

第7章　救済と相談窓口



この章では、被害のあとに使える窓口と制度をまとめます。本書は法律の判断はしないので、自分の場合は窓口に相談してください。

会社の窓口・補填・お詫び

まず、自分で開いた会社の公式サイト・公式アプリのお知らせに載っている窓口に連絡し、自分が対象か、何が漏れたかを確かめます。届いた通知の中の番号やリンクは使いません（第5章）。受付時間は変わることがあるので、最新のお知らせを見ます（本書の推奨）。

実際に起きた事例 お金の被害を会社が補填する（埋め合わせる）とした例があります。アンケートサイトの件（2026年10月公表）では、運営会社が、本人の意思によらずギフトコードに交換されたポイントを、全額補填するとしています。交換は611件・計2,869,500円分でした（10月14日の第2報）[1]。

実際に起きた事例 漏えいそのものへのお詫びとして、金券などを送った例も過去にはあります。2014年に発覚した通信教育会社の件（顧客の情報の持ち出し）では、会社がお詫びとして500円分の金券などを送りました（のちの判決が触れています）[2]。

実際に起きた事例 カーシェアの件（2026年9月公表）では、会社が10月23日の第5報で、お見舞いとして3,000円相当の現金または金券を渡すと公表しました。対象は、暗号化して保管していた運転免許証などの画像のデータに、外部へ送られた痕跡が確認された人です。内容と渡し方は検討中で、決まったら対象の人に案内するとしています[3]。

実際に起きた事例 仮想のパソコンを貸すクラウドの件（2026年10月公表）では、会社が10月24日の第4報で、お見舞金を払うと公表しました。対象はこのサービスを利用しているすべての人で、金銭的な被害の有無にかかわらず一律5,000円です。不正アクセスによって本人の意思によらない取引が行われ、取引口座に損失（取引の差損と手数料など）が出た場合は、それも補償するとしています。市場の変動による損失や、得られたはずの利益は対象外で、取引所などから返金があれば、その分を差し引きます。案内は登録のメールアドレスに届くとし（お見舞金は10月30日ま

で、補償の申請は11月6日までに案内の予定)、補償の手続きで、パスワード(閲覧専用のものを除く)や暗証番号を尋ねることはない、としています[4]。

実際に起きた事例 同じ件で、会社は10月27日の第9報で、ランサムウェアの被害にあった利用者には、新しいパソコンを渡すとしました。被害を確かめたうえで、同等の性能のものを渡すという内容です[5]。同じ日の第10報では、攻撃者とみられる者が、情報と称するものを公開したのを確認したとしました。そこに自分の情報があると確認された人への、第4報とは別のお見舞金の検討を始めたとしています。検討を始めた段階で、まだ決まったものではありません(10月27日時点)[6]。

自分の情報が含まれているかを確かめるために、公開されたとされる情報を見に行くことはしません(6-5。本書の推奨)。



お見舞金や補償の案内が届きました。本物かどうか、分かりません。

相談者



お詫びや補償があるかは、会社によって違います。案内は会社の公式サイトのお知らせで確かめ、「お詫び」「返金」「お見舞金」をかたる連絡に注意しましょう(第5章。本書の推奨)。

専門家

損が出たときは、記録を残して(第5章のステップ4)、会社の窓口に補償を問い合わせます(本書の推奨)。カードの不正利用の補償は第6章 6-4 で、信用情報機関(ローンやクレジットの契約の情報を集める機関)への本人申告(書類の紛失や漏えいを登録して、会員の会社へ注意をうながす手続き)は 6-9 で説明します。銀行や証券の口座が不正に使われたときは、気づいたときの手順を第6章 6-7 に、補償の制度をこの章の「口座が不正に使われたときの補償」の節にまとめました。

自分の情報の開示・消去を求める制度

制度・公式情報 個人情報保護法は、本人が会社に次のことを請求できると定めています。対象は、会社が開示や利用の停止などをする権限を持つ個人データで、法律の言葉では「保有個人データ」といいます。委託などで複数の会社が関わるときは、どの会社が応じる権限を持つかは、契約などの実態で決まります[7]。

- **開示**(第33条): 会社が持っている自分の保有個人データを見せるよう求めることです。方法は、データ(電磁的記録)での提供、書面の交付、そのほか会社が定める方法のうち、本人が求めた方法です。その方法が難しいときは、会社はその旨を知らせて、書面で開示します。データがないときも、その旨を知らせます。手数料がかかることがあります。
- **第三者提供記録の開示**(第33条第5項): 会社が自分の個人データをほかの会社などの第三者に渡したとき・受け取ったときに、法律にもとづいて作る記録も、開示を請求できます。保有個人データとは別の対象です。
- **漏えいなどのときの利用の停止・消去**(第35条第5項): 次の3つのときに、利用の停止や消去、第三者への提供の停止を請求できます。①報告の対象になる漏えい(第5章の4つのどれか。おそれを含む)が自分の情報に起きた、②会社が使う必要がなくなった、③本人の権利や正当な利益が害されるおそれがある。
- **法律に反した扱いのときの利用の停止・消去**(第35条第1項・第3項): 法律の決まりに反して、同意なく目的の外で使われた、不適正に使われた、偽りなどの不正な手段で取られた、のどれかのときに請求できます。法律の決ま

りに反して同意なく第三者に渡されたときは、提供の停止を請求できます。法律には、同意が要らない場合(法令にもとづく場合など)や、委託のように第三者への提供に当たらない場合も定められています。

不正アクセスなどによる漏えいは、会社が自分の意思で渡す「提供」ではありません。そのため、漏れた先や漏れた経緯は、第三者提供記録では分からないと考えられます(資料からの本書の読み取り)。

制度・公式情報 個人情報保護委員会(個人情報の扱いを監督する国の機関)のガイドライン(法律の運用の手引き)は、③の例を挙げています。会社が安全管理の措置を十分にとっておらず、本人のデータが漏えいするおそれがある場合です。一方、料金の支払いを免れるためや、審査に必要な信用情報を消させるための請求は、認められない例とされています[7]。

制度・公式情報 ただし、会社が応じるのには限りがあります[7]。

- 消去などに応じるのは、本人の権利や利益を守るのに必要な限度です。多額の費用がかかるなど難しいときは、代わりの措置も認められています。代わりの措置は、本人の権利や利益が害されるおそれに対応し、その保護に役立つものでなければなりません。例として、重大な漏えいが起きても、契約が続いていて利用の停止などが難しいときに、再発防止策を講じることが挙がっています。
- 次のどれかに当たるときは、全部または一部を開示しないことができます。開示すると本人やほかの人の生命・身体・財産などを害するおそれがある、会社の業務に「著しい支障」がある、ほかの法令に違反する、の3つです。「著しい支障」は例外的なときに限られ、データの量が多いという理由だけでは、ふつうは当たりません。
- 応じたときも、応じないと決めたときも、会社は本人に遅滞なく知らせます。開示しないときは、理由の説明に努めることになっています。
- 応じる期間は、開示も利用の停止なども「遅滞なく」とだけ定められ、日数の定めはありません。
- 法律が手数料を取れると定めているのは、利用目的の通知を求められたときと、開示を請求されたときです。額は、実費を勘案して合理的な範囲で会社が決め、本人が知ることのできる状態に置きます。

制度・公式情報 会社は、請求の手続きと手数料の額、苦情の申出先などを、本人が知ることのできる状態に置くことになっています。請求は、会社が定めた受付の方法(申出先・書面の様式・本人確認の方法・手数料の払い方)に従います。会社は本人確認で、持っているデータに比べて必要以上に多くの情報を求めてはいけません。未成年者の法定代理人や、本人が委任した代理人も請求できます[7]。

制度・公式情報 会社が認定個人情報保護団体(個人情報保護委員会が認定した民間の団体)の対象事業者なら、その団体にも苦情を申し出られます。団体は、当事者の間で解決が難しい場合に、公正な立場から苦情の処理にあたります[8]。対象事業者なら、プライバシーポリシー(個人情報の扱い方を書いたページ)などに団体の名前と苦情の申出先も書かれています[7]。

求めるときは、次の順に進めます(本書の推奨)。

1. 会社の公式サイトを自分で開き、「プライバシーポリシー」で、窓口・手続き・手数料を確かめます。
2. 求めることは、一度で要点をまとめて書きます。利用の停止や消去を求めるときは、何が問題かを具体的に書きます。
3. 公式の窓口と様式で、日付の分かる方法で出し、控えを残します。届いたメールや SMS(携帯電話の番号あてに届く短いメッセージ)のリンクからは手続きしません。
4. 解決しないときは、この章の「相談窓口」の表にある個人情報保護法相談ダイヤルに相談します。会社が認定個人情報保護団体の対象事業者なら、その団体に申し出る方法もあります。

口座が不正に使われたときの補償

銀行や証券会社の口座からお金を不正に引き出されたときの補償は、引き出され方（被害の経路）で、よりどころの制度が違います。この節は制度の説明で、気づいたときの手順と記録の残し方は第6章 6-7 にあります。自分の場合に補償されるかは本書では判断しないので、取引している銀行や証券会社に確かめます（本書の推奨）。

被害の経路ごとの制度

制度・公式情報 主な経路と制度は次の表のとおりです。全国銀行協会は銀行の業界団体で、申し合わせは会員の銀行の間で決めた方針です。ネットバンキングは、ネットで振込などができる銀行のサービスです。

被害の経路	よりどころの制度	補償の考え方
キャッシュカードを偽造された・盗まれて、ATM で引き出された	預金者保護法（2005年の法律。対象は個人）[9]	法律で定めている（偽造と盗難で条文が別）
通帳を盗まれて払い戻された	全国銀行協会の申し合わせ（2008年）と、各銀行の預金規定[10,11]	参考例では、条件を満たせば補償。銀行が預金者の過失（注意を怠ったこと）を証明すると4分の3。重大な過失などは対象外（下の本文）
個人のネットバンキングで不正に払い戻された	全国銀行協会の申し合わせ（2008年）[10]	過失がなければ全額。過失があれば個別に対応
会社のネットバンキングで不正に払い戻された	全国銀行協会の考え方（2014年）[12]	補償するかは各銀行の判断（第8章 8-5）
だまされて自分で振り込んだ	振り込め詐欺救済法[13]	補償ではない。犯罪に使われた口座に残ったお金から支払われる
証券口座で、他人に勝手に売買された	日本証券業協会と証券会社10社の申し合わせ（2025年）[14]	一定の被害補償を行う方針。個別の事情に応じて対応

補償を受けるための条件

制度・公式情報 個人のネットバンキングについては、全国銀行協会の申し合わせ（2008年2月19日）があります。顧客自身の責任によらない被害は、銀行に過失がなくても補償するとしています。補償の要件は次の3つです[10]。

- 「金融機関への速やかな通知」
- 「金融機関への十分な説明」
- 「捜査当局への被害事実等の事情説明（真摯な協力）」

制度・公式情報 顧客に過失がなければ「全額補償」、過失や重大な過失（わざとと同じに見られるほど、注意を大きく怠ること）があれば「個別対応」です。個別対応では、被害にあった人の行動や、そのときの状況をふまえて判断するとされています。盗難通帳の「過失（重大な過失を除く）があれば75%」という基準は、ネットバンキングには当てはまりません[10]。

制度・公式情報 盗まれたキャッシュカードで ATM から引き出されたときは、預金者保護法が適用されます。対象は、預貯金の契約をしている個人です。補償（法律の言葉では「補てん」）を受けるには、次のことなどが要件です[9]。

- 盗まれたと気づいたら、速やかに金融機関に知らせる
- 金融機関の求めに応じて、遅滞なく十分な説明をする
- 警察などの捜査機関に届け出たことを、金融機関に申し出る

制度・公式情報 補償の対象は、原則として、知らせた日の30日前の日から後の払い戻しです。盗まれたことを知りえなかったなど、知らせられなかったやむを得ない特別の事情があれば、その日数だけ前に延びます。その事情は預貯金者が証明します。盗まれた日(分からないときは、最初に不正に引き出された日)から2年を過ぎて知らせたときは、適用されません。法律の定めより預貯金者に不利な特約(契約に付けた特別の取り決め)は、無効とされています[9]。

制度・公式情報 偽造カードによる払い戻しは、同じ法律の別の条文(第4条)が扱いを定めています。上の3つの要件と、30日・2年の期間は、盗難カードについての定めです[9]。

制度・公式情報 盗まれた通帳で払い戻されたときの条件は、全国銀行協会の預金規定の参考例(2008年)に示されています。次の3つです[11]。

- 盗難に気づいたら、すみやかに銀行に知らせる
- 銀行の調査に、十分に説明する
- 警察署に被害届を出したことなど、盗難にあったと推測できる事実を確認できるものを示す

制度・公式情報 対象は、原則として、知らせた日の30日前の日から後の払い戻しです。知らせられなかったやむを得ない事情があることを預金者が証明したときは、その事情が続いた期間だけ延びます。盗まれた日(分からないときは、最初に不正に払い戻された日)から2年を過ぎて知らせたときは、対象外です。銀行が、自らの善意・無過失と、預金者の過失(重大な過失を除く)の両方を証明した場合は、4分の3になります。補てんしないのは、銀行が自らの善意・無過失と、次のどれかを証明した場合などです。預金者の重大な過失、親族などによる払い戻し、重要な事項についてのうその説明です[11]。

参考例なので、通帳の場合の実際の条件は、取引している銀行の預金規定で確かめます(本書の推奨)。

ネットバンキング・盗まれたキャッシュカード・盗まれた通帳のどれでも、すぐ知らせる、十分に説明する、警察に届け出る(説明する)ことが条件に入っています。偽造カードの場合も、気づいたらすぐ銀行に知らせ、警察に相談します。期限を過ぎたと思っても、自分で決めつけず、まず銀行に連絡します。通帳の記帳やネットの明細、取引の通知をこまめに見ておくと、早く気づけます(通知の設定は第6章 6-7。本書の推奨)。

補償が減ったり、されなかったりする例

制度・公式情報 全国銀行協会の申し合わせ(2008年)では、盗難通帳とネットバンキングのどちらでも、次の場合は補償を行わないとしています[10]。

- 被害が起きた日から30日後までに、銀行に知らせなかった
- 親族などによる払い戻しだった
- うその説明をした
- 戦争・暴動など、社会の混乱に乗じた払い戻しだった

盗難通帳の知らせる期間の扱い(やむを得ない事情による延長、2年の上限)は、上の預金規定の参考例のとおりです。実際の条件は、取引している銀行の規定で確かめます(本書の推奨)。

制度・公式情報 全国銀行協会は、会員の銀行の一部にアンケートを行いました(2016年6月14日公表)。各銀行の実務で、ネットバンキングの補償を減らすか、しない扱いとされる例が挙がっています。協会の基準ではなく、銀行の実務を調べた結果です[15]。

- 銀行が何度も個別に注意していた手口にだまされて、ID・パスワードなどを入力した
- 警察や銀行などを名乗る者に、ID・パスワードなどを安易に答えた。正当な理由なく他人に教えた
- ID・パスワードなどを手帳に書いたり携帯電話に保存したりしていて、不注意で盗まれた

- こうしたことや、身に覚えのない残高の変化、ウイルス感染に気づいていたのに、銀行に知らせない間に被害にあった

制度・公式情報 キャッシュカードでは、全国銀行協会の申し合わせ（2005年）が、「重大な過失」となりうる典型例を挙げています。本人が他人に暗証を知らせた場合と、暗証をカードに書いていた場合です。他人にカードを渡した場合も入ります（病気の人が介護ヘルパーに渡したなど、やむをえない事情がある場合を除く）。「過失」となりうる例には、暗証のメモをカードと一緒に持っていた場合があります。銀行から何度も個別に働きかけがあったのに、生年月日などを暗証にして、それが分かる免許証などと一緒にカードを持っていた場合も入ります[16]。

制度・公式情報 1つの銀行の例として、ある大手銀行の個人向けのネットバンキングの案内を挙げます。ID・パスワードなどを盗まれて不正に使われた損害は、利用規定にもとづいて補償するとしています。一方で、お客さま自身が操作したことなどによって生じた損害は、補償の対象外と明記しています[17]。

制度・公式情報 同行は、次のような場合は支払われないことがあるとしています。被害の翌日から30日以内に届け出なかった、警察に相談していない、速やかな通知・十分な説明・調査への協力がない、などです。手口を調べるため、パソコンやスマホを預かる場合もあるとしています。無過失と認められない場合でも、同行の判断で一部を支払うことがあるとも書いています[17]。

次のような場合は、補償が減ったり、されなかったりすることがあります（全国銀行協会・銀行の公表）。たとえば、フィッシング（本物そっくりの偽のメールやサイトで、情報をだまし取る手口）のサイトに ID・パスワードを入力した場合です。電話で教えた場合や、自分で操作して送金した場合もあります。ただし、「必ず補償されない」とは限りません。まず取引銀行に連絡し、補償の対象になるかを銀行に確かめます。端末は、初期化する前に銀行と警察に相談します（第6章 6-7。本書の推奨）。

遠隔操作（離れた所から端末を操作すること）のソフトを入れられて、本人がログインした状態で送金された場合はどうでしょうか。この場合の補償の扱いを具体的に書いた公式の説明は、本書の調査では見つかりませんでした（2026年10月23日時点）。

「証明できないと補償されない」のか

「利用者が不正を証明できなければ補償しない」という公式の文言は、本書の調査では見つかりませんでした（2026年10月23日時点）。調べたのは、全国銀行協会・金融庁・警察庁・法律の条文・1つの大手銀行・日本証券業協会・楽天証券の文書です。ほかの銀行の規定は確かめていません。ネットバンキングの申し合わせの文書にも、誰が何を証明するかの定めは見当たりませんでした。

制度・公式情報 公式の文書に書かれているのは、上の条件（速やかな通知・十分な説明・警察への届け出や説明）と、うその説明は補償しない理由になることです[10,11]。

制度・公式情報 預金者保護法は、補償を減らしたり、しなかったりする場合を、「金融機関が…証明した場合」と書いています。金融機関が次の2つを証明した場合は、補償は4分の3です。自らの善意・無過失（不正と知らず、注意も怠っていなかったこと）と、預貯金者の過失（重大な過失を除く）です。補償しなくてよいとされるのは、金融機関が、自らの善意・無過失に加えて、次のどれかを証明した場合です。預貯金者の重大な過失、親族などによる払い戻し、重要な事項についてのうその説明です。戦争・暴動などの混乱に乗じた盗難だと証明した場合も、補償しなくてよいとされています[9]。

制度・公式情報 同じ法律は、金融機関が払い戻しの状況をビデオテープや写真などに記録して、保存するものとしています。預貯金者から事実の確認に必要な資料の提供などを求められたら、誠実に協力するものともしています。預貯金者も、金融機関の求める情報の提供などに、誠実に協力するものとされています[9]。

制度・公式情報 金融庁の監督指針（銀行を監督するときの手引き。2026年10月版）にも、同じ趣旨の着眼点があります。銀行が不正な払い戻しの記録を適切に保存し、資料の提供などを求められたら誠実に協力することです[18]。

気づいた時点からの記録を残し、事実どおりに説明します。分からないことは「分からない」と伝えます。銀行には、ログインや送金の日時などの取引の記録を確かめてもらうよう頼みます（残す記録は第6章 6-7。本書の推奨）。

補償の割合（全国銀行協会の統計）

実際に起きた事例 全国銀行協会のアンケート（2026年9月29日公表、6月末時点）によると、個人の補償率は次のとおりです。補償率は、銀行が対応の方針を決めた件のうち、補償した件の割合です。件数の割合で、被害額の何割が戻ったかを示す数字ではありません。補償した件に、一部だけ補償した件が入るかの説明は、資料にはありません（2026年10月23日時点）[19]。

期間	ネットバンキングの不正な払い戻し	盗難キャッシュカード
2023年度	94.9%	85.1%
2024年度	91.9%	79.2%
2025年度	69.6%（877件のうち610件）	85.3%（502件のうち428件）
2026年4～6月	65.5%（87件のうち57件）	86.0%（43件のうち37件）

- 補償率は、調査に時間がかかるため、修正される可能性があります。2026年4～6月は暫定の値です。
- 警察官・銀行員・銀行協会の職員などを名乗る者に、キャッシュカードをだまし取られたり盗まれたりした場合があります。この場合の払い戻しは、盗難キャッシュカードの統計に入っていません。
- 統計は個人だけで、会社（法人）の補償率はありません。2026年4～6月のネットバンキングの被害は、個人190件・4億3,300万円、法人48件・14億5,300万円でした。

法律や申し合わせに補償の仕組みがあっても、補償されない例はあります。補償されなかった理由の内訳や、2025年度に補償率が下がった理由の説明は、本書の調査では見つかりませんでした（2026年10月23日時点）。補償をあてにしすぎず、被害を小さくする備えもしておきます。振込の上限額を下げる、取引の通知を有効にする、などです（第6章 6-7。本書の推奨）。

だまされて自分で振り込んだとき

制度・公式情報 だまされて自分で振り込んだときは、上の補償とは別の制度になります。全国銀行協会は、振り込め詐欺などの被害の連絡先として、振込先の銀行の一覧を載せています。そこでは、振り込みを頼んだ銀行ではなく、「振り込んだ先の口座がある銀行」に連絡するよう案内し、必ず警察にも被害を届け出るよう求めています[13]。

制度・公式情報 振り込め詐欺救済法は、犯罪に使われた口座に残っているお金を、被害者に支払う手続きを定めています。口座の残高が1,000円未満のときは対象になりません。残高が被害の総額より少なければ、被害額に応じて分けられます。全国銀行協会は、支払いの手続きまでに少なくとも90日以上かかるとしています[13]。

制度・公式情報 SNS 型投資詐欺やロマンス詐欺は、SNS などで知り合った相手に、投資や恋愛の話でお金をだまし取られる詐欺です。金融庁は、これらも口座への振り込みで被害にあった場合は、この法律の対象になるとしています。「犯人が預金口座等からお金を引き出してしまうと支払は受けられません」とし、支払いまでは少なくとも半年以上かかるのが一般的だとしています[20]。

制度・公式情報 申請の期間は、支払いの手続きの公告（広く知らせること）の翌日から30日以上あり、期間内に申請しないと受けられません。全額が支払われない場合や、支払われない場合もあります。金融庁によると、申請書は振込先の金融機関に出しますが、振り込みをした金融機関から出すこともできます[20]。

だまされたと気づいたら、直ちに振込先の銀行と警察に連絡します。振り込みを頼んだ自分の銀行にも、事情を伝えて相談します。振込の明細や控え、相手とのやりとり(メッセージや電話の日時)を残しておきます(本書の推奨)。

証券口座の補償

制度・公式情報 日本証券業協会(証券会社の業界団体)と大手・ネット証券の10社は2025年5月2日、証券口座の不正な取引の被害について申し合わせました。フィッシング詐欺などで不正にログインされ、他人が顧客の資産で株などの有価証券を売買した被害が対象です。「各社の約款等の定めに関わらず、一定の被害補償を行う方針」とし、2025年1月以降の被害を対象にしています[14]。

制度・公式情報 補償は、個別の事情に応じて対応するとしています。そのときは、ID やパスワードなどの管理を含めた顧客の行動や状況と、証券会社の注意喚起などの対策をふまえるとしています。10社は、SMBC日興証券、SBI証券、大和証券、野村證券、松井証券、マネックス証券、みずほ証券、三菱UFJ eスマート証券、三菱UFJモルガン・スタンレー証券、楽天証券です[14]。補償の割合の公式の数値は、本書の調査では見つかりませんでした(2026年10月23日時点)。

制度・公式情報 日本証券業協会のガイドライン(2025年10月15日改正)は、証券会社に、顧客から申告があったらすぐに取引・出金を止めることを求めています。被害補償を含めて、被害の回復に向けて「誠実かつ迅速に対応する」ことも求めています[21]。

制度・公式情報 楽天証券は、不正が疑われる取引の対象者には会社から連絡するとしたうえで、「不正取引の補償を騙る詐欺の手口も発生しております」と注意しています[22]。

身に覚えのない取引の報告書や通知が届いたら、すぐに取引している証券会社に申し出て、警察にも相談します。「補償します」という連絡が来ても、メールや SMS のリンクは開きません。公式アプリか、自分で登録しておいた公式サイトで確かめます(本書の推奨)。

口座の補償で覚えておくこと

1. 不正な払い戻しに気づいたら、直ちに取引銀行(証券口座なら証券会社)に連絡し、続けて警察に相談します。夜間・休日の緊急の連絡先も、ふだんから控えておきます。手順は第6章 6-7 です(本書の推奨)。
2. 補償されるかは自分で決めつけず、銀行に確かめます。だまされて入力した・教えた場合も同じです(本書の推奨)。
3. 説明は事実どおりにします。分からないことは「分からない」と伝えます(本書の推奨)。
4. だまされて振り込んだときは、直ちに振込先の銀行と警察に連絡し、振り込みを頼んだ自分の銀行にも相談します(本書の推奨)。
5. 銀行と話がつかないときの相談先(全国銀行協会相談室など)は、付録C にあります(本書の推奨)。

賠償と裁判の例

大規模なサイバー攻撃による漏えいで、2024～2026年に確定した判決は、本書の調査では見つかりませんでした(2026年10月22日時点)。紹介するのは、内部の持ち出しによる通信教育会社の件の判決です。支払いが命じられた額は、1人2,000円や3,300円でした。

実際に起きた事例 通信教育会社の顧客の情報が、委託先のさらに委託先の元従業員に持ち出された事件(2014年に発覚)です。最高裁判所は2017年10月23日、子どもの氏名・住所・電話番号なども「プライバシーに係る情報として法的保護の対象」だとし、漏えいでプライバシーが侵害されたとしました。そのうえで、この会社の過失の有無と、精神的な損害の有無・程度を調べ直させるため、大阪高裁に差し戻しました[23]。

実際に起きた事例 別の訴訟で東京高等裁判所は2019年6月27日、訴えた側（原告）の3人に各2,000円を支払うよう、通信教育会社に命じました（請求は1人5万～10万円）[2]。

実際に起きた事例 東京地裁でも、別々の訴訟で次の判決があったと報じられています[24]。

- 2018年12月27日: 委託先の関連会社に、1人3,300円の支払いを命じた（通信教育会社への請求は退けた）
- 2023年2月27日: 漏えいが確認された原告に、1人3,300円の支払いを命じた
- 2024年3月25日: 3,338人に、各3,300円の支払いを命じた

どの判決も、確定したかは確かめられていません。会社からの通知は、自分の情報が対象になったことを示す記録にもなるので、とっておきます（第5章のステップ4。本書の推奨）。

実際に起きた事例 カーシェアの件では、損害賠償を求める人の参加の登録を、弁護士が9月30日から受け付けました[25]。この弁護士は10月26日に会見を開き、東京地裁に訴訟を起こす方針を発表しました[26,27]。報道によると、運営会社と親会社などを相手に、本人確認書類の画像が漏れた人は5万円、ほかの情報の人は3万円を求める方針です。信用情報機関への申告や免許証の再交付をした人は、かかった費用を上乗せするとしています。求めるのは精神的な苦痛への慰謝料で、なりすましによるお金の被害は、この訴訟では扱わない方針と報じられています[28]。「年内には提訴したい」として、これから委任の手続きを進めるとしています[26]。専用サイトの登録は10万人を超えたと報じられていますが、登録した人の数で、原告の数ではありません。2026年10月27日時点で、提訴はまだです。

ほかの2026年の漏えいで、集団訴訟の動きを伝える報道は、本書の調べた範囲では見つかっていません（10月27日時点）。



図7-1　訴訟や補償の誘いは、届いた番号ではなく自分で調べて確かめる

上の判決の額や、訴訟で求める額を、ほかの漏えいの補償の目安にはしないでください。本書は、訴訟への参加を勧めるものでも、止めるものでもありません。参加を考えるときは、参加の費用・着手金（依頼するときに払うお金）・成功報酬（結果に応じて払うお金）と、委任の手続きを確かめます。確かめるのは、届いた連絡の番号やリンクではなく、自分で調べた弁護士の事務所の連絡先です（本書の推奨）。賠償を求めたいときや、訴訟への参加に誘われたときなど、法律の判断が要るときは、弁護士会か法テラス（日本司法支援センター。法制度や相談先を案内する公的な機関）に相談します（本書の推奨）。

消費者団体が代わりに訴える制度

制度・公式情報 消費者団体訴訟制度は、国が認めた消費者団体が、消費者に代わって事業者に訴訟などをする制度です。差止め（やめさせること）を求める適格消費者団体が全国に27、被害の回復を求める特定適格消費者団体が4あります（2026年8月末現在）。2023年10月からは、被害の回復の対象に慰謝料（心の苦痛への賠償）が加わりまし

た。ただし、慰謝料の額を算定する基礎となる主な事実関係が、多くの消費者に共通していることが前提です。そのうえで、財産的な損害と合わせて請求する場合か、事業者の故意による場合に限られます[29]。

漏えいのように慰謝料が中心になる被害が対象になるかは、この条件しだいです（資料からの本書の読み取り）。個人情報保護法には、団体が差止めや被害の回復を求める制度はありません（次の節の改正法）。団体を名乗る連絡が来たときの確かめ方は、次の囲みのとおりです。

「取り戻せる」「代わりに訴える」に注意

制度・公式情報 国民生活センターは、同センターをかたる電話などに注意を呼びかけています（2026年10月20日更新。「削除してあげる」という電話への対応は第5章）[30]。消費者庁も、職員を名乗って個人情報を聞き出そうとする電話に注意を呼びかけ、こうした電話で個人情報を聞くことはないと説明しています（2026年1月9日）[31]。消費者ホットラインのページの冒頭にも、国民生活センターと消費者庁をかたる偽ハガキへの注意が載っています。

制度・公式情報 国民生活センターは、相談したことのない人に、同センターが連絡をとることは「絶対にありません」とし、例に「訴訟で〇〇するように」という連絡を挙げています[30]。仮想のパソコンを貸すクラウドの件の会社も、「被害金を取り戻す」などとして費用を求める連絡には応じないよう呼びかけています[32]。

制度・公式情報 消費者庁は、適格消費者団体などの名をかたる団体にも注意を呼びかけています[29]。

「代わりに訴える」「登録料を払えば補償金が出る」などの連絡では、書かれた番号やリンクは使いません。消費者団体を名乗るなら国が認めた団体の一覧（消費者庁）で名前を、弁護士なら事務所の連絡先を自分で調べて確かめます。名前が合うだけでは本物とは限らないので、迷ったら 188 に相談します（本書の推奨）。

改正個人情報保護法

制度・公式情報 改正個人情報保護法は2026年7月17日に公布（国が法律を広く知らせること）されました（成立は7月10日）。施行（実際に始まること）は原則として公布から2年以内（本書の計算で遅くとも2028年7月まで）で、2026年10月22日時点では施行前です。個人に関わる主な点は次のとおりです[33]。

- **通知**: 「本人の権利利益の保護に欠けるおそれが少ない場合」に、通知の代わりに公表などで対応できるようになります。想定されているのは、社内の ID など、それだけではほぼ意味を持たない情報だけが漏れた場合などです。範囲は今後、規則で決まります。
- **課徴金**（違反で得た利益などに相当する額を国に納めさせる仕組み）: 新しく入りますが、漏えいが起きたことだけでは対象になりません。
- **団体の制度**: 団体が差止めや被害の回復を求める制度は入りませんでした。衆参両院の附帯決議（国会が法律に添えた要望）が、導入の検討を続けるよう求めています。

課徴金は国に納めるもので、被害者に支払われるお金ではありません（資料からの本書の読み取り）。通知が来ない場合への備えは第5章、見通しは第9章で述べます。

相談窓口



図7-2　一人で抱えず、公的な窓口に相談する

相談先は困りごとで使い分けます。カードや口座の不正な利用は、まずカード会社や銀行に連絡します。だまされて振り込んだときは、振込先の銀行と警察に連絡し、振り込みを頼んだ銀行にも相談します（本書の推奨）。表は個人向けの窓口で（番号などは2026年10月22～23日時点。かける前に確かめます）、すべての窓口は付録Cにあります。

困りごと	窓口	電話・受付
契約・請求・勧誘のトラブル	消費者ホットライン	188（近くの消費生活センターなどへ）
まだ被害はないが不安	警察相談専用電話	＃9110（受付時間は都道府県で異なる）
詐欺・なりすましの被害	警察署、警察庁のオンライン受付	被害届は最寄りの警察署へ
会社や役所などの個人情報の扱いへの苦情・疑問	個人情報保護委員会「個人情報保護法相談ダイヤル」	03-6457-9849（9時30分～17時30分、土日祝日・年末年始を除く）
パスワードや端末の相談	IPA 情報セキュリティ安心相談窓口	03-5978-7509（10時～17時、土日祝日・年末年始を除く）
法律の相談先や制度を知りたい	法テラス・サポートダイヤル[34]	0570-078374（IP 電話は 03-6745-5600。平日9時～21時、土曜日9時～17時。祝日・年末年始を除く）
弁護士に相談したい	日弁連「ひまわりお悩み110番」[35]	0570-783-110（近くの弁護士会の法律相談センターで面談を予約）
身の危険を感じる	最寄りの警察署	緊急は110番（身を守る制度は第6章 6-3）
性的な画像の被害・脅し	性犯罪被害相談電話	＃8103（都道府県警察の窓口へ。匿名でもよい）
ネット上の人権侵害	法務省「みんなの人権110番」	0570-003-110（平日8時30分～17時15分。最寄りの法務局へ）
削除の方法を相談したい	違法・有害情報相談センター[36]	ウェブのフォームからだけ
国の行政機関への苦情	総務省「行政苦情110番」	0570-090110（平日9時～16時45分）

- 188 の相談は無料ですが、窓口につながると通話料がかかります。緊急の通報は110番です。
- 相談ダイヤルでは、個人情報保護委員会（個人情報の扱いを監督する国の機関）が間に入る「あっせん」もあります。使えるのは、会社に苦情を申し出ても解決しないときなどです。お金の賠償や謝罪を求めるものは対象外で、

委員会から会社に、相談した人の氏名と連絡先を伝えることへの同意なども要ります。役所など（国や自治体の機関）への苦情は、あっせんの対象外です（相談は受けます）。

- 法テラスのサポートダイヤルは、法制度や相談の窓口を案内するところで、個別の法律相談はしません（利用料は0円、通話料はかかる）。犯罪の被害にあった人には、別に「犯罪被害者支援ダイヤル」（0120-079714）があります。受付時間は、法テラスの公式サイトで確かめてください。
- 法テラスには、収入と資産が一定以下の人への無料の法律相談もあります。1回30分、同じ問題について3回まで無料で、原則として予約が要ります。
- ひまわりお悩み110番は、日弁連（日本弁護士連合会）の面談の予約の窓口です。通話料がかかり、050 の IP 電話（回線による）からはつながりません。
- 弁護士会の法律相談センターの相談は、おおむね30分です。相談料は地域や内容で異なり、5,500円前後が目安とされています（日弁連）。無料になる全国共通の条件は、本書の調査では見つかりませんでした（地域・分野で異なります）。住んでいる地域の弁護士会のお知らせで、無料や割引の相談がないかを確かめます。費用が心配なら、先に法テラスの無料法律相談の条件を確かめます（本書の推奨）。

実際に起きた事例 東京の三つの弁護士会などのサイトは10月22日付の告知で休止し、全国組織のサイトも見られない状態になっていました。10月23日には、どちらも見られるようになりました（全国組織は同日、復旧と公表）。ただし、日弁連のネット予約「ひまわり相談ネット」は、10月23日16時の時点でも止まっています[35]。ネットで予約できないときは電話で予約します（本書の推奨）。

身の安全と、ネット上の情報の削除の窓口

手順は第6章 6-3・6-9 に、「消してあげる」と持ちかける連絡への対応は第5章にあります。

制度・公式情報 性犯罪被害相談電話は、全国共通の番号「＃8103（ハートさん）」にかけると、その地域の都道府県警察の窓口につながります。警察庁は「性別・年齢にかかわらず相談できます」とし、匿名でもよく、秘密は守るとしています。IP 電話ではつながらない場合があり、その際は都道府県ごとの番号（警察庁のページに一覧）にかけます。

制度・公式情報 法務省によると、法務局は、ネット上の名誉毀損（社会的な評価を下げること）やプライバシーの侵害について、削除依頼の方法を助言し、侵害にあたると認めた情報はプロバイダー（ネットの接続やサービスを提供する会社）などに削除を要請します。法務省のページには、依頼書の見本や手引きもあります[37]。法務局の電話の窓口は「みんなの人権110番」（0570-003-110、平日8時30分～17時15分）で、かけた場所の最寄りの法務局につながります。2025年10月1日に「女性の人権ホットライン」はこのダイヤルに統合され、1番で女性の人権の相談ができます。一部の IP 電話からは使えません。ネットの「インターネット人権相談受付窓口」のフォームからも相談できます。

制度・公式情報 総務省の支援事業の「違法・有害情報相談センター」は、ネット上の書き込みなどについて、サイトの管理者などへの削除依頼の方法の相談を受けています。相談はウェブのフォームからだけ受け付けています[36]。

削除の相談は、持ちかけてくる相手ではなく、こうした公的な窓口にします（本書の推奨）。

役所・学校・病院から漏れたときの窓口

通知を出した機関の確かめ方と相談の順は、第5章の「役所・学校・病院から届いたとき」にあります。自治体や公立の学校・病院の対応は、個人情報保護法相談ダイヤル（番号は上の表）にも相談できます。

制度・公式情報 総務省の「行政苦情110番」（0570-090110、平日9時～16時45分）は、行政相談（担当の機関とは別の立場で、行政への苦情や要望を受ける仕組み）の窓口です。「どこに相談したらよいか分からない」といった相談も受け、窓口の案内や、関係する機関への働きかけをします。通話料がかかり、一部の IP 電話からは使えません。メールやオンラインでも相談できます。

小さな会社編

第8章　小さな会社の担当者へ



IT の専任者がいない会社・お店の担当者に向けて、漏えいが起きたときに「誰に・いつまでに・何を」するかと、ふだんの対策をまとめます。

この章の使い方

- **いま漏えい（おそれを含む）が起きた:** 8-2 の「まず、すぐにすること」から始めます。相談先の表は、そのすぐあとにあります。
- **取引先・委託先から「漏れたおそれがある」と連絡が来た:** 8-3
- **ふだんの対策を始めたい:** 章末の「まず今週やること」「今月やること」から始めます。くわしくは各項目に示した節（主に 8-4）
- **送金の指示や、銀行を名乗る電話が来た／覚えのない送金に気づいた:** 8-5
- **予約・レジなどのシステムが止まった:** 8-6
- **公的な支援や、取引先から求められる評価を知りたい:** 8-7

8-1 小さな会社でも起きる

実際に起きた事例 2026年上半期に警察庁に報告されたランサムウェア（データを暗号化して身代金を求める不正なプログラム）の被害123件のうち、約6割は中小企業でした。警察庁のアンケートで、調査・復旧の費用の総額を答えた35組織のうち、1,000万円以上かかったのは21組織（6割）でした[1]。個人情報保護委員会（個人情報の扱いを監督する国の機関）が事業者から直接受け付けた報告（2025年度）で多いのは、書類の誤交付（別の人に渡すこと）や送り先の間違いです[2]（第2章）。

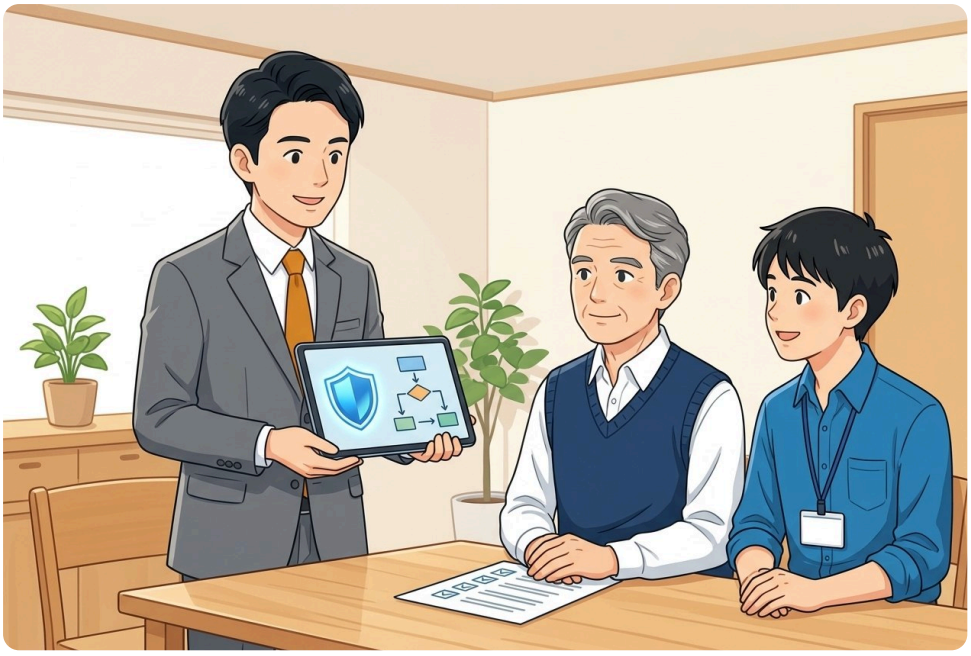


図8-1　漏えいに備えて、社長・担当者・相談先で手順を決めておく

まず、書類やメールの宛先の確かめ方を決め、8-4 の対策から始めます。経営者をよそおって送金させる詐欺には、8-5 の手順で備えます（本書の推奨）。

8-2 漏えいが起きたら

まず、すぐにすること

漏えい（おそれを含む）に気づいたら、次の1〜5を手分けして、並行して進めます。IPA（情報処理推進機構）のインシデント（事故）対応の手引きと、委員会の制度をもとにした本書の整理です。

1. 気づいた日時と、何が起きたかを記録用紙に書きます（用紙は下の「ふだんから決めておくこと」）。その後の経過も、日時と一緒に書き足していきます。
2. 被害が広がるおそれのある機器を、ネットワークから切り離します（LAN ケーブルを抜く、Wi-Fi を切るなど）。電源を切ったり初期化したりはしません。残った記録が消えるおそれがあるためです。
3. 社内の責任者に知らせます。カード情報やアカウントの情報が漏れたおそれがあれば、カード会社への連絡やアカウントの停止も進めます。
4. 不正アクセス（許可なく他人のシステムに入ること）やランサムウェアのおそれがあれば、報告を待たずに警察と IPA に相談します（下の「困ったときの相談先」）。
5. 漏れた（おそれがある）情報の種類・件数・暗号化の有無と、本人の人数を確かめます。人数が決まらないときは、漏れたおそれがある最大の人数を控えます。委員会への報告と本人への通知が要るかは、下の「報告・通知の対象かを確かめる」で確かめます。迷うときは、個人情報保護法相談ダイヤルに聞きます。

制度・公式情報 IPA の手引きは、最初の対応として、被害が広がるおそれのある機器をネットワークから切り離すよう求めています。ただし、電源を切るなどの不用意な操作で記録を消さないよう注意しています。漏えいのときは、漏れた情報の種類・件数・暗号化の有無を確かめます。カード情報やアカウントの情報が漏れたら、カード会社への連絡やアカウントの停止をするとしています[3]。

困ったときの相談先

窓口	使いどころ	連絡先
IPA 不正アクセス特別相談窓口（事業者向け・臨時）[4]	被害の可能性への助言、応急処置の案、専門業者の紹介	03-6759-5760（平日9時30分～17時30分、12時～13時を除く）、incident-support@ipa.go.jp
個人情報保護法相談ダイヤル	法律・制度の質問（違法性の判断には応じない）	03-6457-9849（9時30分～17時30分、土日祝日・年末年始を除く）
警察	サイバー事案の通報・相談、被害届	警察庁の全国統一のオンライン受付窓口、最寄りの警察署

制度・公式情報 上の表は、会社向けの主な窓口です（2026年10月22日時点。全体は付録C）。

制度・公式情報 IPA の手引きは、届け出の先を次のように挙げています。個人情報なら個人情報保護委員会、犯罪のおそれがあれば警察、ウイルスや不正アクセスなら IPA です。業法（銀行や通信など、業種ごとの法律）などで求められるときは、所管の省庁などにも届け出ます。手引きは相談先として、有償で緊急の対応を引き受ける企業の一覧も載せています[3]。

制度・公式情報 ランサムウェアの身代金について、警察庁は「犯罪グループ等の活動資金となることが懸念される」「暗号化されたデータの復号が保証されるわけではない」と説明しています。そのうえで、早めに警察や関係機関に通報・相談するよう呼びかけています。警察庁が開発した復号（暗号を元に戻すこと）のツールで、これまでに国内の41の被害企業の約2,011万件のデータを元に戻したとしています[1]。

ランサムウェアの見極めと、戻すときの注意

制度・公式情報 JPCERT/CC の FAQ（よくある質問と答え）は、どんな攻撃の被害を受けた可能性があるかを、気づいた状況から「総合的に判断」するとしています。攻撃がどこまで進んでいるかも同じです。まだ被害を受けていないバックアップは、安全が確かめられるまで切り離したり、別の場所に移したりすることを検討するとしています。自動でバックアップを取る仕組みによっては、無事だったバックアップが上書きされて消えるおそれがあるためです。復旧の前には、侵入の経路として考えられる原因に、必ずすべて対処するとしています。経路を塞がないと、復旧したあとに別の攻撃を受けるおそれがあるためです[5]。

制度・公式情報 IPA の教訓集（2026年9月）は、対応が情報システムの担当に集中しやすい一方、公表・法務・取引先への対応なども要るとしています。そこで経営者が、総務・広報・営業なども含めて、会社全体の役割分担を事前に決めておくよう求めています。また、汚染された可能性があるバックアップは復旧に使えません。少なくとも侵入が始まった時期より前のバックアップは安全だとしています。そこで、必要なログ（機器やシステムの動きの記録）を保存し、安全に戻せる時点を判断できるようにしておくよう求めています[6]。



図8-2　感染のおそれがあれば、ネットから切り離して相談する

いつまでに・誰に・何を

委員会への報告には、まず出す「速報」と、調べた結果を出す「確報」があります。表の「本人」は、漏れた個人データ（名簿やデータベースのように整理して持っている個人情報）が指している人です。図8-3と次の表は、並行して進める対応の整理です。警察や IPA には、報告を待たずに相談します（本書の推奨）。

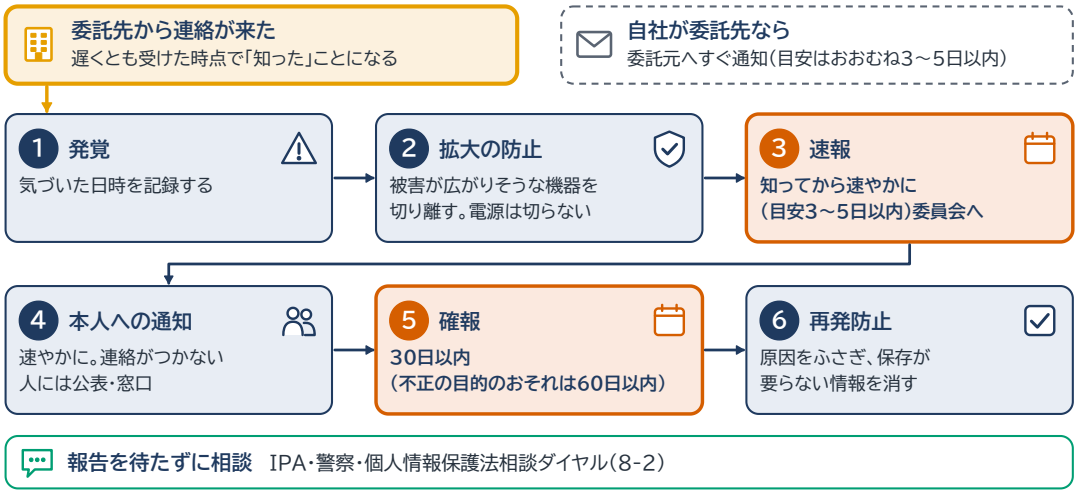


図8-3　漏えいが起きたときの会社の対応の流れ

いつまでに	誰に	何を
すぐ	社内の責任者	起きたことを知らせる
すぐ	（自社で）	日時を記録し、被害が広がりそうな機器をネットから切り離す（不用意に電源を切らない）
すぐ（報告を待たない）	警察・IPA	不正アクセス・ランサムウェアの相談
速やかに（目安3〜5日以内）	委員会	速報
速やかに	本人	5つの事項を通知（連絡がつかない人には公表・窓口）

いつまでに	誰に	何を
30日以内(不正の目的のおそれは60日以内)	委員会	確報

制度・公式情報 速報は、事態を知った後「速やかに」(目安はおおむね3〜5日以内)出します。確報は、知った日から「30日以内」(不正の目的によるおそれがあるものは「60日以内」)です。報告は原則としてオンラインのフォームで行い、マイナンバーを含むかどうかで報告先が分かれます。報告先と様式は、委員会の「漏えい等の対応とお役立ち資料」のページで案内されています。ランサムウェアの事案を国家サイバー統括室の共通の様式で報告する案内(2025年10月1日から)も、このページにあります[7]。

制度・公式情報 期限は、事態を「知った」ときから数えます。委託先から知らせを受けたときは、遅くともその時点で知ったことになります(8-3)[8]。

制度・公式情報 本人には「当該事態の状況に応じて速やかに」、郵送やメールなどで直接知らせます。伝えるのは、次の5つの事項です[8]。

- 概要
- 漏えいした(おそれがある)個人データの項目
- 原因
- 二次被害(漏れた情報が使われて、あとから起きる被害)やそのおそれの有無と内容
- その他の参考になる事項

制度・公式情報 連絡がつかないなどで直接知らせるのが難しいときは、「代わりの措置」をとります。事案の公表や、本人が自分のデータが対象かを確かめられる問い合わせ窓口の設置などです[8]。

報告・通知の対象かを確かめる

制度・公式情報 民間の事業者は、個人データの漏えいなど(おそれを含む)が次の①〜④のどれかに当たるとき、個人情報保護委員会に報告し、本人に通知しなければなりません。「漏えいなど」には、データがなくなる「滅失」や、改ざんされたり、ランサムウェアで暗号化されて戻せなくなったりする「毀損」も含まれます[7,8,9]。

- ① 病歴など、とくに配慮が必要な情報(要配慮個人情報)が含まれる
- ② カード番号など、不正に使われるとお金の被害が出るおそれがある
- ③ 不正アクセス(許可なく他人のシステムに入ること)など、不正の目的で行われたおそれがある
- ④ 1つの漏えいの事案で、情報が漏れた(またはそのおそれがある)人が1,000人を超える。漏れた情報の種類は問いません

  ④は、法律の言葉では「本人の数が1,000人を超える」と書かれています。「本人」は、漏れた情報が指している人のことです。お客様・会員・従業員など、その情報の持ち主です。データの件数ではなく、人数で数えます。

制度・公式情報 ①〜③は1人分でも対象で、人数の条件は④だけです。高度な暗号化などで守られ、復号の鍵も適切に管理されていたデータは、どれに当たっても報告を要しないとされています[7,8,9]。暗号化してあるだけでは足りません。「高度な暗号化」は、その時点の技術の水準で、第三者が読めないようにする暗号化です。鍵の管理は、暗号化したデータと鍵を分けて鍵の漏えいを防ぐ、遠隔で削除できる、第三者が鍵を使えない設計にする、のどれかです[9]。

「1,000人を超える」の数え方（個人情報保護委員会のガイドライン）

制度・公式情報 ④の人数が確定できないときは、漏れたおそれがある人数の最大で考えます。見つかったときは1,000人以下でも、あとで1,000人を超えたら、その時点で④に当たります。委員会は④の例として、2つの場合を挙げています。システムの設定ミスで、ネット上から見られる状態になった場合です。また、会員（1,000人超）へのメールマガジンを、受け取る人どうしのアドレスが見えない BCC ではなく、見える CC の欄に入れて一斉に送った場合です[7,8]。

制度・公式情報 ①～③に当たるかの目安は、委員会のガイドラインと Q&A で、次のように示されています。②に当たらなくても、不正アクセスによるものなら③、本人の数が1,000人を超えれば④で、報告の対象になります[8,9]。

漏れた（おそれがある）情報・起きたこと	報告・通知の対象か
医療機関が、健康診断の結果を本人以外に誤って渡した	対象（①）。件数にかかわらない
カードを発行した会社が、カードを誤って別の人に郵送した	対象（②）と考えられる。未開封のまま回収できたときは、通常は漏えいに当たらない
カード番号だけ	対象（②）と考えられる
カード番号の下4桁と有効期限だけ	直ちには②に当たらない
銀行口座の情報だけ	直ちには②に当たらない
銀行口座の情報と、ネットバンキング（ネットで振込などができる銀行のサービス）のパスワード	対象（②）
住所・電話番号・メールアドレスだけ	直ちには②に当たらない
入力のページが書き換えられて、お客様が入れた情報が第三者に送られた	対象（③）。データベースに入れる予定で受け取った、または受け取ろうとしている情報も対象

会社の規模・マイナンバー・古い手順書について

制度・公式情報 従業員が100人以下の会社など（ガイドラインの「中小規模事業者」）には、ふだんの安全管理の方法を簡単にできる特例があります。ただし、漏えいの報告と本人への通知の決まりには、会社の規模による例外は書かれていません。従業員が少ない会社でも、①～④に当たれば報告と通知が必要です[8]。

制度・公式情報 マイナンバーを含む情報（特定個人情報）の漏えいは、番号法（マイナンバーの扱いを定めた法律）の決まりで報告します。給与の源泉徴収票や社会保険の届出に従業員のマイナンバーを書くため、委員会は、およそ従業員のいるすべての会社がマイナンバーを扱うとしています。報告と本人への通知が義務になるのは、次のときなどです。どれにも当たらない漏えいも、委員会に報告するよう努めるとされています[10]。

- 不正の目的によるおそれがあるとき
- ネット上などで、不特定多数に見られる（おそれがある）とき
- 本人の数が100人を超えるとき

制度・公式情報 個人情報保護法の個人データの漏えいなどについて、報告と本人への通知が義務になったのは、2022年4月1日からです。それまでは、委員会の告示（委員会が定めて公に示した決まり）で「報告するよう努める」とされていました[11]。マイナンバーを含む漏えいの報告は、上の番号法の決まりによります（義務に当たらない漏えいの報告は、いまも努力義務です）。古い解説や社内の手順書に「努力義務」とあれば、いまの決まりに合わせて直します（本書の推奨）。

制度・公式情報 改正個人情報保護法は2026年7月に公布(国が法律を広く知らせること)されましたが、まだ施行(実際に始まること)されていません。第三者の確認を前提にした速報の免除など、報告の見直しも示されています。ただし細かい条件はこれから決まり、いまの義務は変わっていません[12]。

報告の対象か迷うときは、個人情報保護法相談ダイヤル(上の「困ったときの相談先」)で確かめます。対象外の事故でも、お詫びと説明、記録、再発防止はします(本書の推奨)。

ふだんから決めておくこと

社内の責任者と報告の担当者を決め、記録用紙も用意しておきます。用紙には、気づいた日時、その後の経過、原因、被害を受けたシステム、漏れた情報の種類・件数・暗号化の有無、本人の人数(決まらないときは最大の人数)を書く欄を作ります。委員会への速報を書くときにも使えます(本書の推奨)。



社長

対応は、パソコンに詳しい担当者に任せておけばいいだろう。



コンサルタント

IPA によると、ランサムウェアの対応は、システムの担当に集中しがちです。でも、公表や取引先への対応も要ります。社長が、総務・広報・営業も含めた役割分担を、前もって決めておきましょう[6]。

お客様への説明と、その後

お客様へのお知らせや公表文は、次の欄に分けて書きます。調べている途中でも、分かった範囲で早めに出します。本人に知らせる5つの事項(上)と IPA の手引き(下)をもとにした、本書の推奨です。公的なひな形は見当たりません(2026年10月23日時点)。

欄	書くこと(例)
分かっていること	起きたこと、漏れた(おそれがある)情報の項目、原因、二次被害やそのおそれの有無と内容(分かった範囲で)
まだ分かっていないこと	調べていること(対象になる人の数、詳しい原因など)
お客様へのお願い	同じパスワードを使っているほかのサービスでの、パスワードの変更、会社を名乗る不審な連絡への注意。会社から聞かないこと(パスワードやカード番号など)も書く
問い合わせの窓口	専用の窓口の電話番号・受付時間・ウェブのフォーム
次のお知らせ	続報を出す時期の予定と、載せる場所

お知らせを出す前に1・2を済ませ、出したあとは3・4のように進めます(本書の推奨)。

1. 専用の問い合わせ窓口を決め、受付時間をお知らせに書きます。
2. お知らせの内容と、よくある質問への答え方を、社内の全員に知らせます。従業員ごとに説明が食い違わないようにします。

3. 続報は予定の時期に出し、分かったことを足していきます。最終報で、調査の結果と再発防止策を知らせます。
4. お知らせを出した日時と、問い合わせの内容は、記録用紙に残します。

8-3 の、鉄道会社の問い合わせフォームの件のお知らせも、分かっていること・お願い・窓口を分けて早めに出した例です。

制度・公式情報 IPA の手引きは、第一報（最初のお知らせ）の出し方にも触れています。すべての関係者に知らせるのが難しいときや、影響が広く一般に及ぶときは、ウェブサイトやメディアで公表します。そのときは「公表によって被害の拡大を招かないよう、時期、内容、対象などを考慮」するよう求めています。顧客や消費者に関わるときは「受付専用の問い合わせ窓口を開設し」、被害の動きを速やかにつかみます[3]。

制度・公式情報 同じ手引きは、第二報以降と最終報で、被害者や影響が及んだ取引先・顧客に、対応の状況や再発防止策などを報告するとしています。被害者への損害の補償なども「必要に応じて」行います。ID・パスワードなどが悪用されるおそれがあれば、同じ情報を使っているほかのサービスの登録情報を変えるよう促すなど、二次被害を防ぐ注意を呼びかけます[3]。

お金の備え：サイバー保険

サイバー保険（サイバー攻撃などの事故による損害に備える保険）に入っているなら、事故のときに連絡する先（保険会社・代理店）と補償の条件を、事故の前に確かめておきます。お助け隊サービス（8-7）に付く簡易な保険も同じです。本書では、保険の商品は比べていません（本書の推奨）。

制度・公式情報 IPA の手引きは、事故で想定される直接の被害も挙げています。対応の人件費、原因の調査や復旧を外部に頼む費用、「取引先・顧客等への謝罪対応費」、「法的対応のための弁護士費用」などです。間接の被害には、会社の信用の低下や、事業が止まることによる機会の損失を挙げています[3]。

制度・公式情報 日本損害保険協会の説明では、サイバー保険は一般に、次の3つの事故による損害を補償します[13]。

- 情報の漏えい（おそれを含む）
- ネットワークの所有・使用・管理に起因する他人の業務の阻害（ほかの会社などの仕事を妨げてしまうこと）
- サイバー攻撃に起因する他人の身体の傷害・財物の損壊

制度・公式情報 協会は、補償される費用に、事故対応費用・損害賠償費用・利益損害や営業継続費用があるとしています。ただし、「補償内容は、保険会社や保険会社が提供するサイバー保険のプランにより異なります」としています。「ランサムウェアの被害によって支払った身代金はサイバー保険の対象になりません」とも書いています[13]。

会社のメールや SNS の公式アカウントが乗っ取られたら

会社のメールや SNS の公式アカウントが乗っ取られると、お客様や取引先に、会社の名前で偽の連絡が送られるおそれがあります。次の1〜3は、手分けして並行して進めます。記録のために、取り戻す操作やお知らせを遅らせません（本書の推奨）。

1. 乗っ取られた画面や届いた連絡、気づいた日時を、画面の保存や写真で残します。覚えのない投稿・設定・つながったアプリなどは、急いで消さず、画面を残してから直します。
2. サービスの手順で、アカウントを取り戻します。パスワードの変更や、登録のメールアドレス・電話番号、ログイン中の端末の確かめ方は、第6章 6-5 の「SNS・メッセージアプリが乗っ取られたとき」と同じです。
3. 乗っ取られていない手段（公式サイト、店頭の掲示、電話、ほかの SNS など）で、お客様や取引先に知らせます。乗っ取られたアカウントから届いた連絡のリンクを開かないよう書きます。会社から確認コード（ログインのときに SMS などで届く番号）やパスワードを聞くことはない、とも書きます。支払いや振込先の変更を求める連絡が届いたら、ふだんの連絡先で会社に確かめてもらうよう添えます。

4. 会社のメールが乗っ取られたときは、取引先へはメール以外の方法で連絡します。転送や振り分けの設定(確かめ方は第6章 6-1 の「メールのアカウントが乗っ取られたとき」)と、ほかの社員のアカウントも確かめます。
5. 警察に相談します(上の「困ったときの相談先」)。不正に見られた・取られた(またはそのおそれがある)メールやメッセージに顧客の個人データが含まれていれば、上の①〜④にあたるかを確かめます(迷うときは個人情報保護法相談ダイヤル)。

制度・公式情報 IPA には、ビジネスメール詐欺(取引先や経営者になりすましたメールで、偽の口座に送金させる詐欺)の被害のあとの手引きがあります(2022年9月更新)。メールが盗み見られているおそれがあるとして、取引先へはメール以外の方法で連絡するよう求めています。関係者のパソコンのウイルスチェック、メールのパスワードの変更、不審なアクセスの痕跡の調査もします。「外部へのメールの転送設定や、普段見ないフォルダへの振り分け設定等がないか調査」することも挙げています。自分の組織を詐称された場合は、今後も偽のメールが送られうるので、「社内外へ注意喚起」するとしています[14]。

ふだんから、公式アカウントにログインできる人と、登録したメールアドレス・電話番号を把握しておきます(8-4。本書の推奨)。

8-3 委託先・委託元のとき

個人データの扱いを任せる側を委託元、任される側を委託先といいます。



同僚

取引先から「漏れたおそれがある」と連絡が来ました。うちは何をすればいいでしょう。

自社が委託先なら、委託元にすぐ知らせます。自社が委託元で、取引先から漏えい(おそれ)の連絡が来たら、次のようにします(本書の推奨)。

1. 連絡を受けた日時を記録し、委託先の報告を待たずに速報の準備を始めます。
2. 自社の顧客が対象か、漏れた項目は何かを確かめます。
3. 管理画面のパスワードを変え、ログインの履歴を確かめます。
4. 顧客に知らせます(8-2 の「お客様への説明と、その後」)。

制度・公式情報 委託先で報告の対象になる事態が起きたとき、委託元は、遅くとも委託先から知らせを受けた時点で、事態を「知った」ことになります。そこから速やかに(目安3〜5日以内)速報を出します。報告の義務は原則として両方にあります。委託先は、委託元に知らせれば(目安はおおむね3〜5日以内)自分の報告の義務を免れますが、委託元の義務は残ります[8]。

実際に起きた事例 店舗向けの予約・POS(レジ)などのクラウド(ネット上で使うソフトや保存場所)のサービスの件です。提供する会社は10月22日、不正アクセスで「お客様情報の流出とみなされる事実」を確認し、24のサービスを止めました。10月23日の第二報では、最大で20のサービスで氏名・電話番号・メールアドレスなどが漏れた可能性があるとしつつ、漏れた事実はまだ確認できていないとしています(人数は未公表)[15]。

実際に起きた事例 ある鉄道会社は10月7日、外部の会社から、その会社のサーバーに不正アクセスがあったと報告を受けたと公表しました。問い合わせフォームのサービスを提供している会社です。鉄道会社に関する情報の閲覧・取得の形跡は確認されていないとしつつ、念のため、不審なメールのリンクや添付ファイルを開かないよう呼びかけ、問い合わせの窓口を設けました[16]。

この例のように、調べている途中でも、分かっていることとお願い・窓口を早めに知らせます（欄の分け方は 8-2 の「お客様への説明と、その後」。本書の推奨）。

委託の契約で確かめること

制度・公式情報 国家サイバー統括室は2026年10月9日、2つのことを挙げました。漏えいのときの報告の義務を契約に入れることと、業務が終わったら委託先にデータを消させることです[17]。

第2章で見たカラオケ店の件のように、委託先のパソコン1台から漏えいのおそれが広がることもあります。委託の契約では、次の点を確かめます（本書の推奨）。

- 漏えいのときに知らせる義務と、事故のときの連絡先・手順
- 委託先の端末の管理と、脆弱性（ソフトや機器の弱点）への対応
- 業務が終わったら、預けたデータを消すこと（消したかも確かめる）

制度・公式情報 個人情報保護委員会の「WARNING」（2026年10月7日改訂）は、報告された不正アクセスの事案の型に、利用するクラウドサービスからの漏えいを挙げています。「クラウドの利用は委託にあたらない」と考えて監督していなかった例や、保守の契約に脆弱性への対応が入っていなかった例も載っています[18]。

予約・会計・メール配信などのクラウドのサービスも、事故のときの連絡先と手順を確かめておきます。使っているサービスの事故は、自社の顧客の漏えいとして対応が要る場合があります。事故の知らせが来たら、上の4つの手順で進めます（本書の推奨）。

8-4 まずやる対策

第2章で見た不正アクセスの原因（脆弱性の放置、推測されやすいパスワード、設定ミスなど）を、1つずつふさいでいきます。小見出しごとに、番号の順に進めます。章末の「まず今週やること」「今月やること」は、この章全体のまとめです（項目ごとに節を示しています。本書の推奨）。

すぐに点検する

制度・公式情報 IPA は2026年10月9日、不正アクセスによる漏えいなどの事案をふまえて、すぐに行う点検を示しました[19]。次の1〜4は、この点検にそった手順です（3 は本書の推奨）。

1. 点検するものを書き出します。外部に公開しているアプリ（ホームページや予約・通販のシステムなど）、使っている外部のサービス、持っているデータの3つです。
2. それぞれについて、ログ（操作や通信の記録）の異常、身に覚えのないアカウントや消したはずのアカウントの復活、当てていない修正プログラムがないかを確かめます。
3. ホームページや予約のシステムなど、自分で点検できないものは、制作会社や機器を入れた業者に点検を頼みます。
4. 異常が見つかったら、インシデント（事故）として扱います。IPA は、専門の業者に詳しい調査を頼むよう強く勧めています。初めの動き方は 8-2 の「まず、すぐにすること」です。

VPN 機器やホームページを更新する

次の1〜4は本書の推奨です。

1. VPN 機器（社外から社内のネットワークにつなぐための機器）を使っているかを確かめます。分からなければ、機器を入れた業者に聞きます。

2. VPN 機器や社内の管理システムも更新の対象にします。保守の契約に「脆弱性への対応（更新）」が入っているかも確かめます。
3. レンタルサーバーや管理画面などの初期のパスワードは、すぐに自分のものに変えます。
4. 自社のホームページや予約・通販のシステムが PHP などを使っているかを、制作会社やレンタルサーバー会社に確かめます。使っているならサポート中の版かも確かめ、更新を頼みます（下の囲み）。

制度・公式情報 リモートデスクトップ（離れた所のパソコンを、手元のパソコンから操作する仕組み）を使う会社は、手元のドライブの共有にも注意します。Microsoft は、2026年4月のセキュリティ更新プログラム以降、接続の設定のファイル（RDP ファイル）を開くと、接続の前に警告が出て、手元のドライブなどの共有は既定でオフになるとしています。ドライブの共有は、接続先から手元のファイルを読み書きできるようにするもので、最も危険な共有だとしています[20]。更新を入れ、必要のない共有はオンにしません（本書の推奨）。

実際に起きた事例 警察庁がランサムウェアの被害組織に聞いた侵入の経路（2026年上半期、有効回答36件）は、VPN 機器が18件でした[1]。

制作会社に確かめるときの参考（10月の更新の呼びかけ）

制度・公式情報 IPA と JPCERT/CC（国内のセキュリティの事故の情報を集め、対応を調整する組織）は10月21～22日、PHP の深刻な脆弱性について注意喚起を出しました。PHP は、Web サイトなどで広く使われているプログラムの言語です。悪用されると、外から好きなプログラムを動かされるおそれがあります。JPCERT/CC は、速やかな対策と、侵害を受けていないかの調査を求めています。IPA は、製品の内部で使われている PHP は利用者には分からない場合があるとして、開発元・提供元の情報を確かめるよう勧めています[21]。サービスを予防のために止めた会社の例は第2章にあります。

実際に起きた事例 Web サイトを作るのに使われる部品の Next.js（10月14日）と Node.js（10月21日）でも、開発元が脆弱性を直した更新を公開し、利用者に更新を求めました[22]。

使うサービスを整理し、多要素認証をかける

次の順で進めます（1～4 は本書の推奨）。

1. 使っているクラウドなどの外部のサービスを洗い出します。メール、会計ソフト、予約システム、ネットバンキング、SNS の公式アカウントなどです。
2. 退職した人のアカウントを消します。ただし、消したはずなのに残っていた、退職のあとに使われた形跡がある、というときは消さずに、3 と同じように扱います。
3. 身に覚えのないアカウントは侵入の手がかりかもしれないので、すぐには消しません。使えないように止め、画面などの記録を残して、上の IPA の点検のとおり業者に調べてもらいます。
4. SNS の公式アカウントは、ログインできる人と、登録したメールアドレス・電話番号も控えておきます。
5. 管理者のアカウントから、多要素認証（パスワード・スマホ・指紋など、種類の違う確かめ方を2つ以上組み合わせる仕組み）を有効にします[23]。

制度・公式情報 IPA の「情報セキュリティ6か条」の解説編は、ファイルなどの共有の設定は範囲を限り、異動や退職のときは速やかに変える・消すよう求めています[23]。

バックアップを戻せる形で取る

制度・公式情報 同じ解説編は、バックアップを次のように取るよう勧めています（1～3 が「3-2-1ルール」）[23]。

1. 元のデータを含めて、3つ以上のコピーを持ちます。

2. コピーは、2種類の媒体(外付けの記憶装置など)に分けて持ちます。
3. 1つは、ふだん使うシステムとは別の場所に置きます。
4. 装置はバックアップのときだけつなぎ、戻せるかを定期的に確かめます。

まず一度、バックアップから実際に戻せるかを試します(本書の推奨)。

実際に起きた事例 警察庁の調査(2026年上半期)では、ランサムウェアの被害でバックアップから戻せたかを聞いた40件のうち、戻せたのは11件でした[1]。

誤送信を防ぐ

次の1〜3で進めます(1・2 は本書の推奨、3 は IPA の手引き〔下〕のとおり)。

1. 一斉送信は BCC(ほかの受信者にアドレスが見えない欄)か、メール配信のサービスを使います。
2. 送る前に確認を促す表示を出す、ほかの人に宛先を見てもらう(1人なら声に出して読み上げる)などの手順を決めます。
3. 誤って送り、送り先が分かるときは、受信者に削除を頼みます。

制度・公式情報 IPA の手引きは、メールを誤って送り、送り先が分かるときは、受信者に削除を頼むとしています。あわせて、作業の手順に確認の仕組みを加えるよう書いています[3]。

持つ情報を減らす

持っていない情報は漏れません。次の1〜4は本書の推奨です。

1. 持っている個人情報を「何を・どこに・何人分・いつまで」の形で書き出します。書き出しには、8-7 の IPA のガイドラインの付録にある資産管理台帳のひな形も使えます。
2. 法令で保存が求められていないか、業務に必要かを確かめてから、要らなくなったもの(退会者・退職者の情報、本人確認書類の画像など)を消します。漏えいの調査中は、調査や証拠のために要る記録を先に残します。
3. 予約の備考欄などに、カード番号や体調など要らない情報を書かない決まりを作ります。
4. 社員が生成 AI(文章などを作る AI)を使うときに、入れてよい情報といけない情報を決めておきます。

8-5 送金をねらう詐欺に備える

経営者や銀行をよそおって、会社にお金を送らせる詐欺が起きています(下の実例)。次のことを決めて、社内で共有しておきます(本書の推奨)。

1. 送金の指示は、メールだけで進めません。あらかじめ登録してある連絡先など、今回の依頼とは別に知っている連絡先で、本人に確かめます。メールに書かれた番号や返信先は使いません。
2. 銀行や取引先を名乗る電話で、ソフトの導入やメールアドレスを求められたら、いったん切ります。公式サイトなどで自分で調べた番号にかけ直します。
3. いつも使う会社の端末からの操作でも、安全とは限りません。覚えのない操作や送金に気づいたら、直ちに銀行と警察に連絡します(下の「送金の被害に気づいたら」)。

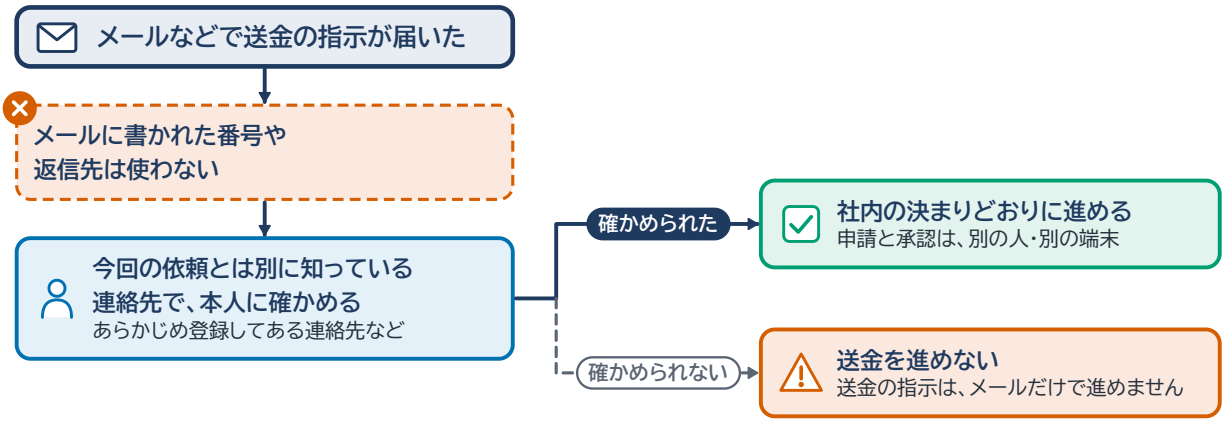


図8-4　送金の指示が届いたときの確かめ方

実際に起きた事例 警察庁によると、2026年1月ごろから「ニセ社長詐欺」が起きています。経営者になりすまして、ネットなどで公開されている会社のメールアドレスにメールを送り、業務をよそおって送金させる手口です。実在する社長の名前や会社名が使われるので、見分けにくいのが特徴です。2026年1～6月の認知件数（警察が把握した件数）は127件、被害額は約38億8,000万円で、既遂（実際にお金をだまし取られたもの）1件あたり約3,100万円でした[1]。

制度・公式情報 警察庁は、社内で情報を共有すること、送金のルールを確かめ直すこと、SNS のグループを作るよう指示されたら特に注意することを勧めています[1]。



図8-5　社長を名乗る送金の依頼は、本人に別の方法で確かめる

実際に起きた事例 電話から始まる手口もあります。警察庁によると、2024年秋から法人口座の不正送金が急増しました。犯罪グループが会社に電話をかけ、ネットバンキングの更新の手続きなどを口実にメールアドレスを聞き出し、偽のメールを送る手口（ボイスフィッシング）です。2026年5月には、電話をきっかけに遠隔操作のソフトを入れさせる新しい手口が急増しました。偽のサイトに誘導して ID・パスワードを盗みながら、会社の端末を外から操作して送金させるものです[1]。



銀行を名乗る電話で信用させ、偽のメールや、遠隔操作のソフトを入れさせる方へ誘います[1]。

詐欺師

制度・公式情報 警察庁は2026年6月、ボイスフィッシングによる法人口座をねらった不正送金の被害が、手口を変えて再発しているとしました。そのうえで企業に、次のことを社内で徹底するよう求めています[24]。

- 銀行をかたるメールや SMS（携帯電話の番号あてに届く短いメッセージ）に書かれたリンクなどを開かない
- 銀行から電話があったら、営業店や代表電話に折り返して、本物かを確かめる
- 被害にあったら、警察に通報・相談する

会社の口座の補償は銀行ごとに違う

被害の前に、次のことをしておきます（本書の推奨）。

1. 契約している法人向けのネットバンキングについて、補償の有無・上限・届け出の期限を、取引銀行の規定で確かめます。
2. 申請と承認を、別の人・別の端末にします。
3. 振込の限度額を、必要な範囲まで下げます。
4. 取引の通知メールを確かめます。

補償の扱いは、銀行ごとに違います（下）。だまされて入力してしまったときも、補償されないと決めつけず、直ちに取引銀行と警察に連絡します（下の「送金の被害に気づいたら」。本書の推奨）。

制度・公式情報 会社（法人）の口座は、個人向けの補償の申し合わせ（第7章）の対象ではありません。全国銀行協会（銀行の業界団体）は2014年7月17日、法人向けのネットバンキングの補償について、考え方を示しました。不正な払い戻しの補償は、「個別行の経営判断として検討する」としています[25]。

制度・公式情報 協会によると、個人向けの申し合わせは、預金者保護法（偽造・盗難カードの被害から預金者を守る法律）の対象が個人であることなどをふまえたものです。法人のセキュリティ対策の力は、一般に個人より相対的に高いと考えられる、ともしています。補償を検討するときは、法人が求められた対策を自ら講じているかを考慮し、補償の対象や上限などを個別に決めるとしています。銀行に法的な責任はないと考えられる場合でも、補償するとの判断はありうる、としています[25]。

制度・公式情報 全国銀行協会は法人に、次の対策を「実施していただく」ものとしています[25]。

- 銀行が導入している対策を実施する
- OS（スマホやパソコンの基本のソフト）やブラウザ（インターネットを見るアプリ）を更新する
- サポートが切れたソフトを使わない
- セキュリティ対策ソフトを使う

制度・公式情報 協会が「推奨する」対策には、次のものがあります[25]。

- ネットバンキングに使うパソコンの用途を限る
- 取引の申請者と承認者で、異なるパソコンを使う
- 振込・払戻しなどの限度額を、必要な範囲内でできるだけ低く設定する
- 不審なログインの履歴や、身に覚えのない取引の履歴・取引の通知メールがないかを、定期的に確かめる

制度・公式情報 協会は、補償を減らす、またはしない取り扱いとなりうるケースとして、次のものを挙げています。どうするかは、それぞれの銀行が個別に判断します[25]。

- 求められた対策をしていない。身に覚えのない残高の変化や不正な取引があったのに、一定の期間内に銀行・警察に知らせていない。銀行の調査や警察の捜査に協力しない
- 正当な理由なく、他人に ID・パスワードなどを答えた。認証に使う乱数表やトークン(確認の番号を出す小さな機器)などを、安易に渡した
- パソコンや携帯電話を盗まれたときに、ID・パスワードなどを保存していた
- 銀行が注意していた方法で、メールによるフィッシング(本物そっくりの偽のメールやサイトで、情報をだまし取る手口)にだまされるなど、不用意に ID・パスワードなどを入力した
- 会社の関係者の犯行と分かった

実際に起きた事例 全国銀行協会のアンケート(2026年9月29日公表)によると、2026年4～6月の法人のネットバンキングの被害は48件・14億5,300万円でした。補償率の統計は個人だけで、法人の補償率はありません[26]。

1つの銀行の例

制度・公式情報 1つの銀行の例として、ある大手銀行の法人向けの補償を挙げます。ウイルス対策ソフトを入れて、最新の状態に保っていることが前提です。補償の上限は、指定の対策のどれかをしていれば5,000万円、それ以外は1,000万円です。指定の対策には、トランザクション認証(振込先などの取引の内容も確かめて承認する仕組み)の導入などがあります[27]。

制度・公式情報 同行は、実際に不正に振り込まれた日の翌日から10日以内に届け出なかった場合は、対象にならないとしています。警察に被害届を出していない場合、被害の調査に協力しない場合なども、対象になりません[27]。個人向けの申し合わせの「30日」(第7章)より短い期限の例です。

送金の被害に気づいたら

連絡する先は、被害の種類で違います。担当者には、「身に覚えのない送金に気づいたら、直ちに銀行と警察へ連絡する」と決めておきます(本書の推奨)。

被害の種類	まず連絡する先	続けて
乗っ取りや遠隔操作で、身に覚えのない送金をされた	取引銀行(法人向けの窓口・緊急の連絡先)	警察
だまされて自分で振り込んだ(ニセ社長詐欺など)	振り込んだ先の口座がある銀行と、振り込みに使った取引銀行	警察

次の順で進めます(本書の推奨)。

1. 遠隔操作などが続いているおそれがある端末は、すぐにネットワークから切り離します。電源を切ったり初期化したりはせず、銀行と警察に相談します(8-2 の IPA の手引きと同じ考え方)。
2. 並行して、表の「まず連絡する先」に、直ちに電話します。銀行への連絡は、その端末ではなく、電話や別の端末でします。取引銀行の法人向けの緊急の連絡先は、ふだんから控えておきます。社内の責任者にも、並行して知らせます。
3. 続けて、警察に通報・相談します(8-2 の「困ったときの相談先」)。被害届を出していることを、補償の条件にしている銀行の例もあります(上の囲みの銀行)。

4. 気づいた日時、送金の日時・金額・相手先、画面の写真、銀行・警察とのやりとり（日時・相手・内容）を、8-2 の記録用紙に書きます。
5. だまされて振り込んだときは、振り込め詐欺救済法の手続き（第7章）の対象になるかを、振込先の銀行に確かめます。
6. ID・パスワードや顧客の情報が漏れたおそれがあれば、社内の責任者に知らせ、8-2 の手順で進めます。

制度・公式情報 全国銀行協会の案内も、振り込んだ先の口座がある銀行への連絡と、警察への届け出を求めています（第7章）[28]。

制度・公式情報 IPA のビジネスメール詐欺の手引き（8-2）は、偽の口座に送金してしまったときのことも書いています。送金に使った銀行に早く、送金のキャンセルや組み戻し（振り込みを取り消してもらう手続き）を頼むよう勧めています。必ずお金が戻るとは限らないとしつつ、送金後すぐに銀行に連絡することは有効だとしています[14]。

8-6 Web のシステムが止まったときに備える

この節は、漏えいそのものではなく、使っているサービスが止まったときの備えです。予約・レジ（POS）・勤怠・受発注・ネットショップなどをクラウドのサービスに任せていると、サービスが止まれば店の仕事も止まります。止まった理由で、することが少し違います。することは、「ふだんの備え」の表と、「止まったとき」「復旧したとき」の手順にまとめました。

実際に起きた事例 まず、予防のための停止です。保育・教育施設向けのサービスの会社は10月21日、全サービスを止めました。PHP の重大な脆弱性（8-4）の公表を受けた措置で、不正アクセスや漏えいは確認されていないとしています（第2章）[29]。

実際に起きた事例 次に、攻撃の被害による停止です。8-3 で見た、店舗向けの予約・POS のクラウドの件です。提供する会社は10月22日、不正アクセスで「お客様情報の流出とみなされる事実」を確認しました。WEB予約や POS など24のサービスを止めています。10月22日の発表では、復旧は最短で10月26日中の予定としていました。原因は同じ日に、PHP ではなく自社のサービスの脆弱性と訂正されました[15]。10月23日の第二報では、漏れた事実はまだ確認できていないとしています（8-3）。

実際に起きた事例 攻撃ではない障害もあります。スマホ決済サービスの障害の件です。運営会社は2026年7月16日、利用するクラウドの障害で、一部の支払いなどが使えない場合があったと公表しました。戻った時刻は、支払い・サイト・アプリの機能ごとに違いました[30]。

どの場合も、止まっている間の仕事の続け方と、お客さまへの知らせ方が要ります。攻撃の被害なら、8-2・8-3 の対応も加わります。初めの発表の原因が直されることもあるので、続報も確かめます（本書の推奨）。

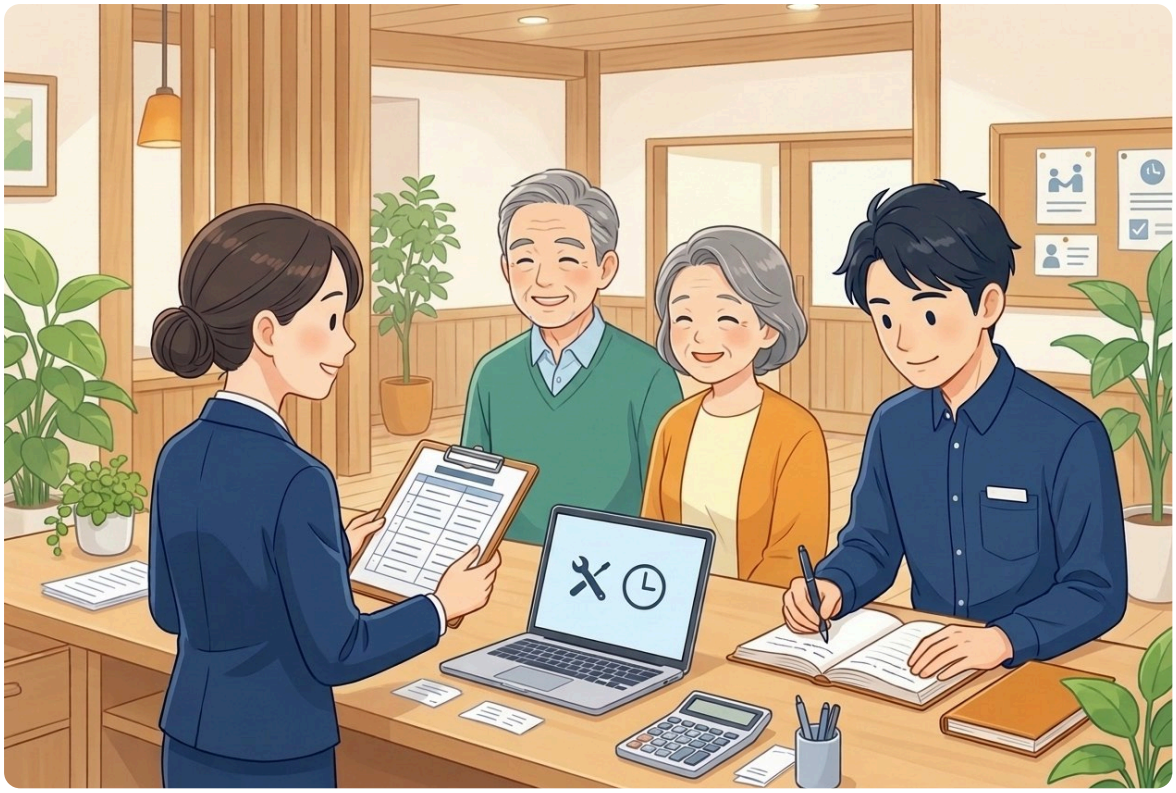


図8-6　止まっても、紙の控えがあれば落ち着いて受け付けられる

ふだんの備え

業務ごとに、代わりの方法を決めておきます（本書の推奨）。

業務	前もって用意するもの	止まったときの代わり
予約	当日・翌日の予約の一覧（支払い済みか・連絡先）を毎朝印刷	紙の一覧で受け付け、電話の予約は1冊に書く
レジ	釣り銭、手書きの領収書	現金などで受け、控えを残す
勤怠	紙の出勤簿	出勤・退勤の時刻を紙に書く
受発注	主な取引先の電話・FAX の一覧	電話・FAX で受け、控えを残す
ネットショップ	SNS など、別のお知らせの手段	注文を受けられないことと、問い合わせ先を知らせる

表のほかに、次のことも決めておきます（本書の推奨）。

1. 自店のレジで何ができるかは、製品の案内で確かめておきます（下の Airレジの例）。
2. お客さまへの知らせ方は、ホームページのほかに、店頭の掲示・電話・SNS と複数決めます。
3. 印刷した一覧は人目に触れない所に置きます。障害がなかった日の一覧は、次の日の一覧を印刷したら細断します。障害のときに使った一覧と手書きの記録は、復旧後の突き合わせが済み、法令で保存が求められていないか、業務に必要かを確かめてから処分します（下の「復旧したとき」の5）。
4. 年に一度は紙の手順を30分ほど試し、手が足りるかを確かめます。

制度・公式情報 レジのアプリには、ネットにつながらなくても会計できるものもあります。例として Airレジでは、オフラインでも現金などで会計できます。ただし、キャッシュレスの決済は使えず、ログインも前もって済ませておく必要があります。

制度・公式情報 中小企業庁の BCP（緊急のときに事業を続けるための計画）の指針は、次の備えがあるかを問うています。IT の機器やシステムが使えないときの代わりの方法と、主な顧客などの連絡先の一覧です[31]。IPA のクラウドサービスの手引きは、停止に備えて重要な情報を手元に確保し、サポートの受付時間（週末・夜間）も確かめるよう挙げています[32]。

制度・公式情報 観光の業界向けの BCP の記入例は、停電などに備えて、当日の宿泊予約者の名簿をチェックインの前に印刷する例を示しています。精算のシステムが使えなければ後日に精算する、という代替策も挙げています[33]。飲食店向けの記入例は、POS の代わりに現金・手作業で会計し、システムが戻ってから入力する例を挙げています[34]。

実際に起きた事例 千葉県木更津市のホテルが、予約のシステムを使えず、紙の予約リストで対応したと報じられました（10月23日）。事前に代金を受け取ったかを判断するためだったといいます。鳥取県では、遊覧船の会社のホームページが見られず、欠航を知らずに来た客がいたと伝えられています[35]。

止まったとき

制度・公式情報 IPA のインシデント対応の手引き（8-2）は、停止の原因は攻撃のほか、ソフトの不具合や機器の故障などさまざまだとしています。原因がわからないうちは、セキュリティの問題の可能性も含めて対応します。止まっている間は、業務の代わりの策があれば提供するとしています[3]。

次の順で動きます（本書の推奨）。

1. 時刻と画面の表示を記録します。店のネットでほかのサイトが開くか、スマホの回線（Wi-Fi を切る）でそのサービスが開くかを試し、店のネットの不調か、サービスの側の障害かの見当をつけます。
2. サービス会社の公式のお知らせ（障害情報のページや公式の SNS）で、止まった機能と理由を確かめます。
3. 紙の手順に切り替えると全員に伝えます。手作業の記録は1冊にまとめ、書く人を決めます。
4. 予約サイトから新しい予約が入り続けるなら、販売を一時止めることを検討します。
5. キャッシュレスで払えないときは、入口とレジに掲示します。
6. パスワードの変更などの指示は、公式のお知らせで確かめてから従います。

実際に起きた事例 上の保育・教育施設向けのサービスの会社は、保護者向けのアプリも止めるため、保護者に個別に案内できないと伝えました。代わりに、保護者への通知の文書と、出席簿などのひな形を施設に用意しました[36]。

予約のあるお客さまには、電話やメールで早めに知らせます。分かっていること、分かっていないこと、次に知らせる時刻を分けて書きます（本書の推奨）。

復旧したとき

次の順で戻します（本書の推奨）。

1. 自店が使う機能（予約の受け付け・決済・お知らせのメールなど）が戻ったかを、一つずつ確かめます。
2. 紙の記録と、システムの予約・売上・入金を突き合わせます。システムに自動で入った分と、まだ入力していない紙の分を分け、紙の分は重ならないように入れます。二重の予約・二重の請求・入力の漏れも探します。オフラインで会計したデータは早めに送ります（Airレジは当日中に送るよう案内しています）。
3. 食い違いがあったお客さまには、早めに連絡しておわびします。
4. 予約サイトの販売を止めていたら、空きを確かめてから戻します。
5. 手作業の紙は、法令で保存が求められていないか、業務に必要かを確かめてから、要らなくなったものを処分します。
6. 漏えい（おそれ）の知らせがあれば、8-2・8-3 に進みます。困ったことは、上の表に書き足します。

制度・公式情報 内閣府の事業継続ガイドラインは、手作業で処理したときの戻し方の例を挙げています。「情報システム復旧後もすぐに入力処理は行わず、手作業で行った処理がシステムへ反映されたことを確認する」というものです[37]。

実際に起きた事例 保育・教育施設向けのサービスの会社は、22日3時22分に主なサービスを再開しました。そのあとも、来ていない子どもを知らせる機能を、その日は終日止めました。欠席の連絡などが正しく反映されていないおそれがあるためです。施設には、打刻と目視で確かめるよう求めました（23日に再開）[29]。

止まっている間・戻ったあとの不審な連絡に備える

予約や注文の情報を使った偽の連絡の実例と、予約サイトの案内は、第6章 6-10 にあります。停止のあとに来る連絡も、本物のお知らせと見分けられるよう、次のことをしておきます（本書の推奨）。

- 店のお知らせに、支払いやログインを求めるリンクを入れません。カード番号やパスワードをメールで聞かないことも、お客さまに伝えておきます。
- 返金や予約の取り直しは、店の電話など、お客さまが自分で確かめられる方法で受けます。
- サービス会社を名乗る「障害の補償」などの連絡も、リンクを開かず、自分で調べた窓口で確かめます（8-5）。
- 従業員にも、止まったあとに来る「返金」「振込先の変更」の連絡を疑うよう伝えます。

まず、業務ごとの表を作り、当日の予約の一覧を印刷するところから始めます（本書の推奨）。

8-7 公的な支援を使う

6か条から始める

制度・公式情報 IPA の「中小企業の情報セキュリティ対策ガイドライン」は、2026年3月27日に第4.0版になりました。「情報セキュリティ5か条」にバックアップを加え、「情報セキュリティ6か条」にしています。付録には、5分でできる自社診断、基本方針のひな形、資産管理台帳、インシデント対応の手引き（8-2）などがあります[38]。6か条は次のとおりです（OS はスマホやパソコンの基本のソフト）[23]。

1. OSやソフトウェアは常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. バックアップを取ろう！
6. 脅威や攻撃の手口を知ろう！

制度・公式情報 IPA の「SECURITY ACTION」は、中小企業が対策に取り組むことを自分で宣言する制度です。一つ星は6か条に取り組む宣言で、対策の前でも申し込めます。二つ星は、「5分でできる！情報セキュリティ自社診断」（25項目）を行い、情報セキュリティの基本方針を作って公開したうえで宣言します[39]。

取引先から求められる評価に備える

取引先から対策の状況を聞かれることに備えて、まず6か条と一つ星の宣言から始めます（本書の推奨）。

制度・公式情報 経済産業省と国家サイバー統括室は、「SCS評価制度」を2026年度末ごろに始めることをめざしています（IPA の表記では2027年3月ごろ）。取引先のセキュリティ対策の状況を、共通の基準で「見える化」（外から分かるようにすること）する制度です。段階は星の数で表します。★3は専門家の確認を経た自己評価、★4は第三者の評価機関による評価で、★5は今後の検討です。格付けの制度ではなく、特定の製品の導入を求めるものでも、法律ですべての中小企業に課す基準でもありません[40]。

お助け隊サービスを検討する

制度・公式情報 IPA の「サイバーセキュリティお助け隊サービス」は、中小企業向けの民間の事業者のサービスです。相談の窓口、異常の監視、事故が起きたときの初動の対応（駆けつけの支援など）、簡易なサイバー保険などを、安く一つのパッケージにまとめています。IPA は、基準に合うサービスに「お助け隊マーク」を付けています[41]。

制度・公式情報 サービスの基準は、月額の上限を、ネットワークを見張る型で1万円、端末を見張る型で1台あたり2,000円としています。月額とは別に、初期の導入費用など契約のときに払う費用の合計にも上限があります（それぞれの型で50万円、両方を使うと100万円。いずれも税抜き）。どの型も端末1台から契約でき、最低の契約期間は2年以内です。初期費用や途中で解約したときの違約金などは、契約書に書いて説明することになっています。サービスの一覧は、IPA の利用者向けのサイトで、地域や監視の種類から探せます[41]。

制度・公式情報 SCS評価制度の★3・★4を中小企業が効率よく取れるよう、新しい種類のサービス（「新類型」）もつくられました。これは、2026年10月～2027年9月（予定）の実証の事業（効果を確かめるために、無料で試す事業）です。公募（広く募集すること）で選ばれた15の事業者のサービスから選んで、直接申し込みます。最大1年程度、無料で参加できます。事業者ごとに募集が終わることがあり、複数の事業者には重ねて参加できません。参加すると、意見の提出や、検知した情報の提供に協力します[42]。

まず今週やること（3つ）

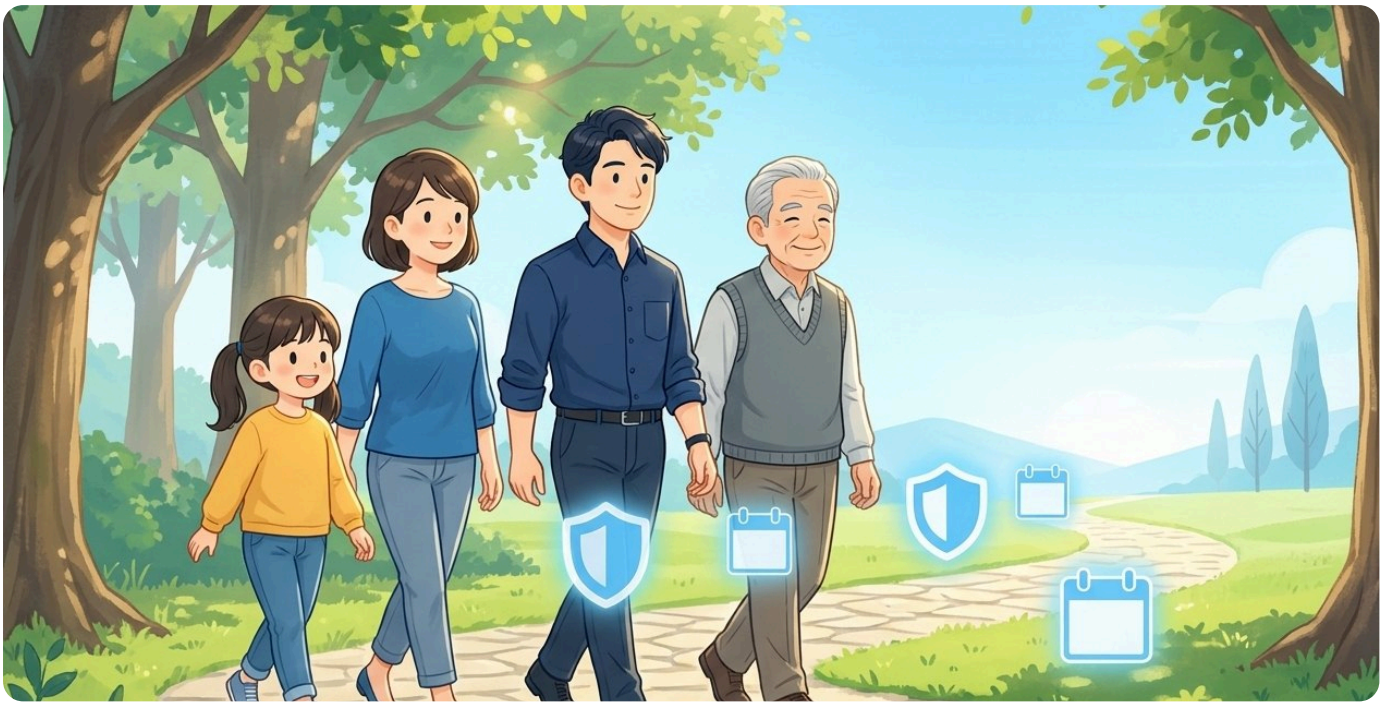
1. 漏えいのときの責任者と報告の担当者を決め、記録用紙を用意します（8-2）。
2. 管理者のアカウントから（SNS の公式アカウントも）、多要素認証を有効にします（8-4）。
3. バックアップから実際に戻せるか、一度試します（8-4）。

今月やること

1. お客様へのお知らせの欄と、問い合わせの窓口の担当を決めます。サイバー保険に入っていれば、事故のときの連絡先と補償の条件を確かめます（8-2）。
2. VPN 機器やホームページの更新を業者に確かめます。初期のパスワードが残っていれば、気づいた日にすぐ変えます（8-4）。
3. 送金の指示は、今回の依頼とは別に知っている連絡先で本人に確かめる決まりを作ります（8-5）。
4. 取引銀行の法人向けのネットバンキングの補償の条件（上限・届け出の期限）を確かめ、振込の限度額を下げます（8-5）。
5. 業務ごとに、止まったときの代わりの方法を決めます。予約は、当日・翌日の一覧を毎朝印刷します（8-6）。
6. 6か条に取り組み、SECURITY ACTION の一つ星を宣言します（8-7）。

■ 共通

第9章　これからの見通し



第1〜8章の事実をもとに、これからの見通しを4つの時間軸で整理します。

9-1 予測の読み方

本書の予測は、本文の事実から本書が考えた推論です。予測（本書の推論）の札を付け、根拠にした章・節と、外れる条件を添えます。予定の制度（制度・公式情報）も、日付や中身が変わることがあります。

主要なセキュリティ企業による、信頼できる「2027年の予測」の資料は、本書の調査では見つかりませんでした（2026年10月22日時点）。全体は図9-1にまとめました。予測を待たずに、各章の「今日やること」を進めましょう（本書の推奨）。

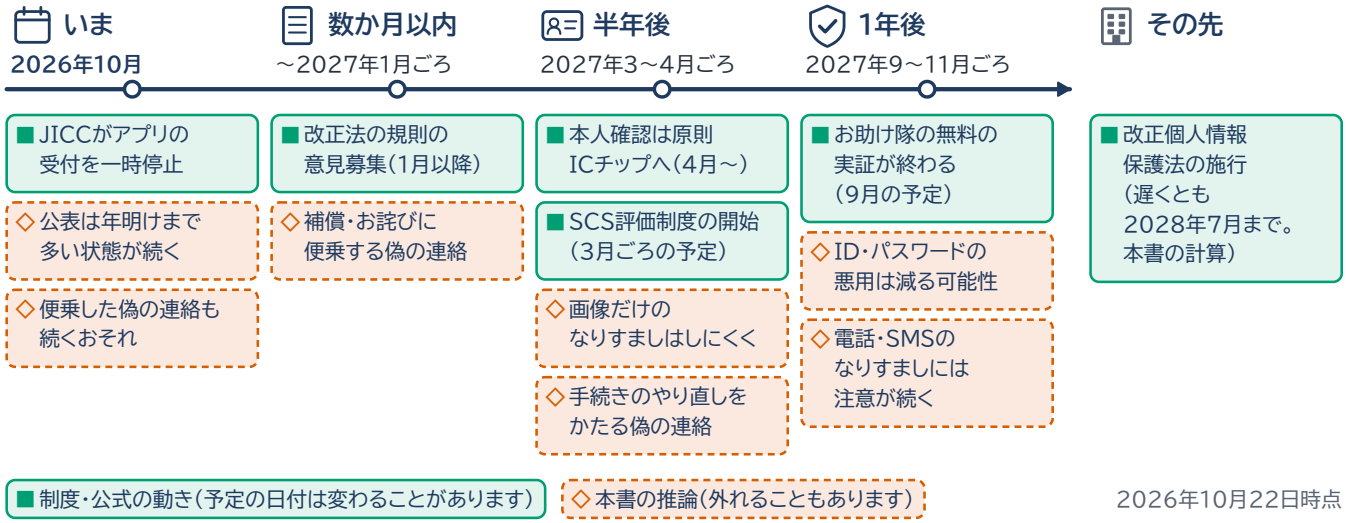


図9-1　これからの見通し（■は制度・公式の動き、◇は本書の推論）

9-2 いま進行中(2026年10月)

実際に起きた事例 9〜10月は、信用情報機関(ローンやクレジットの契約の情報を集める機関)への申込みが急増しました。本人申告(書類の紛失や漏えいを登録して、会員の会社へ注意をうながす手続き)や開示の申込みで、各機関が手続きの遅れなどを告知しました[1]。

制度・公式情報 JICC(日本信用情報機構)は10月22日、予防のためアプリでの受付などを一時停止しました。自社のシステムへの不正アクセス(許可なく他人のシステムに入ること)などは確認されていないとしています。再開は「準備が整い次第」知らせるとしていて、10月27日時点でも再開していません。手書きの申込書での郵送の受付は続いています[2]。

実際に起きた事例 大きな漏えいの公表も続いています。東京商工リサーチ(調査会社)は、上場企業とその子会社が公表した漏えい・紛失事故を集計しています。10月23日の集計では、1回で1,000万件以上のものが、2026年は10月23日までに8件(速報値)でした。2025年までの14年間では3件です[3]。メール配信サービス(企業が顧客にメールを送るためのサービス)の件(10月19日公表)では、10月26日の第二報で、漏えいは49システムで延べ51,628,280件とされました。件数を調べている最中のシステムが16あり、延べ件数は増える可能性があります[4]。

専門家の予測・懸念 トレンドマイクロ(セキュリティ企業)は、国内の組織が公表したサイバー攻撃の被害の件数を、独自に集計しています(第1章。10月9日時点のデータ)。同社は10月16日、例年は年の後半に公表件数が増えることが多く、2026年もこの増えるペースが年末まで続く可能性があるとしました。ランサムウェア(データを暗号化して身代金を求める不正なプログラム)の被害の公表は、10〜12月と翌年1〜3月に増える傾向がある、とも述べています[5]。

予測(本書の推論) 漏えいの公表は、年明けまで多い状態が続くと本書はみています。公表が続く間は、第3章で見たような、それに便乗した偽の連絡も続くおそれがあります。根拠: 第1章「数字で見る2026年」と、この節の東京商工リサーチの集計、トレンドマイクロの見方です。10月19日公表のメール配信サービスの件で、件数をまだ調べている最中のシステムがあることもふまえました。第8章で見た、PHP(Web サイトで広く使われるプログラムの言語)の深刻な脆弱性(ソフトや機器の弱点)への注意喚起(10月21〜22日)と、第3章「本物の情報を使った偽の連絡」もふまえました。外れる条件: 秋の集中が主に各社の調査や開示の時期の重なりによるなら(第1章)、早く落ち着く可能性があります。

何をすればよいか 個人は、通知が届いたら第5章の手順で確かめます。信用情報機関の手続きは、公式サイトで受付の状況を見てから申し込みます。会社は、第8章の対策を今月から始めます(本書の推奨)。

9-3 数か月以内(〜2027年1月ごろ)

実際に起きた事例 カーシェアの件(2026年9月公表)では、運営会社が10月23日の第5報で、外部の専門機関の調査が終わったと公表しました。運転免許証などの画像のデータのうち、外部へ送られた痕跡があったものは約146万件です。画像は暗号化して保管されていましたが、同社は、将来、暗号が解かれる可能性を完全には否定できないとしています。痕跡があった人には、お見舞いとして3,000円相当の現金または金券を渡すとしています(内容と渡し方は検討中)。持っている本人確認書類の画像は10月末までにすべて削除し、セキュリティなどの強化策は年内をめどに公表する予定です[6]。

制度・公式情報 個人情報保護委員会(個人情報の扱いを監督する国の機関)は、改正個人情報保護法の政令・規則の「基本的な考え方」をテーマごとに示しています。スケジュールのイメージでは、2027年1月以降に意見募集(パブリックコメント)を行います[7]。

予測(本書の推論) 補償やお詫び(お見舞いなど)の案内に便乗する偽の連絡が出るおそれがあると本書はみています。根拠: 第3章「本物の情報を使った偽の連絡」、第5章「お詫び・返金をかたる偽の連絡」と、この節のカーシェアの件の

お見舞いの公表(渡し方は検討中)です。外れる条件: 受け取りの手続きは公式のアプリやサイトの中だけで行うと広く知られれば、便乗した連絡は目立たない可能性があります。

何をすればよいか 個人は、お見舞いや補償、返金の案内も、リンクを開かず公式サイトで確かめます。会社は、年末年始も委員会への速報(まず出す報告)を出せるよう、担当を決めておきます(本書の推奨)。速報は、報告の対象になる漏えいなど(第8章 8-2)を知ってから、速やかに(目安はおおむね3〜5日以内)出します[8]。

9-4 半年後(2027年3〜4月ごろ)

制度・公式情報 第3章で見たように、2027年4月から、金融機関の非対面の本人確認は IC チップ(カードに埋め込まれた、情報を記録する部品)の読み取りに原則として一本化されます。携帯電話の対面の契約も、IC チップの読み取りが原則必須になります。金融庁(10月9日)と総務省(7月29日)は、施行を待たない対応を事業者に求めています[9,10]。総務省は、事業者からの本人確認の案内を装う詐欺のメール・SMS(携帯電話の番号あてに届く短いメッセージ)に注意を呼びかけています[11]。口座開設などで使える書類や、対面のときの方法は、第6章 6-9 で説明しています。

制度・公式情報 経済産業省などは、SCS評価制度(第8章)を2026年度末ごろに始めることをめざしています(IPA〔情報処理推進機構〕の表記では2027年3月ごろ)。取引先のセキュリティ対策を、共通の基準で「見える化」する制度です。評価の手引き(評価ガイド)は「2026年秋頃」に公表の予定とされ、2026年10月22日時点では IPA のサイトにまだ載っていません[12]。

制度・公式情報 個人情報保護委員会は10月7日、ガイドラインの「技術的安全管理措置」(個人データを守るための、システムの面の対策)の手法の例の見直し案を示しました。確定は2027年4月の予定です。見直し案には、社外からのアクセスや管理者の権限での多要素認証(パスワード・スマホ・指紋など、種類の違う確かめ方を2つ以上組み合わせる仕組み)が挙がっています。ログ(操作や通信の記録)の保管と定期的な分析、侵害を受けた機器の切り離しなども挙がっています。呼びかけの対象は、とくに大量の個人情報や機微な情報を持つ事業者です[13]。

予測(本書の推論) 本人確認書類の画像だけで、他人の名義の口座や携帯電話を作ることは、しにくくなると本書はみています。施行を待たずに切り替える会社もあるとみられ、切り替えの時期は会社ごとに違う可能性があります。その前後は、手続きのやり直しをかたる偽の連絡に注意が要ります。根拠: 第3章「本人確認書類を使ったなりすまし」と、この節の金融庁・総務省の要請と呼びかけ。外れる条件: IC チップのない書類などの「原則」の例外や、切り替えの済まない手続きが広く悪用されれば、画像だけのなりすましはしにくくならない可能性があります。



専門家

本人確認の手続きが切り替わる前後は、手続きのやり直しをかたる連絡に気をつけましょう。届いた連絡のリンクは使わず、契約している会社の公式サイトで確かめます(本書の推奨)。

何をすればよいか 個人は、本人確認の案内が届いたら、自分で開いた公式アプリやマイページで確かめます。会社は、本人確認書類の画像を集めているなら、法令で保存が求められていないか、業務に必要かを確かめてから、要らなくなった画像を消します。漏えいの調査中は、調査や証拠のために要る記録を先に残します。管理者のアカウントの多要素認証は、見直し案の確定を待たずに進めます(本書の推奨)。

9-5 1年後(2027年9〜11月ごろ)

制度・公式情報 中小企業向けの「サイバーセキュリティお助け隊サービス(新類型)」の、無料で参加できる実証事業は2027年9月まで(予定)で、実証期間のあとも使い続けるときは有償です。IPA は、実証事業の成果をふまえ、

2027年度以降の有償の試行運用に向けた検討を進めているとしています[14]。改正個人情報保護法の施行（実際に始まること）は、原則として公布（国が法律を広く知らせること）から2年以内（本書の計算で遅くとも2028年7月まで）です[7]。

制度・公式情報 施行後は、本人の権利利益の保護に欠けるおそれが少ない場合に、本人への通知の代わりに公表などで対応できるようになります（第7章）。その範囲は委員会の規則で決まり、報告・通知の細かい規則が決まるのは2027年以降の見込みです。衆議院の附帯決議（国会が法律に添えた要望）は、「恣意的な判断、濫用及び拡大解釈」で本人の権利利益が損なわれないよう、規則で範囲や判断の基準を明記するよう求めました[7]。

専門家の予測・懸念 Sophos（セキュリティ企業）の2026年の報告は、17か国の組織への調査（回答は2026年1～3月）をまとめたものです。報告は、最先端の AI（人工知能）が脆弱性を見つける速さと規模に注目しています。そのうえで、報告の時点から見た「今後1年」は、脆弱性を原因とするランサムウェア攻撃が増える可能性に注意するよう求めています[15]。Verizon（米国の通信会社）は、音声や SMS など、スマホを中心にしたなりすましが進化しているとしています[16]。トレンドマイクロは、攻撃者の AI の悪用を確認しつつ、「基本対策を行う重要性は変わらない」としています[5]。

実際に起きた事例 一方で、減っている被害もあります。カードの不正利用の被害額は、2025年は前年より8.0%減りました（第3章）。警察庁によると、2026年上半期のインターネットバンキングの不正送金の被害総額は約20億7,000万円で、前年同期より51%減りました。減ったのは被害総額で、件数ではありません。だまされて自分で振り込む詐欺とは別の集計です[17]。ただし、法人の口座をねらう新しい手口は2026年5月に急増しました（第8章）。

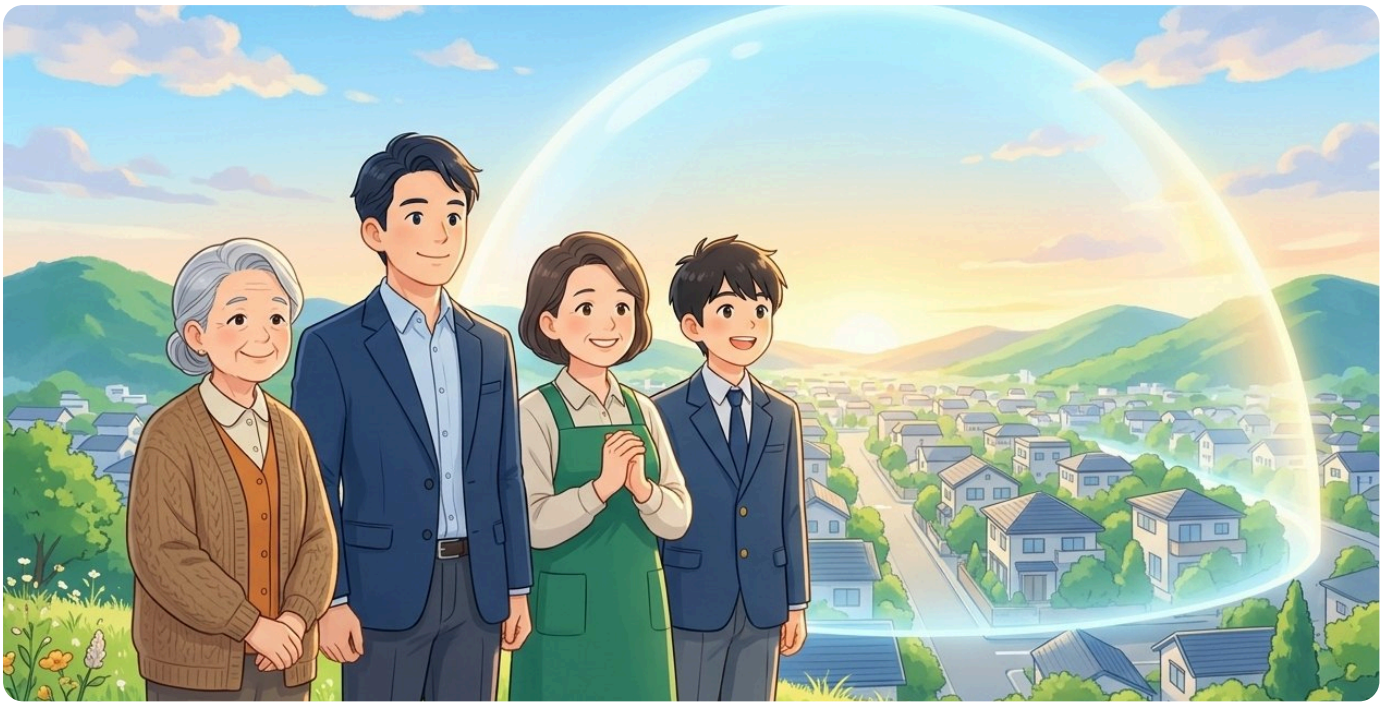
実際に起きた事例 FIDO アライアンス（業界団体）の2026年の調査は、日本を含む10か国の消費者11,000人などが対象です。パスキー（パスワードの代わりに、スマホなどの機器と指紋・顔・PIN〔暗証番号〕で本人を確かめる仕組み）を少なくとも1つのアカウントで設定した人は75%、日常的に使っている人は49%でした。日本だけの数値は示されていません[18]。

予測（本書の推論） パスキーなどの強い認証が広がり、盗まれた ID・パスワードによる被害は減っていく可能性があると本書はみています。一方で、電話や SMS を使ったなりすましへの注意は、1年後も欠かせないとみています。根拠: 第4章「パスキー・2段階認証を使う」、第3章「数字で見る詐欺の被害」、この節の専門家の見方と FIDO アライアンスの調査です。第4章の証券口座への不正アクセスの件数の推移は暫定値で、金融庁は必須化との関係を述べていません。外れる条件: 強い認証を設定する人やサービスが増えなかったり、確認コードや認証の操作をだまし取る手口に攻撃が移ったりすれば、被害は減らない可能性があります。

何をすればよいか 個人は、大事なサービスからパスキーや2段階認証（パスワードのほかに、確認コードなどでも本人かを確かめる仕組み）を設定します（第4章）。通知が来なくても、使っているサービスのお知らせを確かめる習慣をつけます（第5章）。会社は、無料の支援を使えるうちに、VPN 機器（社外から社内のネットワークにつなぐための機器）の更新と、管理者のアカウントの多要素認証を済ませます（本書の推奨）。

■ 共通

第10章　本書の見解



第1～9章の事実をふまえた、株式会社アルファテックとしての意見です。事実には根拠の章を示し、意見と分けます。

「漏れる前提」で守る

本書の見解 第2章で見たように、委託先（仕事を任された会社）や共通の仕組みへの不正アクセス（許可なく他人のシステムに入ること）は、多くの会社の利用者に広がります。利用者がどれだけ気をつけても、預けた先からの漏えいは防げません。本書は、「漏れないように」だけでなく、「漏れても被害にならないように」備えることが大切だと考えます。個人にとっての柱は、パスワードを使い回さないこと、強い認証、利用通知の3つです（第4章）。

制度・公式情報 個人情報保護委員会（個人情報の扱いを監督する国の機関）は10月7日の注意喚起で、要らなくなった個人データを遅滞なく消すよう（法律上は努力義務）、あらためて求めました[1]。

本書の見解 カーシェアの件では、本人確認書類の画像をすぐ削除するルールに改めました。焼肉チェーンの公式アプリの件では、氏名と電話番号を持たない仕組みへの切り替えを予定しています（第2章）。持っていない情報は漏れません。本書は、会社にとっての近道は「持たない・残さない」ことだと考えます。

強い認証に効果の兆し

本書の見解 証券会社などでは、偽のサイトにだまされても破られにくい認証の必須化が進められています。パスキー（パスワードの代わりに、スマホなどの機器と指紋・顔・PIN〔暗証番号〕で本人を確かめる仕組み）などです。金融庁は2026年2月、銀行などにも初期設定で必須にするよう求めました（第4章）。証券口座への不正アクセスの件数も、第4章で見たように大きく下がっています（暫定値。金融庁は必須化との関係を述べていません）。それでも本書は、強い認証が効いている兆しとみています。パスキーは、パスワードが漏れても、それだけでは入られにくくする備えです。

被害者の手間と費用

本書の見解 本人確認書類の画像が漏れると、身を守るための手続きは、本人が自分で選んで進めることになります。必要に応じて、信用情報機関（ローンやクレジットの契約の情報を集める機関）への本人申告（書類の紛失や漏えいを登録して、会員の会社へ注意をうながす手続き）や開示、運転免許証の再交付をします。本人申告には手数料がかかり、額は機関や申し込みの方法ごとに違います（第6章）。窓口も混み合いました（第9章）。本人申告は、審査の判断を縛るものではないとされています（第6章）。漏えいの原因を作っていない人が、この費用と手間を負うのは、重い負担だと本書は考えます。

制度・公式情報 米国では、消費者は信用情報を無料で凍結できます。米国連邦取引委員会の説明では、凍結の間は、本人を含めて誰も、その人の名義で新しい与信（ローンやカードなど）の口座を開けません。新しく申し込むときなどは、一時的に解除できます[2]。

本書の見解 そのため、漏えいした会社が手数料の負担や手続きの案内をすること、日本でも無料で使える凍結のような仕組みを検討することを期待します。

本人確認は画像から IC チップへ

本書の見解 2027年4月から、金融機関の非対面の本人確認では、書類の画像を送る方式が廃止されます。IC チップ（カードに埋め込まれた、情報を記録する部品）の読み取りに原則として一本化されます。携帯電話の対面の契約でも、2027年4月以降は IC チップの読み取りが原則必須になります（第3章・第6章・第9章）。漏れた画像は取り戻せず、本人は申告や再交付の手間を負います（第6章）。本書は、書類の画像に頼る確かめ方から離れるこの切り替えを、漏れた画像が悪用される余地を小さくする方向として歓迎します。

本書の見解 ただし、確かめ方が変わるだけでは、会社が集めて残す情報が減るとは限りません。集める情報を必要なものに絞り、要らなくなった画像を消す取り組みは、切り替えとは別に要ると本書は考えます。

本書の見解 金融庁と総務省は、施行を待たない対応も事業者に求めています（第9章）。本書も、事業者が早めに切り替えることを期待します。切り替えの前後は、手続きのやり直しをかたる偽の連絡が出るおそれがあります（第9章）。事業者には、本人確認の案内をどこから、どんな方法で送るのかを、前もってはっきり示してほしいと考えます。IC チップのない書類を使う例外の手続きが、なりすましの抜け道にならないよう、丁寧な確認も求められます。

救済の仕組みの限界

本書の見解 改正法の課徴金は国に納めるもので、漏えいが起きたことだけでは対象になりません。団体が差止め（やめさせること）や被害の回復を求める制度も、改正法に入りませんでした。本書が紹介した、2014年に発覚した通信教育会社の件の判決は、1人2,000円や3,300円でした（いずれも第7章）。本書は、被害者が手間に見合う救済を受けにくいのが現状だと考えます。附帯決議（国会が法律に添えた要望）が求める、団体による制度の検討が進むことを期待します。そのうえで個人には、救済を待つより、被害を防ぐ備えを先にすることを勧めます。

会社に求めたいこと

本書の見解 本書は、漏えいが起きた会社に3つのことを求めます。1つ目は、分かっていること・分かっていないこと・お願い・窓口を分けて早く知らせ、続報を出すことです（第8章 8-2。早めに知らせた例は 8-3 の、鉄道会社の問い合わせフォームの件）。2つ目は、本人申告などの手続きを案内し、被害者の手間を減らすことです。3つ目は、委託先を含めて「持たない・残さない」を進めることです。漏えいはどの会社にも起こりうるからこそ、起きたあとの対応が信頼を決めると考えます。

本書の見解 10月には、PHP（Web サイトで広く使われるプログラムの言語）の深刻な脆弱性（ソフトや機器の弱点）が公表されました。このとき、被害が確認されていない段階で、予防のためにサービスを止めた会社もありました（第2章）。利用者には一時の不便になりますが、本書は、こうした予防の判断と、その理由をすぐに説明することも、信頼につながると考えます。

今日やること

個人

1. メールと銀行のパスワードを、ほかと違うものにします（第4章）。
2. よく使うサービスを1つ選び、パスキーか2段階認証（パスワードのほかに、確認コードなどでも本人かを確かめる仕組み）を設定します（第4章）。
3. カードの利用通知を有効にします（第4章）。
4. 漏えいの通知が届いていたら、第5・6章の手順で確かめます。

会社

1. 持っている個人情報を棚卸しし、法令で保存が求められていないか、業務に必要かを確かめてから、要らなくなったものを消します。漏えいの調査中は、調査や証拠のために要る記録を先に残します（第8章）。
2. VPN 機器（社外から社内のネットワークにつなぐための機器）の更新を確かめます。管理者のアカウントには、多要素認証（パスワード・スマホ・指紋など、種類の違う確かめ方を2つ以上組み合わせる仕組み）をかけます（第8章）。
3. 漏えいのときの責任者・担当者と、記録用紙を決めておきます（第8章）。
4. 送金の指示は、メールだけで進めない決まりを作ります。メールに書かれた番号ではなく、前から知っている連絡先や自分で調べた番号で、本人に確かめます（第8章）。

付録

付録A　個人のチェックリスト

印刷して使えます。確かめるのは、自分のアカウントと自分の情報に限ります。付録では用語の説明を（ ）で付けず、付録Dの用語集にまとめています。各項目の終わりの（ ）は、くわしく説明した章・節です。「ふだんの備え」の「 」は、とくに断りがなければ第4章の節の名前です。

ふだんの備え（第4章・第6章）

パスワードと会員サービス

☐ 大事なサービスから順に、パスワードをサービスごとに別のものに変えます。最初に変えるのはメールです（「パスワードを使い回さない」）。

☐ パスワードはブラウザに保存せず、パスワードマネージャーか紙のノートに控えます。メールやスマホのメモ・写真には残しません（「パスワードを安全に保管する」）。

☐ パスキーが選べるならパスキーを、選べなければ2段階認証を使います。確認コードは、誰にも教えません（「パスキー・2段階認証を使う」）。

☐ 使っていないサービスは、カード情報など消せる情報を消してから退会します（「渡す情報・残す情報を減らす」）。

連絡・電話

☐ 連絡のリンクは押さず、ふだん使っている公式アプリや、登録済みの公式サイトから確かめます（「連絡のリンクを開かない」）。

☐ 知らない番号には出ず、留守番電話で用件を聞きます。かけ直すときは、公式サイトなどで自分で調べた番号にかけます（「電話・SMS の詐欺に備える」）。

☐ 国際電話を使わないなら、固定電話・ひかり電話の発信と着信の休止を申し込みます（同。申し込み先は付録C）。

カード・口座・支払い

☐ カードの利用通知を有効にし、明細を確かめます（「カード・口座の通知を受け取る」）。

☐ ネットバンキングは、振込の上限額をふだん必要な額まで下げ、ログインや送金の通知を有効にします。入出金明細もこまめに確かめます。補償の届け出には期限があるので、早く気づけるようにします（同・6-7・第7章）。

☐ ふだんのカードのほかに、もう1つ支払いの手段と、少しの現金（小銭を含む）を持っておきます（「支払いの手段を1つに頼らない」）。

☐ カードで払っている継続払いの登録先を、一覧にしておきます。カードの番号が変わったとき、登録を変える先がすぐ分かります（同・6-4）。

スマホ

☐ 2段階認証のバックアップ コードを印刷し、大事な書類と同じ場所にしまいます。本人の確かめ方は2つ以上登録します（「予備のコードとバックアップ」）。

☐ パソコンのバックアップは、記憶装置をバックアップのときだけつなぎ、2つ以上の記憶装置にそれぞれ取ります（第4章「予備のコードとバックアップ」）。

☐ 写真や連絡先の自動のバックアップを有効にします。カード会社・銀行・携帯電話会社の連絡先は紙にも控えます（同）。

☐ スマホの機種を変えるときは、古いスマホを手放す前に、認証のアプリの引き継ぎとパスキーの登録を済ませます（同）。

☐ スマホやパソコンの OS やブラウザに更新の知らせが来たら、早めに更新します。iPhone は「自動アップデート」と「バックグラウンドでのセキュリティ改善」の「自動インストール」をオンにし、Android は「ソフトウェア アップデート」の画面で更新を確かめます（「連絡のリンクを開かない」「更新を自動にする」）。

☐ 画面ロックを有効にし、ロックまでの時間を短めにします。「探す」（Android は Find Hub）がオンかを確かめ、iPhone は「盗難デバイスの保護」もオンにします（「なくしたときに備える」）。

☐ 更新の期間が終わったら、買い替えを計画します。古いスマホは、スマホに入れたマイナンバーカードを先に削除し、そのあとログアウトして初期化してから手放します（「更新が終わったスマホ」）。

☐ 家族で安否確認の方法と集合場所を決め、災害用伝言ダイヤル（171）を、毎月1日・15日などの体験利用日に試します（「通信が止まったとき」）。

家族

☐ 家族と「責めない約束」をし、メッセージでお金や確認コードを頼まれたら、電話か対面で本人に確かめると決めておきます（「家族で決めておくこと」）。

☐ 離れて暮らす家族とは、本人かを確かめる「合言葉」を決めておきます（「電話・SMS の詐欺に備える」）。

☐ 子どもや家族の写真を SNS などに載せるかどうかを、家族で決めておきます（「家族で決めておくこと」）。

☐ 相談先（188、＃9110 など）を、家族の電話番号と一緒に紙に控えます（同）。

本人確認書類

☐ 運転免許証の2つの暗証番号と、マイナンバーカードの暗証番号・パスワードを覚えているか確かめます。控えは、免許証やカードと一緒に持ち歩きません（6-6・6-9）。

☐ 顔写真つきの本人確認書類を2種類持つことを考えます（6-9「確かめる手段を複数持つ」）。

通知が届いたら・被害にあったら（第5～7章）

通知が届く前に気づいたら

☐ 身に覚えのない請求や引き落とし、自分ではしていないログインやパスワード変更の通知に気づいたら、漏えいの通知を待たずに動きます（第5章「通知が届く前に気づいたら」）。

☐ サービスの会社（カード会社・銀行も）にすぐ連絡し、パスワードを変え、ログインの履歴の画面を残して、警察に相談します。記録を集めるために、連絡を遅らせません（同）。

通知が届いたら（第5章）

☐ 本物か確かめる（リンクは開かず、公式サイトで）

☐ 漏れた項目を読む（「漏れた項目」と「二次被害のおそれ」）。項目ごとの手順は第6章

☐ すぐに守る（パスワードを変え、明細を見る）

☐ 記録を残す（通知・領収書・相談の記録）

☐ 続報を確かめる（項目が増えることも）

☐ 最初のお知らせで対象外とされても、続報を確かめます（第5章）。

☐ 攻撃者が公開したとされる情報には、アクセスしたり広めたりしません（6-5）。

☐ 役所・学校・病院から届いたら、通知を出した機関と運営する主体、その機関の個人情報の問い合わせの窓口を確かめます。電話で知らされたら、書面かメールでも送ってもらいます（第5章「役所・学校・病院から届いたとき」）。

脅しや「削除」の持ちかけ

☐ 漏れたパスワードを示して脅すメールには、お金を払わず、返信もしません。書かれたパスワードをいまも使っていれば変え、2段階認証かパスキーを設定します（第5章「パスワードを示して脅すメール」）。

☐ 画像が本物か、心当たりがあるかにかかわらず、私的な画像を示された、脅しが続く、不安が消えないときは、早めに警察に相談します。性的な画像の被害や脅しは、＃8103 に匿名でも相談できます（同）。

☐ 写真や家族のことを持ち出して脅されたら、払わず、返信もせず、記録を残して警察に相談します。攻撃者が公開したとされる場所は、自分では開きません（第5章「写真や家族のことを持ち出して脅されたとき」）。

☐ 「漏れた個人情報を消してあげる」という連絡には応じず、188 に相談します（第5章「『消してあげる』という持ちかけ」）。

アカウント・スマホ・パソコンの被害

☐ メールのアカウントが乗っ取られたら、パスワードを変えます。自分で設定していない転送・振り分け・IMAP や POP の設定、再設定用の電話番号とメールアドレス、ログインしている端末を確かめます（6-1「メールのアカウントが乗っ取られたとき」）。

☐ SNS・メッセージアプリが乗っ取られたら、取り戻す手続きと並行して、電話や対面など別の方法で家族や友人に知らせます（6-5「SNS・メッセージアプリが乗っ取られたとき」）。

☐ スマホをなくしたら、別の機器から「探す」か Find Hub でロックし、位置を確かめます。見つからなければ回線を止めて警察に届け、マイナンバーカードの機能やスマホの決済も止めます。消去は最後の手段です（6-5「スマホをなくしたとき」・6-4）。

☐ Android のスマホに不正なアプリを入れてしまったら、まず機内モードにし、Wi-Fi も切って通信を止めます。続きは6-5「スマホに不正なアプリを入れてしまったとき」の手順で進めます。

☐ パソコンにお金を求める画面が出た・ファイルが開けないときは、ネットワークから切り離し（電源は切らない）、外部の記憶装置も外して画面を残します。身代金は払わず、警察に相談します。初期化は、調査に要る記録の扱いを確かめてからです。バックアップで戻すときは、記憶装置を検査してから開き、安全か迷うときは使う前に相談します（6-5「パソコンがランサムウェアに感染したおそれがあるとき」）。

お金の被害

☐ カードや口座の不正な利用は、まずカード会社や銀行に連絡します（第7章「相談窓口」）。

☐ 身に覚えのない送金に気づいたら、直ちに取引銀行の緊急の連絡先に電話し、続けて警察に相談します。不正なアプリなどを入れたおそれがあれば、先にその端末の通信を止め、別の電話からかけます。記録を残して事実どおりに説明し、端末は初期化する前に銀行と警察に相談します（6-7「身に覚えのない送金に気づいたら」）。

☐ だまされて自分で振り込んだときは、振り込んだ先の口座がある銀行と警察に直ちに連絡し、振り込みを頼んだ自分の銀行にも相談します（6-7・第7章「だまされて自分で振り込んだとき」）。

☐ 詐欺・なりすましの被害は最寄りの警察署へ。まだ被害はないが不安なときは ＃9110 に相談します（第7章「相談窓口」）。

本人確認書類・写真

☐ 本人確認書類の画像が漏れた、または漏れたおそれがあるときは、信用情報機関への本人申告を考えます（6-9）。

☐ 写真や住所がネットに出たら、画面を保存します。性的な画像で脅されたり出回ったりしたら、削除の結果を待たずに警察（＃8103）に相談します。削除は、載っているサイトや SNS の申出の窓口に依頼し、難しいときは法務局に相談します（6-9「写真や住所がネットに出たとき」）。

その後も続けること

☐ カードの明細と口座の入出金を少なくとも毎月(漏えいの直後はもっとこまめに)確かめます。口座の補償は、被害から30日を過ぎて知らせると受けられないことがあるので(6-7)、入出金の通知も有効にします。そのうえで、漏えいした会社の続報を見て、相談や手続きの記録をとっておきます(第5章「その後、何を確かめ続けるか」)。

☐ 自分のことを知っているような電話・メール・SMS が届いても、届いたリンクや番号は使わず、公式の窓口で確かめます(同)。

制度・公式情報 漏えいを調べるサービスの一つ、Have I Been Pwned(海外)は、収録している記録は漏えいしたすべての記録の「一部にすぎない」と説明しています。調べるのは自分のメールアドレスだけにし、見つからなくても安心せず、会社からの通知や公表を優先します(本書の推奨)。

付録B　会社のチェックリスト

漏えいが起きたら(8-2・8-3)

☐ 日時を記録し、社内の責任者に知らせます。被害が広がりそうな機器は、ネットから切り離します(不用意に電源を切らない)。

☐ 不正アクセス・ランサムウェアは、報告を待たずに警察・IPA に相談します。

☐ ランサムウェアのときは、まだ無事なバックアップを切り離して守ります。ログを保存して侵入の時期と経路を調べ、経路に対処してから、安全を確かめたバックアップで戻します(8-2)。

☐ 漏れた情報の種類・件数・暗号化の有無と本人の人数を確かめ、委員会への報告と本人への通知の対象かを確かめます。迷うときは個人情報保護法相談ダイヤルに聞きます(8-2「報告・通知の対象かを確かめる」)。

☐ 対象に当たるときは、個人情報保護委員会へ、速報を速やかに(目安3〜5日以内)、確報を30日以内(不正の目的のおそれは60日以内)に出します[1]。

☐ 対象に当たるときは、本人に5つの事項を通知します(連絡がつかない人には公表・窓口)。

☐ お知らせを出す前に、専用の問い合わせ窓口を決め、答え方を社内の全員でそろえます(8-2「お客様への説明と、その後」)。

☐ お客様へのお知らせは、「分かっていること」「まだ分かっていないこと」「お客様へのお願い」「問い合わせの窓口」「次のお知らせ」の欄に分け、調べている途中でも、分かった範囲で早めに出します。続報は予定の時期に出し、最終報で調査の結果と再発防止策を知らせます(同)。

☐ 会社のメールや SNS の公式アカウントが乗っ取られたら、乗っ取られていない手段でお客様や取引先に知らせます。会社のメールなら、取引先へはメール以外の方法で連絡し、転送や振り分けの設定を確かめます(8-2「会社のメールや SNS の公式アカウントが乗っ取られたら」)。

☐ 委託先から連絡が来たら、委託先の報告を待たずに速報の準備を始めます(8-3)。

ふだんの対策(8-2〜8-4)

☐ 社内の責任者と報告の担当者を決め、記録用紙も用意しておきます(8-2)。

☐ サイバー保険に入っていれば、事故のときに連絡する先と補償の条件を、事故の前に確かめます(8-2)。

☐ 外部に公開しているアプリ、使っている外部のサービス、持っているデータを点検します。自分で点検できないものは、制作会社や機器を入れた業者に頼みます(8-4「すぐに点検する」)。

☐ VPN 機器を更新し、ホームページや予約・通販のシステムの対応を制作会社などに確かめます。初期のパスワードも変えます。

☐ 使っている外部のサービス（SNS の公式アカウントを含む）を洗い出し、退職した人のアカウントを消します。身に覚えのないアカウントは消さずに止め、記録を残して業者に調べてもらいます（8-4）。管理者のアカウントから多要素認証を有効にします。

☐ SNS の公式アカウントは、ログインできる人と、登録したメールアドレス・電話番号を控えておきます。

☐ バックアップは「3-2-1ルール」で取り、戻せるかを定期的に確かめます。

☐ 法令で保存が求められていないか、業務に必要かを確かめてから、要らなくなった個人情報を消します。

☐ 一斉送信は BCC かメール配信のサービスを使います。

☐ 委託の契約で、漏えいのときの報告の義務、業務が終わったらデータを消させること、事故のときの連絡先と手順を確かめます（8-3）。

送金をねらう詐欺に備える（8-5）

☐ 送金の指示は、メールだけで進めず、あらかじめ登録してある連絡先など、今回の依頼とは別に知っている連絡先で本人に確かめます。メールに書かれた番号や返信先は使いません。

☐ 法人向けネットバンキングの補償の有無・上限・届け出の期限を、被害の前に取引銀行の規定で確かめます（8-5「会社の口座の補償は銀行ごとに違う」）。

☐ 申請と承認を別の人・別の端末にし、振込の限度額を必要な範囲まで下げて、取引の通知メールを確かめます（同）。

☐ 取引銀行の法人向けの緊急の連絡先を控えておきます。身に覚えのない送金に気づいたら、直ちに銀行と警察に連絡します（8-5「送金の被害に気づいたら」）。

Web のシステムが止まったときに備える（8-6）

☐ 業務ごとに、止まったときの代わりの方法を決めておきます。予約は、当日・翌日の一覧を毎朝印刷します（8-6「ふだんの備え」）。

☐ お客様への知らせ方を、ホームページのほかに、店頭の掲示・電話・SNS と複数決めておきます（同）。

☐ 止まったら、サービス会社の公式のお知らせで、止まった機能と理由を確かめます。パスワードの変更などの指示も、公式のお知らせで確かめてから従います（8-6「止まったとき」）。

☐ 戻ったら、紙の記録とシステムの予約・売上・入金を突き合わせ、二重の予約・二重の請求・入力の漏れを探します（8-6「復旧したとき」）。

付録C　相談窓口の一覧

困りごとで使い分けます。カードや口座の不正な利用は、まずカード会社や銀行に連絡します。だまされて振り込んだときは、振込先の銀行と警察に連絡し、振り込みを頼んだ自分の銀行にも相談します（第7章「相談窓口」。本書の推奨）。

個人向け

困りごとの窓口（第7章の表の順）

困りごと	窓口・電話番号・受付時間
カード・口座の 不正な利用	**カード会社**（カードの裏面の番号） **取引している銀行・証券会社** （キャッシュカードの裏面や公式サイトで確かめた番号） だまされて振り込んだときは、 **振り込んだ先の口座がある銀行**と警察。 振り込みを頼んだ自分の銀行にも相談[2]
契約・請求・ 勧誘のトラブル	**消費者ホットライン**　188 近くの消費生活センターなどへ。受付時間はつながる窓口で異なる
まだ被害はないが 不安	**警察相談専用電話**　#9110（受付時間は都道府県で異なる）
詐欺・なりすまし の被害	**警察署、警察庁のオンライン受付** 被害届は最寄りの警察署へ。緊急は110番
会社や役所などの 個人情報の扱い への苦情・疑問	**個人情報保護法相談ダイヤル**（個人情報保護委員会） 03-6457-9849（9時30分～17時30分、土日祝日・年末年始を除く）
パスワードや 端末の相談	**IPA 情報セキュリティ安心相談窓口**　03-5978-7509 10時～17時（土日祝日・年末年始を除く）
法律の相談先や 制度を知りたい	**法テラス・サポートダイヤル**　0570-078374 （IP 電話は 03-6745-5600） 平日9時～21時、土曜日9時～17時（祝日・年末年始を除く） 犯罪の被害にあった人は **犯罪被害者支援ダイヤル**[3]　0120-079714 受付時間は法テラスの公式サイトで確かめてください
弁護士に 相談したい	**日弁連「ひまわりお悩み110番」**[4]　0570-783-110 近くの弁護士会の法律相談センターで面談を予約 ネット予約は停止中（10月23日時点）
身の危険を感じる	**最寄りの警察署**　緊急は110番 支援措置は、住んでいる市区町村の窓口（6-3）
性的な画像の 被害・脅し	**性犯罪被害相談電話**　#8103（ハートさん） かけた地域の都道府県警察の窓口につながる 匿名でもよい。緊急は110番
ネット上の 人権侵害	**法務省「みんなの人権110番」**　0570-003-110 平日8時30分～17時15分。最寄りの法務局につながる ネットでは「インターネット人権相談受付窓口」から
削除の方法を 相談したい	**違法・有害情報相談センター**（総務省の支援事業）[5] ウェブのフォームからだけ 大手の SNS などの削除の申出の窓口は、 総務省のページに一覧

困りごと	窓口・電話番号・受付時間
国の行政機関への苦情	**総務省「行政苦情110番」** 0570-090110 平日9時～16時45分。メールやオンラインでも相談できる

種類別の窓口（第6章・第4章ほか）

困りごと	窓口・電話番号・受付時間
偽のメール・サイトの報告	**フィッシング対策協議会**[6] メール info@antiphishing.jp か Web のフォーム
固定電話・ひかり電話の国際電話の休止（無償）	**国際電話不取扱受付センター**[7] 0120-210-364（通話料無料） オペレーターは平日9時～17時、自動音声は24時間 **NTT東日本** 0120-325-263、**NTT西日本** 0120-931-965[8] 9時～17時（土日と12月29日～1月3日を除く）
カード会社と話が進まない	**日本クレジット協会 消費者相談室** 03-5645-3361 月～金曜日の10時～12時と13時～16時（祝日・年末年始を除く）
ビューカード（Suica・定期券つき）	**紛失・盗難デスク** 03-6685-4800（24時間・年中無休） **再発行受付デスク** 03-6685-5851 **ご利用覚えなし相談デスク** 03-6685-5861 どちらも9時～17時30分
スマホの決済を止める・覚えのない利用	**PayPay 携帯電話紛失・盗難専用窓口** 0120-990-633 24時間受付、土日祝日を含む365日 **楽天ペイ** なくしたら利用停止の申請フォームで申請 楽天ポイント・楽天ペイ残高・楽天銀行口座の覚えのない利用は、楽天ペイ カスタマーデスク 0570-000-348（9時30分～23時） **d払いお問い合わせダイヤル**[9] ドコモの携帯から #9785（無料） ほかから 0570-018-360（有料） ドコモの回線を契約している人の利用停止は24時間受付 番号は、アプリや公式サイトでも確かめる
SNS・メッセージアプリの乗っ取り	**運営者の公式の問い合わせフォーム** LINE は本人からだけ受け付ける （家族などの代理は原則として受け付けない）
マイナンバーカード・スマホをなくした	**マイナンバー総合フリーダイヤル** 0120-95-0178 の2番 カードの一時利用停止は24時間365日。ほかの用件は第6章の表 番号の変更の相談は、住んでいる市区町村の窓口（6-6）
銀行との取引の相談・苦情	**全国銀行協会相談室**[10] 0570-017109 または 03-5252-3772 月～金曜日の9時～17時（祝日・銀行の休業日を除く）
金融サービスの相談	**金融庁 金融サービス利用者相談室**[11] 0570-016811 IP 電話からは 03-5251-6811。平日10時～17時
パスポートをなくした・盗まれた	**警察署**に届けたうえで、**都道府県のパスポートの申請窓口**へ[12] 紛失届はマイナポータルでもできる

困りごと	窓口・電話番号・受付時間
運転免許証の 再交付・ 暗証番号	**住所地の都道府県警察**（運転免許センター・警察署など）[13]
本人申告などの 問い合わせ （信用情報機関）	**KSC**　0120-540-558（携帯電話などは 03-3214-5020） 月～金曜日の9時～12時と13時～17時 **CIC**　0570-666-414 オペレーターは平日の10時～16時（土日祝日・年末年始を除く） **JICC**　0570-055-955（通話料がかかる） 月～金曜日の10時～16時（祝日・年末年始を除く）
スマホをなくした （回線の停止）	**契約している携帯電話会社の紛失の窓口** 例: au は Web か電話で24時間365日、 ソフトバンクは24時間受け付ける （本人が連絡できないときは家族からの電話も） 番号は公式サイトで調べ、紙に控えておく
災害で電話が つながりにくい	**災害用伝言ダイヤル** 171（声の伝言） **災害用伝言板（web171）**[14] 前もっての登録は要らない 体験利用日は毎月1日・15日など

会社向け

困りごと	窓口・電話番号・受付時間
被害の可能性 への助言、 応急処置の案	**IPA 不正アクセス特別相談窓口**（事業者向け・臨時）[15] 03-6759-5760 （平日9時30分～17時30分、12時～13時を除く） メール incident-support@ipa.go.jp
漏えい等の報告	**個人情報保護委員会「漏えい等の対応とお役立ち資料」**[1] 原則としてオンラインのフォーム マイナンバーを含むかどうかで報告先が分かれる 報告の対象か迷うときは、 個人情報保護法相談ダイヤル（個人向けの表）
サイバー事案の 通報・相談、 被害届	**警察** 警察庁の全国統一のオンライン受付窓口、最寄りの警察署
会社の口座の 不正な送金	**取引銀行**の法人向けの窓口・緊急の連絡先（ふだんから控えておく） だまされて振り込んだときも、取引銀行（組み戻しの依頼）と、 **振り込んだ先の口座がある銀行**に直ちに。続けて警察[2]
中小企業向けの 相談・監視の サービス	**サイバーセキュリティお助け隊サービス**（民間の事業者のサービス）[16] IPA の利用者向けのサイトで、地域や監視の種類から探せる

番号・受付時間は2026年10月22～23日時点です。かける前に公式サイトで確かめてください。188 の相談は無料ですが、窓口につながると通話料がかかります。

付録D　用語集

本文で（ ）内や文の中で説明した主な用語です。英字の語を先に、そのあとは50音順です。

用語	意味
3D セキュア	ネットの買い物のときに、カード会社がもう一度本人かを確かめる仕組み
AI	人工知能
API	ソフト同士がやりとりする窓口
BCC	ほかの受信者にアドレスが見えない欄
BI ツール	データを集計・分析する業務ソフト
CTO	技術の責任者
DM	ほかの人には見えない個別のメッセージ
DV	配偶者などからの暴力
FAQ	よくある質問
Find Hub	Google の、端末を探す機能。以前の名前は「デバイスを探す」
IC チップ	カードに埋め込まれた、情報を記録する部品
ID	ログインに使う名前
IMAP・POP	ほかのメールソフトでメールを読むための設定
IP 電話	インターネットを使う電話
IPA	情報処理推進機構
ISP	インターネット接続事業者
JPCERT/CC	国内のセキュリティの事故の情報を集め、対応を調整する組織
OS	スマホやパソコンの基本のソフト
PHP	Web サイトで広く使われるプログラムの言語
PIN	暗証番号
RaaS	ランサムウェアを、攻撃に必要な道具や場所ごと貸し出す犯罪の分業
SIM・USIM カード	スマホなどで通信するためのカード
SMS	携帯電話の番号あてに届く短いメッセージ
SNS	X・Instagram・Facebook など、人とつながって投稿や連絡をするサービス
VPN 機器	社外から社内のネットワークにつなぐための機器
あっせん	個人情報保護委員会が間に入って、歩み寄りを促すこと
暗号化	決まった鍵がないと読めない形に、データを変えること
慰謝料	心の苦痛への賠償
委託先・委託元	委託先は、仕事を任された会社。個人データの扱いを任せる側を委託元、任される側を委託先ともいいます

用語	意味
位置情報（画像の）	撮った場所の情報
インシデント	事故
ウェブメール	インターネットのサイトで読み書きするメール
ウォレット	カードを登録して、スマホで払う機能
遠隔操作	離れた所から端末を操作すること
オートチャージ	残高が減ると、登録したカードから自動で入金する機能
ガイドライン（個人情報保護委員会の）	法律の運用の手引き
確認コード	ログインなどのときに SMS などで届く確認用の番号。LINE では「認証番号」
過失	注意を怠ったこと
課徴金	違反で得た利益などに相当する額を国に納めさせる仕組み
機内モード	スマホの通信をまとめて止める設定
キャッシュレス決済	現金を使わない支払い
キャリア決済	買い物の代金を携帯電話の料金と一緒に払う仕組み
行政相談	担当の機関とは別の立場で、行政への苦情や要望を受ける仕組み
共通ショートコード	携帯電話会社が企業ごとに審査して出す、SMS の送信元の番号（「0005」で始まる）
組み戻し	振り込みを取り消してもらう手続き
クラウド	ネット上で使うソフトや保存場所
継続払い	公共料金・携帯電話料金・定額のサービスなどの決まった支払い
原告	訴えた側
公布・施行	公布は国が法律を広く知らせること、施行は実際に始まること
コード決済	スマホの画面のバーコードなどで払う決済
誤交付・誤送付	誤交付は書類などを別の人に渡すこと、誤送付は別の宛先に送ること
国際ブランド	Visa・JCB など、カードの支払いの仕組みの名前
個人情報保護委員会	個人情報の扱いを監督する国の機関
個人データ	会社などが、名簿やデータベースのように探しやすく整理して持っている個人情報（個人情報保護法の言葉）
サイバー保険	サイバー攻撃などの事故による損害に備える保険
差し替え（カードの）	カードの番号を変える再発行
差止め	やめさせること
サプライチェーン	委託先や取引先のつながり
サポート詐欺	ウイルスを見つけたという偽の警告で、遠隔操作のソフトなどを入れさせる手口

用語	意味
支援措置	ストーカーや DV の加害者からの、住民票の写しなどの交付の請求を制限する、市区町村の仕組み
資格確認書	健康保険証の代わりの書類
重大な過失	わざとと同じに見られるほど、注意を大きく怠ること
情報流通プラットフォーム対処法	SNS などでの権利の侵害への対応を定めた法律
初期化	買ったときの状態に戻すこと
信用情報機関	ローンやクレジットの契約の情報を集める機関（CIC・JICC・KSC）。法律による指定は CIC と JICC で、3つとも民間の会社・団体です[17]
信用情報の開示	自分の信用情報を見る手続き
スクリーンショット	画面をそのまま画像で保存すること
スミッシング	SMS を使うフィッシング
脆弱性	ソフトや機器の弱点
生成 AI	文章や画像を作る AI
速報・確報	個人情報保護委員会への漏えいの報告のうち、速報はまず出す報告、確報は調べた結果の報告
ダークウェブ	一般の方法では見られない闇サイト
第一報	最初のお知らせ
第三者	本人と会社以外の人や会社
第三者提供記録	会社が自分の情報を第三者に渡したとき・受け取ったときに作る記録
多要素認証	パスワード・スマホ・指紋など、種類の違う確かめ方を2つ以上組み合わせる仕組み
地方独立行政法人	自治体が設立した法人
提訴	裁判を起こすこと
デビットカード	使うとすぐに口座から代金が引き落とされるカード
電子決済	スマホのアプリで払う決済
転送不要郵便	ほかの住所へ転送されない郵便
特殊詐欺	電話などで相手を信じさせ、会わずにお金をだまし取る詐欺
名寄せ	同じ人の重複をまとめること
二次被害	漏れた情報が使われて、あとから起きる被害
二重恐喝	ランサムウェアの被害で、盗んだデータを公開すると脅す手口
ニセ警察詐欺	警察官などをかたる詐欺
2段階認証	パスワードのほかに、確認コードなどでも本人かを確かめる仕組み
認証情報	ID・パスワードなど
認定個人情報保護団体	個人情報保護委員会が認定した民間の団体

用語	意味
ネットバンキング	ネットで振込などができる銀行のサービス
パスキー	パスワードの代わりに、スマホなどの機器と指紋・顔・PIN で本人を確かめる仕組み
パスコード	iPhone の画面のロックを解く暗証番号
パスワードマネージャー	パスワードを保存し、ログインのときに入力してくれる専用のアプリ
ハッシュ値	元に戻しにくい形に変換した値
番号盗用	カードの番号などを盗んで使う手口
犯罪収益移転防止法	犯罪で得たお金の受け渡しを防ぐための法律
ひかり電話	光回線を使う固定電話
ビジネスメール詐欺	取引先や経営者になりすましたメールで、偽の口座に送金させる詐欺
平文	そのまま読める形
フィッシング	本物そっくりの偽のメールやサイトで、情報をだまし取る手口
不正アクセス	許可なく他人のシステムに入ること
附帯決議	国会が法律に添えた要望
ブックマーク	よく見るページを登録しておく機能
プライバシーポリシー	個人情報の扱い方を書いたページ
ブラウザ	インターネットを見るアプリ（Chrome や Safari など）
振り込め詐欺救済法	犯罪に使われた口座に残っているお金を、被害者に支払う手続きを定めた法律
プロバイダー	ネットの接続やサービスを提供する会社
法テラス	日本司法支援センター。法制度や相談先を案内する公的な機関
防犯機能付き電話	通話を自動で録音したり、鳴る前に録音することを伝える警告を流したりする電話
補填	埋め合わせること
本人（個人情報の）	その情報が指している人。お客様や会員など、情報の持ち主。漏えいの報告の「本人の数が1,000人を超える」は、情報が漏れた（おそれを含む）人が1,000人より多いこと
本人申告	信用情報機関に書類の紛失や漏えいを登録して、会員の会社へ注意をうながす手続き
マイナ免許証	運転免許証の機能をマイナンバーカードに入れたもの
マルウェア	不正なプログラム
申し合わせ（全国銀行協会の）	会員の銀行の間で決めた方針
要配慮個人情報	病歴など、とくに配慮が必要な情報
預金者保護法	偽造・盗難カードの被害から預金者を守る法律（2005年の法律。対象は個人）
与信	ローンやカードなど
予兆電話	住所・氏名・資産などを探る、特殊詐欺が疑われる電話
ランサムウェア	データを暗号化して身代金を求める不正なプログラム

用語	意味
リークサイト	盗んだデータをさらすサイト
リスト型攻撃	ほかで漏れた ID・パスワードの組を、次々に試す手口
リモートデスクトップ	離れた場所からパソコンを操作する仕組み
レコード	データの1行分
ワンタイムパスワード	1回だけ使えるパスワード

付録E　出典について

出典は、別冊の「出典一覧」に、発行元・題名・公開日・リンク（URL）を付けて、章ごとに載せています。本文の小さな番号が、別冊の章ごとの番号です。スマホの操作の手順と、相談窓口の番号・受付時間は、2026年10月に各社・各機関の公式サイトで確かめました。ページを減らすため、これらの出典の注は省いています。同じ発行元の続報が続くときは、最新の発表だけを載せています。公的機関、企業・団体の公式発表、業界団体、セキュリティ企業の報告、信頼できる報道を使い、研究論文は使っていません。調査の基準日は2026年10月22日です。主な事案の続報と新しい事案は10月27日まで、一部の窓口・制度は10月23～24日に確かめ、本文に「2026年10月23日時点」「10月27日の第10報」などと書いています。主な公的機関の公式サイトは次のとおりです。

- 個人情報保護委員会 https://www.ppc.go.jp/ ／警察庁 https://www.npa.go.jp/
- 消費者庁 https://www.caa.go.jp/ ／国民生活センター https://www.kokusen.go.jp/
- IPA https://www.ipa.go.jp/ ／金融庁 https://www.fsa.go.jp/
- 国家サイバー統括室 https://www.cyber.go.jp/ ／デジタル庁 https://www.digital.go.jp/
- 総務省 https://www.soumu.go.jp/ ／法務省 https://www.moj.go.jp/
- 外務省 https://www.mofa.go.jp/

奥付

書名　情報漏えいから身を守る対応ガイド
流出した情報の種類別に、被害を防ぐ・被害にあったら

版　2026年10月版（2026年10月発行）

調査の基準日　2026年10月22日（主な事案は10月27日まで確認）

著作・発行　株式会社アルファテック
千葉県君津市浦田635

本書は、情報漏えいの被害を防ぎ、被害にあったときに落ち着いて動けるようにするための資料です。内容は調査の基準日（2026年10月22日。主な事案の続報と新しい事案は10月27日まで確認）の時点の公開情報にもとづきます。漏えいした会社・団体も攻撃の被害者なので、本文では名前を書かず、業種と仕組みで呼んでいます（もとの発表は別冊の出典一覧で確かめられます）。相談窓口の番号・受付時間、制度、各社の発表の内容は変わることがあるので、使う前に公式の情報で確かめてください。本書は法律の助言ではありません。個別の判断は、本書で紹介した相談窓口や専門家に相談してください。調査・執筆・図版の制作には生成AIを使い、主張は公的機関・団体・会社の公式発表などの一次情報と照らし合わせました（研究論文は使っていません）。

© 2026 株式会社アルファテック