

TRAINING

AI時代に学ぶサイバーセキュリティ

2日目 世界のハッキング事例と個人での対処法

スタッフサービス・エンジニアリング様 派遣エンジニア向けオンラインセミナー

2026年11月25日（水） 全3回の2回目



本資料の二次転載禁止について

本資料は株式会社ギブリーが作成した研修教材であり、著作権法により保護されています。受講者ご本人の学習目的に限りご利用いただけます。無断での複製、改変、第三者への提供、社外への公開は禁止です。本資料に掲載した外部サービスとニュースの画面は、各社の権利に帰属します。

講師紹介



人的資本インテリジェンス部門講師
生成AIエバンジェリスト

安田 光喜

Mitsuki Yasuda

メッセージ

みなさんがこれから生成AIをパートナーに新しい時代を生き
ていけるように、3日間全力でサポートしていきます！なに
かご不明点などありましたら、講師陣になんでも気軽にご質
問ください。

#ClaudeCode #Codex #Cursor #Antigravity
#全国統一生成AI活用技能試験S1 #生成AIサポート #G検定

得意領域

- ・生成AIをはじめとした世界最先端トレンド
- ・生成AIを用いた新規事業の開発、運営、補助
- ・アプリケーション開発/自動化プログラム環境構築
- ・教育（大学講師、研修、スクール運営など）

実績

- ・生成AI研修
- ・大手企業、外資、教育機関(小中高大)での
ITトレンド講演
- ・自治体と連携した地域教育実績
- ・上場企業社員対象のリスキリング支援

公立はこだて未来大学 大学院（メディアデザイン領域）を卒業し、街づくり会社での複合商業ビルの立ち上げにおける情報インフラ整備やデザイン全般業務の責任として関与。その後デザイン事務所を立ち上げ、飲食店を中心としたデザイン業務や美術館展示のアートコンテンツ開発などを行う。また、地域ブランディングにも注力し、市主催の企画運営業務を行なった。2018年10月『小中学生向けのプログラミング教育』に注目し、函館市で初めての小中学生向けプログラミングスクール『D-SCHOOL北海道』を立ち上げて運営。その後北海道のドラッグストア『サッポロドラッグストアー』からスクールの買収を受け、教育を専門とするグループ会社『株式会社シーラクス』にて技術開発責任者として運営。スクール設計・運営、20以上の自治体連携（イベントや出張教室運営）、大人向けプログラミングスクールメンターなどさまざまな『次世代IT教育』に取り組む。

Dify公式資料の日本語翻訳や、SecondMeアンバサダーなど生成AI最新トレンドに注力。

全3回の進み方

全3回は「知る」「守る」「対応する」の3ステップ

1日目 知る

11月17日（火）
生成AIと情報セキュリティ。AIが攻撃と社内の使い方をどう変えたかを知ります

2日目 守る

11月25日（水）
世界のハッキング事例と個人での対処法。自分のアカウントと端末を点検します

3日目 対応する

11月27日（金）
会社としての対処法とこれからの考え方。事故の初動と報告文を作ります

各回だけの参加でも分かるように作っています。前の回の要点は、毎回の始めに振り返ります。

1日目の要点

1日目に出ていない方も、**ここだけ**押さえれば進めます

1 攻撃する側は、AIを日常の道具として使っている

悪意ある侵害の4件に1件でAIが使われ、その45%はディープフェイクのなりすましでした

2 会社が把握していないAI利用が、事故の4割に関わった

禁止の生成AIに個人情報を入れた事例では、約33万人分が報告の対象になりました

3 AIに入れる前に、情報を3段階に仕分ける

社外可、加工して可、入れないの3つ。最後は常駐先と派遣元のルールに従います

本日の流れ

前半は事件の経緯で後半は**自分の守り**の点検

枠	内容	形式	時間
S01	前回の振り返りと本日の到達点	講義	[10min]
S02	世界の大型事件と顛末	講義	[25min]
S03	国内の事件と業務停止	講義	[25min]
S04	ハンズオン 自分の守りを点検	ハンズオン	[40min]
S05	個人の持ち帰り	講義	[10min]
閉会	質疑応答		[10min]

本日の到達点

本日の終わりにできるようになること

- 1 大きな事件が、どこから入られてどう広がったかを説明できる**
VPN機器、盗まれたIDとパスワード、ヘルプデスクへのなりすまし電話
- 2 漏れた情報が、別のサービスの乗っ取りに使われる流れを説明できる**
証券口座の乗っ取りと、パスワードの使い回し
- 3 自分のアカウントの守りを点検し、偽のメールを見分けられる**
ハンズオンで、点検シートとメールの判定シートを作ります

S02

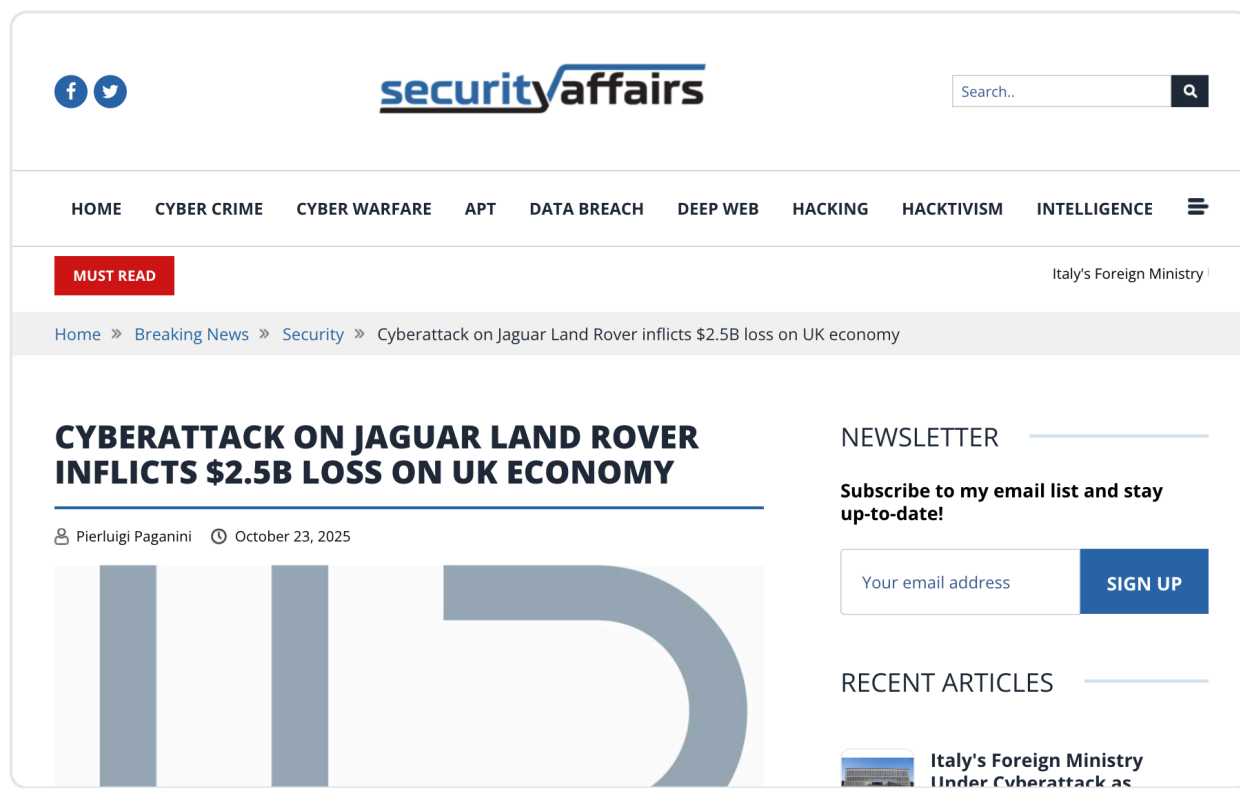
世界の大型事件と顛末

工場と店が止まり、実行役は捕まり、首謀者は逃れている

-
- 英国の自動車メーカーJLRの生産停止
 - 英国の小売を襲ったヘルプデスクへのなりすまし
 - 攻撃集団と摘発の顛末
 - 攻撃の裏にある検閲のないAI

英国JLRの生産停止

1社の停止で英国経済に19億ポンドの損失

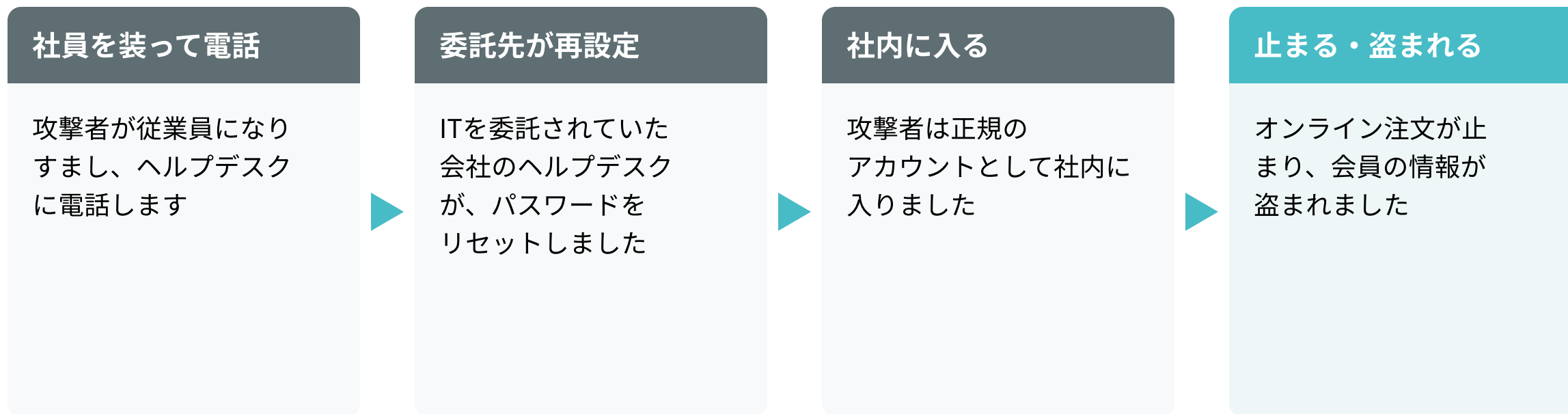


- 2025年8月31日に攻撃を受け、英国の工場は約5週間止まりました
- 影響を受けた英国の組織は5,000を超えます
- 英国政府は9月28日に、15億ポンドの融資保証を発表しました

出典 Security Affairs（JLRへの攻撃と英国経済の損失）、GOV.UK（JLRへの15億ポンドの融資保証）

英国の小売への攻撃の流れ

入口はメールではなく電話一本



出典 TechRadar（英国小売への攻撃とヘルプデスクの悪用）

M&SとCo-opの被害

注文が**46日**止まり会員650万人の情報が盗まれた

46日

M&Sがオンライン注文を止めていた日数

約3億ポンド

M&Sが見込んだ営業利益への影響

650万人

Co-opで情報を盗まれた会員の数。会員全員にあたります

出典 ESM Magazine (M&S、46日ぶりにオンライン注文を再開)、AJ Bell (M&Sの営業利益への影響)、The Record (Co-opの売上への影響)

攻撃集団の顔ぶれ

英語圏の若者の集団はデータを盗んで脅す

集団	特徴	主な手口
Scattered Spider、ShinyHunters、LAPSUS\$	英語圏の10代と若者が中心。2025年8月に合流を名乗った	ヘルプデスクへのなりすまし電話、SIMの乗っ取り、多要素認証の通知の連打
Qilin、The Gentlemen	ロシア語圏。暗号化の道具を貸し出し、身代金を分け合う	VPN機器の弱点や盗んだ認証情報から入り、暗号化と公開の脅しを組み合わせる
北朝鮮の攻撃者	国家が背後にいるとされる。暗号資産の窃取が最大	2025年2月に暗号資産の取引所から約15億ドルを盗んだとFBIが発表

▶ 59秒の動画で見る

出典 米国司法省（Scattered Spiderの構成員の起訴）、警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」

攻撃の裏にある検閲のないAI

安全策を外したAIが月50ドルで手に入る

1 WormGPT 4は、月額50ドルで売られている

2025年9月ごろから販売され、Telegramの販売チャンネルの登録者は500人を超えます

2 KawaiiGPTは無料で公開され、5分足らずで使い始められる

フィッシングのメールや身代金の要求文を書かせることができます

3 公開されたモデルの安全策は、すぐに外される

拒否する機能を消す手法で、GPU1枚と200ドル足らずの費用で拒否率が約1%まで下がりました

出典 Palo Alto Networks Unit 42（悪用されるLLMの分析）、CTC Sentinel（公開モデルの安全策が外される問題）

実行役は捕まり**首謀者**は国外で逃れている

- 2025年7月 ● 英国家犯罪対策庁が、M&SとCo-opへの攻撃で17～20歳の4人を逮捕
- 2025年8月 ○ 米国で20歳の構成員に禁錮10年の判決
- 2026年4月 ○ 19歳の構成員が、日本行きの便に乗る前にヘルシンキ空港で逮捕され、7月に米国へ引き渡し
- 2026年10月 ● 大阪で拘束された28歳のロシア人が、Qilinの中核とされドイツへ引き渡された（報道）
- 現在 ○ ロシアにいるとされる首謀者は、起訴や指名手配のまま拘束されていない

出典 BleepingComputer（英国で4人逮捕）、米国司法省（フィンランドで逮捕された構成員の引き渡し）、SecurityWeek（日本で拘束されたQilinの容疑者、ドイツへ引き渡し）

160億件は新しい漏えいではなく過去の寄せ集め

No, the 16 billion credentials leak is not a new data breach

By [Lawrence Abrams](#) June 19, 2025 05:51 PM 9



News broke today about "one of the largest data breaches in history," sparking wide media coverage filled with warnings and fear-mongering. However, it appears to just be a compilation of previously leaked credentials stolen by infostealers, exposed in data breaches, and via credential stuffing attacks.

AdaptiveSecurity

Cybersecurity Awareness Month, already built for you.

Four weeks of ready-to-go assets built around the threats your team faces.

Download Toolkit

POPULAR STORIES



Engineer sentenced for locking over 3,000 devices on employer network

- 2025年6月に「160億件の認証情報が流出」と報じられました
- 中身は、過去に漏れたIDとパスワードを集め直したデータでした
- 大きな数字を見たら、確定か、最大か、攻撃者の主張かを確認めます

出典 BleepingComputer（160億件の認証情報は新しい漏えいではない）

英国のM&SとCo-opへの攻撃で、攻撃者が社内に入るために最初に使った手口はどれですか。

- A VPN機器の弱点を突いた
- B 社員のパソコンにウイルス付きのメールを送った
- C 公衆Wi-Fiの通信を盗み見た
- D 従業員を装ってヘルプデスクに電話した

D

答えはD 従業員を装ってヘルプデスクに電話した

攻撃者は従業員になりすまし、ITを委託されていた会社のヘルプデスクにパスワードをリセットさせました。
電話で頼まれたときに本人をどう確かめるかは、3日目の会社としての対処で扱います。

S03

国内の事件と業務停止

国内でも、受注と出荷が数か月止まる事件が続いた

-
- アサヒグループの出荷停止
 - アスクルと委託先のアカウント
 - 1,000万件を超える会員情報の漏えい
 - 証券口座の乗っ取り

アサヒグループの事件の流れ

暗号化から出荷の再開まで約6か月

- 
- A vertical timeline with a light blue line and circular markers. The markers are white with a blue outline for the first three events and solid blue for the last two. The text is in Japanese.
- 2025年9月19日** ○ このころ最初の侵入（日経クロステックの報道）。グループ拠点のネットワーク機器から入られた
 - 9月29日 7時** ● システム障害が起き、暗号化されたファイルが見つかる
 - 9月29日 11時** ○ ネットワークを遮断し、データセンターを隔離
 - 12月2～3日** ○ 電子受発注を再開。それまでは紙とExcelで受注を続けた
 - 2026年4月7日** ● 全商品の出荷を再開。システム障害の関連費用は約170億円

出典 アサヒグループホールディングス（2025年11月27日の発表）、issoh（アサヒの出荷再開までの経緯）、日本経済新聞（アサヒの決算とシステム障害の関連費用）

アサヒグループの漏えい

漏えいのおそれは調べるほど増えた

ランサム被害のアサヒ、漏えいの可能性229万件に拡大 当初は191万件

公開 2026年07月17日 18時30分

著者 梅林日奈子 [ITmedia]

印刷する

Googleで優先するソースとして追加

PR レノボの法人タブレット「Lenovo ThinkTab X11 Gen 1」がもたらす現場革新

PR CRM導入企業の50.4%が管理できず！ 定着させる選び方5ステップを公開

アサヒグループホールディングス（HD）は7月17日、2025年9月に受けたサイバー攻撃を巡り、漏えいのおそれがある個人情報を計228万9000件に修正したと発表した。取引先の役員や従業員などなどの情報37万8000件を新たに加えた。同社は25年11月に漏えいのおそれがある個人情報を約191万件と公表し、26年2月にはうち約11万件の漏えいを確認したと発表していた。

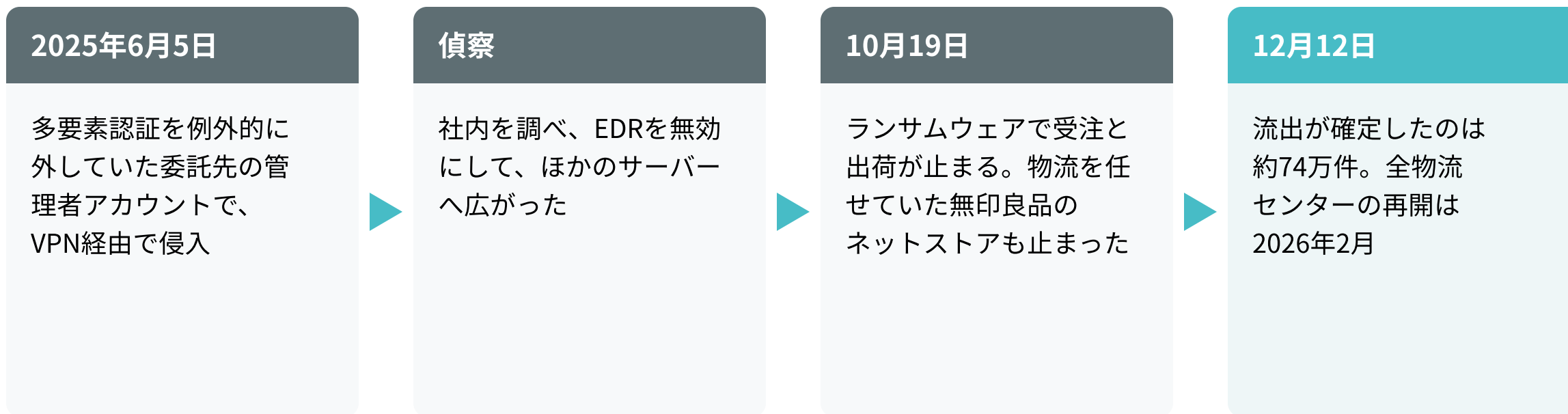
取引先の役員、個人事業主、従業員の氏名、生年月日、性別、住所、電話番号、メールアドレスなど37万8000件を追加。そのほか、すでに発表した「祝電・弔電などの慶弔対応を実施した関係先の氏名や住所、電話番号」「従業員（退職済み含む）の家族の氏名、生年月日、性別」も件数を変更した。

- 2025年11月の公表は約191万件でした
- 2026年7月17日に、漏えいのおそれを約228.9万件に修正しました
- 身代金は払わず、攻撃者とも接触していません。バックアップから戻せると早く分かったためです

出典 アサヒグループホールディングス（2026年7月17日の発表）

アスクルの事件の流れ

例外として残した1つのアカウントが入口



出典 Impress Watch（アスクルの侵入口と流出の件数）、マイナビニュース（アスクルの侵入から暗号化まで）、FASHIONSAP（無印良品ネットストアの受注再開）

ランサムウェアの侵入口は半分以上がVPN機器

123 件

2026年上半期に警察庁へ報告されたランサムウェアの被害件数で、半期で過去最多です

約5 割

侵入経路が分かった36件のうち、VPN機器から入られた割合

64.2 %

被害を受けた組織のうち、中小企業の割合

出典 警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」

▶ 36秒の動画で見る

1,000万件を超える会員情報の漏えい

2026年は会員の情報が**桁違いの件数**で漏れた

会社とサービス	件数	漏れたもの
佐川急便（2026年10月23日）	最大 約5,323万件	送り主と届け先の氏名、住所、電話番号
Gyazo（9月）	約2,362万件	ユーザー情報。非公開画像のURLを含む画像の情報も
KDDIのメール基盤（6月）	パスワード 約762万件	メールアドレスとパスワード。6つのプロバイダーに及ぶ
カプコン（10月22日）	約1,177万件	メールアドレスとログインの記録
焼肉きんぐ公式アプリ（10月5日）	約1,079万件	会員番号、氏名、メールアドレス、電話番号

出典 ITmedia NEWS（佐川急便への不正アクセス）、INTERNET Watch（Gyazoへの不正アクセス）、セキュリティ対策Lab（2026年の国内の主な事件）、INTERNET Watch（カプコンのユーザー情報漏えい）、物語コーポレーション（焼肉きんぐ公式

佐川急便への不正アクセス

約100日分の荷物の送り主と届け先が対象

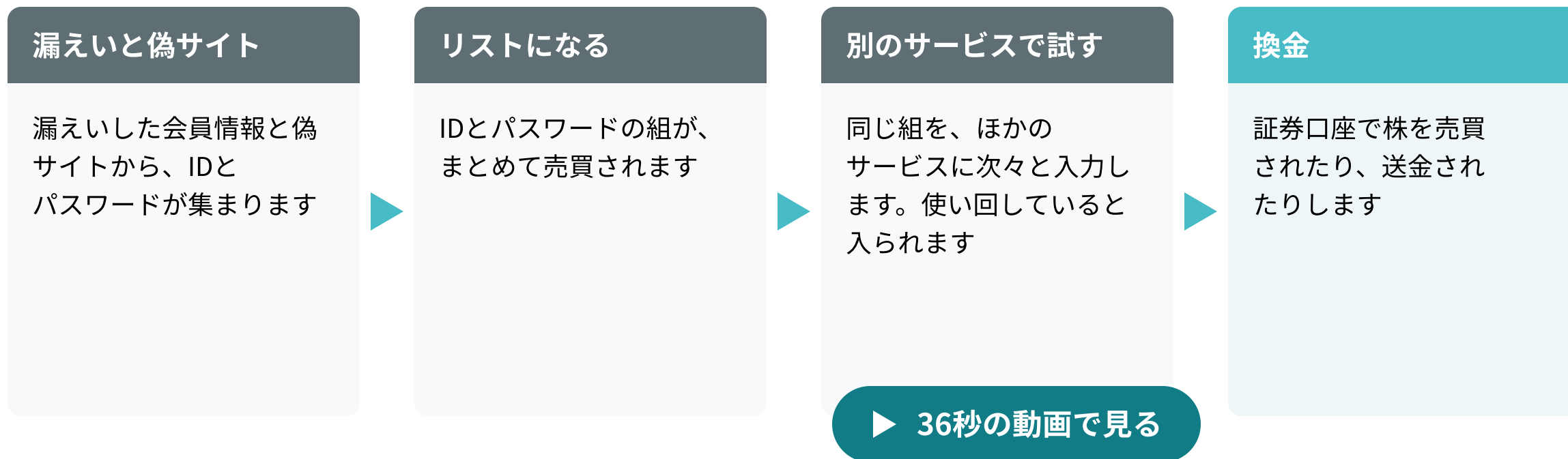


- お荷物問い合わせサービスへの不正アクセスです
- 対象は最大で約5,323万件で、重複を含みます
- カード情報とパスワードは含まれていません

出典 ITmedia NEWS（佐川急便への不正アクセス）

漏れた情報が換金されるまで

漏れたパスワードは別のサービスで使われる



出典 警察庁「令和7年におけるサイバー空間をめぐる脅威の情勢等について」、金融庁「インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています」

証券口座の乗っ取り

不正取引は1年で**9,752件**

9,752件

2025年の1年間に証券口座で起きた不正取引の件数

約7,393億円

乗っ取られた口座で行われた売買の累計額で、被害額そのものではありません

245万件

2025年のフィッシングの報告件数。過去最多

出典 時事ドットコム（証券口座の不正取引、2025年通年）、金融庁「インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています」、警察庁「令和7年におけるサイバー空間をめぐる脅威の情勢等について」

アスクルの事件で、攻撃者が最初に入るのに使ったものはどれですか。

A 多要素認証の対象から外されていた委託先の管理者アカウント

B 社員の私物のパソコン

C 倉庫の監視カメラ

D 取引先から届いた請求書のファイル

A

答えはA 多要素認証の対象から外されていた委託先の管理者アカウント

攻撃者はこのアカウントでVPN経由で入り、約4か月かけて偵察し、EDRを無効にしてから暗号化しました。
例外として残したアカウントが1つあるだけで、多要素認証はその入口では働きません。

S04

ハンズオン 自分の守りを点検

自分のメールアドレスとアカウントを点検し、偽のメールを見分ける

- STEP1～2 メールアドレスの漏えいを調べる
- STEP3 パスワードの使い回しを洗い出す
- STEP4 パスキーの設定を確かめる
- STEP5～6 5通のメールを判定し、Geminiと見比べる

どんな場面か

あなたのメールアドレスとパスワードも、どこかの漏えいに含まれているかもしれません。今日の事件と同じ流れで乗っ取られないように、自分のアカウントを点検し、偽のメールを見分ける練習をします。

使うもの

Have I Been Pwned、Gemini、配布フォルダ
day2_handson

つくるもの

記入した点検シートと、メールの判定シート

目安の時間

[40min]

気をつけること

シートにはパスワードやアドレスの本体を書きません

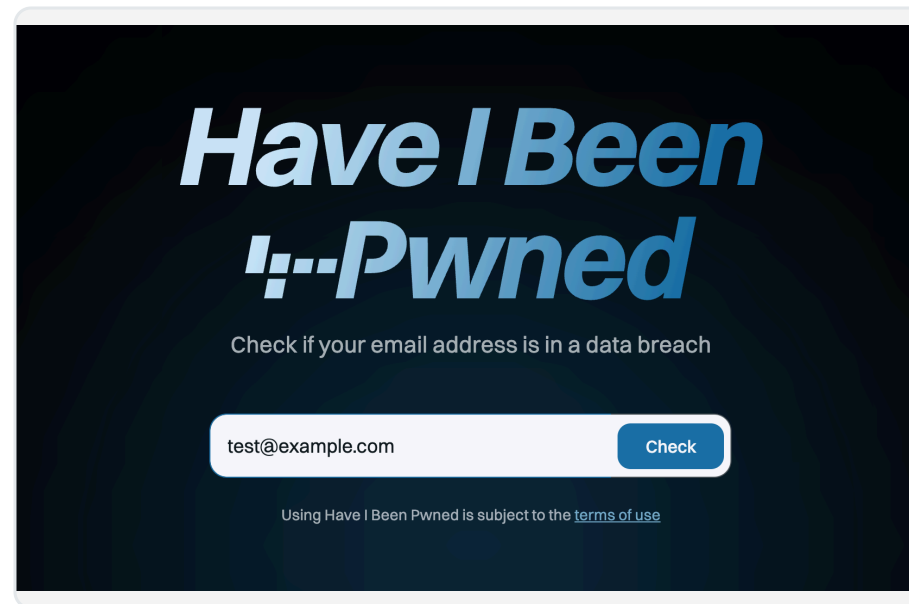
この演習で身に付くこと

自分のアカウントが漏えいに含まれていないかを確認、偽のメールを送信元とリンク先と依頼の内容で見分けられるようになります。

STEP1～2 漏えいを調べる

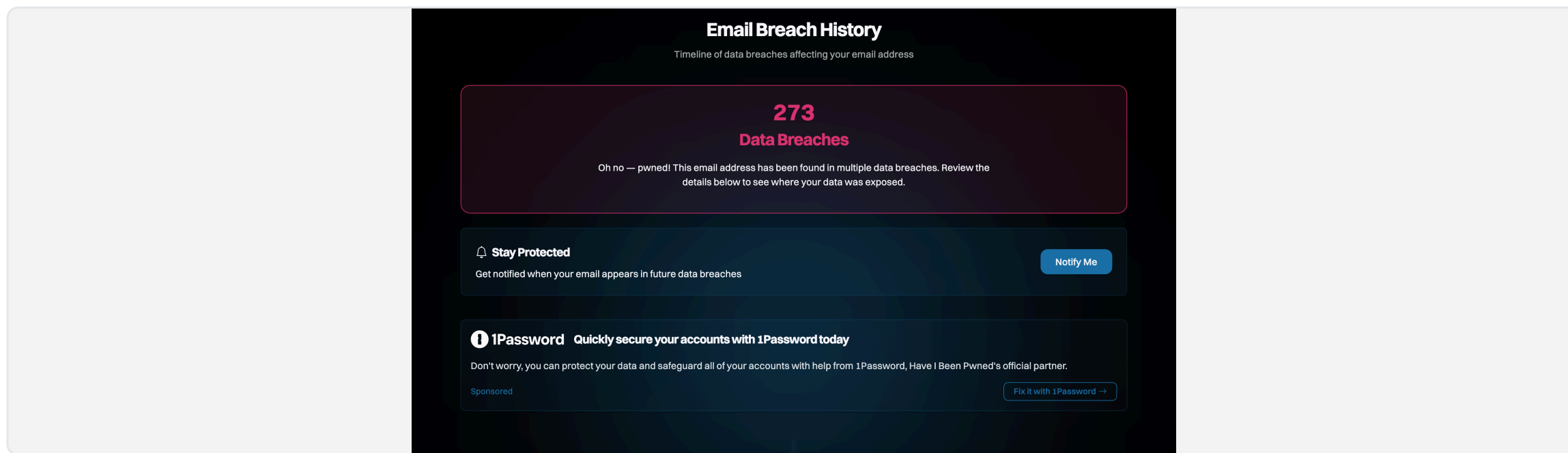
Have I Been Pwnedで、自分のメールアドレスを照会します

- 1 ブラウザで haveibeenpwned.com を開きます
- 2 入力欄に、自分のメールアドレスを入れて「Check」を押します
- 3 漏えいの記録が出たら、どのサービスから漏れたかを点検シートの2行目に書きます
- 4 「Good news」と出たら、記録は見つかっていません。別のアドレスでも試せます



画面は例示用のアドレス test@example.com で照会した様子です

漏えいの記録が出たら、そのサービスの名前を確かめます



例示用のアドレスでは273件の漏えいの記録が出ました。下にサービスの名前と漏れた項目が並びます

出典 Have I Been Pwned (FAQ)

STEP3 使い回しを洗い出す

AIは開かずに、点検シートに書き出します

- 1 STEP2で名前が出たサービスと、同じパスワードを使っているサービスを思い出します
- 2 その数だけを点検シートの3行目に書きます。パスワードそのものは書きません
- 3 数が1以上なら、それぞれのサービスで別のパスワードに変える日を4列目に書きます

パスワード管理アプリやブラウザの保存を使うと、サービスごとに別のパスワードを覚えずに使えます。

STEP4 パスキーを確かめる

銀行、証券、メールのアカウントで、強い認証を確かめます

- 1 Googleアカウントのヘルプ「パスワードの代わりにパスキーでログインする」を開きます
- 2 自分のGoogleアカウントで、パスキーか2段階認証が設定されているかを確かめます
- 3 銀行と証券のアプリで、パスキーか2段階認証と、ログイン通知が有効かを確かめます
- 4 結果を点検シートの4～6行目に書きます



Googleアカウントのヘルプのページ

まず自分の目で、本物か詐欺かを決めます

受信トレイ メール1 研修用に作った架空のメールです

【重要】お客様の口座のご利用を一時的に制限しました

差出人 サンプル銀行（架空） <info@sample-bank-login.example.com>

宛先 あなた

日時 2026年11月25日

サンプル銀行をご利用いただき、ありがとうございます。

お客様の口座で、第三者による不正なログインの可能性のある取引を検知しました。

安全のため、口座のご利用を一時的に制限しております。

24時間以内に下記のページから本人確認を行わない場合、口座を凍結いたします。

本人確認ページ <http://sample-bank-login.example.com/verify>

（ログインID、パスワード、取引暗証番号をご入力ください）

メール1 口座の利用を制限したというお知らせ

受信トレイ メール4 研修用に作った架空のメールです

至急の依頼（他言無用）

差出人 田中 社長 <tanaka.ceo.a-sha@example.org>

宛先 あなた

日時 2026年11月25日

お疲れさまです。田中です。

取引先との交渉で、今日中に支払いが必要になりました。

会議中で電話に出られないので、メールで対応をお願いします。

電子ギフトカードを5万円分×6枚購入し、裏面の番号をこのメールに返信してください。

この件は、まだ社内のほかの人には話さないでください。

メール4 社長を名乗る至急の依頼

AIは開かずに、判定シートに書きます

- 1 配布フォルダの「02_メール判定」にあるメール1～5の画像を開きます
- 2 「メール本文.txt」の先頭にある、正規のドメインの一覧を確かめます
- 3 送信元のドメイン、リンク先のドメイン、依頼の内容の3点を見て、本物、詐欺、迷うのどれかを判定シートに書きます
- 4 見分けた理由を1行ずつ書きます

STEP6 Geminiと見比べる

迷ったメールを1通選び、Geminiに判定させます

- 1 下の文面に続けて、「メール本文.txt」から迷ったメールを1通貼り付けて送ります
- 2 Geminiの判定と根拠を、自分の判定シートと見比べます

Geminiに送る文面

次のメールが、フィッシングなどの詐欺メールかどうかを判定してください。判定と、そう判断した根拠を、送信元、リンク先、依頼の内容の3点に分けて書いてください。

（研修用のメールである旨と、正規のドメインの一覧を添えます。
全文はコピペ用のファイルにあります）

ご提示いただいたメールが詐欺（フィッシング）メールであるかどうかの判定と、その根拠について、ご指定の3点に分けて解説します。

結論として、このメールはフィッシング詐欺（あるいは不審ななりすましメール）と判定されます。

1. 送信元

- **判定：**怪しい（なりすましの疑い）
- **根拠：**
 - 差出人のメールアドレスのドメインが `@a-sha-helpdesk.example.net` となっています。
 - 提示されたA社（受け取った人の勤め先）の正規ドメインは `a-sha.example.jp` です。
 - サポート窓口やヘルプデスクを装ったメールであっても、組織の正規ドメイン（`a-sha.example.jp`）とは異なる外部の別ドメイン（`.example.net`）から送信されているため、送信元を偽装した攻撃や、無関係な第三者による送信の可能性が高いと言えます。

メール3を判定させた結果。正規のドメインとの違いを根拠に挙げています

できたと判断する基準

- ☒ 点検シートの1～7行目が埋まっていて、パスワードやアドレスの本体がどこにも書かれていない
- ☒ 使い回しがあったサービスについて、パスワードを変える日が決まっている
- ☒ 5通のメールすべてに判定と理由があり、理由が送信元、リンク先、依頼の内容のどれかに当たっている
- ☒ Geminiと判定が違ったメールについて、どちらの根拠が正しいかを自分で確かめた

5通のメールの答え

メール	判定	見分けるところ
1 口座の利用を制限	詐欺	送信元とリンク先が正規のドメインと違う。24時間で急がせ、暗証番号まで入力させる
2 お届け予定	本物	送信元が正規のドメイン。リンクを押させず、公式アプリでの手続きを案内している
3 パスワードの有効期限	詐欺	A社のドメインではない。今のパスワードを入力させ、当日の期限で急がせる
4 社長からの至急の依頼	詐欺	会社のドメインではない。電話で確かめられないようにし、ギフトカードの番号を送らせる
5 新しい端末からのログイン	本物	送信元が正規のドメイン。リンクを使わず公式アプリから確かめるよう案内している

[▶ 33秒の動画で見る](#)

この演習とセキュリティの仕事

今日の点検はセキュリティの現場の仕事と同じ形

今日やったこと	セキュリティの現場での仕事	担う人
漏えいの記録を照会した	社員のアカウントが漏えいしたデータに含まれていないかを見張る	SOCのアナリスト、脅威インテリジェンス
メールを判定した	届いた警告や通報が本物の攻撃かを判定し、対応の要否を決める	SOCのアナリスト
パスキーを確かめた	全社のアカウントに強い認証を行き渡らせ、例外を残さない	情報システム部門、セキュリティエンジニア

家族に送るメッセージを作ります

- 1 下の文面をGeminiに送り、家族あての短いメッセージを作らせます
- 2 できた文を読んで、リンクを押させる表現や、不安をあおる表現が入っていないかを確認めます

Geminiに送る文面

家族に送る短いメッセージを作ってください。銀行や宅配業者を名乗るメールやSMSのリンクを押さず、公式アプリから確かめてほしいという内容です。読む人は60代で、200字以内にしてください。

S05

個人の持ち帰り

今日から直す3点と、漏えいの通知が届いたときの確かめ方

今日から直す3点

1 パスワードの使い回しをやめる

パスワード管理アプリかブラウザの保存を使い、サービスごとに別のパスワードにします

2 銀行、証券、メールにパスキーか2段階認証とログイン通知を設定する

金融庁も銀行に、パスキーのようなフィッシングに強い認証を求めています

3 メールやSMSのリンクから開かず、公式アプリか自分で開いた公式サイトから入る

公的機関や銀行を名乗る電話で、遠隔操作ソフトの導入を求められても応じません

出典 警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」

漏えいの通知が届いたとき

通知のリンクは押さず**公式サイト**で同じ発表を探す

- 1 通知のリンクを押さず、会社の公式サイトか公式アプリで同じ発表があるかを確認する
- 2 法令で決まった本人への通知の項目は、概要、漏えいした項目、原因、二次被害の有無、参考事項の5つ
パスワードやカード番号の入力を求める項目はありません
- 3 同じパスワードを使っていたほかのサービスも変え、カードと口座の明細を確認する
- 4 通知のあとに届く、補償の手続きを名乗るメールや電話に気をつける

出典 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」

**リンクは押さずに公式アプリから
電話の依頼はいったん切ってかけ直す**

家族あてのメッセージは、早く終わった方への課題でGeminiに作らせた文を使えます。言い回しを自分の言葉に直してから送ってください。

3日目は**11月27日（金）** 19時から 会社としての対処法とこれからの考え方

架空の会社で起きたランサムウェアの被害を題材に、最初の1時間の動き方と、経営層へ送る第一報を作ります。セキュリティエンジニアの仕事の全体も紹介します。

Security Affairs (JLRへの攻撃と英国経済の損失)

<https://securityaffairs.com/183733/security/cyberattack-on-jaguar-land-rover-inflicts-2-5b-loss-on-uk-economy.html>

BleepingComputer (JLRの費用)

<https://www.bleepingcomputer.com/news/security/jaguar-land-rover-cyberattack-cost-the-company-over-220-million/>

GOV.UK (JLRへの15億ポンドの融資保証)

<https://www.gov.uk/government/news/government-backs-jaguar-land-rover-with-15-billion-loan-guarantee>

TechRadar (英国小売への攻撃とヘルプデスクの悪用)

<https://www.techradar.com/pro/avoiding-service-desk-exploitation-deconstructing-the-modern-retail-attack>

ESM Magazine (M&S、46日ぶりにオンライン注文を再開)

<https://www.esmmagazine.com/technology/ms-resumes-online-orders-after-46-day-cyberattack-pause-290083>

AJ Bell (M&Sの営業利益への影響)

<https://www.ajbell.co.uk/news/articles/ms-warns-cyberattack-may-cost-ps300-million-despite-earnings-rise>

The Record (Co-opの売上への影響)

<https://therecord.media/retailer-the-co-op-cyberattack-lost-revenue>

BleepingComputer (英国で4人逮捕)

<https://www.bleepingcomputer.com/news/security/four-arrested-in-uk-over-mands-co-op-harrods-cyberattacks/>

米国司法省 (Scattered Spiderの構成員の起訴)

<https://justice.gov/opa/pr/united-kingdom-national-charged-connection-multiple-cyber-attacks-including-critical>

米国司法省 (フィンランドで逮捕された構成員の引き渡し)

<https://www.justice.gov/opa/pr/alleged-member-criminal-cyber-hacking-group-scattered-spider-arrested-finland-and-extradited>

SecurityWeek（日本で拘束されたQilinの容疑者、ドイツへ引き渡し）

<https://www.securityweek.com/qilin-ransomware-suspect-arrested-in-japan-extradited-to-germany/>

BleepingComputer（160億件の認証情報は新しい漏えいではない）

<https://www.bleepingcomputer.com/news/security/no-the-16-billion-credentials-leak-is-not-a-new-data-breach/>

Palo Alto Networks Unit 42（悪用されるLLMの分析）

<https://unit42.paloaltonetworks.com/dilemma-of-ai-malicious-llms/>

CTC Sentinel（公開モデルの安全策が外される問題）

<https://ctc.westpoint.edu/feature-commentary-guardrails-under-test-terrorist-misuse-of-ai-models-and-the-open-weight-abliteration-problem/>

アサヒグループホールディングス（2025年11月27日の発表）

<https://www.asahigroup-holdings.com/newsroom/detail/20251127-0104.html>

アサヒグループホールディングス（2026年7月17日の発表）

<https://www.asahigroup-holdings.com/newsroom/detail/20260717-0101.html>

日本経済新聞（アサヒの決算とシステム障害の関連費用）

<https://www.nikkei.com/article/DGXZQ0UB074LA0X00C26A7000000/>

issoh（アサヒの出荷再開までの経緯）

<https://www.issoh.co.jp/column/details/10035/>

Impress Watch（アスクルの侵入口と流出の件数）

<https://www.watch.impress.co.jp/docs/news/2070955.html>

マイナビニュース（アスクルの侵入から暗号化まで）

<https://news.mynavi.jp/techplus/article/20251215-3818168/>

FASHIONSnap（無印良品ネットストアの受注再開）

<https://www.fashionsnap.com/article/2025-12-02/muji-online-restart/>

警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf

警察庁「令和7年におけるサイバー空間をめぐる脅威の情勢等について」

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

ITmedia Mobile（KDDIのメール基盤への不正アクセス）

<https://www.itmedia.co.jp/mobile/articles/2606/23/news115.html>

セキュリティ対策Lab（2026年の国内の主な事件）

<https://rocket-boys.co.jp/security-measures-lab/2026-japan-major-security-incidents-17-gyazo-epark-fines-times/>

INTERNET Watch（Gyazoへの不正アクセス）

<https://internet.watch.impress.co.jp/docs/news/2141538.html>

物語コーポレーション（焼肉きんぐ公式アプリの会員情報）

https://www.monogatari.co.jp/news/261005_news/

ITmedia NEWS（佐川急便への不正アクセス）

<https://www.itmedia.co.jp/news/article/2610/23/2000002553/>

INTERNET Watch（カプコンのユーザー情報漏えい）

<https://internet.watch.impress.co.jp/docs/news/2150509.html>

INTERNET Watch（クロネコ代金後払いサービスへの不正アクセス）

<https://internet.watch.impress.co.jp/docs/news/2148860.html>

東京商工リサーチ（上場企業の個人情報漏えい、2026年）

https://www.tsr-net.co.jp/data/detail/1203305_1527.html

時事ドットコム（証券口座の不正取引、2025年通年）

<https://www.jiji.com/jc/article?k=2026011401050&g=eco>

金融庁「インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています」

https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

Have I Been Pwned（FAQ）

<https://haveibeenpwned.com/FAQs>

Google アカウント ヘルプ「パスワードの代わりにパスキーでログインする」

<https://support.google.com/accounts/answer/13548313?hl=ja>

個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」

https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

ご質問をお受けします

ZOOMのチャットか、手を挙げる機能でお知らせください。



株式会社ギブリー (Givery, Inc.)

〒150-0036 東京都渋谷区南平台町15-13 帝都渋谷ビル8F